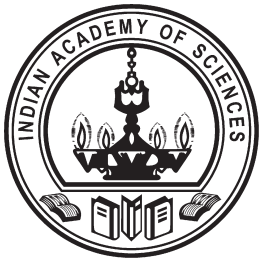
Number Theory and Combinatorics

B SURY

Stat-Math Unit, Indian Statistical Institute, Bengaluru, India.



All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior permission of the publisher.

© Indian Academy of Sciences 2017
Reproduced from *Resonance–journal of science education*
Reformatted by TNQ Books and Journals Pvt Ltd, www.tnq.co.in
Published by **Indian Academy of Sciences**

Foreword

The Masterclass series of eBooks brings together pedagogical articles on single broad topics taken from *Resonance*, the Journal of Science Education, that has been published monthly by the Indian Academy of Sciences since January 1996. Primarily directed at students and teachers at the undergraduate level, the journal has brought out a wide spectrum of articles in a range of scientific disciplines. Articles in the journal are written in a style that makes them accessible to readers from diverse backgrounds, and in addition, they provide a useful source of instruction that is not always available in textbooks.

The third book in the series, 'Number Theory and Combinatorics', is by Prof. B Sury. A celebrated mathematician, Prof. Sury's career has largely been at the Tata Institute of Fundamental Research, Mumbai', and the Indian Statistical Institute, Bengaluru, where he is presently professor. He has contributed pedagogical articles regularly to *Resonance*, and his articles on Number Theory and Combinatorics comprise the present book. He has also served for many years on the editorial board of *Resonance*.

Prof. Sury has contributed significantly to research in the areas of linear algebraic groups over global and local fields, Diophantine equations, division algebras, central extensions of p-adic groups, applications of density theorems in number theory, K-theory of Chevalley groups, combinatorial number theory, and generation of matrix groups over rings. The book, which will be available in digital format, and will be housed as always on the Academy website, will be valuable to both students and experts as a useful handbook on Number Theory and Combinatorics.

Amitabh Joshi
Editor of Publications
Indian Academy of Sciences
August 2017

About the Author

B Sury is a Professor of Mathematics at the Indian Statistical Institute in Bangalore since 1999. He was earlier at the Tata Institute of Fundamental Research, Mumbai, where he also got his PhD. Sury's professional interests have been very diverse: from the theory of algebraic groups and arithmetic groups, to algebraic K-theory, and number theory. He has contributed to these areas both through research papers and also through books.

Sury enjoys thinking about mathematical problems at all levels, and has taken keen interest in promoting problem solving skills. As a result of his abilities and willingness to shoulder responsibilities both in training students, and in writing exposition for students, he is universally sought after for any student activity in the country: he has been associated with several student magazines in the country, perhaps the important of them all, '*Resonance*' for the last two decades, as well the *Ramanujan Math Societies Newsletter*. He has been an important member of the Mathematical Olympiad Program of the country. Sury is known to friends and colleagues for his wit and humor, which seems to come almost instantaneously; one can enjoy some of his limericks on his webpage at ISI. The present volume brings together some of the writings of B Sury on Number Theory and Combinatorics which have appeared in '*Resonance*' during the last two decades. Each of the articles is a masterpiece! I am sure it will be a feast for the intellect of any reader with some mathematical inclination.

Dipendra Prasad
TIFR, Mumbai

Contents

Preface

Over the last two decades, my expositions in *Resonance* are on roughly two topics – (i) number theory and combinatorics, and (ii) group theory. In this volume, some of the expositions related to the former topic have been put together. The chapter on the work of Chowla and Pillai is part of an article written in collaboration with R Thangadurai that appeared in *Resonance*. I would like to thank Thangadurai for allowing me to include it here. I have attempted to retain the original write-ups of the articles as much as possible other than carrying out some corrections and (minor) additions. As this is a compendium of articles that appeared in *Resonance*, at times some material is repeated in different chapters. Further, this makes the compilation somewhat uneven in terms of levels of mathematical maturity required of the reader despite my efforts to ensure uniformity.

Concerning my philosophy of mathematics dissemination, I have staunchly held the opinion that many topics in mathematics which are supposedly advanced in nature, can be exposed in a manner understandable to a motivated undergraduate or postgraduate student. It may be somewhat of a challenge to make it comprehensible while still retaining the essential depth and technicality of the content, but it should nevertheless be possible. Over the years, I have tried to put this in practice. One of the best compliments I have received from Professor K R Parthasarathy, who told a visitor that he had learnt some number theory through these articles. Despite this obvious exaggeration (or rather because of this perhaps!), I was encouraged to keep trying to share some of the beautiful number theoretic and combinatorial ideas I myself enjoyed learning. To my surprise, I have occasionally found references to some of these articles in university courses in various places, and that has been fulfilling. The years 1981-1999 at the Tata Institute of Fundamental Research – where I first saw what excellence means – have had a positive effect on me in terms of being able to appreciate good mathematics (irrespective of whether I could originally contribute to it or not). During those years, it was a lot of fun to learn over conversations near the sea-side, at the coffee-table, and during ping-pong sessions from Madhav Nori, Venkataramana, Dipendra Prasad, C S Rajan, Ravi Rao, Raja Sridharan, Amit Roy, R R Simha, Bhatwadekar, Subramaniam, Parameswaran, Nitin Nitsure, Kapil Paranjape, Stephen Lobo, Kumaresan, and many others. In most instances, I would excitedly come up to them with something I had "seen", and they would be willing listeners and teachers. In later years, I have always benefited by talking to students and realizing time and again what they found simultaneously enjoyable as well

as not easy to understand. In almost all cases, after a meeting or discussion with some students, I felt compelled to write on a certain topic. Incidentally, some of the summer projects that students worked on have appeared in *Resonance* as well and, many of them were rewritten by me – showing my desire to communicate in a particular way. I personally know several colleagues who are much better at writing such expositions but, not many of them seem to find the time to write at this level. I wish they would.

Finally, I am indebted to Professor Ram Ramaswamy for suggesting the publication of this volume, for convincing me that it could be useful, and for pushing me to finish this process.

B Sury
July 2017

Cyclotomy and Cyclotomic Polynomials: The Story of how Gauss Narrowly Missed Becoming a Philologist

A person who does arouse
much admiration and a million wows!
Such a mathematicians' prince
has not been born since.
I talk of Carl Friedrich Gauss!

Cyclotomy – literally 'circle-cutting' – was a puzzle begun more than 2000 years ago by the Greek geometers. In this pastime, they used two implements – a ruler to draw straight lines and a pair of compasses to draw circles. The problem of cyclotomy was to divide the circumference of a circle into n equal parts using only these two implements.

As these n points on the circle are also the corners of a regular n-gon, the problem of cyclotomy is equivalent to the problem of constructing the regular n-gon using only a ruler and a pair of compasses. Euclid's school constructed the equilateral triangle, the square, the regular pentagon and the regular hexagon. For more than 2000 years mathematicians had been unanimous in their view that for no prime p bigger than 5 can the p-gon be constructed by ruler and compasses. The teenager Carl Friedrich Gauss proved a month before he was 19 that the regular 17-gon is constructible. He did not stop there but went ahead to completely characterise all those n for which the regular n-gon is constructible! This achievement of Gauss is one of the most surprising discoveries in mathematics. This feat was responsible for Gauss dedicating his life to the study of mathematics instead of philology[1] in which too he was equally proficient.

In his mathematical diary[2] maintained from 1796 to 1814, he made his first entry on the 30th of March and announced the construction of the regular 17-gon. It is said that he was so proud of this discovery that he requested that the regular 17-gon be engraved on his tombstone! This wish was, however, not carried out.

An amusing story alludes to Kästner, one of his teachers at the university of Göttingen, and an amateur poet. When Gauss told him of his discovery, Kästner was skeptical and did not take him seriously. Gauss insisted that

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 4, No. 12, pp. 41–53, December 1999.

[1] By 18, Gauss was already an expert in Greek, Latin, French and German. At the age of 62, he took up the study of Russian and read Pushkin in the original.

[2] The diary was found only in 1898!

he could prove his result by reducing to smaller degree equations and, being fond of calculations, also showed the co-ordinates of the 17 points computed to several decimal places. Kästner is said to have claimed that he already knew such approximations long before. In retaliation, some time later, Gauss described Kästner as the best poet among mathematicians and the best mathematician among poets!

Gauss's proof was not only instrumental in making up his mind to take up mathematics as a career but it is also the first instance when a mathematical problem from one domain was rephrased in another domain and solved successfully. In this instance, the geometrical problem of cyclotomy was reset in algebraic terms and solved. So, let us see more in detail what cyclotomy is all about.

The unit circle is given to us[3] and we would like to divide it into n equal parts using only the ruler and compasses. It should be noted that the ruler can be used only to draw a line joining two given points and not for measuring lengths. For this reason, one sometimes uses the word *straightedge* instead of a ruler.

If we view the plane as the complex plane, the unit circle has the equation $z = e^{i\theta}$. Since arc length is proportional to the angle subtended, the n complex numbers $e^{2\pi ik/n}, 1 \leq k \leq n$ cut the circumference into n equal parts.

As we might fix a diameter to be on the x-axis, the problem may also be variously posed as the problem of using only the ruler and the compasses to:

(i) find the roots of $z^n = 1$, or
(ii) construct the angle $2\pi/n$.

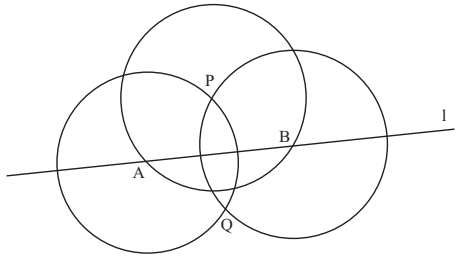
Since, by coordinate geometry, a line and a circle have equations, respectively, of the form $ax + by = c$ and $(x - s)^2 + (y - t)^2 = r^2$, their points of intersection (if any) are the common roots. Eliminating one of x, y leads to a quadratic equation for the other. Therefore, the use of ruler and compasses amounts in algebraic terms to solving a chain of quadratic equations.

Before we go further, we need to clarify one point. On the one hand, we seem to be talking of constructing lengths and, on the other hand, we seem to want to mark off certain specific points on the plane corresponding to the vertices of a regular n-gon. To remove any confusion due to this, let us explain how these are equivalent.

1. Some Easy Constructions Possible with a Ruler and a Pair of Compasses

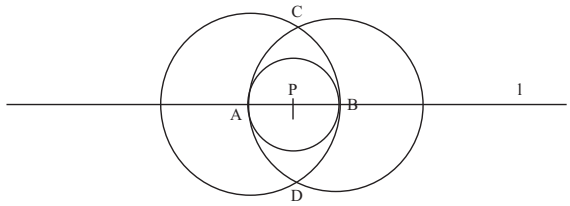
1. *Drop a perpendicular on a given line l from a point P outside it* (*Figure* 1).

[3]It is understood that the centre is also given.



Draw a circle centred at P cutting l at A and B. Draw circles centred at A and B having radii AP and BP, respectively. The latter circles intersect at P and Q and PQ is perpendicular to l.

2. *Draw a perpendicular to a given line l through a point P on it* (*Figure* 2).



Draw any circle centred at P intersecting l at A and B. Then, the circles centred at A and B with the common radius AB intersect at two points C and D. Then, CD passes through P and is perpendicular to l.

3. *Draw a line parallel to a given line through a point outside.*

This follows by doing the above constructions in succession.

4. *Bisect a given segment AB.*

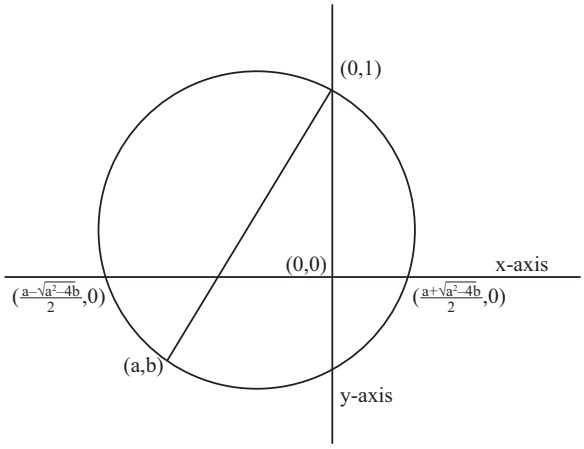
This is obvious from *Figure* 2. The circles centred at A and B having the common radius AB intersect at two points. The line joining these two points is the perpendicular bisector.

Marking the point (a, b) on the plane is, by these observations, equivalent to the construction of the lengths $|a|$ and $|b|$. Further, one can view the same as the construction of the complex number $a + ib$.

5. *If a and b are constructed real numbers, then the roots of the polynomial $x^2 - ax + b = 0$ are constructible as well.*

Actually, in the discussion of cyclotomy, we will need to deal only with the case when the roots of such a quadratic equation are real. In this case (*Figure* 3), draw the circle with the segment joining the points $(0, 1)$ and (a, b) as its diameter. The points of intersection of this circle with tile x-axis are the roots $\frac{a \pm \sqrt{a^2 - 4b}}{2}$ of the given quadratic equation $x^2 - ax + b = 0$.

Even when the roots of $x^2 - ax + b = 0$ are not real, they can be constructed easily. In this case, we need to construct the points $(\frac{a}{2}, \pm\frac{\sqrt{4b-a^2}}{2})$. But, as we



observed earlier, we can drop perpendiculars and it suffices to construct the absolute value of these roots which is $\sqrt{b}$. This is accomplished by drawing the circle with the segment joining $(0, 1)$ and $(0, -b)$ as diameter and noting that it meets the x-axis at the points $(\pm\sqrt{b}, 0)$.

With this renewed knowledge, let us return to cyclotomy.

For $n = 2$, one needs to draw a diameter and this is evidently achieved by the ruler.

For $n = 3$, the equation $z^3 - 1 = 0$ reduces to the equations $z - l = 0$ or $z^2 + z + l = O$. The roots of the latter are $\frac{-1\pm i\sqrt{3}}{2}$. So, we have to bisect the segment $[-1, 0]$ and the points of intersection of this bisector with the unit circle are the points we want to mark off on the circle.

For $n = 4$, again only bisection (of the x-axis) is involved. This already demonstrates clearly that if the regular n-gon can be constructed, then so can the $2^r n$-gon be for any r. In particular, the 2^r-gons are constructible.

To construct the regular pentagon, one has to construct the roots of $z^5 - 1 = 0$. These are the 5-th roots of unity ζ^k; $i \leq k \leq 5$ where $\zeta = e^{2i\pi/5}$. Now the sum of the roots of $z^5 - 1 = 0$ is

$$0 = \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5.$$

On using this and the fact that $\zeta^5 = 1$, we get

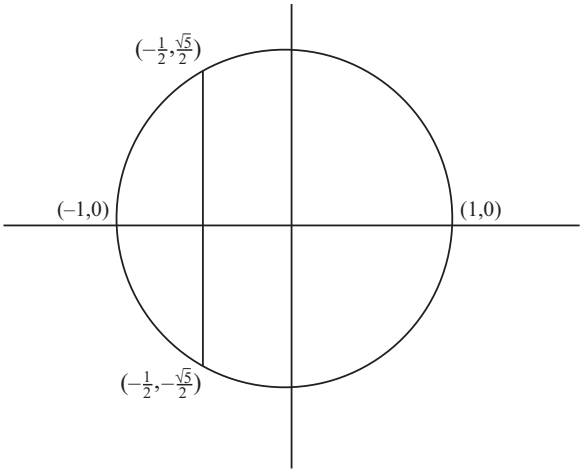
$$(\zeta^2 + \zeta^3)(\zeta + \zeta^4) = \zeta + \zeta^2 + \zeta^3 + \zeta^4 = -1.$$

On the other hand, we also have their sum

$$(\zeta^2 + \zeta^3) + (\zeta + \zeta^4) = -1.$$

This means that $\zeta^2+\zeta^3$ and $\zeta+\zeta^4$ are the two roots of the quadratic polynomial $T^2+T-1=0$. Thus, $\zeta+\zeta$ (being positive, equal to $2\mathbf{C}\mathrm{os}(2\pi/5)$) equals $\frac{-1+\sqrt{5}}{2}$. Multiplying this equality by ζ and using $\zeta^5=1$, one gets a quadratic equation for ζ!

This is the algebraic reasoning behind the construction. Following it, we can geometrically make the construction also with the aid of the dictionary between algebra and geometry that we have established above.



Let us now turn to the construction of the 17-gon. There are many ways of doing it – [4], [5] contain explicit geometric algorithms; Gauss's own construction appears in [6], Art.365 – and all of them succeed essentially because $17-1$ is a power of 2! This is the reason why the degree 16 equation $\frac{x^{17}-1}{x-1}=x^{16}+x^{15}+\cdots+x+1=0$ reduces to a chain of quadratic equations.

It would be ideal to use the language of Galois theory (see *Resonance*, Vol. 4, No. 10, 1999) to discuss the constructibility or non-constructibility of a regular polygon. However, we will keep the discussion elementary and will only make a few remarks for the reader familiar with basic Galois theory so that she/he can grasp the conceptual reason behind various explicit expressions, the appearance of which will seem magical without the added understanding[4] provided by Galois theory.

In the light of our dictionary, we describe a construction as follows:

Denote by ζ, the 17-th root of unity $e^{2i\pi/17}$. Then, $\zeta^{17}=1$ gives

$$\zeta^{16}+\zeta^{15}+\cdots+\zeta+1=0.$$

That is,

$$(\zeta+\zeta^{-1})+(\zeta+\zeta^{-2})+\cdots+(\zeta^8+\zeta^{-8})=-1.$$

[4]Perhaps an outstanding feature of mathematics is that knowing the conceptual reason behind a phenomenon is often much more important than a proof of the phenomenon itself.

Let us write $\alpha_1, \alpha_2, \alpha_3$ for the three real numbers

$$\zeta^3 + \zeta^{-3} + \zeta^5 + \zeta^{-5} + \zeta^6 + \zeta^{-6} + \zeta^7 + \zeta^{-7},$$
$$\zeta^3 + \zeta^{-3} + \zeta^5 + \zeta^{-5},$$

and

$$\zeta + \zeta^{-1},$$

respectively. Look at the sequence of four quadratic equations:

$$\begin{aligned} T^2 - \alpha_3 T + 1 &= 0; \\ T^2 - \frac{\alpha_2^3 - 6\alpha_2 - 2\alpha_1 + 1}{2} T + \alpha_2 &= 0; \\ T^2 - \alpha_1 T - 1 &= 0; \\ T^2 - T - 4 &= 0. \end{aligned}$$

A routine calculation shows that $\zeta, \alpha_3, \alpha_2, \alpha_1$ are roots of the four equations in that order. The roots of the last equation are evidently constructible as it has integer coefficients. This means that one can construct ζ by recursively constructing the roots of these equations using a ruler and a pair of compasses. The reader may geometrically make the construction based on the dictionary above or consult one of the references quoted.

The reader familiar with basic Galois theory would recall that the four successive quadratic extension fields generated by the polynomials give a tower of corresponding Galois groups. The Galois group of the cyclotomic field[5] $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$ is a cyclic group of order 16 generated by the automorphism

$$\sigma : \zeta \mapsto \zeta^3$$

(in other words, 3 is what is known as a primitive root modulo 17; in other words, 16 is the smallest positive integer such that $3^{16} - 1$ is divisible by 17). The automorphisms σ^2 (that is, σ applied twice in succession), σ^4, σ^8 fix $\alpha_1, \alpha_2, \alpha_3$ respectively.

Now, the question remains as to what made this work and which other n-gons are constructible. Look at the regular n-gon for some n. To construct it, one needs to mark off the complex number $\zeta = e^{2i\pi/n}$. The question is whether ζ can be expressed in terms of a nested chain of square roots.

For example, for the 17-gon, one gets

$$\begin{aligned} \mathrm{Cos}(2\pi/17) &= \frac{-1}{16} + \frac{\sqrt{17}}{16} + \frac{\sqrt{34 - 2\sqrt{17}}}{16} \\ &\quad + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}. \end{aligned}$$

[5]This consists of all polynomial expressions in ζ with rational coefficients.

Thus, $\sin(2\pi/17)$ can also be expressed similarly.

Of course, ζ is a root of the polynomial $z^n - 1$, but it is a root of an equation of smaller degree. What is the smallest degree equation of which ζ is a root? By the division algorithm, there is such a unique monic polynomial (that is, a polynomial with top coefficient 1) which divides any other polynomial of which ζ is a root. This polynomial is called a cyclotomic polynomial. The degree of this polynomial is of paramount importance because if it is a power of two, we know from our earlier discussion that ζ can be constructed. The cyclotomic polynomials are useful in many ways and have several interesting properties some of which will be discussed in the last three sections.

For a prime number p such that $p - 1$ is a power of 2, our discussion shows that the regular p-gon is constructible. Such a prime p is necessarily of the form $2^{2^n} + 1$ since $2^{\text{odd}} + 1$ is always a multiple of 3. Fermat thought that the numbers $2^{2^n} + 1$ are primes for all n. However, the only primes of this form found until now are $3, 5, 17, 257$ and 65537(!). The number $2^{2^5} + 1$ was shown by Euler to have 641 as a proper factor. The primes of the form $2^{2^n} + 1$ are called Fermat primes. For coprime numbers m and n, if the m-gon and the n-gon are constructible, then so is the mn-gon. The reason is, if we write $ma + nb = 1$ for integers a, b, then

$$\operatorname{Cos}\left(\frac{2\pi}{mn}\right) = \operatorname{Cos}\left(\frac{2\pi b}{m} + \frac{2\pi a}{n}\right)$$

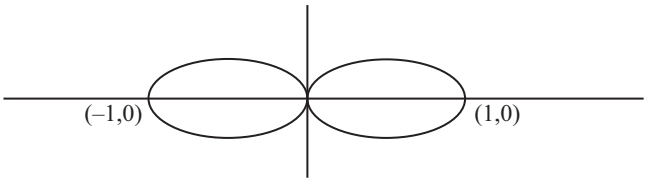
which is constructible when $\operatorname{Cos}\left(\frac{2\pi b}{m}\right)$ and $\operatorname{Cos}\left(\frac{2\pi a}{n}\right)$ are. Thus, Gauss's analysis shows that if n is a product of Fermat primes and a power of 2, the regular n-gon can be constructed by a ruler and compasses. The converse is also true; that is, if the regular n-gon is constructible, then n is of this special form. Gauss did not give a proof of this although he asserted it to be true – see [5]. The construction of the regular 257-gon was published in four parts in *Crelle's Journal*. Details of the 65537-gon fill a whole trunk kept at the University of Göttingen!

We must see Gauss's feat in the light of the fact that complex analysis was in its infancy at that time. In fact, Gauss was the first one to give a rigorous proof (in his doctoral thesis) of the so-called fundamental theorem of algebra which asserts that every nonconstant complex polynomial has a root.

2. Abel's Theorem for the Lemniscate

Abel earned fame by proving that the general equation of degree at least five is not solvable by a 'formula' involving only arithmetical operations and extraction of square roots, cube roots and higher roots of the coefficients – in other words, there is no such formula which can be prescribed so that

when we apply the formula to any collection of coefficients, we obtain the roots of the corresponding polynomial equation. One of his lesser-known achievements involves a problem analogous to cyclotomy viz., the division of the lemniscate. The name lemniscate literally means a ribbon and comes from its shape (*Figure* 5); this curve – also called the elastic curve – was discovered by Bernoulli.



It has an equation of the form $(x^2+y^2)^2 = x^2 - y^2$. The total arc length of the lemniscate is given by the integral $4\int_0^1 \frac{dt}{\sqrt{1-t^4}}$. Thus, the number ω which is half of this integral is the analogue for the lemniscate of what π is for the unit circle. It is approximately $2.6205\cdots\cdots$ Gauss had already asserted as entry 62 in his diary (see [7]) that the lemniscate is divisible into five equal parts by a ruler and a pair of compasses. The previous two entries show clearly that Gauss knew that the lemniscatic trigonometric functions are doubly-periodic functions; they are called elliptic functions nowadays. He hinted at a vast theory of his behind these functions but this work never appeared. It was Abel who published a comprehensive treatise on elliptic functions and in it he also looked at the problem of dividing the lemniscate into 77, equal parts for any 77, (see [8] for a more modern discussion). He discovered the remarkable fact that the answer is the same as for the circle! In other words, the lemniscate can be divided into n equal parts with the aid of a ruler and compasses if, and only if, n is a product of a power of 2 and distinct Fermat primes. The reason can again be understood using Galois theory. In the case of the circle, the Galois group of the cyclotomic extension is the multiplicative group of integers modulo n which are coprime to n. This latter group is a group of order a power of 2 precisely when n is a product as above. For the lemniscate, it turns out that one needs to know when the unit group of $\mathbf{Z}[i]/n\mathbf{Z}[i]$ is a group of order a power of 2 where the set $\mathbf{Z}[i]$ of Gaussian integers consists of the complex numbers $a+bi$ with integers a, b. This is again a 'ring' – like the integers, we can add and multiply elements.

3. Cyclotomic Polynomials

We introduced for any positive integer n, the cyclotomic polynomial $\Phi_n(X)$ as the unique monic integer polynomial of least degree having $\zeta = e^{2i\pi/n}$ as a root. What does $\Phi_n(X)$ look like? Obviously $\Phi_1(X) = X - 1$

and $\Phi_2(X) = X + 1$. Moreover, for a prime number p, $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. For any n, the n-th roots of unity are the complex numbers $e^{2ir\pi/n}; l \leq r \leq n$. In other words, $X^n - l = \prod_{r=1}^{n}(X - \zeta^r)$ where $\zeta = e^{2i\pi/n}$. The crucial fact is that along with ζ, all the powers ζ^r with r coprime [6] to n are the roots of $\Phi_n(X)$! So,

$$X^n - 1 = \prod_{d|n} \prod_{(r,n)=d} (X - \zeta^r) = \prod_{d|n} \Phi_d(X).$$

Here, we have denoted by (r, n) the greatest common divisor of r and n. Note that the degree of $\Phi_n(X)$ is the number of positive integers $r \leq n$ that are coprime to n; this is usually denoted by $\phi(n)$, and called Euler's totient. If we only look at the above expression, it is not clear that $\Phi_n(X)$ has integer coefficients. One may use elementary number theory to invert the identity $X^n - 1 = \prod_{d|n} \Phi_d(X)$. This is accomplished by what is known as the Möbius inversion formula and, yields the identity

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}$$

where the Möbius function $\mu(m)$ is defined to take the value $0, 1$ or -1 according as whether m is divisible by a square, is a square-free product of an even number of primes, or is a square-free product of an odd number of primes. The inversion formula is a very easy and pleasant exercise in elementary number theory. Note that from the above expression, it is not clear that the fractional expression on the right side is indeed a polynomial but that this follows from induction on n using the expression $X^n - 1 = \prod_{d|n} \Phi_d(X)$.

By observing this among the cyclotomic polynomials $\Phi_p(X)$ for prime p and for $\Phi_n(X)$ for small n, an interesting feature is that the coefficients seem to be among $0, 1$ and -1. One might wonder whether this is true about $\Phi_n(X)$ for any n. It turns out that Φ_{105} has one coefficient equal to 2. This is not an aberration. Indeed, using some nontrivial results on how prime numbers are distributed, one can show that every integer occurs among the coefficients of the cyclotomic polynomials!

4. Infinitude of Primes Ending in 1

$11, 31, 41, 61, 71, 101, \cdots$ are primes – where does it stop? Are there infinitely many primes ending in 1? Equivalently, does the arithmetic progression $\{10n + 1; n \geq 1\}$ contain infinitely many prime numbers? Any prime number other than 2 must obviously end in $1, 3, 7$ or 9. The natural

[6] These are the primitive n-th roots of unity i.e., they are not m-th roots of unity for any smaller m.

question is whether there are infinitely many of each type? The answer is 'yes' by a deep theorem due to Dirichlet – infinitely many primes occur in any arithmetic progression $\{a + nd; n \geq 1\}$ with a, d coprime.

If d is a positive integer, then for the arithmetic progression $\{nd + 1; n \geq 1\}$, one can use cyclotomic polynomials to prove this! This is not surprising because we have already noted in the last section that cyclotomic polynomials are related to the way prime numbers are distributed. Let us prove this now.

Suppose $p_1, p_2, \cdots, p_r$ are prime numbers in this arithmetic progression. We will use cyclotomic polynomials to produce another prime p in this progression different from the above p_i's. This would imply that there are infinitely many primes in such a progression. We will use the simple observation that a polynomial $p(X)$ with integer coefficients has the property that $p(m) - p(n)$ is an integer multiple of $m - n$.

Consider the number $N = dp_1p_2 \cdots p_r$. Then, for any integer n, the two values $\Phi_d(nN)$ and $\Phi_d(0)$ differ by a multiple of N. But, $\Phi_d(0)$ is an integer which is also a root of unity and must, therefore, be ± 1. Moreover, as $n \to \infty$, the values $\Phi_d(nN) \to \infty$ as well since Φ_d is a nonconstant monic polynomial. In other words, $n > 0$, the integer $\Phi_d(nN)$ has a prime factor p. As $\Phi_d(nN)$ is ± 1 modulo any of the $p_1, p_2, \cdots, p_r$ and modulo d, the prime p is different from any of the p_i's and does not divide d. One might wonder which primes divide some value $\Phi_d(a)$ of a cyclotomic polynomial. The answer is that these are precisely the primes occurring in the arithmetic progression $\{nd+1; n > 0\}$. To show this, we use the idea that the nonzero integers modulo p form a group of order $p - 1$ under the operation of multiplication modulo p. So, it is enough to prove that if p divides $\Phi_d(a)$ for some integer a, then a has order d in this group (for, then Lagrange's theorem of finite group theory tells us that d divides the order $p - 1$ of the group, which is just re-stating that p is in the arithmetic progression $\{nd+1; n > 0\}$. Let us prove this now. Since $X^d - 1 = \prod_{l|d} \Phi_l(X)$, it follows that p which divides $\Phi_d(a)$ has to divide $a^d - 1$ also. If d were not the order of a, let k divide d with $k < d$ and p divides $a^k - 1$. Once again, the relation $a^k - 1 = \prod_{l|k} \Phi_l(a)$ shows that p divides $\Phi_l(a)$ for some positive integer l dividing k. Therefore, p divides both $\Phi_d(a + p)$ and $\Phi_l(a + p)$. Now,

$$(a + p)^d - 1 = \prod_{m|d} \Phi_m(a + p) = \Phi_d(a + p)\Phi_l(a + p) \quad (\text{other terms}).$$

The expression on the right hand side is divisible by p^2. On the other hand, the left side is equal, modulo p^2, to $a^d + dpa^{d-1} - 1$. Since p^2 divides $a^d - 1$, it must divide dpa^{d-1} as well. This is clearly impossible since neither a nor d is divisible by p. This proves that any prime factor p of $\Phi_d(nN)$

occurs in the arithmetic progression $\{1+nd; n > 0\}$ and thereby, proves the infinitude of the primes in this progression. Interestingly, Euclid's classical proof of the infinitude of prime numbers is the special case of the above proof where we can use $d = 2$.

5. Sum of Primitive Roots

For a prime number p, Gauss defined a primitive root modulo p to be an integer a whose multiplicative order modulo p is $p-1$. In other words, a is a generator of the multiplicative group of non-zero integers modulo p. More generally, for a positive integer n, every integer a coprime to n is such that $a^{\phi(n)}$ is 1 modulo n. A primitive root modulo n is an integer a such that $\phi(n)$ is the smallest $r > 0$ for which a^r is 1 modulo n. Gauss also showed that primitive roots modulo n exist if, and only if, n is $2, 4, p^a$ or $2p^a$ for some odd prime p.

For instance, the primitive roots modulo 5 among the integers 1 to 4 are 2 and 3. Their sum is 0 modulo 5. Now, look at the primitive roots modulo 7 among 1 to 6. These are 3 and 5. Modulo 7, these sum to 1. What about 11? The primitive roots here are $2, 6, 7$ and 8 and these give the sum 1 modulo 11. What is the pattern here? Without letting out the secret, let us go on to investigate the problem for a general prime p.

When is an integer modulo p a primitive root? As we already observed, an integer a is a primitive root modulo p precisely when p divides the integer $\Phi_{p-1}(a)$. This means when the polynomial $\Phi_{p-1}(X)$ is regarded as a polynomial with coefficients integers modulo p, a is a root. Hence the sum of all the primitive roots modulo p is simply the sum modulo p of the roots of Φ_{p-1} modulo p. As we will prove below, the above sum is $\mu(p-1)$, where $\mu(n)$ is the Möbius function.

6. Cyclotomic Polynomials and Ramanujan Sums [9]

In his famous paper ([10]), Ramanujan discussed the properties of certain finite sums – the so-called Ramanujan sums. Even though Dirichlet and Dedekind had already considered these sums in the 1860's, according to G H Hardy, "Ramanujan was the first to appreciate the importance of the sum and to use it systematically." Ramanujan sums play a key role in the proof of a famous result due to Vinogradov asserting that every large odd number is the sum of three primes. These sums have numerous other applications in diverse branches of mathematics as well as in some parts of physics. So, what are these sums?

For integers $n \geq 1, k \geq 0$, the sum

$$c_n(k) = \sum_{(r,n)=1; r \leq n} e^{2ikr\pi/n}$$

is called a Ramanujan sum. In other words, it is simply the sum of the k-th powers of the primitive n-th roots of unity – 'primitive' here means that the number is not an m-th root of unity for any $m < n$. Note that the primitive n-th roots of unity are the numbers $e^{2ikr\pi/n}$ for all those $r \leq n$ which are relatively prime to n.

The first remarkable property $c_n(k)$ have is that they are integers. Ramanujan showed that several arithmetic functions (that is, functions defined from the set of positive integers to the set of complex numbers) have 'Fourier-like' of expansions in terms of the sums; hence, nowadays these expansions are known as Ramanujan expansions. They often yield very pretty elementary number-theoretic identities. Recently, the theory of group representations of the permutation groups (specifically, the so-called supercharacter theory has been used to re-prove old identities in a quick way and also, to discover new identities.

It is convenient to write

$$\Delta_n = \{e^{2ir\pi/n} : (r, n) = 1, 1 \leq r \leq n\}.$$

Then, the set of all n-th roots of unity $\{e^{2ik\pi/n} : 0 \leq k < n\}$ is a union of the disjoint sets Δ_d as d varies over the divisors of n. This is because an n-th root of unity is a primitive d-th root of unity for a unique divisor d of n. It is also convenient to introduce the 'characteristic' function $\delta_{k|n}$ which has the value 1 when k divides n and the value 0 otherwise. Before stating some properties of the $c_k(n)$'s, let us recall two arithmetic functions which are ubiquitous in situations where elementary number-theoretic counting is involved. The first one is Euler's totient function

$$\phi(n) = |\{r : 1 \leq r \leq n, (r, n) = 1\}|.$$

The other arithmetic function is the Möbius function defined by

$\mu(1) = 1, \mu(n) = (-1)^k$ or 0 for $n > 1$ according as to if n is a square-free integer that is a product of k distinct primes or otherwise.

The Möbius function keeps tab when we use the principle of inclusion-exclusion to do counting. The basic result which can be easily proved by induction on the number of prime factors, is the Möbius inversion formula:

If g is an arithmetic function and

$$f(n) = \sum_{d|n} g(d),$$

then

$$g(n) = \sum_{d|n} f(d)\mu(n/d).$$

With these notations, here are some elementary properties of the Ramanujan sums.

(i) $c_n(k) = c_n(-k) = c_n(n-k)$.
(ii) $c_n(0) = \phi(n)$ and $c_n(1) = \mu(n)$.
(iii) $c_n(ks) = c_n(k)$ if $(s,n) = 1$; in particular, $c_n(s) = \mu(n)$ if $(s,n) = 1$.
(iv) $c_n(k) = c_n(k')$ if $(k,n) = (k',n)$; in particular, $c_n(k) \equiv c_n(k') \bmod n$ if $k \equiv k' \bmod n$.
(v) $\sum_{k=0}^{n-1} c_n(k) = 0$.
(vi) $\sum_{d|n} c_d(k) = \delta_{n|k} n$ and $c_n(k) = \sum_{d|n} d\mu(n/d)\delta_{d|k} = \sum_{d|(n,k)} d\mu(n/d)$; in particular, for prime powers p^r, we have $c_{p^r}(k) = p^r - p^{r-1}$ if $p^r|k$; $= -p^{r-1}$ if $p^{r-1}||k$; and $= 0$ otherwise.
(vii) $c_{mn}(k) = c_m(k)c_n(k)$ if $(m,n) = 1$.
(viii) $\sum_{k=1}^{n} c_m(k)c_n(k) = \delta_{mn} n\phi(n)$.

The property (vi) shows that these sums actually have integer values.

The proof of (i) follows already from the definition and, so do the first parts of (ii) and (iii). The second parts of (ii), (iii) as well as the assertions (iv) and (vii) will follow from (vi). We shall prove (v) and (vi).

For (v), we have

$$\sum_{k=0}^{n-1} c_n(k) = \sum_{k=0}^{n-1} \sum_{\zeta \in \Delta_n} \zeta^k = \sum_{\zeta \in \Delta_n} \sum_{k=0}^{n-1} \zeta^k = 0$$

where the last equality is because

$$\sum_{k=0}^{n-1} \zeta^k = \frac{1-\zeta^n}{1-\zeta} = 0$$

for each $\zeta \in \Delta_n$.

For proving (vi), we note that the second statement follows from the first by the Möbius inversion formula. Let us prove the first one now. We have

$$\sum_{d|n} c_d(k) = \sum_{d|n} \sum_{\zeta \in \Delta_d} \zeta^k = \sum_{m=0}^{n-1} e^{2imk\pi/n}$$

because, as we observed, the disjoint union of Δ_d as d varies over the divisors of n is the set of all n-th roots of unity. Now, if the above sum $\sum_{m=0}^{n-1} e^{2imk\pi/n}$ is multiplied by $e^{2ik\pi/n}$, we get the same sum which means that it is equal to 0 unless $n|k$. When $k|n$, the sum is clearly equal to n. This proves (vi).

The other parts easily follow from (vi).

The equality $c_n(k) = \sum_{d|n} d\mu(n/d)\delta_{d|k}$ is very useful.[7] For instance, if n is a prime power p^r, as we noted above in (vi), we have

$$c_{p^r}(k) = p^r\delta_{p^r|k} - p^{r-1}\delta_{p^{r-1}|k}.$$

Using this expression in (vii) above, we get

$$c_k(n) = \frac{\mu(\frac{k}{(k,n)})\phi(k)}{\phi(\frac{k}{(k,n)})}.$$

The right hand side was studied by R D Von Sterneck in 1902 and is known by his name. The equality above itself was known before Ramanujan and is due to J C Kluyver in 1906.

7. Connection of Ramanujan Sums with Cyclotomic Polynomials

The cyclotomic polynomials $\Phi_n(x) = \prod_{\zeta\in\Delta_n}(x-\zeta)$ have some fascinating properties and have surprising consequences (see [9], where applications such as the infinitude of primes in arithmetic progressions of the form $\{1 + an\}$ are proved). We have:

$$x^n - 1 = \prod_{d|n}\prod_{\zeta\in\Delta_d}(x-\zeta) = \prod_{d|n}\Phi_d(x)$$

and – by Möbius inversion, we deduce

$$\Phi_n(x) = \prod_{d|n}(x^d-1)^{\mu(n/d)}.$$

Taking the logarithmic derivative, we obtain

$$\frac{\Phi_n'(x)}{\Phi_n(x)} = \sum_{d|n}\frac{dx^{d-1}\mu(n/d)}{x^d-1}.$$

Multiplying by $x(x^n-1)$, we get a polynomial in x, viz.,

$$x(x^n-1)\frac{\Phi_n'(x)}{\Phi_n(x)} = \sum_{d|n} d\mu(n/d)(x^d + x^{2d} + \cdots + x^n).$$

[7] Note that even computationally the defining sum for $c_n(k)$ requires approximately n operations whereas the other sum requires roughly $\log(n)$ operations.

Thus, the coefficient of x^k in the polynomial on the right is $\sum_{d|(n,k)} d\mu(n/d)$, which is simply the Ramanujan sum $c_n(k)$. Hence, we have:

Proposition. *For each $k < n$, the Ramanujan sum $c_n(k)$ is the coefficient of x^{k-1} in the polynomial $(x^n - 1)\frac{\Phi_n'(x)}{\Phi_n(x)}$.*

Note a special case of the above discussion.

The sum of the roots of $\Phi_n(X)$ is $c_n(1) = \mu(n)$ as seen above. In particular, if $n = p - 1$ for a prime p, the sum of primitive roots modulo p is the sum of the roots of the polynomial $\Phi_{p-1}(X)$ modulo p, which is therefore $\mu(p-1)$. More generally, the sum of the r-th powers of the primitive roots mod p equals the Ramanujan sum $c_{p-1}(r)$.

8. Equal Sums of Powers via Cyclotomic Polynomials

One has the elementary identity

$$1^3 + 3^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2.$$

By raising both sides to the k-th power, we have the identity

$$(1^3 + 2^3 + 3^3 + \cdots + n^3)^k = (1 + 2 + 3 + \cdots + n)^{2k}.$$

Are there other such identities? It turns out that there are no others. We shall prove this now using cyclotomic polynomials. To be more precise, let us set up the notation

$$p_r(n) = 1^r + 2^r + \cdots + n^r.$$

for any natural numbers n, r. Let us look for natural numbers $r_1 < r_2 < \cdots < r_k$ and $s_1 < s_2 < \cdots < s_l$ different from the r_i's and, also some natural numbers $a_1, a_2, \cdots, a_k, b_1, b_2, \cdots, b_l$ such that, for any natural number n, one has identities

$$p_{r_1}(n)^{a_1} p_{r_2}(n)^{a_2} \cdots p_{r_k}(n)^{a_k} = p_{s_1}(n)^{b_1} p_{s_2}(n)^{b_2} \cdots p_{s_l}(n)^{b_l}.$$

If we have such an identity, then (for $n = 2$),

$$(1 + 2^{r_1})^{a_1} \cdots (1 + 2^{r_k})^{a_k} = (1 + 2^{s_1})^{b_1} \cdots (1 + 2^{s_l})^{b_l} \cdots (A)$$

Now, we look at the larger number among r_k or s_l, say s_l. If $s_l \leq 3$, then the identity can be shown to be just

$$p_3(n)^a = p_1(n)^{2a},$$

that is,

$$(1^3 + 2^3 + 3^3 + \cdots + n^3)^a = (1 + 2 + 3 + \cdots + n)^{2a}$$

which we have already seen. This is an easy check. Now, let us suppose $s_l > 3$. Below, we will prove the nice fact that any number of the form $1 + 2^b$ with $b > 3$ always has a prime factor which is not a factor of any $1 + 2^c$ for any $c < b$. This beautiful observation was first made by A S Bang 120 years ago. This observation shows immediately that an equality of the form (A) cannot hold good because the prime factor p of the largest $1 + 2^{s_l}$ cannot divide any term on the left hand side. Seeing why Bang's observation is valid requires some discussion about cyclotomic polynomials which we proceed to do now.

Generally, if one has an infinite sequence of natural numbers $u_1 < u_2 < u_3 < \cdots$ such that for every n, there exists a prime factor of u_n which does not divide u_m for every $m < n$ usually called a primitive prime divisor of u_n. From any such sequence admitting primitive prime divisors, we have a proof of infinitude of primes because we find at least one new prime divisor at each step as we move along the sequence of u_n's.

We show now that the sequence $\{2^n + 1\}_{n>3}$ has primitive divisors.

An advantage of knowing that the cyclotomic polynomials $\Phi_n(x)$ have integer coefficients is the following. For any integer a and any natural number n, one has

$$a^n - 1 = \prod_{d|n} \Phi_d(a)$$

which is a product of integers. Thus, if p is any prime dividing $a^n - 1$ for some a, then p divides $\Phi_d(a)$ for some $d|n$.

Now, we make the following interesting assertion :

Proposition. *Let $n > 2$. If p is a prime dividing $\Phi_n(a)$ for some integer $a > 1$, then p divides $a^n - 1$ and in this case n is the smallest natural number such that p divides $a^n - 1$ unless $p|n$ in which case the smallest number is of the form n/p^i for some $i \geq 1$. In the latter case, p is the largest prime dividing n. Finally, given $a > 1$ and $n > 2$, if there are no primes p for which a has order n mod p, then $\Phi_n(a)$ is actually a prime.*

Let us prove this. Indeed, p divides $a^n - 1$ since $\Phi_n(a)$ divides $a^n - 1$. Also, if p divides $a^m - 1$ for some $m < n$ as well, then p divides $a^{(m,n)} - 1$ where (m, n) is the GCD of m and n.

Therefore, if n were not the smallest for which p divides $a^n - 1$, we would have a factor d of n such that $d < n$ and $p|(a^d - 1)$. As $d < n$ and $d|n$, there is some prime q such that $qd|n$. Thus, d divides n/q and so p divides $a^{n/q} - 1$. Writing $b = a^{n/q}$, we see that b leaves a remainder 1 on division by p. So, we have

$$\frac{a^n - 1}{a^{n/q} - 1} = \frac{b^q - 1}{b - 1} = 1 + b + b^2 + \cdots + b^{q-1}$$

leaves a remainder of q on division by p. On the other hand, the left hand side is a multiple of $\Phi_n(a)$ which is a multiple of p. Thus, we must have that $p = q$ and that it divides n.

This also shows that $a^{n/q} - 1$ is not a multiple of p for any prime divisor $q \neq p$ of n. Thus, the order of a mod p (which means the smallest natural number d such that p divides $a^d - 1$) is either n or of the form n/p^i for some $i \geq 1$.

To say that when the order of a mod p is $< n$, then the prime p (which we have shown to be a divisor of n) is the largest prime divisor, we need to use Fermat's little theorem.

In the case when the order of a mod p is $< n$, we have seen that it is of the form n/p^i. Thus, n/p^i divides $p - 1$ which means every other prime divisor of n is $< p$. This proves the proposition except for the last assertion.

To see that the last assertion of the proposition also holds, consider $n > 2$, $a > 1$ and a prime divisor p of $\Phi_n(a)$. Under the hypothesis that there are no primes modulo which a has order n, we have seen that p is the largest prime dividing n and that $\Phi_n(a) = p^k$ for some $k \geq 1$. We assert that $k = 1$. Now, $\Phi_n(a)$ divides

$$\frac{a^n - 1}{a^{n/p} - 1} = 1 + a^{n/p} + a^{2n/p} + \cdots + a^{(p-1)n/p}.$$

As $a^{n/p} = 1 + pb$ for some b, the right hand side above is

$$\begin{aligned} &1 + (1 + pb) + \cdots + (1 + pb)^{(p-1)} \\ &\quad = p + p(b + 2b + \cdots + (p-1)b) + p^2 c = p + p^2 d \end{aligned}$$

for some c, d if $p > 2$.

Therefore, p^2 does not divide $\Phi_n(a)$; hence $\Phi_n(a) = p$.

When $p = 2$, the argument is again easy remembering that $n > 2$ is a power of 2 as p is the largest prime divisor of n.

This proves the proposition.

How does one relate what we need about primitive prime divisors for the sequence $\{2^n + 1\}_{n>3}$ with the above discussion? For each $n > 3$, if we find a prime p such that the order of 2 mod p is $2n$, then from $(2^{2n} - 1) = (2^n - 1)(2^n + 1)$, we would have $p|(2^n + 1)$ because p does not divide $2^n - 1$. Also, if p divided $2^m + 1$ for some $m < n$, then it would divide $2^{2m} - 1$ which would contradict the fact that the order of 2 mod p is $2n$.

In order to get a prime p such that 2 has order $2n$ mod p, we need to get a prime p dividing $\Phi_{2n}(2)$ and not dividing $2n$. If there is no such prime, then as we saw in the discussion above, we must have that $\Phi_{2n}(2) = p$ is the largest prime dividing n, and p is odd. Writing $2n = p^i d$ with d dividing $p - 1$. On the other hand,

$$\Phi_{2n}(2) = \frac{\Phi_d(2^{p^i})}{\Phi_d(2^{p^{i-1}})} = \frac{\prod_{r=1}^{\phi(d)}(b^p - \zeta_r)}{\prod_{r=1}^{\phi(d)}(b - \zeta_r)} > (\frac{b^p - 1}{b + 1})^{\phi(d)},$$

where $b = 2^{p^{i-1}}$ and ζ_r are the $\phi(d)$ primitive d-th roots of unity (the roots of $\Phi_d(x)$).

As $b^p - 1 \geq b^{p-2}(b^2 - 1)$, the right side above is $> b^{(p-2)\phi(d)}(b-1)^{\phi(d)}$. As $b \geq 2$, this last expression is at least 2^{p-2}. Therefore, we have

$$p = \Phi_{2n}(2) > 2^{p-2},$$

which is possible only if $p = 3$. In that case we must also have $2n = 6$ which we rule out. In other words, when $n > 3$, then there does exist a prime divisor p of $\Phi_{2n}(2)$ which does not divide n; the above discussion then shows that n is the smallest natural number for which p divides $2^n + 1$. This finishes the whole argument.

9. Cyclotomic Polynomials and a Problem in Geometry

Let us first start with the following simple question. On the unit circle, take n points dividing the circumference into n equal parts. From one of these n points, draw the $n-1$ chords joining it to the other points. It is easy to see that the product of the lengths of these chords is n. A more difficult problem is to start from one of the points and – going in one direction (say, the anticlockwise direction) – drawing the chords joining it to the k-th point from it for each k relatively prime to n, what is the product of the lengths of these chords in this case?

We prove:

Let $n > 1$ and let $P_1, \cdots, P_n$ be points on a circle of radius 1 dividing the circumference into n equal parts. Then, we have :

The product of lengths $\prod_{(l,n)=1, l<n} |\overline{P_1 P_{l+1}}| = p$ or 1 accordingly as to whether $n = p^k$ for a prime p or n is not a power of a prime.

We may assume that the origin is the centre and that points are $P_{d+1} = e^{2id\pi/n}$ for $d = 0, 1, \cdots, n-1$. Note that the product of lengths of all the chords $P_1 P_i$ is simply $\prod_{d=1}^{n-1} |1 - e^{2id\pi/n}|$. Since the polynomial $1 + X + \cdots + X^{n-1}$ has as roots all the n-th roots of 1 excepting 1 itself, we have

$$\prod_{d=1}^{n-1} (1 - e^{2id\pi/n}) = n,$$

by evaluating at $X = 1$. Notice that we have the equality $\prod_{d=1}^{n-1}(1 - e^{2id\pi/n}) = n$ as complex numbers; that is, even without considering absolute values.

Now, let us consider our problem. Here, the product under consideration is

$$\prod_{(d,n)=1} |1 - e^{2id\pi/n}|.$$

First, let us look at the case when $n = p^k$ for some prime p. Then,

$$\prod_{(d,p^k)=1, d<p^k} |1 - e^{2id\pi/p^k}| = \frac{\prod_{d=1}^{p^k-1} |1 - e^{2id\pi/p^k}|}{\prod_{dp<p^k} |1 - e^{2idp\pi/p^k}|} = \frac{p^k}{p^{k-1}} = p.$$

Now, suppose that n has at least two prime factors.

Let us start with the identity $\prod_{d=1}^{n-1}(1 - e^{2id\pi/n}) = n$.

If p is a prime dividing n, suppose p^k is the highest power of p dividing n. Then, the product $\prod_{d=1}^{n-1}(1 - e^{2id\pi/n})$ contains the products of terms corresponding to d running through multiples of n/p^k; that is, $\prod_{d=1}^{p^k-1}(1-e^{2id\pi/p^k})$ (which is p^k). We observe that factors occurring for a different prime q dividing n are disjoint from those occurring corresponding to p. Therefore, the factors corresponding to the various primes dividing n contribute $\prod_{p^k||n} p^k = n$.

On removing these factors corresponding to each prime divisor of n, we will get $\prod_{d\in D}(1 - e^{2id\pi/n}) = 1$, where D consists of those d for which $e^{2id\pi/n}$ does not have prime power order. Thus, if $d \in D$, then $1 - e^{2id\pi/n}$ is a unit since n is not a prime power. Therefore, $1 - e^{2i\pi/n}$ is a unit in the cyclotomic field $\mathbf{Q}(e^{2i\pi/n})$. From Galois theory, we have that the product $\prod_{(d,n)=1}(1 - e^{2id\pi/n})$ is the norm of $1 - e^{2i\pi/n}$ from $\mathbf{Q}(e^{2i\pi/n})$ to $\mathbf{Q}$. As this element is a unit, this product is ± 1. Hence we get $\prod_{(d,n)=1} |1-e^{2id\pi/n}| = 1$ which proves our assertion in the case when n is not a prime power. The proof is complete.

In the above proof, the second part can also be deduced from the first part of the proof in a different fashion as follows.

Writing $P(n) = \prod_{l=1}^{n-1}(1 - \zeta^l)$ and $Q(n) = \prod_{(d,n)=1}(1 - \zeta^d)$, where $\zeta = e^{2i\pi/n}$, we can see that

$$P(n) = \prod_{r|n} Q(r).$$

By Möbius inversion, $Q(n) = \prod_{d|n} P(d)^{\mu(n/d)} = \prod_{d|n} d^{\mu(n/d)}$ by the simpler first assertion observed at the beginning of the pr of the proposition. The function

$$\log Q(n) = \sum_{d|n} \mu(n/d) \log(d),$$

can be identified with the so-called von Mangoldt function $\Lambda(n)$ which is defined to have the value $\log(p)$ if n is a power of p and 0 otherwise. Using this identification, exponentiation gives also the value asserted in the proposition; viz., $Q(n) = p$ or 1 according as to whether n is a power of a prime p or not.

To see why $\Lambda(n) = \sum_{d|n} \mu(n/d)\log(d)$, we write $n = \prod_{p|n} p^{v_p(n)}$ and note that

$$\log(n) = \sum_{p|n} v_p(n)\log(p)$$

But, the right hand side is clearly $\sum_{d|n} \Lambda(d)$. Hence, Möbius inversion yields

$$\Lambda(n) = \sum_{d|n} \log(d)\mu(n/d).$$

We shall use the solution of the above elementary geometric problem (obtained using cyclotomic polynomials) to unearth interesting information about the so-called cyclotomic field $\mathbf{Q}(\zeta_n)$ which consists of polynomial expressions in $\zeta_n = e^{2i\pi/n}$. This section requires a bit of background in basic field theory. It also implies by the so-called Dedekind–Kummer criterion, the well-known fact that the primes ramifying in $\mathbf{Q}(\zeta_n)$ are exactly those which divide n.

Discriminant of $\mathbf{Q}(\zeta_n)$. *Let $n > 2$ be a positive integer and ζ_n be a primitive n-th root of unity. Then, the discriminant of the cyclotomic field is $(-1)^{\phi(n)/2}\frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}$.*

Recall that the ring O_K of algebraic integers of $K = \mathbf{Q}(\zeta_n)$ is $\mathbf{Z}[\zeta_n]$.

The minimal polynomial of ζ_n is the cyclotomic polynomial

$$\Phi_n(X) = \prod_{(r,n)=1} (X - \zeta_n^r).$$

Thus, the discriminant of O_K is that of the polynomial Φ_n up to sign. The polynomial Φ_n has another expression $\Phi_n(X) = \prod_{d|n}(X^d - 1)^{\mu(n/d)}$ which is obtained by Möbius inversion formula to the decomposition

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

Let us prove the first result.

Since

$$\Phi_n(X) = \prod_{d|n}(X^d - 1)^{\mu(n/d)} = (X^n - 1) \prod_{d|n, d<n} (X^d - 1)^{\mu(n/d)},$$

we may write

$$\Psi(X) := \frac{X^n - 1}{\Phi_n(X)} = \prod_{d|n, d<n} (X^d - 1)^{-\mu(n/d).}$$

Now, differentiating $X^n - 1 = \Phi_n(X)\Psi(X)$ and putting $X = \zeta_n$, we get $n\zeta_n^{-1} = \Phi_n'(\zeta_n)\Psi(\zeta_n)$.

We have the discriminant $d(K) = \pm N_{K/\mathbf{Q}}\Phi_n'(\zeta_n) = \pm n^{\phi(n)} N_{K/\mathbf{Q}}(\Psi(\zeta_n))^{-1}$.

Now $\Psi(\zeta_n)^{-1} = \prod_{d|n, d<n}(\zeta_n^d - 1)^{\mu(n/d)}$ which is convenient to write (using n/d instead of d) as:

$$\Psi(\zeta_n)^{-1} = \prod_{d|n, d>1} (\zeta_n^{n/d} - 1)^{\mu(d)},$$

Separating the terms corresponding to $\mu(d) = 1$ and to $\mu(d) = -1$, we have

$$\Psi(\zeta_n)^{-1} = \frac{\prod_{d|n, d>1, \mu(d)=1}(\zeta_n^{n/d} - 1)}{\prod_{d|n, d>1, \mu(d)=-1}(\zeta_n^{n/d} - 1)}.$$

Now, for each divisor d of n, $\zeta_n^{n/d}$ is a primitive d-th root of unity. By proposition 1 above, $1 - \zeta_n^{n/d}$ is a unit unless d is a prime power. In the above expression for $\Psi(\zeta_n)^{-1}$, a nontrivial term in the denominator corresponds to $\mu(d) = -1$ which can happen for a prime power d only if d is prime. In the numerator, the condition $\mu(d) = 1$ cannot happen for any prime power d. In other words,

$$\Psi(\zeta_n)^{-1} = (\text{unit}).\prod_{p|n}(\zeta_n^{n/p} - 1)^{-1}.$$

So, its norm is $\pm\prod_{p|n} N_{K/\mathbf{Q}}(\zeta_n^{n/p} - 1)^{-1}$ as units have norm ± 1.

As $\zeta_n^{n/p}$ is a primitive p-th root of unity, it is in the subfield $\mathbf{Q}(\zeta_p)$ generated by a primitive p-th root of unity, and we have

$$N_{K/\mathbf{Q}}(\zeta_n^{n/p} - 1) = (N_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(\zeta_p - 1))^{[K:\mathbf{Q}(\zeta_p)]} = (\pm p)^{\phi(n)/(p-1)}.$$

Thus, we get

$$d(K) = \pm\frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

Finally, it is well-known (and easy to deduce from the definition) that for any number field L, the discriminant $d(L)$ has sign $(-1)^s$ where s is the number of complex places of L. Our field $K = \mathbf{Q}(\zeta_n)$ has $s = \phi(n)/2$ because primitive n-th roots of unity are all complex.

10. Reducibility of Cyclotomic Polynomials Modulo Primes

The cyclotomic polynomial Φ_n is the monic, irreducible polynomial of a primitive n-th root of unity but it may happen to be reducible modulo certain primes. In this section, we investigate when this happens.

We recall:

For a positive integer $n > 2$, if $disc(\Phi_n)$ is a perfect square, then Φ_n is reducible modulo every prime.

This proof is a standard application of Galois theory. Indeed, it is well-known that if the discriminant of a Galois extension is a square, its Galois group would be contained in the subgroup of even permutations ([1], Lemma 12.3). So, if Φ_n were irreducible modulo some prime p, then the reduction of Φ_n mod p generates over $\mathbf{F}_p$ a Galois extension of degree $\phi(n)$; the Galois group would contain a $\phi(n)$-cycle which is an odd permutation since $\phi(n)$ is even for n

We prove:

For $n > 2$, the polynomial Φ_n is reducible modulo every prime if, and only if, $disc(\Phi_n)$ is a perfect square. If $disc(\Phi_n)$ is not a perfect square – which happens if, and only if, $n = 4, p^k$ or $2p^k$ – then there are infinitely many primes p such that Φ_n is irreducible modulo p.

Let us prove this now.

We have already seen that if $disc(\Phi_n)$ is a perfect square in $\mathbf{Z}$, then Φ_n is reducible modulo every prime. Conversely, suppose $disc(\Phi_n)$ is not a perfect square. Then, looking at the expression $(-1)^{\phi(n)/2}\frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}$ for the discriminant, we shall deduce that $n = 4, p^k$ or $2p^k$ for some odd prime. Indeed, write

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Firstly, if n is odd and $r > 1$, clearly,

$$\frac{\phi(n)}{2} = \frac{\prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)}{2},$$

is even and the power of p_i dividing the discriminant is

$$\Big(\alpha_i(p_i - 1) - 1\Big)\Big(\prod_{k=1}^{r} p_k^{\alpha_k - 1}\Big)\Big(\prod_{j \neq i}(p_j - 1)\Big),$$

which is even.

Thus, if $n > 2$ is odd, then the discriminant is a perfect square unless $n = p^k$.

If $n = 2p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ for some odd primes, $\Phi_n = \Phi_{n/2}$ and the discriminant is a perfect square excepting the case $r = 1$; i.e., $n = 2p^k$.

Now, if $n = 2^{\alpha} p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ with either $\alpha > 2$ or $\alpha = 2$ and $r \geq 1$, then again the powers of 2 and each p_i dividing the discriminant are all even.

Thus, the exceptional case is $n = 4$.

Therefore, we have deduced that the expression for discriminant is a perfect square excepting the cases $n = 4, p^k$ and $2p^k$ for an odd prime.

These exceptional cases are when the Galois group of the cyclotomic field is cyclic.

The Galois group of Φ_n over $\mathbf{Q}$ is a cyclic group of order $\phi(n)$ and contains a $\phi(n)$-cycle. By the Frobenius density theorem discussed in a later chapter, there are infinitely many prime numbers l such that the decomposition group at l is cyclic of order $\phi(n)$ which means that Φ_n modulo l is irreducible and generates the extension of degree $\phi(n)$ over $\mathbf{F}_l$. This proves the proposition.

References

[1] P Morandi, *Field and Galois theory*, Graduate texts in Mathematics 167, Springer-Verlag, 1996.

[2] M Ram Murty and J Esmonde, *Problems in Algebraic Number Theory*, Graduate Texts in Mathematics 190, Springer-Verlag, New York, 2005.

[3] M Artin, *Algebra*, Prentice Hall, 1991.

[4] D Suryaramana, *Resonance*, **Vol. 2**, No. 6, 1997.

[5] Ian Stewart, Gauss, *Scientific American*, 1977.

[6] C F Gauss, *Disquisitiones Arithmeticae*, English Edition, Springer, 1985.

[7] J Gray, English translation and commentary on Gauss's mathematical diary, *Expo. Math.*, **Vol. 2**, 1984.

[8] M Rosen, *Amer. Math. Monthly*, 1981.

[9] B Sury, Ramanujan's Awesome Sums,*Mathematics Newsletter*, **Vol. 24**, no. 2, pp. 31–36, September 2013.

[10] S Ramanujan, On certain trigonometrical sums and their applications in the theory of numbers, *Trans. Cambridge Philos. Soc.,* **Vol. 22**, No. 13, 259-276, 1918.

Polynomials with Integer Values

A quote attributed to the famous mathematician L Kronecker is '*Die Ganzen Zahlen hat Gott gemacht, alles andere ist Menschenwerk.*' A translation might be '*God gave us integers and all else is man's work.*' All of us are familiar already from middle school with the similarities between the set of integers and the set of all polynomials in one variable. A paradigm of this is the Euclidean (division) algorithm. However, it requires an astute observer to notice that one has to deal with polynomials with real or rational coefficients rather than just integer coefficients for a strict analogy. There are also some apparent dissimilarities – for instance, there is no notion among integers corresponding to the derivative of a polynomial. In this discussion, we shall consider polynomials with integer coefficients. Of course a complete study of this encompasses the whole subject of algebraic number theory, one might say. Most of this article sticks to fairly elementary methods (in fact, other than the discussion on Schur's theorem) to address a number of rather natural questions. To give a prelude, since the square of a polynomial with integer coefficients takes perfect square values at all integer points, one such natural question might be "*if an integral polynomial takes only values which are perfect squares, then must it be the square of a polynomial?*" Note that for a natural number n, the polynomial $\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n(n-1)\cdots 1}$ takes integer values at all integers although it does not have integer coefficients.

1. Prime Values and Irreducibility

The first observation about polynomials taking integral values is:

Lemma 1.1. *A polynomial P takes integer values at all integer points if, and only if, $P(X) = a_0 + a_1\binom{X}{1} + \cdots + a_n\binom{X}{n}$ for some a_i in $\mathbf{Z}$.*

Proof. The sufficiency is evident. For the converse, we first note that any polynomial whatsoever can be written in this form for some n and some (possibly non-integral) a_i's. Writing P in this form and assuming that $P(\mathbf{Z}) \subset \mathbf{Z}$, we have

$$\begin{aligned} P(0) &= a_0 \in \mathbf{Z} \\ P(1) &= a_0 + a_1 \in \mathbf{Z} \\ P(2) &= a_0 + a_1\tbinom{2}{1} + a_2 \in \mathbf{Z} \end{aligned}$$

and so on. Inductively, since $P(m) \in Z \forall m$, we get $a_n \in \mathbf{Z}\ \forall\ n$.

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 6, No. 9, pp. 46–60, September 2001.

COROLLARY 1.2

If a polynomial P takes integers to integers and has degree n, then $n!P(X) \in \mathbf{Z}[X]$.

Lemma 1.3. *A nonconstant integral polynomial $P(X)$ cannot take only prime values.*

Proof. If all values are composite, then there is nothing to prove. So, assume that $P(a) = p$ for some integer a and prime p. Now, as P is nonconstant, $\lim_{n\to\infty} |P(a+np)| = \infty$. So, for big enough n, $|P(a+np)| > p$. But $P(a + np) \equiv P(a) \equiv 0 \bmod p$, which shows $P(a + np)$ is composite.

Remark 1.4. Infinitely many primes can occur as integral values of a polynomial. For example, if $(a, b) = 1$, then the well-known (but deep) Dirichlet's theorem on primes in progression shows that the polynomial $aX+b$ takes infinitely many prime values. In general, it may be very difficult to decide whether a given polynomial takes infinitely many prime values. For instance, it is not known if $X^2 + 1$ represents infinitely many primes. In fact, there is no known polynomial of degree ≥ 2 which takes infinitely many prime values.

Lemma 1.5. *If P is a nonconstant polynomial that takes integers to integers, the number of prime divisors of its value set $\{P(m)\}_{m\in\mathbf{Z}}$, is infinite i.e. not all terms of the sequence $P(0), P(1), \cdots$ can be built from finitely many primes.*

Proof. It is clear from the note above that it is enough to prove this for $P(X) \in Z[X]$, which we will henceforth assume. Now, $P(X) = \sum_{i=0}^{n} a_i X^i$ where $n \geq 1$. If $a_0 = 0$, then clearly $P(p) \equiv 0 \bmod p$ for any prime p. If $a_0 \neq 0$, let us consider for any integer t, the polynomial

$$P(a_0tX) = \sum_{i=0}^{n} a_i(a_0tX)^i = a_0 \left\{ 1 + \sum_{i=1}^{n} a_i a_0^{i-1} t^i X^i \right\} = a_0 Q(X).$$

There exists some prime number p such that $Q(m) \equiv 0 \bmod p$ for some m and some prime p, because Q can take the values 0,1,-1 only at finitely many points. Since $Q(m) \equiv 1 \bmod t$, we have $(p, t) = 1$. Then $P(a_0tm) \equiv 0 \bmod p$. Since t was arbitrary the set of p arising in this manner is infinite.

Remark 1.6. (a) Note that it may be possible to construct infinitely many terms of the sequence $\{P(m)\}_{m\in Z}$ using only a finite number of primes. For example take $(a, d) = 1, a \geq d \geq 1$. Since, by Euler's theorem, $a^{\varphi(d)} \equiv 1 \bmod d$, the numbers $\frac{a(a^{\varphi(d)n}-1)}{d} \in Z \ \forall\ n$. For the polynomial $P(X) = dX + a$, the infinitely many values $P(\frac{a}{d}(a^{\varphi(d)n} - 1)) = a^{\varphi(d)n+1}$ have only prime factors coming from primes dividing a.

(b) In order that the values of an integral polynomial $P(X)$ be prime for infinitely many integers, $P(X)$ must be irreducible over Z and of content 1. By content, we mean the greatest common divisor of the coefficients. In general, it is difficult to decide whether a given integral polynomial is irreducible or not. We note that the irreducibility of $P(X)$ and the condition that it have content 1, are not sufficient to ensure that $P(X)$ takes infinitely many prime values. For instance, the polynomial $X^n + 105X + 12$ is irreducible, by Eisenstein's criterion (see *Box* 1). But, it cannot take any prime value because it takes only even values and it does not take either of the values ± 2 since both $X^n + 105X + 10$ and $X^n + 105X + 14$ are irreducible, again by Eisenstein's criterion.

Lemma 1.7. *Let* $a_1, \cdots, a_n$ *be distinct integers.*
Then $P(X) = (X - a_1) \cdots (X - a_n) - 1$ *is irreducible.*

Proof. Suppose, if possible, $P(X) = f(X)g(X)$ with $\deg . f, \deg . g < n$. Evidently, $f(a_i) = -g(a_i) = \pm 1 \ \forall 1 \leq i \leq n$. Now, $f(X) + g(X)$ being a polynomial of degree $< n$ which vanishes at the n distinct integers $a_1, \cdots, a_n$ must be identically zero. This gives $P(X) = -f(X)^2$ but this is impossible as can be seen by comparing the coefficients of X^n.

Exercise 1.8. *Let* n *be odd and* $a_1, \cdots, a_n$ *be distinct integers. Prove that* $(X - a_1) \cdots (X - a_n) + 1$ *is irreducible.*

Let us consider the following situation. Suppose $p = a_n \cdots a_0$ is a prime number expressed in the usual decimal system i.e. $p = a_0 + 10a_1 + 100a_2 + \cdots + 10^n a_n, 0 \leq a_i \leq 9$. Then, is the polynomial $a_0 + a_1 X + \cdots + a_n X^n$ irreducible? For example 1289 is a prime the following result due to A Cohn and $x^3 + 2x^2 + 8x + 9$ is irreducible. This is, in fact, true more generally and, we have:

Lemma 1.9. *Let* $P(X) \in Z[X]$ *and assume that there exists an integer* n *such that*

(*i*) *the zeros of* P *lie in the half plane* $Re(z) < n - \frac{1}{2}$.
(*ii*) $P(n-1) \neq 0$
(*iii*) $P(n)$ *is a prime number.*

Then $P(X)$ *is irreducible.*

Proof. Suppose, if possible $P(X) = f(X)g(X)$ over Z with f, g having positive degrees. All the zeros of $f(X)$ also lie in $Re(z) < n - \frac{1}{2}$. Writing f as a product of its irreducible factors over R, we can observe that $f(x + n - 1/2)$ has ALL coefficients non-zero and of the same sign. Thus, the coefficients of $f(-x + n - 1/2)$ have alternate signs. Therefore, $|f(n - \frac{1}{2} - t)| < |f(n - \frac{1}{2} + t)| \forall t > 0$. Since $f(n-1) \neq 0$ and $f(n-1)$ is integral, we have $|f(n-1)| \geq 1$. Thus $|f(n)| > |f(n-1)| \geq 1$. A similar

thing holding for $g(X)$, we get that $P(n)$ has proper divisors $f(n), g(n)$ which contradicts our hypothesis.

Remark: Michael Filaseta and collaborators have generalized this vastly. They show that there exists an integer polynomial f of degree 129 explicitly written down whose largest coefficient is 4959866698915122609810424451291 9 such that $f(10)$ is prime but f has the factor $x^2 - 20x + 101$. Further, every integer polynomial g of any degree whose coefficients are non-negative and strictly less than the above number must be irreducible if $g(10)$ is prime!

2. Irreducibility and Congruence Modulo p

For an integral polynomial to take the value zero at an integer or even to be reducible, it is clearly necessary that these properties hold modulo any integer m. Conversely, if $P(X)$ has a root modulo any integer, it must itself have a root in $\mathbb{Z}$. In fact, if $P(X) \in \mathbb{Z}[X]$ has a linear factor modulo all but finitely many prime numbers, the $P(X)$ itself has a linear factor. This fact can be proved only by deep methods viz. using the so-called Ćebotarev density theorem. On the other hand, (see lemma 2.3) it was first observed by Hilbert that the reducibility of a polynomial modulo every integer is not sufficient to guarantee its reducibility over $\mathbb{Z}$. Regarding roots of a polynomial modulo a prime, there is following general result due to Lagrange:

Lemma 2.1. *Let p be a prime number and let $P(X) \in \mathbb{Z}[X]$ be of degree n. Assume that not all coefficients of P are multiples of p. Then the number of solutions mod p to $P(X) \equiv 0$ mod p is, at the most, n.*

The proof is obvious using the division algorithm over Z/p. In fact, the general result of this kind (provable by the division algorithm again) is that a nonzero polynomial over any field has at the most its degree number of roots.

Remark 2.2. Since $1, 2, \cdots, p-1$ are solutions to $X^{p-1} \equiv 1 \bmod p$, we have

$$X^{p-1} - 1 \equiv (X-1)(X-2)\cdots(X-(p-1)) \bmod p$$

For odd p, putting $X = 0$ gives Wilson's theorem that $(p-1)! \equiv -1 \bmod p$.

Note that we have observed earlier that any integral polynomial has a root modulo infinitely many primes. However, as first observed by Hilbert, the reducibility of a polynomial modulo every integer does not imply its reducibility over Z. For example, we have the following result:

Lemma 2.3. *Let p, q be odd prime numbers such that $(\frac{p}{q}) = (\frac{q}{p}) = 1$ and $p \equiv 1$ mod 8. Here $(\frac{p}{q})$ denotes the Legendre symbol defined to be 1 or -1*

according as p is a square or not modulo q. Then, the polynomial $P(X) = (X^2-p-q)^2-4pq$ is irreducible whereas it is reducible modulo any integer.

Proof.

$$\begin{aligned} P(X) &= X^4 - 2(p+q)X^2 + (p-q)^2 \\ &= (X-\sqrt{p}-\sqrt{q})(X+\sqrt{p}+\sqrt{q})(X-\sqrt{p}+\sqrt{q})(X+\sqrt{p}-\sqrt{q}). \end{aligned}$$

Since $\sqrt{p}, \sqrt{q}, \sqrt{p} \pm \sqrt{q}, \sqrt{pq}$ are all irrational, none of the linear or quadratic factors of $P(X)$ are in $Z[X]$ i.e. $P(X)$ is irreducible. Note that it is enough to show that a factorisation of P exists modulo any prime power as we can use Chinese reminder theorem to get a factorisation modulo a general integer.

Now, $P(X)$ can be written in the following ways:

$$\begin{aligned} P(X) &= X^4 - 2(p+q)X^2 + (p-q)^2 \\ &= (X^2+p-q)^2 - 4pX^2 \\ &= (X^2-p+q)^2 - 4qX^2 \\ &= (X^2-p-q)^2 - 4pq. \end{aligned}$$

The second and third equalities above show that $P(X)$ is reducible modulo any p^n and any q^n. Also since $p \equiv 1 \bmod 8, p$ is a quadratic residue modulo any 2^n and the second equality above again shows that $P(X)$ is the difference of two squares modulo 2^n, and hence reducible mod 2^n.

If ℓ is a prime $\neq 2, p, q$, let us show now that $P(X)$ is reducible modulo l^n for any n.

At least one of $(\frac{p}{\ell}), (\frac{q}{\ell})$ and $(\frac{pq}{\ell})$ is 1 because, by the product formula for Legendre symbols, $(\frac{p}{\ell}) \cdot (\frac{q}{\ell}) \cdot (\frac{pq}{\ell}) = 1$. According as $(\frac{p}{\ell}), (\frac{q}{\ell})$ or $(\frac{pq}{\ell}) = 1$, the second, third or fourth equality shows that $P(X)$ is reducible mod ℓ^n for any n.

We end this section with a result of Schur whose proof is surprising and elegant as well. This is:

Schur's Theorem 2.4. *For any n, the truncated exponential polynomial $E_n(X) = n!(1 + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!})$ is irreducible over $\mathbf{Z}$.*

Just for this proof, we need some nontrivial number theoretic facts. A reader unfamiliar with these notions but one who is prepared to accept at face value a couple of results can still appreciate the beauty of Schur's proof. Here is where we have to take recourse to some very basic facts about prime decomposition in algebraic number fields. Start with any (complex) root α of f and look at the field $K = \mathbf{Q}(\alpha)$ of all those complex numbers which can be written as polynomials in α with coefficients from $\mathbf{Q}$. The basic fact that we will be using (without proof) is that any nonzero ideal in 'the ring of integers of K' (i.e., the subring O_K of K made up of those elements

which satisfy a monic integral polynomial) is uniquely a product of nonzero prime ideals and a prime ideal can occur only at the most the 'degree' times. This is a good replacement for K of the usual unique factorisation of natural numbers into prime numbers. The proof also uses a fact about prime numbers observed by Sylvester but is not trivial to prove.

Sylvester's Theorem. *If $m \geq r$, then $(m+1)(m+2)\cdots(m+r)$ has a prime factor $p > r$.*

The special case $m = r$ is known as Bertrand's postulate. (see the next chapter for two proofs).

Proof of Schur's Theorem. Suppose, if possible, that $E_n(X) = f(X)g(X)$ for some nonconsant, irreducible integral polynomial f. Let us write $f(X) = a_0 + a_1X + \cdots + X^r$ (evidently, we may take the top coefficients of f to be 1).

Now, the proof uses the following observation which is interesting in its own right:

Observation: Any prime dividing the constant term a_0 of f is less than the degree r of f.

To see this, note first that $N(\alpha)$, the 'norm of α' (a name for the product of all the roots of the minimal polynomial f of α) is a_0 upto sign. So, there is a prime ideal P of O_K so that $(\alpha) = P^kI$, $(p) = P^lJ$ where I, J are indivisible by P and $k, l \geq 1$. Here, (α) and (p) denote, respectively, the ideal of O_K generated by α and p. Since $E_n(\alpha) = 0$, we have

$$0 = n! + n!\alpha + n!\alpha^2/2! + \cdots + \alpha^n.$$

We know that the exact power of p dividing $n!$ is

$$h_n = [n/p] + [n/p^2] + \cdots\cdots$$

Thus, in O_K, the ideal $(n!)$ is divisible by P^{lh_n} and no higher power of P. Similarly, for $1 \leq i \leq n$, the ideal generated by $n!\alpha^i/i!$ is divisible by $P^{lh_n - lh_i + ki}$. Because of the equality

$$-n! = n!\alpha + n!\alpha^2/2! + \cdots + \alpha^n,$$

it follows that we cannot have $lh_n - lh_i + ki$ cannot be strictly bigger than lh_n which is the exact power of P dividing the left hand side. Therefore, there is some i so that $-lh_i + ki \leq 0$. Thus,

$$i \leq ki \leq lh_i = l([i/p] + [i/p^2] + \cdots) < \frac{li}{p-1}.$$

Thus, $p - 1 < l \leq r$ i.e., $p \leq r$. This confirms the observation.

To continue with the proof, we may clearly assume that the degree r of f at most $n/2$. Now, we use Sylvester's theorem to choose a prime $q > r$ dividing the product $n(n-1)\cdots(n-r+1)$. Note that we can use this

theorem because the smallest term $n - r + 1$ of this r-fold consecutive product is bigger than r as $r \leq n/2$. Note also that the observation tells us that q cannot divide a_0. Now, we shall write $E_n(X)$ modulo the prime q. By choice, q divides the coefficients of X^i for $0 \leq i \leq n - r$.

So, $f(X)g(X) \equiv X^n + n!\frac{X^{n-1}}{(n-1)!} + \cdots + n!\frac{X^{n-r+1}}{(n-r+1)!} \bmod q$.

Write $f(X) = a_0 + a_1X + \cdots + X^r$ and $g(X) = b_0 + b_1X + \cdots + X^{n-r}$.

The above congruence gives $a_0b_0 \equiv 0$, $a_0b_1 + a_1b_0 \equiv 0$ etc. mod q until the coefficient of X^{n-r} of $f(X)g(X)$. As $a_0 \not\equiv 0 \bmod q$, we get recursively (this is just like the proof of Eisenstein's criterion – see box) that

$$b_0 \equiv b_1 \equiv \cdots b_{n-r} \equiv 0 \mod q.$$

This is impossible as $b_{n-r} = 1$. Thus, Schur's assertion follows.

3. Polynomials Taking Square Values

If an integral polynomial takes only values which are squares, is it true that the polynomial itself is a square of a polynomial? In this section, we will show that this, and more, is indeed true (see also [1]).

Lemma 3.1. *Let $P(X)$ be a Z-valued polynomial which is irreducible. If P is not a constant, then there exist arbitarily large integers n such that $P(n) \equiv 0$ mod p and $P(n) \not\equiv 0$ mod p^2 for some prime p.*

Proof. First, suppose that $P(X) \in Z[X]$. Since P is irreducible, P and P' have no common factors. Write $f(X)P(X) + g(X)P'(X) = c$ for some $f, g \in Z[X]$ and some non-zero integer c. By lemma 1.5, there is a prime p such that $P(n) \equiv 0 \bmod p$ where n can be as large as we want. So, $P'(n) \not\equiv 0 \bmod p$ as $f(n)P(n) + g(n)P'(n) = c$. Since $P(n + p) - P(n) \equiv P'(n) \bmod p^2$, either $P(n + p)$ or $P(n)$ is $\not\equiv 0 \bmod p^2$. To prove the result for general P, one can replace P by $m! \cdot P$ where $m = \deg P$.

Lemma 3.2. *Let $P(X)$ be a Z-valued polynomial such that the zeros of smallest multiplicity have multiplicity m. Then, there exist arbitrarily large integers n such that $P(n) \equiv 0$ mod $p^m, P(n) \not\equiv 0$ mod p^{m+1} for some prime p.*

Proof. Let $P_1(X), \cdots, P_r(X)$ be the distinct irreducible factors of $P(X)$. Write $P(X) = P_1(X)^{m_1} \cdots P_r(X)^{m_r}$ with $m = m_1 \leq \cdots m_r$. By the above lemma, one can find arbitrarily large n such that for some prime p, $P_1(n) \equiv 0 \bmod p$, $P_1(n) \not\equiv 0 \bmod p^2$ and, $P_i(n) \not\equiv 0 \bmod p$ for $i > 1$. Then, $P(n) \equiv 0 \bmod p^m$ and $\not\equiv 0 \bmod p^{m+1}$.

COROLLARY 3.3.

If $P(X)$ takes at every integer, a value which is the k-th power of an integer, then $P(X)$ itself is the k-th power of a polynomial.

Proof. If $P(X)$ is not an exact k-th power, then one can write $P(X) = f(X)^k g(X)$ for polynomials f, g so that $g(X)$ has a zero whose multiplicity is $< k$. Once again, we can choose n and a prime p such that $g(n) \equiv 0 \mod p$, $\not\equiv 0 \mod p^k$. This contradicts the fact that $P(n)$ is a k-th power.

Remark: The above results and much more general properties of polynomials are consequences of the so-called Hilbert irreducibility criterion which implies: if $f(X, Y)$ is an irreducible polynomial with rational coefficients, then there exist infinitely many rational values a of x such that the polynomials $f(a, Y)$ are irreducible in $Q[Y]$. One application of the above theorem is:

Given two non-constant polynomials f, g with rational coefficients such that $f(Q)$ is contained in $g(Q)$, there exist a polynomial h with rational coefficients so that $f(X) = g(h(X))$.

4. Cyclotomic Polynomials

These were already referred to in the earlier chapter. It was also shown there that one could use these polynomials to prove the existence of infinitely many primes congruent to 1 modulo n for any n. For a natural number d, recall that the cyclotomic polynomial $\Phi_d(X)$ is the irreducible, monic polynomial whose roots are the primitive d-th roots of unity i.e. $\Phi_d(X) = \prod_{a \leq d:(a,d)=1}(X - e^{2\pi a/d})$. Note that $\Phi_1(X) = X - 1$ and that for a prime p, $\Phi_p(X) = X^{p-1} + \cdots + X + 1$. Observe that for any $n \geq 1$, $X^n - 1 = \prod_{d/n} \Phi_d(X)$.

Exercise 4.1.

(*i*) *Prove that for any d,* $\Phi_d(X)$ *has integral coefficients.*
(*ii*) *Prove that for any d,* $\Phi_d(X)$ *is irreducible over* $\mathbf{Q}$.

Factorising an integral polynomial into irreducible factors is far from easy. Even if we know the irreducible factors, it might be difficult to decide whether a given polynomial divides another given one.

Exercises 4.2.

(*a*) *Given positive integers* $a_1 < \cdots < a_n$, *consider the polynomials* $P(X) = \prod_{i>j}(X^{a_i - a_j} - 1)$ *and* $Q(X) = \prod_{i>j}(X^{i-j} - 1)$. *By factorizing into cyclotomic polynomials, prove that* $Q(X)$ *divides* $P(X)$. *Conclude that* $\prod_{i>j} \frac{a_i - a_j}{i-j}$ *is always an integer.*

(*b*) *Consider the* $n \times n$ *matrix A whose* (i, j)*-th entry is the Gaussian polynomial* $\begin{bmatrix} a_i \\ j-1 \end{bmatrix}$.

Compute detA to obtain the same conclusion as in part (a).

Here, for $m \geq r > 0$, the Gaussian polynomial is defined as

$$\left[\begin{array}{c} m \\ r \end{array} \right] = \frac{(X^m - 1)(X^{m-1} - 1) \cdots (X^{m-r+1} - 1)}{(X^r - 1)(X^{r-1} - 1) \cdots (X - 1)}.$$

Note that $\left[\begin{array}{c} m \\ r \end{array} \right] = \left[\begin{array}{c} m-1 \\ r-1 \end{array} \right] + X^r \left[\begin{array}{c} m-1 \\ r \end{array} \right]$.

Recall from the earlier chapter that from looking at $\Phi_p(X)$ for prime p, it seems as though the coefficients of the cyclotomic polynomials $\Phi_d(X)$ for any d are among 0, 1 or -1. However, the following rather amazing thing was discovered by Schur. His proof uses a consequence of a deep result about prime numbers known as the prime number theorem. The prime-number theorem tells us that $\pi(x) \sim x/\log(x)$ as $x \to \infty$. Here $\pi(x)$ denotes the number of primes until x. The reader does not need to be familiar with the prime number theorem but is urged to take on faith the consequence of it that for any constant c, there is n such that $\pi(2^n) \geq cn$.

PROPOSITION 4.3.

Every integer occurs as a coefficient of some cyclotomic polynomial.

Proof. First, we claim that for any integer $t > 2$, there are primes $p_1 < p_2 < \cdots < p_t$ such that $p_1 + p_2 > p_t$. Suppose this is not true. Then, for some $t > 2$, every set of t primes $p_1 < \cdots < p_t$ satisfies $p_1 + p_2 \leq p_t$. So, $2p_1 < p_t$. Therefore, the number of primes between 2^k and 2^{k+1} for any k is less than t. So, $\pi(2^k) < kt$. This contradicts the prime-number theorem as noted above. Hence, it is indeed true that for any integer $t > 2$, there are primes $p_1 < p_2 < \cdots < p_t$ such that $p_1 + p_2 > p_t$.

Now, let us fix any odd $t > 2$. We shall demonstrate that both $-t+1$ and $-t+2$ occur as coefficients. This will prove that all negative integers occur as coefficients. Then, using the fact that for an odd $m > 1$, $\Phi_{2m}(X) = \Phi_m(-X)$, we can conclude that all integers are coefficients.

Consider now primes $p_1 < p_2 < \cdots < p_t$ such that $p_1 + p_2 > p_t$. Write $p_t = p$ for simplicity. Let $n = p_1 \cdots p_t$ and let us write $\Phi_n(X)$ modulo X^{p+1}. Since $X^n - 1 = \prod_{d/n} \Phi_d(X)$, and since $p_1 + p_2 > p_t$, we have

$$\begin{aligned} \Phi_n(X) &\equiv \prod_{i=1}^{t} \frac{1 - X^{p_i}}{1 - X} \equiv (1 + \cdots + X^p)(1 - X^{p_1}) \cdots (1 - X^{p_t}) \\ &\equiv (1 + \cdots + X^p)(1 - X^{p_1} - \cdots - X^{p_t}) \mod X^{p+1}. \end{aligned}$$

Therefore, the coefficients of X^p and X^{p-2} are $1-t$ and $2-t$ respectively. This completes the proof. Note that in the proof, we have used the fact that if $P(X) = (1-X^r)Q(X)$ for a polynomial $Q(X)$, then $Q(X) = P(X)(1+X^r + X^{2r} + \cdots + \cdots)$ modulo any X^k.

Exercise 4.4.

(a) Let $A = (a_{ij})$ be a matrix in $GL(n, Z)$ i.e., both A and A^{-1} have integer entries. Consider the polynomials $p_i(X) = \sum_{j=0}^{n} a_{ij}X^j$ for $0 \leq i \leq n$. Prove that any integral polynomial of degree at most n is an integral linear combination of the $p_i(X)$. In particular, if $a_0, \ldots, a_n \in Q$ are distinct, show that any rational polynomial of degree at most n is of the form $\sum_{i=0}^{n} \lambda_i(X + a_i)^n$ for some $\lambda_i \in Q$.

(b) Prove that $1 + X + \ldots + X^n = \sum_{i=0}^{[\frac{n}{2}]} (-1)^i \binom{n-i}{i} X^i(1 + X)^{n-2i}$. Conclude that $\sum_{i\geq 0} \binom{n-i}{i} = \frac{1+\rho+\cdots+\rho^n}{(1+\rho)^n}$ where ρ is either root of $X^2 + 3X + 1 = 0$. Further, compute $\sum_{i\geq 0} (-1)^i \binom{n-i}{i}$.

Remark 4.5. It is easily seen by induction that $\sum_{i\geq 0} \binom{n-i}{i}$ is just the $(n+1)$-th Fibonacci number F_{n+1}. Thus, exercise (b) provides an expression for F_{n+1}. This expression makes it easy to prove the following identities:

(a) $F_n + F_{n+1} = F_{n+2}$.
(b) $F_{n+1}F_{n-1} = F_n^2 + (-1)^n$.
(c) $\sum F_n z^n = \frac{z}{1-z-z^2}$.
(d) $F_n^2 + F_{n+1}^2 = F_{2n+1}$.

Notice that only (a) seems obvious from the expression $F_{n+1} = \sum_{i\geq 0} \binom{n-i}{i}$.

As we remarked earlier, even for a polynomial of degree 2 (like $X^2 + 1$) it is unknown whether it takes infinitely many prime values. A general conjecture in this context is:

Conjecture 4.6. (*Bouniakowsky, Schinzel and Sierpinski.*) A nonconstant irreducible integral polynomial whose set of values has no nontrivial common factor, always takes on a prime value.

It is appropriate to recall here that the polynomial $X^2 + X + 41$ takes prime values at $X = -40, -39, \ldots, 0, 1, \ldots, 39$. We end with an open question which is typical of number-theoretic questions – a statement which can be understood by the proverbial layman but an answer which proves elusive to this day to professional mathematicians.

For any irreducible, monic, integral polynomial $P(X)$, define its *Mahler measure* to be $M(P) = \prod_i \text{Max}(|\alpha_i|, 1)$ where the product is over the roots of P. The following is an easy exercise.

Exercise 4.7. $M(P) = 1$ *if, and only if,* P *is cyclotomic.*

D H Lehmer posed the following question:

Does there exist a constant $C > 0$ such that $M(P) > 1 + C$ for all noncyclotomic (irreducible) polynomials P?

This is expected to have an affirmative answer and, indeed, Lehmer's calculations indicate that the smallest possible value of $M(P) \neq 1$ is 1.176280821...., which occurs for the polynomial

$$P(X) = X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1.$$

Lehmer's question can be formulated in terms of discrete subgroups of Lie groups. One may not be able to predict when it can be answered but it is more or less certain that one will need tools involving deep mathematics.

References

[1] Polya and Szego, *Problems in Analysis*, I & II, Springer-Verlag, 1945.

Box 1. Eisenstein's and Dumas's Criteria

A general criterion known to check whether an integral polynomial of a special kind is irreducible is due to G Eisenstein, a student of Gauss and an outstanding mathematician. Eisenstein died when he was 27.

Let $f(X) = a_0 + a_1X + \cdots + a_nX^n$ be an integral polynomial satisfying the following property with respect to some prime p. The prime p divides $a_0, a_1, \cdots, a_{n-1}$ but does not divide a_n. Also, assume that p^2 does not divide a_0. Then, f is irreducible.

The proof is indeed very simple high school algebra. Suppose, if possible, that $f(X) = g(X)h(X) = (b_0 + b_1X + \cdots + b_rX^r)(c_0 + c_1X + \cdots + c_sX^s)$ with $r, s \geq 1$. Comparing coefficients, one has

$$a_0 = b_0c_0, a_1 = a_0b_1 + b_0a_1, \cdots, a_n = b_rc_s, \quad r + s = n.$$

Since $a_0 = b_0c_0 \equiv 0 \bmod p$, either $b_0 \equiv 0 \bmod p$ or $c_0 \equiv 0 \bmod p$.

To fix notations, we may assume that $b_0 \equiv 0 \bmod p$. Since $a_0 \not\equiv 0 \bmod p^2$, we must have $c_0 \not\equiv 0 \bmod p$. Now $a_1 = b_0c_1 + b_1c_0 \equiv b_1c_0 \bmod p$; so $b_1 \equiv 0 \bmod p$. Proceeding inductively in this maner, it is clear that all the b_i's are multiples of p. This is a manifest contradiction of the fact that $a_n = b_rc_s$ is not a multiple of p. This finishes the proof.

It may be noted that one may reverse the roles of a_0 and a_n and obtain another version of the criterion:

Let $f(X) = a_0 + a_1X + \cdots + a_nX^n$ be an integral polynomial satisfying the following property with respect to some prime p. The prime p divides $a_1, a_2, \cdots, a_n$ but does not divide a_0. Also, assume that p^2 does not divide a_n. Then, f is irreducible.

More generally, we have the following irreducibility criterion due to Gustave Dumas from 1906:

Let $f = \sum_{i=0}^{n} c_iX^i$ be a polynomial with integer coefficients and let p be a prime such that $v_p(c_n) = 0$, $v_p(c_0) < nv_p(c_{n-i})/i$ for $0 < i < n$, and $gcd(n, v_p(c_0)) = 1$. Then, f is irreducible modulo p (hence irreducible over Z itself).

Here $v_p(a)$ denotes the power of p dividing a. Note that the polynomial $X^6 + 2X^5 + 3X^4 + 4x^3 + 5X^2 + 6X + 7$ is irreducible modulo 5 by Dumas's criterion. Usually, this criterion is stated in terms of so-called Newton polygons.

How Far Apart are Primes? Bertrand's Postulate

It is well-known that there are arbitrarily large gaps in between primes. Indeed, given any natural number n, the numbers $(n+1)!+2, (n+1)!+3, \cdots, (n+1)!+(n+1)$ being large multiples of $2, 3, \cdots, n+1$ respectively, are all composite numbers.

Let us now ask ourselves the following question. If we start with a natural number n and start going through the numbers $n+1, n+2$, etc., how far do we have to go before hitting a prime? Trying out the first few numbers, we see that

$$1 \to 2, 2 \to 3, 3 \to 5, 4 \to 5, 5 \to 7, 6 \to 7, 7 \to 11 \quad \text{etc.}$$

Thus, it seems that we need to go 'at most twice the distance' i.e., we seem to be able to find a prime between n and $2n$ for the first few values of n. But there is absolutely no pattern here. In fact, although we have seen above that *there are arbitrarily large gaps between primes*, it is nevertheless true that *'there is regularity in the distribution of primes'*. It is this fascinating clash of tendency which seems to make primes at once interesting and intriguing. It turns out indeed to be true that: *there is always a prime between n and $2n$. This statement, known as Bertrand's postulate*, was stated by Bertrand (1822–1900) in 1843 and proved later by Chebychev in 1852. Actually, Chebychev proves a much stronger statement which was further generalised to yield a fundamental fact about the prime numbers known as the prime number theorem. Interestingly, Bertrand's motivation was to group theory and not really number theory; he made many contributions to differential geometry and probability theory as well.

Proving the prime number theorem is beyond the scope of this article but stating it certainly lies within it. For a positive real number x, let us denote by $\pi(x)$, the number of primes which do not exceed x. The prime number theorem states that the ratio $\frac{\pi(x)\log x}{x}$ approaches the limit 1 as x grows indefinitely large i.e., $\lim_{x\to\infty}\frac{\pi(x)\log x}{x} = 1$.

One usually writes $\pi(x) \sim \frac{x}{\log x}$ to describe such an asymptotic result. What Chebychev proved was that there are some explicit positive constants a, b so that

$$a\frac{\log x}{x} < \pi(x) < b\frac{\log x}{x}.$$

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 7, No. 6, pp. 77–87, June 2002.

If p_n denotes the n-th prime, Bertrand's postulate is equivalent to the assertion that $p_{n+1} < 2p_n$ while the prime number theorem itself is equivalent to the statement $\lim_{n\to\infty} \frac{p_n}{n\log n} = 1$.

It is rather startling to note that the great mathematician Gauss (1777-1855) had, at the age of 15, already conjectured the truth of the prime number theorem. Four years later, in 1796, Legendre also came independently to conjecture something similar.

Legendre conjectured, based on empirical evidence, that $\pi(x) \sim \frac{x}{A\log x+B}$ and also conjectured values of A, B which turned out to be incorrect. Gauss, on the other hand, conjectured that $\pi(x) \sim \int_2^x \frac{dt}{\log t}$; the right side is denoted by $li(x)$ to stand for the 'logarithmic integral'. This seems to have exactly the content of the prime number theorem since clearly $li(x) \sim \frac{x}{\log x}$. However, later research (following Riemann) has confirmed that Gauss's assertion is even more astute than what it appears to be on the face of it. In fact, the function $li(x)$ has the asymptotic expansion (for any fixed n)

$$li(x) = \frac{x}{\log x} + 1!\frac{x}{(\log x)^2} + 2!\frac{x}{(\log x)^3} + \cdots + (n-1)!\frac{x}{(\log x)^n} + O(\frac{x}{(\log x)^{n+1}}).$$

A refined version of the prime number theorem indeed implies that $\pi(x)$ has the same asymptotic expansion.

In particular, this implies that the best possible values for A and B in Legendre's conjecture are $A = 1, B = -1$.

The prime number theorem was proved independently by Hadamard and de la Vallee Poussin. A well-known mathematician quipped once that the proof almost immortalised these two mathematicians – they lived to be 96 and 98 respectively!

Returning to Bertrand's postulate, after Chebychev's first proof, other simpler proofs appeared. A generalization of Bertrand's postulate is Sylvester's theorem which was stated and used in the previous chapter. In this chapter, we shall discuss two of the simplest proofs due to two great minds – Ramanujan and Erdos. Most of us are told stories about Ramanujan and his discoveries and it is rarely that one can find a proof of his which is elementary enough to be actually discussed at this level. Erdos's proof is even more elementary and we start with it.

Erdos's Proof

We start with any natural number n and look at the product $\prod_{p\le n} p$ over all primes $p \le n$.

We shall have occasion to use the well-known and easily proved fact asserting that the highest power to which a prime divides $n!$ is given by the

expression

$$[n/p] + [n/p^2] + [n/p^3] + \cdots\cdots$$

Erdos's proof starts with the following very beautiful observation:

Lemma. $\prod_{p\le n} p \le 4^n$.

Proof. We prove this by induction on n. It evidently holds good for small n. Look at some $n > 1$ such that the result is assumed for all $m \le n$. Then,

$$\begin{aligned}\prod_{p\le n} p &= \prod_{2p\le n+1} p \prod_{n+1<2p\le 2n} p \\ &\le 4^{\frac{n+1}{2}} \prod_{n+1<2p\le 2n} p\end{aligned}$$

by the induction hypothesis.

Now, the surprisingly simple observation that each prime in the last product (i.e., each prime between $(n+1)/2$ and n) divides the binomial coefficient $\binom{n}{[\frac{n+1}{2}]}$, shows that $\prod_{p\le n} p \le 4^{(n+1)/2} 2^{n-1} = 4^n$.

The bound $\binom{n}{[\frac{n+1}{2}]} \le 2^{n-1}$ used above is trivially seen to be true by induction. Thus, we have proved this lemma.

Since we are interested in the possible primes between n and $2n$, it is natural to consider the binomial coefficient $\binom{2n}{n}$ because it 'captures' all these primes as its divisors. Now, obviously, the binomial coefficient $\binom{2n}{n}$ is the largest term in the expansion $(1+1)^{2n}$ which has $2n+1$ terms. Therefore, we have

$$(2n+1)\binom{2n}{n} \ge 2^{2n}. \tag{1}$$

This gives a lower bound for this middle binomial coefficient and, the idea of the rest of the proof is that lot of the contribution comes from primes between n and $2n$. More precisely, if we write

$$\binom{2n}{n} = \prod_{p\le 2n} p^{e_p} = \prod_{p\le n} p^{e_p} \prod_{n+1<p\le 2n} p,$$

then we shall use the lemma to give an upper bound for the first product $\prod_{p\le n} p^{e_p}$. Here, e_p denotes the power of p dividing the middle binomial coefficient $\binom{2n}{n}$ and, the second product stands for 1 if there are no terms.

We want to see which primes $p \le n$ actually contribute to $\binom{2n}{n}$.

If $p^2 > 2n$ i.e., if $n \ge p > \sqrt{2n}$, then clearly, $e_p = [\frac{2n}{p}] - 2[\frac{n}{p}] = 0$ or 1.

Thus, such primes divide $\binom{2n}{n}$ either to a single power or not at all.

If $n \ge 3$, then a prime $p \le n$ with $2n/3 < p$ must be at least 3 and so $p^2 \ge 3p > 2n$. As $1 \le n/p < 3/2$ for $2n/3 < p \le n$, we have $[\frac{n}{p}] = 1$ and $[\frac{2n}{p}] = 2$ i.e.,

$e_p = [\frac{2n}{p}] - 2[\frac{n}{p}] = 2 - 2 = 0$. Thus, these primes do not divide $\binom{2n}{n}$ when $n \geq 3$.

In other words, we have:

$e_p \leq 1$ if $\sqrt{2n} < p \leq 2n/3$, and $e_p = 0$ if $2n/3 < p \leq n$.

Finally, for the primes with $p \leq \sqrt{2n}$, we simply take the trivial bound $p^{e_p} \leq 2n$. Then, we have

$$\begin{aligned}\binom{2n}{n} &= \prod_{p \leq n} p^{e_p} \prod_{n+1<p\leq 2n} p \leq \prod_{p\leq\sqrt{2n}} (2n) \prod_{\sqrt{2n}<p\leq 2n/3} p \prod_{n+1<p\leq 2n} p \\ &\leq \prod_{p\leq\sqrt{2n}} (2n)\ 4^{2n/3} \prod_{n+1<p\leq 2n} p,\end{aligned}$$

using the lemma. We take $n \geq 8$ as we have verified Bertrand's postulate explicitly for $n \leq 7$; so $\sqrt{2n} \geq 4$ and thus, the number of terms in the first product is at most $\sqrt{2n} - 2$ (as 1 and 4 are not primes). Therefore, we have on using (1) that

$$\frac{2^{2n}}{2n+1} \leq \binom{2n}{n} \leq (2n)^{\sqrt{2n}-2} 4^{2n/3} \prod_{n+1<p\leq 2n} p.$$

Replacing the first term by $\frac{2^{2n}}{(2n)^2}$, we get

$$\prod_{n+1<p\leq 2n} p \geq \frac{4^{n/3}}{(2n)^{\sqrt{2n}}}.$$

Thus, to show that the left side has terms (i.e., that it is not 1 according to our convention), it suffices to see whether the right hand side is bigger than 1 for all n. As usual, this will turn out to be true for large enough values of n and will fail for small values (this only means that the inequality is good enough for large values of n and we need to verify the original assertion directly for the smaller values left out).

After a few trials, we arrive at the number $n = 450$ and find that

$4^{n/3} = 4^{150} > (2n)^{\sqrt{2n}} = (900)^{30}$ since $4^5 > 900$.

There is nothing special about 450 excepting the fact that $2n$ is a perfect square and 450 is large enough for the inequality to hold good. This inequality continues to hold for $n > 450$ as the difference $4^{n/3} - (2n)^{\sqrt{2n}}$ is an increasing function. This last statement is simple to see by looking at the derivative of the difference of the corresponding logarithms. Now it is an easy exercise to verify Bertrand's postulate for $n < 450$. The above proof was essentially due to Erdos; it is a slightly simplified version of his original argument which appears in [2].

Ramanujan's Proof

Let us turn to Ramanujan's proof. It is also extremely clever and completely elementary apart from the use of what is known as Stirling's formula – a proof has been discussed in *Resonance* earlier [3].

In the previous proof we used an estimate for $\prod_{p\leq n} p$. Here, we consider an additive version of it viz., look at the so-called Chebychev function $\theta(x) = \sum_{p\leq x} \log p$ defined for any real number $x \geq 2$. One remark about why one considers functions like the Chebychev function instead of just the prime-counting function – weighted prime-counting is easier as the function becomes smoother. We note two things to begin with:

(i) $\theta(n)$ is simply the logarithm of $\prod_{p\leq n} p$,
(ii) Bertrand's postulate is true for a real number x if it is true for $n = [x]$; indeed, a prime between n and $2n$ is between x and $2x$ as well.

Let us also understand that since we are interested in primes between x and $2x$, we need a lower bound for $\theta(2x) - \theta(x)$. In oher words, we need reasonable lower as well as upper bounds for θ values.

Now, the expression $\sum_{i\geq 0}[n/p^i]$ for the power of a prime dividing $n!$ gives us

$$\log[x]! = \sum_{i\geq 1} \Psi(x/i),$$

where Ψ is the function defined by

$$\Psi(x) = \sum_{i\geq 1} \theta(x^{1/i}).$$

This is the reason to introduce real x.

Using an elementary trick of old vintage, we have the following:

$$\log[x]! - 2\log[x/2]! = \sum_{i\geq 1} (-1)^{i-1} \Psi(x/i),$$

$$\Psi(x) - 2\Psi(\sqrt{x}) = \sum_{i\geq 1} (-1)^{i-1} \theta(x^{1/i}).$$

As θ, Ψ are increasing functions, we get inequalities by chopping off at an odd stage and at an even stage as follows:

$$\Psi(x) - \Psi(\frac{x}{2}) \leq \log[x]! - 2\log[\frac{x}{2}]! \leq \Psi(x) - \Psi(\frac{x}{2}) + \Psi(\frac{x}{3}), \tag{2}$$

$$\Psi(x) - 2\Psi(\sqrt{x}) \leq \theta(x) \leq \Psi(x). \tag{3}$$

Here, Ramanujan takes recourse to Stirling's formula which states that $n! \sim \sqrt{2\pi}\frac{n^{n+\frac{1}{2}}}{e^n}$.

We shall not use it but proceed as follows.

For any $x > 1$, we have the binomial coeficient

$$\binom{[x]}{[\frac{x}{2}]} < \sum_{r \geq 0} \binom{[x]}{r} = 2^{[x]}.$$

Taking logarithms, we obtain

$$\log[x]! - 2\log[x/2]! < x\log 2.$$

But, clearly $\log 2 < \frac{3}{4}$ since $16 < e^3$. In other words, we have

$$\log[x]! - 2\log[x/2]! < 3x/4 \ \ \forall \ \ x > 0 \cdots . \tag{4}$$

Now, we find a lower bound. As we observed before Erdos's proof, for $x > 0$, the binomial coefficient $\binom{[x]}{[x/2]}$ (being the largest term in the expansion of $(1+1)^{[x]}$), must be bigger than $\frac{2^{[x]}}{[x]+1}$ since there are $[x]+1$ terms in the binomial expansion of $(1+1)^{[x]}$.

If x is large enough (for instance, if $x > 240$), then $\frac{2^{[x]}}{[x]+1} > e^{\frac{2[x]}{3}}$. Taking logarithms, we get

$$\log[x]! - 2\log[x/2]! > 2[x]/3 \ \ \forall \ \ x > 240. \tag{5}$$

By (2),(4) and (5), we have

$$\Psi(x) - \Psi(x/2) < 3x/4 \ \ \forall \ \ x > 0, \tag{6}$$

$$\Psi(x) - \Psi(x/2) + \Psi(x/3) > 2[x]/3 \ \ \forall \ \ x > 240. \tag{7}$$

By replacing x by $x/2, x/4, x/8$ etc. in (6) and adding all the expressions we get

$$\Psi(x) < 3x/2 \ \ \forall \ \ x > 0. \tag{8}$$

Note that since $\theta(x) < \Psi(x)$, we have a reasonable upper bound for $\theta(x)$ by (8). For the lower bound, let us use the first inequality of (3) viz., $\Psi(x) \leq 2\Psi(\sqrt{x}) + \theta(x)$ and the inequality $\theta(x/2) \leq \Psi(x/2)$ to write

$$\Psi(x) - \Psi(x/2) + \Psi(x/3) \leq 2\Psi(\sqrt{x}) + \theta(x) - \theta(x/2) + \Psi(x/3).$$

If we use the upper bound for Ψ given in (8), we obtain

$$\Psi(x) - \Psi(\frac{x}{2}) + \Psi(\frac{x}{3}) < \theta(x) - \theta(\frac{x}{2}) + \frac{x}{2} + 3\sqrt{x}. \tag{9}$$

For $x > 240$, the left side has a lower bound given in (7) so that we finally obtain

$$\theta(x) - \theta(x/2) > x/6 - 3\sqrt{x} - 2/3 \ \ \forall \ \ x > 240.$$

Evidently, the right side is positive if $x > 361$. Therefore, there is a prime between x and $2x$ if $x > 181$. For smaller values of x, we find primes explicitly as before. This finishes the beautiful proof due to Ramanujan.

More Comments on Primes

The above elementary methods and their modifications are sufficient to prove Chebychev's theorem viz., the assertion

$$\frac{1}{6}\frac{x}{\log x} < \pi(x) < 6\frac{x}{\log x}.$$

The reader is urged to try and use this to prove the following bound for the n-th prime:

$$\frac{1}{6}n\log n < p_n < 12(n\log n + n\log\frac{12}{e}).$$

This last inequality (in fact, the upper bound) shows easily that the series $\sum \frac{1}{p}$ over all primes diverges. How fast does it diverge?

Here is a proof showing that the divergence is at least as fast as $\log\log x$ i.e., we prove

$\exists c > 0$ such that $\sum_{p\leq x} \frac{1}{p} \geq c\log\log x \ \forall x$.

To see this, given $x > 1$, let us look at the area under the curve $y = \frac{1}{x}$ between 1 and x. Evidently, this area $\int_1^x \frac{dx}{x} = \log x$ is less than $\sum_{n=1}^{[x]} \frac{1}{n}$. (see the figure).

So, if we consider the product $\prod_{p\leq x}(1-\frac{1}{p})^{-1}$, then clearly,

$$\prod\nolimits_{p\leq x}(1-\frac{1}{p})^{-1} \geq \sum\nolimits_{n=1}^{[x]} \frac{1}{n} \geq \log x.$$

Now, $(1-\frac{1}{p})^{-1} = (1+\frac{1}{p})(1+\frac{1}{p^2-1})$. Therefore, $\prod_{p\leq x}(1+\frac{1}{p}) \geq a\log x$ where $a = \prod_p(1+\frac{1}{p^2-1})^{-1}$. Using $e^x > 1+x$ for all $x > 0$, we get $\prod_{p\leq x} e^{1/p}$ $\geq \prod_{p\leq x}(1+\frac{1}{p}) \geq a\log x$ so that $\sum_{p\leq x} \frac{1}{p} \geq c\log\log x$ for some $c > 0$.

This finishes the proof of the lower bound.

The more adventurous reader may like to use the Abel summation formula (see [4]) and prove that this lower bound is of the correct order i.e., one has the rather interesting statement:

$$\sum_{p\leq x} \frac{1}{p} \sim \log\log x.$$

Some Applications of Bertrand's Postulate

The original application of Bertrand's postulate was to Galois theory! Let us talk about some elementary number-theoretic applications.

A Recursion for Primes

We recall a curious application of Bertrand's postulate to finding a recursive expression for primes which appeared in [5], p. 289.

We consider the function

$$f_n = \text{Sign}\left(\frac{2((n-1)!)}{n} - \left[\frac{2((n-1)!)}{n}\right]\right)$$

defined for all $n \geq 3$. Here, the sign function is the function which takes the value 0 at 0 and the value $\frac{x}{|x|}$ for any $x \neq 0$. Clearly, $f_n = 1$ or 0 according as n is prime or composite. Now, by Bertrand's postulate, if $p_n \geq 3$, then p_{n+1} occurs as the first prime among $p_n + 2, p_n + 4, \cdots, 2p_n - 1$. Therefore, (writing p_n as p for simplicity of notation),

$$p_{n+1} = (p+2)f_{p+2} + (p+4)f_{p+4}(1 - f_{p+2}) + \cdots$$

$$+(p+6)f_{p+6}(1-f_{p+2})(1-f_{p+4}) + \cdots + (2p-1)f_{2p-1}(1-f_{p+2})\cdots(1-f_{2p-3}).$$

The Harmonic Sum

The sum $\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ is not an integer for any $n \geq 2$.

More generally, $\frac{1}{m+1} + \frac{1}{m+2} + \cdots + \frac{1}{m+n}$ is not an integer for positive integers m, n. An application of Bertrand's postulate gives a very quick proof of this – we leave this as an exercise.

Prime Sums

For any positive integer n, consider the set $\{1, 2, \cdots, 2n\}$ of the first $2n$ positive integers. We claim that this set can be written as the union of n pairs of integers $\{a_i, b_i\}$ $(1 \leq i \leq n)$ such that $a_i + b_i$ is prime! Indeed, this is clear for $n = 1$ as $1 + 2 = 3$ is prime, and we will apply induction on n to prove it in general. Assume that $n > 1$ and that our assertion is valid for every $m < n$. Now, Bertrand's postulate ensures we have a prime p among the numbers in the set $\{2n+1, 2n+2, \cdots, 4n-1\}$. Writing $p = 2n + r$, we have $r \in \{1, 2, \cdots, 2n-1\}$. Thus, note that r is odd as p must be an odd prime. If $r > 1$, then by induction hypothesis, the set $\{1, 2, \cdots, r-1\}$ can be split into pairs $\{a_i, b_i\}$ $(1 \leq i \leq \frac{r-1}{2})$ such that $a_i + b_i$ is prime for each i. Now, $\{r, r+1, \cdots, 2n\}$ is evidently split into the pairs $\{r, 2n\}, \{r+1, 2n-1\}, \cdots$ whose sums are all equal to the prime p.

Another very interesting application is the following one. By refining the above methods, one may prove that for any positive integer k, there is a sufficiently large N such that there is a prime between n and $2n - k$ for all $n > N$. Applying this to $k = 11$, Robert Dressler showed in 1972 that every positive integer other than 1,2,4,6,9 is a sum of distinct odd primes.

References

[1] W H Mills, A prime-representing function, *Bull. Amer. Math. Soc.* **53**, pp. 604, 1947.

[2] I Niven and D Zuckermann, *Introduction to number theory*, John Wiley and Sons, New York, 1960.

[3] S Ramasubramanian, Mathematical Analysis, *Echoes from Resonance*, Universities Press, Hyderabad, 2001.

[4] T Apostol, *Introduction to analytic number theory*, Springer International Students Edition, Narosa Publishers, New Delhi, 1986.

[5] *American Math. Monthly*, 1975.

Sums of Powers, Bernoulli and the Riemann Zeta function

Bernoulli truly stunned us with his number;
woke us up from a deep and ignorant slumber.
Its relation with Riemann zeta
makes us think nothing could be neater.
The connection is much deeper – ask any plumber!

1. Introduction

It is a beautiful discovery due to Jakob Bernoulli that for any positive integer k, the sum $\sum_{i=1}^{n} i^k$ can be evaluated in terms of, what are now known as, Bernoulli numbers. It is said that the Bernoulli numbers were discovered simultaneously and independently by Japanese mathematician Seki Kowa. Seki Kowa's discovery was posthumously published in 1712, in his work Katsuyo Sampo. In this article, we shall discuss several methods of evaluating the above sum. Apart from Bernoulli's method which we shall recall, we give a method akin to using integration, and one using differentiation. These methods are often useful in evaluating more general sums too as we shall indicate. We also discuss connections with the Riemenn zeta function – some old and some new.

2. Bernoulli Polynomials and Numbers

To motivate the introduction of the Bernoulli polynomials, let us start with the sum that we want to evaluate viz., $\sum_{i=1}^{n} i^k$. Evidently, $\frac{\sum_{i=1}^{n} i^k}{k!}$ is the coefficient of x^k in the power series expansion of $e^x + e^{2x} + \cdots + e^{nx}$. In other words,

$$\frac{e^{(n+1)x} - 1}{e^x - 1} = 1 + \sum_{k \geq 0} \frac{1^k + 2^k + \cdots + n^k}{k!} x^k.$$

Now, the function $\frac{x}{e^x - 1}$ can be represented by a power series $\frac{x}{e^x - 1} = \sum_{r \geq 0} B_r \frac{x^r}{r!}$. The numbers B_r are known as Bernoulli numbers and it is easy to evaluate them as follows.

Since the power series x and $(e^x - 1) \sum_{r \geq 0} B_r \frac{x^r}{r!}$ agree in an interval around 0, the numbers are determined recursively as

$$B_0 = 1, \ \sum_{s<r} \binom{r}{s} B_s = 0 \ \forall \ r \geq 2.$$

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 8, No. 7, pp. 54–62, July 2003.

The first few values are $B_0 = 1, B_1 = -1/2, B_2 = 1/6$ and $B_3 = B_5 = B_7 = \cdots = 0$.

Now, consider the function $F_t(x) = \frac{xe^{tx}}{e^x - 1}$ for $x \neq 0$ and $F_t(0) = 1$. Once again, F_t has a power series expansion $F_t(x) = \sum_{k\geq 0} B_k(t)\frac{x^k}{k!}$.

The functions $B_k(t)$ are actually polynomials in t since

$$\sum_{k\geq 0} B_k(t)\frac{x^k}{k!} = F_t(x) = e^{tx}\frac{x}{e^x - 1} = e^{tx}\sum_{k\geq 0} B_k\frac{x^k}{k!}$$

and thus

$$B_k(t) = \sum_{l=0}^{k}\binom{k}{l}B_l t^{k-l}.$$

$B_k(t)$ are called Bernoulli polynomials; note that $B_k(0) = B_k$.

Returning to our sum, we have that $\frac{1^k+2^k+\cdots+n^k}{k!}$ is the coefficient of x^k in $\frac{e^{(n+1)x}-1}{e^x-1}$ i.e., it is the coefficient of x^{k+1} in $\frac{x(e^{(n+1)x}-1)}{e^x-1} = F_{n+1}(x) - F_0(x)$. Thus, $\frac{1^k+2^k+\cdots+n^k}{k!} = \frac{B_{k+1}(n+1)-B_{k+1}}{(k+1)!} = \frac{1}{(k+1)!}\sum_{l=0}^{k}\binom{k+1}{l}B_l(n+1)^{k+1-l}$. In other words,

$$1^k + 2^k + \cdots + n^k = \frac{1}{k+1}\sum_{l=0}^{k}\binom{k+1}{l}B_l(n+1)^{k+1-l}.$$

Note that it is evident from this formula that the sum of the k-th powers of the first n natural numbers is a polynomial function of n of degree $k+1$.

3. Method of 'Integration'

For convenience, let us denote $S_k(n) = 1^k + 2^k + \cdots + n^k$. This is a polynomial function of n i.e., there is a polynomial $S_k(x)$ of degree $k+1$ such that the above equality holds for all n.

The basic idea of the method we will discuss now is that (since $n^k = S_k(n) - S_k(n-1)$), x^k can be thought of as a 'derivative' of the function $S_k(x)$. In other words, $S_k(x)$ itself may be thought of as an 'integral' of the function x^k. Of course, this is only heuristic at the moment because x^k will be the derivative of S_k at some point between $x-1$ and x. The correct tool to make this precise is the 'method of differences' which is really a discrete analogue of differentiation. More precisely, let us recall that the 'backward difference' operator is defined on any function f by $(\nabla f)(x) = f(x) - f(x-1)$ for all x. It is trivial to see that if $P_r(x) = x(x+1)\cdots(x+r-1)$ for $r \geq 1$ and for all x, then $(\nabla P_r)(x) = rP_{r-1}(x)$ for all x.

Let us call g an anti-difference of f if $\Delta g = f$. Note that if f is a polynomial such that $(\nabla f)(n) = 0$ for infinitely many n, then f is a constant. So, if f_1, f_2 are polynomials with $\nabla f_1 = \nabla f_2$, then $f_1 - f_2$ is a constant.

Let us look at our sums $S_k(n)$ now. Let us keep in mind that the polynomial $S_k(x)$ has no constant term. Writing $f_k(x) = x^k$ and $g_k(x)$ for any anti-difference of f_k which is a polynomial function, then we have $(\nabla g_k)(n) = f_k(n) = n^k = S_k(n) - S_k(n-1) = (\nabla S_k)(n)$ for all $n \geq 2$.

Hence, $S_k(x) = g_k(x) + c$ for some constant c. Since $S_k(x)$ has no constant term, we have $c = -g_k(0)$.

In other words, $S_k(n) = g_k(n) - g_k(0)$ for any anti-difference (polynomial) function g_k of f_k.

Note the similarity with the fundamental theorem of calculus.

So, our problem reduces to finding an anti-difference of the function x^k. We observed earlier that the function $P_r(x) = x(x+1)\cdots(x+r-1)$ has an anti-difference $\frac{P_{r+1}(x)}{r+1}$. Therefore, it is just a matter of writing x^k in terms of the P_r's.

For instance, $k = 1$ gives $f_1(x) = x = P_1(x)$ so that $g_1(x)$ can be taken to be $\frac{P_2(x)}{2} = \frac{x(x+1)}{2}$ so that $S_1(n) = g_1(n) - g_1(0) = \frac{n(n+1)}{2}$.

For $k = 2$, one has $f_2(x) = x^2 = x(x+1) - x = P_2(x) - P_1(x)$ so that g_2 can be taken as $g_2(x) = \frac{P_3(x)}{3} - \frac{P_2(x)}{2} = \frac{x(x+1)(x+2)}{3} - \frac{x(x+1)}{2} = \frac{x(x+1)(2x+1)}{6}$. This gives $S_2(n) = \frac{n(n+1)(2n+1)}{6}$ for all n.

The fact that one can indeed write x^k as an integer linear combination of $P_k, P_{k-1}, \cdots, P_1$ can be seen as follows.

Now $P_r(x) = x(x+1)\cdots(x+r-1) = x^r + a_{r-1,r}x^{r-1} + \cdots + a_{0,r}$ for some integers $a_{i,r}$. Indeed, these integers are the symmetric polynomials in $1, 2, \cdots, r-1$.

Then, we have the matrix equation $AF = P$ where A is the upper triangular integer matrix

$$\begin{pmatrix} 1 & a_{k-1,k} & a_{k-2,k} & \cdots & a_{0,k} \\ 0 & 1 & a_{k-2,k-1} & \cdots & a_{0,k-1} \\ & & & \cdots & \\ & & & \cdots & \\ 0 & 0 & \cdots & 0 & 1, \end{pmatrix}$$

F is the column vector $(x^k, x^{k-1}, \cdots, x)$ and, P is the column vector $(P_k(x),\ P_{k-1}(x), \cdots, P_1(x))$.

The matrix A has an inverse which is also an upper triangular integer matrix B with 1's on the diagonal.

Thus, $F = BP$ gives the required expression.

Let us remark here that the above method is general enough to work atleast for any complex polynomial function f instead of f_k. Thus, to

evaluate $f(1) + \cdots + f(n)$, one writes f as a linear combination of the polynomials P_r, say,

$$f(x) = a_0 + a_1 P_1(x) + \cdots + a_d P_d(x)$$

where $d = \deg f$ and a_i are complex numbers. Then, one has

$$f(1) + \cdots + f(n) = a_0 n + a_1 \frac{n(n+1)}{2} + \cdots + a_d \frac{n(n+1)\cdots(n+d)}{d+1}.$$

4. A Method Involving Differentiation

This is an elementary and pretty useful method involving the differential operator $x\frac{d}{dx}$.

Note that $(x\frac{d}{dx})x^n = nx^n$. Therefore, applying it repetitively, one obtains $(x\frac{d}{dx})^k x^n = n^k x^n$.

Hence $1^k + 2^k + \cdots + n^k = (x\frac{d}{dx})^k(1 + x + x^2 + \cdots + x^n)$ at $x = 1$.

This can be rewritten in a more convenient form as

$$\sum_{i=1}^{n} i^k = \lim_{x\to 1}(x\frac{d}{dx})^k \frac{x^{n+1} - 1}{x - 1}.$$

Riemann Zeta Function

We end with some remarks on the sums of the infinite series $\sum_{n\geq 1} \frac{1}{n^k}$ for integers $k \geq 2$. This is a special value of the so-called Riemann Zeta function $\zeta(s)$ defined as the sum of the series $\sum_{n\geq 1} \frac{1}{n^s}$ for any real number $s > 1$ (actually, it can be defined as a complex valued function for any complex number s with Re $s > 1$ by the same series).

Some of the values are $\zeta(2) = \frac{\pi^2}{6}, \zeta(4) = \frac{\pi^4}{90}, \zeta(6) = \frac{\pi^6}{945}$.

The reader will notice that we have not written $\zeta(k)$ for any odd value of k and that, for even k, the value seems to be a rational multiple of π^k. In fact, the value $\zeta(3)$ is known to be irrational but it is still unkown if it can be expressed in terms of 'known' constants! We shall show now that $\zeta(2k)$ is indeed a rational multiple of π^{2k} for any natural number k. In fact, the Bernoulli numbers will surface here again! The reasons for not being able to evaluate ζ at odd values (or even say whether it is irrational in general) are deep and we do not go into them here.

Now, for any complex number z, we have $\operatorname{Sin} z = z\prod_{n\geq 1}(1 - \frac{z^2}{n^2\pi^2})$.

Its logarithmic derivative gives us

$$z \operatorname{Cot} z = 1 + 2\sum_{n\geq 1} \frac{z^2}{z^2 - n^2\pi^2} = 1 - 2\sum_{n\geq 1}\sum_{k\geq 1} \frac{1}{n^{2k}} \frac{z^{2k}}{\pi^{2k}}.$$

On the other hand, in the definition of the Bernoulli numbers as $\frac{x}{e^x-1} = \sum_{r\geq 0} B_r \frac{x^r}{r!}$, if we put $x = 2iz$, we obtain (recalling that $B_{2r+1} = 0$ for $r \geq 1$),

$$z \operatorname{Cot} z = 1 - \sum_{k\geq 1} (-1)^{k-1} B_{2k} \frac{2^{2k} z^{2k}}{(2k)!}.$$

Comparing the two expressions, we obtain

$$\zeta(2k) = (-1)^{k-1} B_{2k} \frac{2^{2k-1}}{(2k)!} \pi^{2k}.$$

We remark in passing that the same cotangent series is the starting point for obtaining an expression via theta series for the number of ways of writing a positive integer as a sum of squares.

Here is a rather surprising observation. The Riemann zeta function $\zeta(s)$ is defined by the series $\sum_{n\geq 1} n^{-s}$ for any complex number with Re $s > 1$. The theory of the zeta function implies that its definition can be extended (not by the same series, of course) to all values of s other than $s = 1$. Moreover, the values at s and $1 - s$ are related by what is known as a functional equation (thus there is the mysterious half line Re $s = 1/2$ in the middle on which the Riemann hypothesis predicts all the nontrivial zeroes of $\zeta(s)$ ought to lie). Let us now think of the naive idea that since $\zeta(k)$ for any natural number $k > 1$ is given by the series $\sum_{n\geq 1} n^{-k}$, it is possible that the value $\zeta(-k)$ is related to the partial sums $\sum_{n\leq N} n^k$. That this is indeed so is a simple, beautiful observation due to J Minac [1]). Recall from the previous discussion that there is a unique polynomial $S_k(x)$ which coincides with the sum $1^k + \cdots + n^k$ at $x = n$ for any natural number n and that S_k has degree $k + 1$. In fact, we saw that

$$S_k(x) = \frac{B_{k+1}(x+1) - B_{k+1}(1)}{k+1}.$$

As $B'_m(x) = mB_{m-1}(x)$ for all m, we see

$$\int_0^1 S_k(x-1)dx = \int_0^1 \frac{B_{k+1}(x+1) - B_{k+1}(1)}{k+1} = (-1)^k \frac{B_{k+1}}{k+1}.$$

We claim:

$$\zeta(-k) = \int_0^1 S_k(x-1)dx = (-1)^k \frac{B_{k+1}}{k+1}.$$

Actually, one can use the functional equation for the zeta function to conclude this but we follow a more elementary method of obtaining analytic continuation of the zeta function which will also prove this claim.

The analytic continuation of the zeta function to all $s \neq 1$ and the fact that $\lim_{s\to 1}(s-1)\zeta(s) = 1$ are obtainable as follows. Now, the zeta function $\zeta(s)$ is defined for a complex variable s by the series $\sum_{n=1}^{\infty} n^{-s}$ which converges for Re $s) > 1$. We shall use Abel's partial summation formula which is an elementary yet very powerful formula – the readers are well aware of its continuous analogue – integration by parts.

If $\{a_n\}, \{b_n\}$ are two sequences of complex numbers, and if $A_n = a_1 + \cdots + a_n$, then we have the identity

$$a_1b_1 + \cdots + a_nb_n = A_nb_{n+1} - \sum_{k=1}^{n} A_k(b_{k+1} - b_k).$$

Thus, $\sum_n a_nb_n$ converges if both the sequence $\{A_nb_{n+1}\}$ and the series $\sum_{k=1}^{\infty} A_k(b_{k+1} - b_k)$ converge.

The proof follows simply by observing that

$$\sum_{k=1}^{n} a_kb_k = \sum_{k=1}^{n}(A_k - A_{k-1})b_k - \sum_{k=1}^{n} A_kb_k - \sum_{k=1}^{n} A_kb_{k+1} + A_nb_{n+1}.$$

In our case, by using Abel's partial summation formula, one has

$$\zeta(s) = s\int_1^{\infty} \frac{[x]}{x^{s+1}}dx = \frac{s}{s-1} - s\int_1^{\infty} \frac{\{x\}}{x^{s+1}}dx.$$

Here $[x]$ and $\{x\}$ respectively denote the integral part and the fractional part of x. Note that the integral converges for Re $(s) > 0$ and thus the last expression gives the analytic continuation of the zeta function to the region Re $(s) > 0$. We shall proceed inductively now. On writing

$$\int_1^{\infty} \frac{\{x\}}{x^{s+1}}dx = \sum_{n=1}^{\infty}\int_n^{n+1} \frac{x-n}{x^{s+1}} = \sum_{n=1}^{\infty}\int_0^1 \frac{udu}{(u+n)^{s+1}}$$

and integrating the last integral by parts, we obtain

$$\zeta(s) = \frac{s}{s-1} - \frac{s}{2}(\zeta(s+1) - 1) - \frac{s(s+1)}{2}\int_1^{\infty} \frac{\{x\}^2}{x^{s+2}}dx.$$

From this, we have analytic continuation of ζ for Re $(s) > -1$ and also that $\zeta(0) = -\frac{1}{2}$. Proceeding inductively, we get

$$\zeta(s) = 1 + \frac{1}{s-1} - \sum_{q=1}^{m} \frac{s(s+1)\cdots(s+q-1)}{(q+1)!}(\zeta(s+q) - 1)$$

$$-\frac{s(s+1)\cdots(s+m)}{(m+1)!}\sum_{n=1}^{\infty}\int_0^1 \frac{u^{m+1}}{(u+n)^{s+m+1}}.$$

The infinite sum on the right hand side converges for Re $(s) > -m$ and thus we have an expression for $\zeta(s)$ for such s. At this point, we evaluate it at $s = 1 - m$. Rather surprisingly, this pretty but simple idea does not seem to have been thought of until very recently when it was done so by Ram Murty and M Reece. We get

$$\zeta(1-m) = 1 - \frac{1}{m} + \frac{(-1)^m}{m(m+1)} - \sum_{q=1}^{m-1} (-1)^q \binom{m-1}{q} \frac{1}{q+1} (\zeta(1-m+q) - 1).$$

The first few values at nonpositive integers are

$$\zeta(0) = -\frac{1}{2}, \zeta(-1) = -\frac{1}{12}, \zeta(-2) = 0, \zeta(-3) = \frac{1}{120}.$$

On the other hand, for $M = 1, 2, 3, \cdots$, we have

$$M^{k+1} = \sum_{r=0}^{k} \binom{k+1}{r+1} (-1)^r S_{k-r}(M-1).$$

Therefore, we get

$$\sum_{r=0}^{k} \binom{k+1}{r+1} (-1)^r \int_0^1 S_{k-r}(x-1)dx = \frac{(-1)^{k+1}}{k+2}.$$

As $\zeta(0) = -\frac{1}{2}$, we arrive at the formula

$$\zeta(-k) = \int_0^1 S_k(x-1)dx = (-1)^k \frac{B_{k+1}}{k+1}$$

which was claimed.

Let us finally remark that the Riemann zeta function vanishes at the negative even integers $-2, -4, -6, \cdots$ and these are its so-called trivial zeroes. The Riemann hypothesis asserts that all other zeroes lie on the line $Re(s) = 1/2$.

References

[1] J Minac, *Expo. Math.,* **Vol. 12**, pp. 459–462, 1994.

Frobenius and His Density Theorem for Primes

A rare sight is seen; yes,
when we spot a genius.
We saw one who made sense
of prime numbers being dense.
This was the great George Frobenius!

1. Introduction

Our starting point is the following problem which appeared in the recent IMO (International Mathematical Olympiad):

If p is a prime number, show that there is another prime number q such that $n^p - p$ is not a multiple of q for any natural number n.

Now, this problem itself can be solved using elementary mathematics (otherwise, it would not be posed in the IMO). However, how does one guess that such a thing ought to be true? Can we produce an abundance of such problems in some systematic manner? We take this problem as a point of reference to discuss some deep number theory (which is already a century old) which not only solves this problem, but also gives us an understanding of why such facts are true and what more one can expect. The main theorem under discussion is known as Frobenius's density theorem.

2. Rephrasing and Generalisation

Let us start by rephrasing the above problem. For a prime p, consider the integral polynomial $f(X) = X^p - p$. For any prime q, one may consider f as a polynomial over $\mathbf{Z}/q\mathbf{Z}$, the integers modulo q by reducing the coefficients of f modulo q. Then, the problem asks us to prove that there is some prime q for which f does not have a root in $\mathbf{Z}/q\mathbf{Z}$. So, when is it true that an integral polynomial has roots in $\mathbf{Z}/q\mathbf{Z}$ for every prime p? Obviously, if the integral polynomial already has an integral root, this happens. Can it also happen when f has no integral root?

Before answering this, let us note that every nonconstant integral polynomial has a root in $\mathbf{Z}/q\mathbf{Z}$ for infinitely many primes q. Here is the simple argument proving it. See also 'Polynomials with integer values', second chapter in this book.

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 8, No. 12, pp. 33–41, December 2003.

Let $P(X) = a_0 + a_1X + \cdots + a_nX^n$ be an integral polynomial with $n > 0$ and $a_n \neq 0$. For any integer d, look at the polynomial

$$P(a_0dX) = a_0(1 + a_1dX + a_0a_2d^2X^2 + \cdots + a_0^{n-1}a_nd^nX^n).$$

Since $Q(X) = 1 + a_1dX + a_0a_2d^2X^2 + \cdots + a_0^{n-1}a_nd^nX^n$ takes the values $0, 1, -1$ at the most for finitely many values of X, it takes a value $Q(m) \neq 0, 1, -1$ which must then be a multiple of some prime p. As $Q(m) \equiv 1 \mod d$, p is coprime to d. Therefore, for any d, we have shown that there is some m such that $P(a_0dm)$ is zero modulo p for some prime p coprime to d. Varying d, we have infinitely many such primes p.

The set of odd primes modulo which the polynomial $X^2 + 1$ has roots, consists precisely of all primes in the arithmetic progression $4n + 1$. In general, every quadratic polynomial has a corresponding arithmetic progression such that the polynomial has roots modulo each prime in this progression, and modulo no other primes. This follows from the famous quadratic reciprocity law.

Returning to our case $f(X) = X^p - p$, let us see whether we can explicitly get an infinite set of primes modulo which f does have roots. Consider any prime q and the group $(\mathbf{Z}/q\mathbf{Z})^*$ of nonzero integers modulo q under multiplication modulo q. If the p-th power map $\theta : a \mapsto a^p$ on $(\mathbf{Z}/q\mathbf{Z})^*$ is not $1 - 1$, then there exists some $a \neq 1$ with $a^p = 1$. Since $a^{q-1} = 1$, we must have $\frac{p}{(q-1)}$. In other words, whenever $q \not\equiv 1 \mod p$, our polynomial f has a root modulo q.

Let us now return to the possibility of producing a polynomial which has no integral roots but has roots modulo every integer. Consider the polynomial

$$g(X) = (X^2 - 13)(X^2 - 17)(X^2 - 221).$$

Evidently, its roots $\pm\sqrt{13}, \pm\sqrt{17}, \pm\sqrt{221}$ are not integral (or even rational). We show that it has roots modulo *any* nonzero integer. Recall that the Chinese remainder theorem tells us that whenever $m_1, \cdots, m_r$ are pairwise coprime integers and $a_1, \cdots, a_r$ are any integers, there is an integer a which is simultaneously $\equiv a_i \mod m_i$ for $i = 1, \cdots, r$. Therefore, by the Chinese remainder theorem, it suffices to prove that g has roots modulo every prime power. In what follows, for any prime p and a coprime to p, the notation $(\frac{a}{p})$ stands for 1 or -1 according as whether a is a square or not mod p. One also says in the respective cases that a is a quadratic residue modulo p and a is a quadratic nonresidue modulo p.

Let us look at g now. If p is an odd prime such that $(\frac{13}{p}) = 1$, then $t^2 \equiv 13 \mod p$ for some integer t. We show by induction on n that $x^2 \equiv 13 \mod p^n$ has a solution. Suppose $t^2 \equiv 13 \mod p^{n-1}$, say $t^2 = 13 + up^{n-1}$. Consider $t_0 = t + p^{n-1}t_1$ where we shall choose t_1 so that $t_0^2 \equiv 13 \mod p^n$.

This requires $u + 2tt_1 \equiv 0 \bmod p$; such a choice of t_1 can be made since $2t$ is coprime to p. Thus, we have shown that if 13 is a quadratic residue modulo an odd prime p, the polynomial g has a root modulo any power p^n. The same argument works if 17 or 221 is a quadratic residue modulo a prime p. For powers of 2 we note that $17 \equiv 3^2 \bmod 2^3$ and work as above but with a minor change; we try $t + 2^{n-2}t_1$ instead of the $n - 1^{st}$ power.

Note that $13 \equiv 8^2 \bmod 17$ and $17 \equiv 2^2 \bmod 13$. Further, for any p, one of $13, 17$ or 221 is a square modulo p. This is because the homomorphism $x \mapsto x^2$ on $(\mathbf{Z}/p\mathbf{Z})^*$ for an odd prime p, has kernel of order 2. Its image, which is the subgroup of squares, is the unique subgroup of index 2. Hence the cosets of 13 and 17 multiply to give the coset of 221. Thus, the above argument goes through for all p and it follows that the polynomial g, indeed, has roots modulo any nonzero integer.

Now, let us ask ourselves what is different about $X^p - p$ in comparison with the above example. It is immediately evident that g is a reducible polynomial over $\mathbf{Z}$ while the famous Eisenstein criterion shows that the polynomial $f(X) = X^p - p$ is irreducible over $\mathbf{Z}$. In fact, irreducibility of f can be proved quite easily even without the Eisenstein criterion.

Ok, but let us look at another obvious irreducible polynomial over $\mathbf{Z}$ - the linear polynomial $h(X) = aX + b$ where $(a, b) = 1$. But, if p is any prime not dividing a, then $aX + b$ has a root modulo p. In other words, h does have a root modulo all but finitely many primes even though it is irreducible over $\mathbf{Q}$. Thus, a reasonable guess for us could be:

$(*)$ *An integral polynomial which is irreducible over* $\mathbf{Z}$ *and has degree* > 1 *cannot have roots modulo all but finitely many primes. In other words, for such a polynomial, there are infinitely many primes modulo which the polynomial has no roots.*

Our intention is to show that this is true. In fact, one may wonder maybe whether we have the much stronger result that an irreducible polynomial f over $\mathbf{Z}$ remains irreducible over all but finitely many primes. But, the following example dashes this hope. It was already observed by Hilbert (this example was already discussed in an earlier chapter).

Let p, q *be odd prime numbers such that* $(\frac{p}{q}) = (\frac{q}{p}) = 1$ *and* $p \equiv 1 \bmod 8$. *Then, the polynomial* $P(X) = (X^2 - p - q)^2 - 4pq$ *is irreducible whereas it is reducible modulo any integer.*

Now

$$\begin{aligned} P(X) &= X^4 - 2(p+q)X^2 + (p-q)^2 \\ &= (X - \sqrt{p} - \sqrt{q})(X + \sqrt{p} + \sqrt{q})(X - \sqrt{p} + \sqrt{q})(X + \sqrt{p} - \sqrt{q}). \end{aligned}$$

Since $\sqrt{p}, \sqrt{q}, \sqrt{p} \pm \sqrt{q}, \sqrt{pq}$ are all irrational, none of the linear or

quadratic factors of $P(X)$ are in $Z[X]$ i.e. $P(X)$ is irreducible over $\mathbf{Z}$. Note, as before, that it is enough to show that a factorisation of P exists modulo any prime power as we can use Chinese reminder theorem to get a factorisation modulo a general integer. Now, $P(X)$ can be written in the following ways:

$$\begin{aligned} P(X) &= X^4 - 2(p+q)X^2 + (p-q)^2 \\ &= (X^2 + p - q)^2 - 4pX^2 \\ &= (X^2 - p + q)^2 - 4qX^2 \\ &= (X^2 - p - q)^2 - 4pq. \end{aligned}$$

The second and third equalities above show that $P(X)$ is reducible modulo any q^n and any p^n respectively. Also since $p \equiv 1 \bmod 8, p$ is a quadratic residue modulo 2 and, therefore, modulo any 2^n; the second equality above again shows that $P(X)$ is the difference of two squares modulo 2^n, and hence reducible mod 2^n.

If ℓ is a prime $\neq 2, p, q$, at least one of $(\frac{p}{\ell})$, $(\frac{q}{\ell})$ and $(\frac{pq}{\ell})$ is 1 by the product formula $(\frac{p}{\ell}) \cdot (\frac{q}{\ell}) \cdot (\frac{pq}{\ell}) = 1$ that we noted earlier. According as $(\frac{p}{\ell}), (\frac{q}{\ell})$ or $(\frac{pq}{\ell}) = 1$, the second, third or fourth equality shows that $P(X)$ is reducible mod ℓ^n for any n.

We mention, in passing, a very simple but important general method of proving the irreducibility of an integral polynomial. This will also set up the notation for our main statement when we address $(*)$. To illustrate it, consider the polynomial $p(X) = X^4 + 3X^2 + 7X + 4$. Modulo 2, we have $p(X) = X(X^3 + X + 1)$ and both factors are irreducible over the field $\mathbf{Z}/2\mathbf{Z}$. We say that the *decomposition type* of $p(X)$ mod 2 is $1, 3$. Therefore, either p is irreducible over $\mathbf{Z}$ or if not, it is a product of a linear factor and an irreducible factor of degree 3 over $\mathbf{Z}$. But, modulo 11, we have $p(X) = (X^2 + 5X - 1)(X^2 - 5X - 4)$ where both factors are irreducible over the field $\mathbf{Z}/11\mathbf{Z}$. That is, the decomposition type of p mod 11 is $2, 2$. Thus, it cannot be that p has a linear factor over $\mathbf{Z}$. In other words, p must be irreducible over $\mathbf{Z}$.

3. The Notion of Density of Primes

Let us get back to the guess quoted above as $(*)$. We need some notations. Let f be a monic integral polynomial of degree n. Suppose that f has distinct roots $\alpha_1, \cdots, \alpha_n \in \mathbf{C}$; equivalently, the discriminant $disc(f) \neq 0$. Let $K = \mathbf{Q}(\alpha_1, \cdots, \alpha_n)$, the subfield of $\mathbf{C}$ generated by the roots; that is, all rational expressions in the α_i's with coefficients from $\mathbf{Q}$. This is the smallest subfield of $\mathbf{C}$ which contains all the α_i's; it is also known as the splitting field of f for the reason that f splits into the product $\prod_{i=1}^{n}(X - \alpha_i)$ over K. We

look at the group G of those permutations of α_i's which give rise to a field automorphism of K. This is known as the Galois group of f and denoted by $\mathrm{Gal}(f)$. For instance, if $f(X) = X^2 - a$ for some nonsquare integer a, then $K = \mathbf{Q}(\sqrt{a})$ where $\sqrt{a}$ denotes a square root of a in $\mathbf{C}$ and G has two elements I, σ where σ interchanges $\sqrt{a}$ and $-\sqrt{a}$. In general, although G is a subgroup of S_n, the permutations which belong to G are rather restricted; for example if f is irreducible over $\mathbf{Q}$, then a permutation in G is necessarily transitive on the α_i's. If $p \not| disc(f)$, then the decomposition type of f modulo p gives a partition of n as we saw above. On the other hand, each element of G has a cycle decomposition as an element of S_n and, thus defines a partition of n as well. Frobenius's wonderful idea is to relate the numbers of such partitions for a particular type. This will be expressed in terms of a notion of density of a set of prime numbers.

A set S of primes is said to have density δ if $\frac{\sum_{p\in S} 1/p}{\sum_{all\ p} 1/p} \to \delta$ as $s \to 1^+$. Here 1^+ means the limit when s tends to 1 from the right. For instance, any finite set of primes has density 0. Using this notion of density, we state more precisely:

4. Frobenius Density Theorem

The set of primes p modulo which a monic integral, irreducible polynomial f has a given decomposition type $n_1, n_2, \cdots, n_r$, has density equal to $N/O(Gal(f))$ where $N = |\{\sigma \in Gal(f) :\ \sigma$ has a cycle pattern $n_1, n_2, \cdots, n_r\}|$.

As we point out now, our guess $(*)$ is vindicated by this theorem and a little bit of group theory; in particular, this also solves the IMO problem.

If f is irreducible, and has roots modulo all but finitely many primes, then the theorem shows that each σ has a cycle pattern of the form $1, n_2, \cdots$ This means that each element of $\mathrm{Gal}(f)$ fixes a root. Since the roots of f are transitively moved around by $\mathrm{Gal}(f)$, this group would be the union of the conjugates of its subgroup H consisting of elements which fix a root of f, say α_1. However, it is an elementary exercise that a finite group cannot be the union of conjugates of a proper subgroup. Thus, in our case $H = \mathrm{Gal}(f)$. This means that $\mathrm{Gal}(f)$ fixes each α_i and is therefore trivial. That is, f is linear.

A famous theorem of Dirichlet on primes in arithmetic progressions asserts that the density of the set of primes $p \equiv a \bmod n$ is $1/\phi(n)$ for any $(a, n) = 1$. Dirichlet's theorem implies Frobenius's theorem for the polynomial $f(X) = X^n - 1$. The converse conclusion cannot quite be made. Thus, Frobenius formulated a conjecture which generalises both his theorem and Dirichlet's theorem. This was proved 42 years later by Chebotarev and is known now as the Chebotarev density theorem. This is an extremely useful result and even effective versions are known (see the end of the article for

what the word 'effective' means here). Chebotarev's idea of proving this has been described by two prominent mathematicians as "a spark from heaven". In fact, this theorem was proved in 1922 ("while carrying water from the lower part of town to the higher part, or buckets of cabbages to the market, which my mother sold to feed the entire family") and Emil Artin wrote to Hasse in 1925: "Did you read Chebotarev's paper? ... If it is correct, then one surely has the general abelian reciprocity laws in one's pocket..." Artin found the proof of the general reciprocity law in 1927 using Chebotarev's technique (he had already boldly published the reciprocity law in 1923 but admitted that he had no proof). Nowadays, Artin's reciprocity law is proved in some other way and Chebotarev's theorem is deduced from it!

To state Chebotarev's theorem, we recall one notion – the Frobenius map. The idea is that given a monic integral polynomial f and its splitting field K, we can associate to any prime $p \not| disc(f)$, an element Φ_p of $Gal(f)$ in a natural manner. If we can do this, one may expect that the decomposition type of f modulo p coincides with the cycle pattern of Φ_p. It can almost be done except that a prime p gives rise to a conjugacy class of elements in $\mathrm{Gal}(f)$. We do not define the Frobenius conjugacy class here as it is somewhat technical and merely explain some properties it has. For any prime number p, the p-th power map $Frob_p$ is an automorphism of the field $\bar{\mathbf{F}}_p$ which is identity on $\mathbf{F}_p$. Therefore, $Frob_p$ permutes the roots of any polynomial over $\mathbf{F}_p$. Indeed, *the Galois theory of finite fields amounts to the statement that if g is a polynomial over $\mathbf{F}_p$ with simple roots, then the cycle pattern of $Frob_p$ viewed as a permutation of the roots of g coincides with the decomposition type of g over $\mathbf{F}_p$*. In our case, we start with an integral polynomial f and look at it modulo p for various primes p. The basic theory of algebraic numbers shows that whenever $p \not| disc(f)$, the automorphism $Frob_p$ gives rise to a *conjugacy class* in $\mathrm{Gal}(f)$, called the Frobenius conjugacy class modulo p.

In Frobenius's density theorem, one cannot distinguish between two primes p, q defining different conjugacy classes $C(x)$ and $C(y)$ but some powers of x and y are conjugate. For instance, for the polynomial $X^{10}-1$, the decomposition type modulo primes congruent to $1, 3, 7, 9$ mod 10 are, respectively, $1,1,1,1,1,1,1,1,1,1$; $1,1,4,4$; $1,1,4,4$; $1,1,2,2,2,2$.

Frobenius's theorem cannot distinguish between primes which are 3 mod 10 and those which are 7 mod 10; they define different conjugacy classes in $\mathrm{Gal}(X^{10}-1)$. Thus, it would imply that the number of primes $\equiv 3$ or 7 mod 10 is infinite but doesn't say whether each congruence class contains infinitely many primes. This is what Chebotarev's theorem asserts.

5. Chebotarev's Density Theorem

Let f be monic integral and assume that disc (f) does not vanish. Let C be a conjugacy class of Gal(f). Then, the set of primes p not dividing disc (f) for which $\sigma_p \in C$, has a well-defined density which equals $\frac{|C|}{|G|}$.

We state here without proof two results which can be proved with the aid of Chebotarev's density theorem. These concrete applications are:

(I) The set of primes which are expressible in the form $3x^2 + xy + 4y^2$ for integers x, y, has density $1/5$.

(II) The set of primes p for which the decimal expansion of $1/p$ has odd period, has density $1/3$.

Finally, we end with the remark that a recent result due to Berend and Bilu [1]) gives an 'effective version' of Chebotarev's theorem. This means in simple terms that given a nonconstant integral polynomial, one has a certain number N, explicitly determined in terms of the irreducible factors of f and their coefficients, so that f will have an integral root if, and only if, it has a root modulo N. See also [2] for a nice historical introduction to Frobenius's and Chebotarev's density theorems.

We conclude by stating that an integral polynomial of degree n is irreducible but reducible modulo all positive integers if and only if, the corresponding Galois group has no element of order n. The proof uses the Chebotarev density theorem.

References

[1] D Berend and Y Bilu, Polynomials with roots modulo every integer, *Proc. Amer. Math. Soc.*, **Vol. 124**, pp. 1663–1671, 1996.

[2] P Stevenhagen and H W Lenstra, Jr., Chebotarev and his density theorem, *Mathematical Intelligencer*, **Vol. 18**, pp. 26–37, 1996.

When is a Decimal Expansion Irrational?

Everyone learns in school that $\sqrt{2}$ is irrational. This, along with Euclid's proof of infinitude of primes, is probably the first time she encounters a proof by contradiction. Most students know in school that the value of $\sqrt{2}$ is approximately 1.414 but, more often than not, this aspect is not pursued further in detail. The decimal $0.999\cdots$ where 9 recurs indefinitely is understood (after some persuasion perhaps) to be none else than the number 1. The problem here is that the concept of limit takes some time to sink in. Given that start, they can see easily that numbers like $0.\overline{142857}$ where the digits overlined recur indefinitely, are rational. Even if the recurring string occurs after an initial string (for example, a decimal expansion like $27.\overline{142857}$), it still gives us a rational value only because it is the sum of a geometric series with a ratio of the form 10^k.

It is not hard to prove that this is a necessary condition as well, that is, *a decimal expansion of a real number represents a rational number if, and only if, after the decimal place, there is a finite (possibly empty) string after which the digits consist of a finite string (possibly consisting entirely of zeroes) recurring indefinitely.*

Thus, for instance, the number $0.101001000\cdots$ where the number of zeroes keeps increasing by 1 has to represent an irrational number. However, from the decimal expansion, sometimes it is not clear whether there is such an eventual recurrence or not. This could be due to our present state of knowledge. For instance, one could define a number $0.1010\cdots$ where the number of zeroes occurring at the n-th step is either increased by one or kept the same according as to whether the number $2^{2^n}+1$ is prime or not. Since one does not know whether there are infinitely many such primes, we cannot say at present as to whether the above decimal represents a rational or an irrational number.

The decimal $0.1234\cdots$, where the natural numbers are written in sequence, is clearly irrational since, for instance, the number of zeroes occurring in the powers of 10 keeps increasing. The decimal $0.235711\cdots$, where the set of primes is written down in sequence, is also irrational. This is because there is a prime of the form $10^n a+1$ for an arbitrary n – this was proved in an earlier chapter. Here is another elementary general result (see [1]).

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 9, No. 3, pp. 78–80, March 2004.

Consider a decimal $x = 0.a_1a_2\cdots$ where $\{a_n\}$ is a strictly increasing sequence of natural numbers having the property that $\sum_n \frac{n^r}{a_n^s}$ diverges for some $r, s > 0$. Then x is irrational.

Note that since the reciprocals of primes do not sum to a finite quantity, this result also implies that $0.23571113\cdots$ is irrational.

To prove this, assume, if possible, that x is rational. Then, by throwing out some of the first a's and scaling, we may assume that the decimal is actually periodic and not just eventually periodic. Let t denote a period. Let $N_1 < N_2 < \cdots$ denote the natural numbers representing the different numbers of digits occurring for the a_i's. Let d_i denote the number of a_i's which have exactly N_i digits. In other words, $a_1, \cdots, a_{d_1}$ are the a's with N_1 digits and, for each $i \geq 1$, the numbers

$$a_{d_1+\cdots+d_i+1}, \cdots, a_{d_1+\cdots+d_i+d_{i+1}}$$

are the a's which have exactly N_{i+1} digits. Let us write for simplicity $d_0 = 0$. Now, if some d_{i+1} were bigger than t, then the numbers

$$a_{d_1+\cdots+d_i+1}, \cdots, a_{d_1+\cdots+d_i+t+1},$$

would all have N_{i+1} digits and since the length of the string

$$(a_{d_1+\cdots+d_i+1})\cdots(a_{d_1+\cdots+d_i+t}),$$

is tN_{i+1} which is a multiple of t, it follows that

$$a_{d_1+\cdots+d_i+1} = a_{d_1+\cdots+d_i+t+1},$$

which is a manifest contradiction of the assumption that $\{a_n\}$ is an increasing sequence. Hence, we have shown that each d_i is $\leq t$.

Now, we also have the evident inequalities

$$a_{d_1+\cdots+d_i+d_{i+1}} \geq \cdots \geq a_{d_1+\cdots+d_i+1} \geq 10^{N_{i+1}-1},$$

since these numbers have N_{i+1} digits. We shall show that $\sum_{n=1}^{\infty} \frac{n^r}{a_n^s}$ converges. Now, for each $i \geq 0$,

$$\sum_{j=d_1+\cdots+d_i+1}^{d_1+\cdots+d_i+d_{i+1}} \frac{j^r}{a_j^s} \leq \sum_{j=d_1+\cdots+d_i+1}^{d_1+\cdots+d_i+d_{i+1}} \frac{(d_1+\cdots+d_{i+1})^r}{10^{s(N_{i+1}-1)}} \leq \frac{d_{i+1}(d_1+\cdots+d_{i+1})^r}{10^{s(N_{i+1}-1)}}.$$

Thus, $\sum_{i\geq 0}\sum_{j=d_1+\cdots+d_i+1}^{d_1+\cdots+d_i+d_{i+1}} \frac{j^r}{a_j^s} \leq \sum_{i\geq 0} \frac{t(i+1)^r t^r}{10^{s(N_{i+1}-1)}} \leq \frac{t^{r+1}}{10^{s(N_1-1)}} \sum_{i\geq 0} \frac{(i+1)^r}{10^{is}}$.

But, the last series converges so that $\sum_{n=1}^{\infty} \frac{n^r}{a_n^s}$ also converges. This is a contradiction of our assumption and the irrationality of x follows.

References

[1] A McD Mercer, *American Mathematical Monthly*, **Vol. 101**, pp. 567–568, 1994.

Revisiting Kummer's and Legendre's Formulae

In a beginning course in number theory, an elementary exercise is to compute the largest power of a prime p dividing $n!$. This number, called the p-adic valuation of $n!$, is easily proved to be

$$v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots . \tag{1}$$

Note that this is a finite series. The number $v_p(n!)$ comes up naturally in a few situations like the following. In the group of permutations of n objects, this would give the power of p which is the order of a p-Sylow subgroup. While discussing p-adic numbers as analogues of the usual real numbers, one looks at the analogue of the exponential series. The expression for $v_p(n!)$ leads one to determine that the exponential series has the radius of convergence $p^{-1/(p-1)}$.

Now, $v_p(n!)$ can also be computed in another manner by a beautiful observation due to the legendary mathematician Legendre. Legendre observed that the p-adic valuation of $n!$ can be read off from the base-p expansion of n. It is simply $\frac{n-s(n)}{p-1}$ where $s(n)$ is the sum of the "digits" of n in this expansion. A related result that Kummer proved is that, if $r \leq n$, then the p-adic valuation of the binomial coefficient $\binom{n}{r}$ is simply the number of 'carry-overs' when one adds r and $n-r$ in base-p. In ([1], pp.229–233) Honsberger deduces Kummer's theorem from Legendre's result and refers to Ribenboim's lovely book [2], pp.30–32) for a proof of the latter. Ribenboim's proof is by verifying that Legendre's base-p formula agrees with the standard formula (1).

Is it possible to prove Legendre's formula without recourse to the above formula? We shall see that this is indeed possible and that the standard formula above follows from such a proof. What is more, Kummer's formula also follows without having to use Legendre's result. Let us start by recalling Legendre's formula.

Legendre's Formula

Let p be a prime number and let $a_k \cdots a_1 a_0$ be the base-p expansion of a natural number n. We shall show that if Legendre's formula

$$v_p(n!) = \frac{n - s(n)}{p-1} = \frac{n - \sum_{i=0}^{k} a_i}{p-1} \tag{2}$$

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 10, No. 2, pp. 62–71, February 2005.

holds good for n, then it also holds good for $pn+r$ for any $0 \leq r < p$. Note that the base-p expansion of $pn+r$ is

$$a_k \cdots a_1 a_0 \ r.$$

Let us denote, for convenience, the number $\frac{m-s(m)}{p-1}$ by $f(m)$ for any natural number m. Evidently,

$$f(pn+r) = \frac{pn - \sum_{i=0}^{k} a_i}{p-1} = n + f(n).$$

On the other hand, it follows by induction on n that

$$v_p\left((pn+r)!\right) = n + v_p(n!). \tag{3}$$

For, if it holds good for all $n < m$, then

$$\begin{aligned} v_p((pm+r)!) &= v_p(pm) + v_p((pm-p)!) \\ &= 1 + v_p(m) + m - 1 + v_p((m-1)!) \ = \ m + v_p(m!). \end{aligned}$$

Since it is evident that $f(m) = 0 = v_p(m!)$ for all $m < p$, it follows that $f(n) = v_p(n!)$ for all n. This proves Legendre's formula.

Note also that the formula

$$v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

follows inductively on using (3).

Kummer's Algorithm

As before p is any prime number. For any natural numbers r and s, let us denote by $g(r,s)$ the number of 'carry-overs' when the base-p expansions of r and s are added. Kummer's result is that for $k \leq n$,

$$v_p\left(\binom{n}{k}\right) = g(k, n-k). \tag{4}$$

Once again, this is clear if $n < p$, as both sides are then zero. We shall show that if the formula holds good for n (and *every* $k \leq n$), it does so for $pn+r$ for $0 \leq r < p$ (and any $k \leq pn+r$). This would prove the result for all natural numbers.

Consider any binomial coefficient $\binom{pn+r}{pm+a}$ for $0 \leq a < p$.

First, suppose $a \leq r$.

Write $m = b_k \cdots b_0$ and $n - m = c_k \cdots c_0$ in base-p. Then the base-p expansions of $pm + a$ and $p(n-m) + (r-a)$ are, respectively,

$$\begin{aligned} pm + a &= b_k \cdots b_0 \; a \\ p(n-m) + (r-a) &= c_k \cdots c_0 \; r - a. \end{aligned}$$

Evidently, the corresponding number of carry-overs is

$$f(pm + a, p(n-m) + (r-a)) = f(m, n-m).$$

By the induction hypothesis, $f(m, n-m) = v_p(\binom{n}{m})$. Now $v_p\left(\binom{pn+r}{pm+a}\right)$ is equal to

$$\begin{aligned} &v_p((pn+r)!) - v_p((pm+a)!) - v_p((p(n-m)+r-a)!) \\ &\quad = n + v_p(n!) - m - v_p(m!) - (n-m) - v_p((n-m)!) \;=\; v_p\left(\binom{n}{m}\right). \end{aligned}$$

Thus, we are through in the case when $a \leq r$.

Now suppose that $r < a$. Then $v_p\left(\binom{pn+r}{pm+a}\right)$ is equal to

$$\begin{aligned} &v_p((pn+r)!) - v_p((pm+a)!) - v_p((p(n-m-1)+(p+r-a))!) \\ &\quad = n + v_p(n!) - m - v_p(m!) - (n-m-1) - v_p((n-m-1)!) \\ &\quad = 1 + v_p(n) + v_p((n-1)!) - v_p(m!) - v_p((n-m-1)!) \\ &\quad = 1 + v_p(n) + v_p\left(\binom{n-1}{m}\right). \end{aligned}$$

We need to show that

$$f(pm + a, p(n-m-1) + (p+r-a)) = 1 + v_p(n) + f(m, n-m-1). \quad (5)$$

Note that $m < n$. Write $n = a_k \cdots a_0$, $m = b_k \cdots b_0$ and $n - m - 1 = c_k \cdots c_0$ in base-p. If $v_p(n) = d$, then $a_i = 0$ for $i < d$ and $a_d \neq 0$. In base-p, we have

$$n = a_k \cdots a_d \; 0 \cdots 0$$

and, therefore,

$$n - 1 = a_k \cdots a_{d+1} a_d - 1 \; p-1 \cdots \; p-1.$$

Now, the addition $m + (n-m-1) = n-1$ gives $b_i + c_i = p-1$ for $i < d$ (since they must be $< 2p-1$). Moreover, $b_d + c_d = a_d - 1$ or $p + a_d - 1$.

Note the base-p expansions

$$\begin{aligned} pm + a &= b_k \cdots b_0 \; a, \\ p(n-m-1) + (p+r-a) &= c_k \cdots c_0 \; p + r - a. \end{aligned}$$

We add these using that fact that there is a carry-over in the beginning and that $1 + b_i + c_i = p$ for $i < d$. Since there is a carry-over at the first step as well as at the next d steps, we have

$$pn + r = * \; * \; \cdots \; a_d \; 0 \cdots \; 0 \; r$$

where there are d zeroes before r, and

$$f(pm + a, p(n-m-1) + (p+r-a)) = 1 + d + f(m, n-m-1).$$

This proves Kummer's assertion also.

We end with the remark that Kummer's result gives an immediate proof of the fact that the n-th Catalan number is odd if and only if n is 1 less than a power of 2.

References

[1] R Honsberger, *In Polya's Footsteps*, published and distributed by the Mathematical Association of America, 1997.

[2] P Ribenboim, *The Book of Prime Number Records*, Springer-Verlag, 1996.

Bessels Contain Continued Fractions of Progressions

1. Introduction

The January 2000 issue of *Resonance* carried a nice article on continued fractions by Shailesh Shirali. After discussing various continued fractions for numbers related to e, he left us with the intriguing question as to how one could possibly evaluate the continued fraction

$$\frac{1}{1+}\frac{1}{2+}\frac{1}{3+}\cdots\cdots\cdots .$$

The question is interesting because this continued fraction is simpler-looking than the ones which were studied in that article. We answer this question here and show that the discussion naturally involves the Bessel functions, thus explaining the title. However, we shall begin with some details about continued fractions which complement his discussion. One place where continued fractions are known to appear naturally is in the study of the so-erroneously-called Pell's equation.

In a series of very interesting articles in *Resonance*, Amartya Kumar Dutta had discussed various aspects of Mathematics in ancient India. In particular, he discussed Brahmagupta's and Bhaskara's work on *Samasabhavana* and the *Chakravala method* for finding solutions to 'Pell's equation'. In fact, it is amusing to recall what Andre Weil, one of the great mathematicians of the last century wrote once, while discussing Fermat's writings on the problem of finding integer solutions to $x^2 - Dy^2 = 1$:

> *What would have been Fermat's astonishment if some missionary, just back from India, had told him that his problem had been successfully tackled there by native mathematicians almost six centuries earlier!*

The Chakravala method can be described in terms of continued fractions. Let us begin with some rather elementary things which were known so long back and have gone out of fashion to such an extent that they are not as widely known as they ought perhaps to be.

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 10, No. 3, pp. 80–87, March 2005.

2. Linear Diophantine Equations with SCF's

Let us denote by

$$[a_0\,;\,a_1, a_2, a_3, \cdots] \tag{1}$$

the SCF (simple continued fraction)

$$a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\cdots\cdots. \tag{2}$$

Here the a_i are natural numbers. Evidently, any rational number has a finite SCF. For instance,

$$\frac{763}{396} = [1\,;\,1, 12, 1, 1, 1, 9].$$

Its successive convergents are $\frac{1}{1}, \frac{2}{1}, \frac{25}{13}, \frac{27}{14}, \frac{52}{27}, \frac{79}{41}, \frac{763}{396}$. Note that if the n-th convergent is $\frac{p_n}{q_n}$, then $p_n q_{n-1} - p_{n-1}q_n = (-1)^n$. This holds for any continued fraction, as can be seen by induction. This gives a method of finding all positive integral solutions (in particular, the smallest one) x, y to a Diophantine equation of the form $ax - by = c$. For instance, consider the equation

$$396x - 763y = 12.$$

Look at the SCF for $\frac{763}{396}$ and compute its penultimate convergent $\frac{79}{41}$. Now, if x, y are positive integers satisfying

$$396x - 763y = 12,$$

then combining with the fact that $396 \times 79 - 763 \times 41 = 1$, we get

$$x - (79 \times 12) = 763t, \quad y - (41 \times 12) = 396t$$

for some integer t. This gives all solutions, and the smallest solution in natural numbers x, y is obtained by taking $t = -1$ and turns out to be $(185, 96)$.

The reader is left with deriving similarly the corresponding expression for any linear equation.

3. Quadratic Equations from SCF's

Evidently, finite CF's give only rational numbers. Given the fact that a periodic decimal expansion gives rational numbers too, a reader might be tempted to guess that a periodic CF gives rationals. After just a little thought, it becomes apparent that an eventually periodic SCF gives a quadratic irrational number. For example, $[1\,;\,1, 1, \cdots]$ is the 'golden ratio'

$(1+\sqrt{5})/2$. This is because the value s satisfies $s = 1 + 1/s$ and is positive. Similarly, the SCF $[1\,;\,3,2,3,2,\cdots] = \sqrt{5/3}$, as it gives the quadratic equation $s - 1 = (s+1)/(3s+4)$, and $[0\,;\,3,2,1,3,2,1,\cdots] = (\sqrt{37}-4)/7$ as it gives the equation $s = (3+2s)/(10+7s)$, etc.

Consider a quadratic Diophantine equation in two variables

$$ax^2 + 2hxy + by^2 + 2gx + 2fy + c = 0 \tag{3}$$

where a, b, c, f, g, h are integers. Thinking of this as a polynomial in x and solving it, one obtains

$$ax + hy + g = \pm\sqrt{(h^2 - ab)y^2 + 2(hg - af)y + g^2 - ac)}.$$

For any integral solution, the expression inside the square root (which we write as $ry^2 + 2sy + t$ now) must be a perfect square, say v^2. Once again, solving this as a polynomial in y, we get

$$ry + s = \pm\sqrt{(s^2 - rt + rv^2)}.$$

Hence, $s^2 - rt + rv^2$ must be a perfect square u^2. In other words, the original equation does not have integral solutions unless the equation $u^2 - rv^2 = w$ has a solution, where w is a constant defined in terms of a, b, c, f, g, h.

An equation of the form $u^2 + rv^2 = w$ for r positive has only finitely many solutions. Therefore, let us discuss the equation $u^2 - rv^2 = \pm w$ where r, w are positive integers and r is not a perfect square. The SCF for $\sqrt{r}$ provides a way of obtaining infinitely many solutions of the special equation $u^2 - rv^2 = 1$. Consequently, for given r, w if we find one solution (u_0, v_0) of $u^2 - rv^2 = w$, one can find infinitely many by the *samasabhavana* (composition) $x = uu_0 + rvv_0$, $y = uv_0 + vu_0$ for any u, v with $u^2 - rv^2 = 1$. However, the method of CF's will provide even one solution only for certain w's; namely, those which appear as one of the denominators while expressing $\sqrt{r}$ as a continued fraction.

Let us now show how $u^2 - rv^2 = 1$ can always be solved in positive integers using the SCF for $\sqrt{r}$. It is a simple exercise to show that the SCF for $\sqrt{r}$ has the form

$$[a_1\,;\,b_1, b_2, \cdots, b_n, 2a_1, b_1, b_2, \cdots, b_n, 2a_1, \cdots]. \tag{4}$$

If p/q is a penultimate convergent of a recurring period, then it is easy to check that $p^2 - rq^2 = \pm 1$. In fact, if the period is even, this is always 1. If the period is odd, then the penultimate convergents of the first, second, third period, ... alternately satisfy the equations

$$x^2 - ry^2 = -1, \qquad x^2 - ry^2 = 1.$$

For example,

$$\sqrt{13} = [3\,;\,1, 1, 1, 1, 6, \cdots].$$

The period is 5 which is odd. The penultimate convergent to the first period is

$$3 + \frac{1}{1+}\frac{1}{1+}\frac{1}{1+}\frac{1}{1} = \frac{18}{5}.$$

Therefore, $(18, 5)$ is a solution of $u^2 - 13v^2 = -1$.

The penultimate convergent to the second period is computed to be $649/180$. Therefore, $(649, 180)$ is a solution of $u^2 - 13v^2 = 1$.

4. SCF's in Arithmetic Progressions

In his discussion, Shirali showed that the following SCF's can be evaluated in terms of the exponential function; he showed

$$[2\,;\,6, 10, 14, \cdots] = \frac{e+1}{e-1}, \qquad [1\,;\,3, 5, 7, \cdots] = \frac{e^2+1}{e^2-1}.$$

The SCF's here involve terms in arithmetic progression. What about a general SCF of the form $[a\,;\,a + d, a + 2d, \cdots]$? For example, can the SCF $[0\,;\,1, 2, 3, \cdots]$ be evaluated in terms of some 'known' numbers and functions? Shirali started with the differential equation $(1 - x)y'' = 2y' + y$ which he remarked "does not seem to solvable in closed form".

We start with any arithmetic progression $a, a + d, a + 2d, \cdots$ where a is *any real number* and d is *any non-zero real number*, and show how it can be evaluated.

Let us consider the differential equation

$$dxy'' + ay' = y. \tag{5}$$

Actually, heuristic reasons can be given as to why one looks at this differential equation but we directly start with it here and show its relation to our problem. Let $y = y(x)$ be a solution of the above differential equation satisfying $y(0) = ay'(0)$. Let us denote the r-th derivative of y by y_r for simplicity of notation. By repeated differentiation, we get $dxy_{r+2} + (a + rd)y_{r+1} = y_r$ for all $r \geq 0$ (with y_0 denoting y). Therefore, we have

$$\frac{y_0}{y_1} = a + \frac{dxy_2}{y_1} = a + \frac{dx}{a + d+}\frac{dx}{a + 2d+} \cdots\cdots . \tag{6}$$

Observe that

$$[a\,;\,a + d, a + 2d, a + 3d, \cdots] \;=\; \frac{y(1/d)}{y'(1/d)}.$$

A solution function such as above can be very easily obtained as a series; we get

$$y = c_0 + c_0 \sum_{n\geq 1} \frac{x^{n+1}}{(n+1)!a(a+d)\cdots(a+nd)}, \tag{7}$$

for any c_0. This evaluates the SCF $[a\,;\, a+d, a+2d, a+3d, \cdots]$ in terms of these series. As we shall see now, these series are special values of modified Bessel functions and, for certain choices of a and d, the series are even expressible in terms of e, etc.

Before proceeding further, let us note that the SCF whose evaluation was asked for by Shirali is:

$$[0\,;\, 1, 2, 3, \cdots] = \frac{\sum 1/\left((n+1)!n!\right)}{\sum 1/(n!)^2}. \tag{8}$$

Its approximate value is 0.7.

For general a, d as above, the solution function

$$y = y(x) = c_0 + c_0 \sum_{n\geq 1} \frac{x^{n+1}}{(n+1)!a(a+d)\cdots(a+nd)} \tag{9}$$

is related to Bessel functions in the following manner. First, the Bessel differential equation $x^2y'' + xy' + (x^2 - \alpha^2)y = 0$ has certain solutions

$$J_\alpha(x) \;=\; \sum_{n\geq 0} \frac{(-1)^n (x/2)^{2n+\alpha}}{n!\Gamma(n+1+\alpha)}; \tag{10}$$

these are usually referred to as Bessel functions of the first kind. Here $\Gamma(s)$ is the Gamma function. If α is not an integer, then $J_{-\alpha}$ (defined in the obvious manner) is another independent solution to the Bessel differential equation above. Closely related to the J_α is the so-called modified Bessel function of the first kind

$$I_\alpha(x) = \sum_{n\geq 0} \frac{(x/2)^{2n+\alpha}}{n!\Gamma(n+1+\alpha)}. \tag{11}$$

Thus, we have

$$\frac{1}{1+}\,\frac{1}{2+}\,\frac{1}{3+}\cdots\cdots\cdots = \frac{I_1(2)}{I_0(2)}.$$

The function $I_\alpha(x)$ is a solution of the differential equation $x^2y'' + xy' - (x^2 + \alpha^2)y = 0$. Indeed, $I_\alpha(x) = i^{-\alpha}J_\alpha(ix)$ for each x. Using the relation $\Gamma(s+1) = s\Gamma(s)$ and the value $\Gamma(1/2) = \sqrt{\pi}$, it is easy to see that the solution function

$$y = c_0 + c_0 \sum_{n\geq 1} \frac{x^{n+1}}{(n+1)!a(a+d)\cdots(a+nd)} \tag{12}$$

above, is related to the modified Bessel function of the first kind as:

$$y(x^2/d) = c_0\Gamma(a/d)(x/d)^{1-a/d} I_{a/d-1}(2x/d). \tag{13}$$

In particular,

$$[a\,;\, a+d, a+2d, a+3d, \cdots] = \frac{y(1/d)}{y'(1/d)} = \frac{I_{a/d-1}(2/d)}{I_{a/d}(2/d)}. \tag{14}$$

Conclusion

Before finishing, we recall some SCF's evaluated out by Shirali:

$$[2\,;\, 6, 10, 14, \cdots] = \frac{e+1}{e-1}, \qquad [1\,;\, 3, 5, 7, \cdots] = \frac{e^2+1}{e^2-1}.$$

Our formula above yields for the same SCF's the expressions:

$$[2\,;\, 6, 10, 14, \cdots] = \frac{I_{-1/2}(1/2)}{I_{1/2}(1/2)}, \tag{15}$$

$$[1\,;\, 3, 5, 7, \cdots] = \frac{I_{-1/2}(1)}{I_{1/2}(1)}. \tag{16}$$

It is clear from the definition that

$$I_{-1/2}(1) = \sqrt{\frac{2}{\pi}} \sum_{n\geq 0} \frac{1}{(2n)!} = \sqrt{\frac{2}{\pi}}\, \frac{e+e^{-1}}{2}, \tag{17}$$

$$I_{1/2}(1) = \sqrt{\frac{2}{\pi}} \sum_{n\geq 0} \frac{1}{(2n+1)!} = \sqrt{\frac{2}{\pi}}\, \frac{e-e^{-1}}{2}. \tag{18}$$

Therefore, for these special parameters, the value of the modified Bessel function is expressible in terms of e and one can recover Shirali's expressions.

The Prime Ordeal

Numbers in their prime
for no reason or rhyme
show up at a rhythm
with probability 1/logarithm.
If this is a law they knew,
they also break quite a few
but that is not a crime!

"There are two facts about the distribution of prime numbers. The first is that, [they are] the most arbitrary and ornery objects studied by mathematicians: they grow like weeds among the natural numbers, seeming to obey no other law than that of chance, and nobody can predict where the next one will sprout. The second fact is even more astonishing, for it states just the opposite: that the prime numbers exhibit stunning regularity, that there are laws governing their behavior, and that they obey these laws with almost military precision."

Don Zagier

Prime numbers have fascinated mankind through the ages. In fact, one may think that we know all about them. However, this is not so! One does not know the answers to many basic questions on primes. We shall concentrate here mainly on questions and discoveries whose statements are elementary and accessible. Right at the end, we mention a result whose statement is simple but whose proof uses rather sophisticated mathematics. Even here, we do not try to be exhaustive. The subject is too vast for that to be possible.

1. Introduction

Let us start with the first major discovery about primes, which is the proof by Euclid's school that there are infinitely many prime numbers. Euclid's proof of the infinitude of primes will eternally remain beautiful no matter what advances modern mathematics makes. In spite of its simplicity, it still retains quite a bit of mystery. For instance, it is unknown as yet whether the product of the first few primes added to 1 takes a prime value infinitely often. It is even unknown whether it takes a composite value infinitely often! Do you see the mystery? What is the first time we get some composite number? Does anyone know the answer already? Anyway,

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 13, No. 9, pp. 866–881, September 2008.

let me tell you that $2.3.5.7.11.13 + 1$ is not a prime.

Actually, it is often the case that for any sequence of natural numbers which does not obviously take only composite values, the question as to whether it does take infinitely many prime values remains unanswered.

Here are some examples (the $p_1, p_2, \ldots$ are prime numbers):

(i) $p_1 p_2 \cdots p_n + 1$,
(ii) $p_1 p_2 \cdots p_n - 1$,
(iii) $n! + 1$,
(iv) $n! - 1$,
(v) $2^n - 1$,
(vi) $2^n + 1$,
(vii) $n^2 + 1$,
(viii) $f(n)$ for any polynomial of degree ≥ 2 such that there is no k dividing all the values $f(r), r \in \mathbf{Z}$.

Of course, in (v), it is obviously necessary that n itself be prime, and in (vi), a necessary condition is that n is a power of 2. As for (vii), it was proved by a contemporary mathematician Henryk Iwaniec in 1978 using some advanced mathematics that infinitely many numbers of the form n^2+1 can be expressed as a product of at most 2 primes. Note that the condition in (viii) cannot be weakened; for instance, if we merely say that all the coefficients of f be not divisible by any k, it is not sufficient. Indeed, $f(x) = x(x+1)$ is a counter example. That the sequence in the last example takes infinitely many prime values was conjectured by Viktor Bouniakowsky in the 19th century. In contrast to the last example, the degree one case is known to take infinitely many prime values – this is the famous theorem of Lejeune Dirichlet on primes in arithmetic progressions. Incidentally, here is a little exercise: If we make the (apparently weaker) conjecture that under the hypothesis of example (viii), every such f takes ONE prime value, it is actually equivalent to asserting that each such f takes infinitely many prime values!

Here is another issue of importance – in cryptography, for example. Given a natural number n, how does one recognize whether it is prime or not? This is of crucial importance in many modern cryptosystems where the belief is that it is comparatively much easier (computationally) to answer this question than to factorize a given number. Basically, the idea would be to unearth properties of prime numbers which characterize them (that is, would not hold for even a single composite number). One such fundamental property (which is an easy exercise) is that a natural number $n > 1$ is prime if, and only if, n divides $(n-1)! + 1$. This is known as Wilson's congruence. Another such property is that any prime p divides the binomial coefficients $\binom{p}{r}$ for each r in the range $0 < r < p$. That this is untrue for every composite number is again a nice little exercise.

Using the above property of primes, one can prove by induction on n that $n^p - n$ is a multiple of p for every n. Equivalently, if p does not divide n, then p divides $n^{p-1} - 1$. This is known as the little theorem of Fermat.

Interestingly, I found that one website in German translated 'the little theorem of Fermat' as 'the small sentence of Fermat'! It is even funnier when we recall that Fermat was a judge who did pass sentences at times!

At this point, it is better to stop and point out the answer to a question which would have crossed the minds of many people. *Is there a 'formula' for the n-th prime?* Indeed, there are many formulae for primes! However, they are all worthless in a practical sense; that is, one cannot hope to computationally produce primes by such formulae. However, later we do talk about a recent algorithm by 3 Indians which tells us in polynomial time whether a given number is prime or not. Here is a 'formula' for primes based on Wilson's congruence. Put $f(x,y) = \frac{1}{2}\{1 + \frac{x-y}{|x-y|}\}$ if $x \neq y$, and $f(x,x) = 0$. Note that $f(x,y)$ is simply 1 or 0 according as to whether $x > y$ or $x \leq y$. Put $\pi(n) = 1 + \sum_{i=3}^{n}\{(i-2)! - i[(i-2)!/i]\}$ for $n \geq 3$ and $\pi(1) = 0, \pi(2) = 1$. This counts the number of primes up to n. Then, the n-th prime p_n is given by the formula:

$$p_n = 1 + \sum_{i=1}^{2^n} f(n, \pi(i)).$$

After some thought, we can see that the formula, although perfectly valid, is of no practical use in finding the n-th prime. A somewhat better formula was given several years ago by an Indian named J M Gandhi.

2. Carmichael Numbers: 'Carm'posites in Prime Clothing

Some avatar of Fermat's little theorem is used in most primality tests even today. But, unfortunately Fermat's little theorem does not characterize primes! It does happen for some composite n that n divides $a^{n-1} - 1$ for some a co-prime to n. In the terminology of cryptography, one says that n is a pseudo-prime to the base a and that a is a strong liar for n. Worse happens – there are, indeed, infinitely many numbers (known as Carmichael numbers after Robert Carmichael) n such that n divides $a^{n-1} - 1$ for every a co-prime to n. The smallest such number is 561. The proof of the infinitude of the Carmichael numbers (as recently as 1994) also showed that there are at least $n^{2/7}$ such numbers $\leq n$ provided n is sufficiently large. The proof used deep, modern-day mathematics. In this article, I will concentrate on two conjectures (one made in 1950 and the other made in 1990) which aim to characterize primes. Ironically, they have turned out to be equivalent! As the conjectures involve Carmichael numbers also, we first prove a nice elementary criterion due to Theodor Korselt which characterizes Carmichael numbers.

In what follows, we will be using the following notations. We will say $a \equiv b \bmod m$ when $a - b$ is a multiple of m. These congruences have a calculus quite similar to equality. Namely, if $a \equiv b \bmod m$ and $c \equiv d \bmod m$ (same m, of course), then $a + b \equiv c + d$ and $ab \equiv cd \bmod m$.

Theorem. *A composite number n is a Carmichael number if, and only if, n is square-free and, for each prime divisor p of n, the number $p - 1$ divides $n - 1$.*

Proof. We shall assume and use the following fact which was first proved by Gauss. For any prime number p, there exist positive integers $a < p$ and $b < p^2$ which have 'orders' $p - 1$ and $p(p - 1)$ in the following sense:

when $a^r \equiv 1 \bmod p$, then $p - 1$ divides r, and

when $b^s \equiv 1 \bmod p^2$, then $p(p - 1)$ divides s.

(It should be noted that neither of these statements is trivial to prove although they are some 200 hundred years old.)

Now, first let $n = p_1 p_2 \cdots p_r$ be a square-free number such that for each $i \leq r$, the number $p_i - 1$ divides $n - 1$. Evidently, for every a co-prime to n, a is co-prime to each p_i. Thus, one has by Fermat's little theorem that $a^{p_i - 1} \equiv 1 \bmod p_i$. So, $a^{n-1} = (a^{p_i - 1})^* \equiv 1 \bmod p_i$. In other words, p_i divides $a^{n-1} - 1$ for each $i \leq r$. Thus, $n = p_1 p_2 \cdots p_r$ itself divides $a^{n-1} - 1$. This shows that n is a Carmichael number.

Conversely, let n be a Carmichael number. If p is a prime dividing n, consider a natural number a of 'order' $p - 1 \bmod p$. We claim that we can always choose such an a which is co-prime to n.

First, if a is co-prime to n, then by hypothesis, $a^{n-1} \equiv 1 \bmod n$, which implies $a^{n-1} \equiv 1 \bmod p$, and thus $p - 1$ divides $n - 1$. If $(a, n) > 1$, then look at the set of primes $p = p_1, \cdots, p_k$ which divide n but not a. Consider $a + p_1 \cdots p_k$ in place of a. Evidently, $a + p_1 \cdots p_k$ is co-prime to n. Moreover, it is of the form $a + pd$, and so, its 'order' $\bmod p$ is the same as that of a.

Now, let p^2 divide n for some prime p, if possible. Let b be of order $p(p-1)$ $\bmod p^2$. If b is co-prime to n, then $b^{n-1} \equiv 1 \bmod n$ which gives $b^{n-1} \equiv 1$ $\bmod p^2$ which again implies that $p(p - 1)$ divides $n - 1$. Thus p divides $(n - 1)$, an impossibility because p divides n. So, n must be square-free if the b can be chosen co-prime to n. But, if $(b, n) > 1$, then once again we look at the set of primes $p = p_1, p_2, \cdots, p_k$ which divide n but not b. Then $b + p_1^2 p_2 \cdots p_k$ is co-prime to n and has the same order $\bmod p^2$ as b has, namely, $p(p - 1)$.

The proof is complete.

We end with an easy exercise:

Suppose $n = p_1 \cdots p_r$ is a Carmichael number and $m \equiv 1 \bmod L$ where $L = LCM$ of $p_1 - 1, \cdots, p_r - 1$. If $q_i = 1 + m(p_i - 1)$ are all primes, then $N = q_1 \cdots q_r$ is also a Carmichael number.

3. 'Nava' Giuga and long 'Agoh'

Let us start with the first of the 2 conjectures we wish to discuss. If p is a prime, then clearly

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \mod p.$$

Giuseppe Giuga conjectured in 1950 that this characterises primes; that is,

Conjecture (Giuga 1950): $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \bmod n \Rightarrow n$ is prime.

As he showed, the conjecture can be reformulated as follows:

Theorem. $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \bmod n$ *if, and only if, for each prime divisor* p *of* n*, both* p *and* $p-1$ *divide* $\frac{n}{p} - 1$*.*

Equivalently, a composite number n *satisfies* $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \bmod n$ *if, and only if, it is a Carmichael number such that* $\sum_{p|n} \frac{1}{p} - \prod_{p|n} \frac{1}{p}$ *is a natural number.*

In the above statement, the sum and the product run over primes and $p|n$ denotes 'p divides n'.

Proof. Note that for any prime p, we have $\sum_{k=1}^{p-1} k^r \equiv -1$ or $0 \bmod p$ according as whether $p-1$ divides r or not.

Therefore, for a prime p dividing n, we have

$$\sum_{k=1}^{n-1} k^{n-1} \equiv \sum_{k=1}^{p-1} k^{n-1} + \sum_{k=p+1}^{2p-1} k^{n-1} + \cdots + \sum_{k=n-p+1}^{n-1} k^{n-1}$$

$\equiv -n/p$ or $0 \bmod p$ according as to whether $p-1$ divides $n-1$ or not.

To prove the theorem, first suppose $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \bmod n$. Then, for every prime $p|n$, we have $(p-1)|(n-1)$ and $\frac{n}{p} \equiv 1 \bmod p$. Note that $(p-1)|(n-1)$ implies $p-1$ divides $p(\frac{n}{p} - 1) = n - p = (n-1) - (p-1)$ and so $(p-1)$ also divides $\frac{n}{p} - 1$.

Conversely, suppose $p(p-1)$ divides $\frac{n}{p} - 1$ for each prime divisor p of n. First of all, this forces n to be square-free. Now, for any prime $p|n$, we also have $\sum_{k=1}^{n-1} k^{n-1} \equiv -\frac{n}{p} \equiv -1 \bmod p$. This proves the first statement. The second assertion is easy. If $p(p-1)|(\frac{n}{p} - 1)$ for each prime $p|n$, we have that n is a Carmichael number (in particular, it is square-free). Then,

$$\sum_{p|n} \frac{1}{p} - \prod_{p|n} \frac{1}{p} = \sum_{p|n} \frac{1}{p} - \frac{1}{n}.$$

So, multiplying by n, we must show that n divides $\sum_{p|n} \frac{n}{p} - 1$. Thus, we need to show that each prime divisor of n divides $\sum_{p|n} \frac{n}{p} - 1$. This follows because each prime divisor p of n satisfies $p|(\frac{n}{p} - 1)$ and $p|\frac{n}{q}$ for $p \neq q$.

Remarks. A composite number n such that $p|(\frac{n}{p}-1)$ for each prime $p|n$, is called a *Giuga number*. Equivalently, $\sum_{p|n}\frac{1}{p}-\prod_{p|n}\frac{1}{p}\in\mathbf{N}$. Then, Giuga's conjecture amounts to the assertion that there is no Giuga number which is also a Carmichael number. As of today, only 12 Giuga numbers are known and all of them have sum minus product (of reciprocals of prime divisors) equal to 1. The numbers $30, 858, 1722$ are Giuga numbers. Until now, no odd Giuga numbers have been found. Any possible odd Giuga number must have at least 10 prime factors because the sum $\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{23}+\frac{1}{29}+\frac{1}{31}<1$.

In an article in Volume 103 of the *American Mathematical Monthly* of 1996, David Borwein, Jonathan Borwein, Peter Borwein and Roland Girgensohn propose that a good way to approach Giuga's conjecture is to study Giuga numbers in general. More generally, they define a *Giuga sequence* to be a finite sequence $n_1<n_2<\cdots<n_r$ of natural numbers such that $\sum_{i=1}^{r}\frac{1}{n_i}-\prod_{i=1}^{r}\frac{1}{n_i}$ is a natural number. Thus, a Giuga sequence consisting of primes gives rise to a Giuga number, viz., to the product of those primes. The smallest Giuga sequence where the sum minus product is >1, has 59 factors! Here is an easy method to produce arbitrarily long Giuga sequences.

Theorem. *Suppose $n_1<n_2<\cdots<n_r$ is a Giuga sequence satisfying $n_r=\prod_{i=1}^{r-1}n_i-1$. Then, the sequence $n_1<n_2<\cdots<\tilde{n}_r,\tilde{n}_{r+1}$ is a Giuga sequence whose sum minus product is the same, where $\tilde{n}_r=\prod_{i=1}^{r-1}n_i+1,\tilde{n}_{r+1}=\tilde{n}_r\prod_{i=1}^{r-1}n_i-1$.*

Starting with a sequence like $2, 3, 5$ say, this gives Giuga sequences of arbitrary lengths whose sum minus product is 1. The proof is a simple exercise of manipulation. In fact, one has the following nice result:

Proposition. *Look at a sequence $n_1<n_2<\cdots<n_r$ which satisfies $\sum_{i=1}^{r}\frac{1}{n_i}+\prod_{i=1}^{r}\frac{1}{n_i}=1$ - for example, the sequence $n_1=2, n_k=\prod_{i<k}n_i+1$ is such a sequence. Then, $n_1<n_2<\cdots<n_k<n_{k+1}:=\prod_{i=1}^{k}n_i-1$ is a Giuga sequence.*

The proof is straightforward verification.

Incidentally, note that the sequence given as an example above proves the infinitude of primes because the pairwise GCD $(n_i,n_j)=1$ for all $i\neq j$.

The Giuga conjecture involved the sums $\sum_{k=1}^{n-1}k^{n-1}$. As we have seen in an earlier chapter, in general, a sum of the form $\sum_{k=1}^{r-1}k^n$ can be 'easily' evaluated in terms of certain rational numbers called the Bernoulli numbers. Let us recall these briefly. These ubiquitous numbers have so many connections that it is impossible to mention most of them here. Suffice it to say that Fermat's last theorem can be proved for a prime p (in an easy, natural

manner) provided p does not divide the numerators of $B_2, B_4, \cdots, B_{p-3}$. How are the B_n's defined? Often, they are defined by means of the generating series $\sum_{n=0}^{\infty} B_n \frac{z^n}{n!} = \frac{z}{e^z-1}$. The equality can be un-winded to give the recursion $\sum_{r=0}^{n} \binom{n+1}{r} B_r = 0$ and using $B_0 = 1$, one can determine them. It turns out that $B_1 = -\frac{1}{2}$ and $B_r = 0$ for all odd $r > 1$. More generally, the Bernoulli polynomials are defined as $B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}$; it is of degree n. Note that $B_n(0) = B_n$.

We showed that

$$\sum_{k=1}^{r-1} k^n = \frac{1}{n+1}(B_{n+1}(r) - B_{n+1}).$$

In this manner, the sums of powers can be expressed in terms of Bernoulli numbers.

The von Staudt–Clausen theorem says that the denominator of B_{2k} is precisely $\prod_{(p-1)|2k} p$; note this is square-free. In particular, it makes sense to talk about $(2k+1)B_{2k} \bmod 2k+1$; note that for $(a,b) = 1$, one talks of $\frac{1}{a} \bmod b$ – it is the unique $c \bmod b$ for which $ac \equiv 1 \bmod b$.

For example, $15B_{14} = 15 \times \frac{7}{6} = \frac{35}{2} \equiv 35 \times 8 \equiv -5 \bmod 15$.

$13B_{12} = 13 \times \frac{-691}{2.3.5.7.13} \equiv -1 \bmod 13$.

Looking at such data, Takashi Agoh conjectured in 1990 (conjectured by 'Agoh' not long 'ago'!):

$nB_{n-1} \equiv -1 \bmod n$ if, and only if, n is prime.

A few years later (in 1994) he used the von Staudt–Clausen theorem and showed that his conjecture is actually equivalent to Giuga's conjecture. Then, in September 2004, Bernd Kellner gave a new proof of the equivalence of the two conjectures (which gives another proof of von Staudt-Clausen theorem) based on the following result:

Theorem (Kellner). *If $m > 1$, and n is even, then*

$$\sum_{k=1}^{m-1} k^n \equiv -\sum_{p|m,(p-1)|n} \frac{m}{p} \equiv mB_n \mod m.$$

The proof is elementary but rather involved and we do not discuss it here. This theorem allows for a further reformulation of the Giuga and Agoh conjectures, and may now be called:

Conjecture (Agoh-Giuga-Kellner): An integer $n \geq 2$ is prime if, and only if,

$$\sum_{p|n,(p-1)|(n-1)} \frac{1}{p} - \frac{1}{n} \in \mathbf{Z}.$$

4. All's Bell

In this section, we discuss a conjecture due to Djuro Kurepa which can be stated in elementary language but the proof which appeared last year involves some sophisticated mathematics. Those who have learnt Galois theory would be able to appreciate it but others can also get a flow of the argument. Of course, the fact that an elementary statement may require very sophisticated methods should not come as a surprise. A case in point is Fermat's last theorem (FLT) which says that for an odd prime p, there do not exist nonzero integers x, y, z such that $x^p + y^p + z^p = 0$. The question of Kurepa doesn't quite require the kind of sophisticated mathematics required in FLT though. Kurepa conjectured in 1971 that for any odd prime p, the sum $K_p := \sum_{n=0}^{p-1} n!$ is not a multiple of p. Of course $K_2 = 2$. This is, of course, not a characterisation of primes; for example, $K_4 = 10$. The proof (only in 2004) of Kurepa's conjecture due to D Barsky and B Benzaghou involves the so-called Bell numbers named after Eric Temple Bell. One way of defining the Bell numbers is as follows. The n-th Bell number P_n is the number of ways of writing an n-element set as s union of nonempty subsets. We see that $P_1 = 1, P_2 = 2, P_3 = 5, P_4 = 15, P_5 = 52$ etc. There is a lot of combinatorics involving the Bell numbers. From combinatorial considerations, one can prove that $P_{n+1} = \sum_{k=0}^{n} \binom{n}{k} P_k$, where we have written P_0 to stand for 1. From this, it is easy to prove (analogously to the proof for Bernoulli numbers) that the generating function for P_n's is given by

$$F(x) = \sum_{n=0}^{\infty} P_n x^n = \sum_{n=0}^{\infty} \frac{x^n}{(1-x)(1-2x)\cdots(1-nx)} \cdots\cdots (\spadesuit).$$

The Kurepa question can be formulated in terms of the Bell numbers easily. It turns out using some elementary combinatorics that $P_{p-1} \equiv \sum_{n=0}^{p-2} n!$ modulo p. Thus, since K_p is the sum of $(p-1)!$ with the right hand side above, Kurepa's conjecture amounts to the statement that $P_{p-1} \not\equiv 1$ modulo p because $(p-1)! \equiv -1$ modulo p. The idea of the proof Kurepa's conjecture is to consider what is known as the Artin–Schreier extension $\mathbf{F}_p[\theta]$ of the field $\mathbf{F}_p$ of p elements, where θ is a root (in the algebraic closure of $\mathbf{F}_p$) of the polynomial $x^p - x - 1$. This is a cyclic Galois extension of degree p over $\mathbf{F}_p$. Note that the other roots of $x^p - x - 1$ are $\theta + i$ for $i = 1, 2, \cdots, p-1$. The theory of such extensions is named after Emil Artin and Otto Schreier. The reason this field extension comes up naturally is as follows. The generating series $F(x)$ of the Bell numbers can be evaluated modulo p; this means one computes a 'simpler' series $F_p(x)$ such that $F(x) - F_p(x)$ has all coefficients multiples of p. Since Kurepa's conjecture is about the Bell numbers P_{p-1} considered modulo p, it makes sense to

consider $F_p(x)$ rather than $F(x)$. Reading the equality (♠) modulo p, one gets

$$\begin{aligned} F_p(x) &= \sum_{n=0}^{p-1}\sum_{i\geq 0}\frac{x^{ip+n}}{(1-x)\cdots(1-(ip+n)x)} \\ &= \sum_{n=0}^{p-1}\sum_{i\geq 0}\frac{x^{n}}{1-(ip+1)x)\cdots(1-(ip+n)x)}\frac{x^{ip}}{(1-x)\cdots(1-ipx)} \\ &\equiv \sum_{n=0}^{p-1}\sum_{i\geq 0}\frac{x^{n}}{1-(ip+1)x)\cdots(1-(ip+n)x)}\left(\frac{x^{p}}{(1-x)\cdots(1-px)}\right)^{i} \end{aligned}$$

modulo p. Therefore,

$$F_p(x) = \frac{\sum_{n=0}^{p-1} x^n(1-(n+1)x)\cdots(1-(p-1)x)}{1-x^{p-1}-x^p}$$

on simplification. Notice that θ^{-1} is a root of the polynomial $1-x^{p-1}-x^p$ above. Thereafter, doing some algebra in the field extension $\mathbf{F}_p[\theta]$ of $\mathbf{F}_p$ expresses the various Bell numbers P_n modulo p as

$$P_n \equiv -Tr(\theta^{c_p})Tr(\theta^{n-c_p-1}),$$

where Tr denotes the trace to $\mathbf{F}_p$ from the Artin–Schreier extension $\mathbf{F}_p[\theta]$ and $c_p = \frac{p^p-t_p}{p-1}$ and $t_p = \frac{p^p-1}{p-1}$. Thereafter, the analysis of the properties of the trace functions implies that if $P_{p-1}-1$ were to be zero modulo p, then θ^{c_p} would be zero, which is absurd since θ is not zero, as it generates a degree p extension. This was one instance of proving an elementary statement on primes which needs some sophisticated mathematics.

5. AKS — A Case of Indian Expertise

Having said that there are no (practically) 'nice' formulae for primes, and having also said that producing large primes is a basic requirement in fields like cryptography, how does one reconcile one with the other? The fact is that there are many probabilistic algorithms to certify primes with very high probability. We shall not discuss them but we raise the mathematical question as to whether there are deterministic algorithms to decide in reasonable computational time whether a given number is prime or not. Until very recently, no deterministic algorithm was known which was polynomial-time and which could detect every prime. Recently, three Indians (Manindra Agrawal, a professor of computer science from IIT Kanpur and his students Neraj Kayal and Nitin Saxena) stunned the world

with the discovery of a polynomial-time deterministic primality testing algorithm. We mention very briefly the Agrawal–Kayal–Saxena algorithm. Most algorithms start with Fermat's little theorem which, apart from other shortcomings, are also infeasible on the first glance because of having to compute p coefficients in order to check the validity of the congruence $(x-a)^p \equiv x^p - a \bmod p$. The basic idea of the A-K-S algorithm is to make it feasible by evaluating both sides modulo a polynomial of the form $x^r - 1$. Their algorithm would take $O(r^2 \log^3 p)$ time to verify $(x-a)^p \equiv x^p - a \bmod x^r - 1$ in $F_p[x]$. As there are composites also which satisfy this congruence, one has to choose r and a suitably. One general comment to note is that it is far easier to test a polynomial over F_p for irreducibility than to test primality of a natural number. In a nutshell, here is the A-K-S algorithm:

A-K-S algorithm to check primality of n

Step I

Check if n is a perfect power; if not go to the next step.

Step II

Find a prime number $r = O(\log^6 n)$ such that $r-1$ has a prime divisor $q > 4\sqrt{r}\log n$ where q divides the order of $n \bmod r$.

Step III

With r as above, check for each $a \leq 2\sqrt{r}\log n$, if

$$(x-a)^n \equiv x^n - a \mod x^r - 1 \text{ in } (Z/nZ)[x].$$

If the congruence is not satisfied for some a, declare n is composite. If it is satisfied for all a, declare n prime.

6. Sundries

We will finish with a few more remarks about primes. We mentioned Bouniakowsky's conjecture which asserts the infinitude of prime values. Can a polynomial take only prime values? It is again an easy, elementary exercise to prove that there is no nonconstant polynomial in some variables $x_1, \cdots, x_r$ which takes only prime values at all integers. However, it is a deep consequence of the solution of Hilbert's 10th problem by Hilary Putnam, Martin Davis, Julia Robinson and Yuri Matiyashevich that there exist polynomials $f(x_1, \cdots, x_r)$ over integers such that the set of positive values taken by f equals the set of prime numbers! Of course, the polynomials does take negative values as well as take certain prime values more than once. Indeed, one can take f to be of degree 25 and r to be 26. This expresses the fact that the set of prime numbers is a Diophantine set.

Joseph Bertrand stated that there is a prime among $n+1, n+2, \cdots, 2n$. This is Bertrand's postulate which was discussed in an earlier chapter; it was proved first by Pafnuty Chebychev and there are many simpler proofs. Incidentally, a generalization of Bertrand's postulate is a theorem of James Joseph Sylvester which asserts that in any sequence $n+1, n+2, \cdots, n+r$ with $n \geq r$, there is a number which is divisible by a prime $> r$.

Of course, the twin prime problem (whether there are infinitely many primes p with $p+2$ also prime) is still open. Viggo Brun proved that the series of reciprocals of twin primes converges. Note that the series of reciprocals of all primes is divergent, as proved by Euler. Indeed, $\sum_{p \leq x} \frac{1}{p}$ behaves asymptotically like the function $\log \log x$ for x tending to infinity.

Then, the Goldbach conjecture (named after Christian Goldbach and asserting that every even number >2 is a sum of two primes) is also open; Ivan Matveevich Vinogradov proved using the Hardy–Ramanujan circle method (named after G H Hardy and S Ramanujan) that every sufficiently large odd number is a sum of three primes. The prime number theorem proved in the beginning of the 20th century shows that the 'prime counting function' $\pi(x)$ which counts the number of primes up to x, behaves asymptotically like the function $\frac{x}{\log x}$ as x tends to infinity. An equivalent formulation is to say that the product of all the primes up to some x is asymptotically like e^x. Here, and elsewhere, one means by the statement $f(x)$ is asymptotically like $g(x)$ that the ratio $f(x)/g(x)$ approaches 1 as x tends to infinity. One can deduce from the prime number theorem that the n-th prime is approximately of size $n \log n$ for large n. That is, very roughly speaking, the probability that a given n is prime is $\frac{1}{\log n}$.

In connection with the fact we mentioned about Gauss showing that for each prime p, there is an integer a whose order mod p is $p-1$, here is a famous conjecture due to Emil Artin. He conjectured that each natural number a which is not a square is the order mod p for infinitely many primes p. It is also open.

Shortly before his death, Paul Erdös, in collaboration with Takashi Agoh and Andrew Granville, showed that any large composite n ($n \geq 400$ would do) satisfies

$$n \leq \left(\sum_{p \leq \sqrt{n}} \frac{1}{p} \right) \left(\prod_{p \leq \sqrt{n}} p \right).$$

Using this, and nothing more than the Chinese remainder theorem, they showed that any prime n can be proved to be prime by expressing it as $n = N_1 + N_2 + \cdots + N_k$ where $p_1, \cdots, p_k$ are the first k primes and n is not divisible by any of them while each N_i is divisible by all the p_j with $j \neq i$ and not by p_i.

Extending Given Digits to Make Primes or Perfect Powers

Any sequence of digits can be amended
by adding a tail and extended
to get a power
more or less of whatever
and maybe even prime opposite ended!

1. Introduction

Start with any string of digits. Can we always put down some more digits on the right of it to get a prime? Can we similarly get a power of 2? How about a power of 3? It turns out that the answers to all these questions are in the affirmative. Our discussion will be elementary excepting a concrete consequence of a weak version of the prime number theorem. For a really detailed analysis of the proportion of primes with given starting digits, the interested reader is referred to look at ergodic theory. There is no prime-producing polynomial in a single variable – this is trivial to see. However, it turns out (as other concrete consequences of the properties of primes like Bertrand's postulate and the prime number theorem) that there are exponential type of functions which produce infinitely many primes. One such is the sequence of integer parts of t^{3^n} for a certain positive real number t. Another is the sequence of integer parts of $2^{2^{\cdot^{\cdot^{\cdot^{s}}}}}$ for a certain real $s > 0$. We shall prove these also.

2. Perfect Powers with a Given Beginning

Let us first deal with the problem of extending a given string of digits to make a power of any natural number a which is at least 2 but not a power of 10. Notice that these exceptions are clearly unavoidable; there is no way to start with, say 11, and get a power of 10 by adding any number of digits. Let $a > 1$ be any natural number other than a power of 10. Let A be any given natural number in base 10. The only property we need is the following observation which can be proved simply by using the pigeon-hole principle. For any real number α, let us write $\{\alpha\}$ for the fractional part of α.

Observation. *For any irrational number $\theta > 0$, the sequence of fractional parts $\{n\theta\}$ as n varies over natural numbers, is dense in the interval $(0, 1)$.*

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 15, No. 10, pp. 941-947, October 2010.

Proof. For any n, consider the intervals $[0,1/n), [1/n,2/n), \cdots, [(n-1)/n, 1)$. By the pigeon-hole principle, among the fractional parts of $\theta, 2\theta, \cdots, n\theta, (n+1)\theta$, there must be at least two (say $r\theta, s\theta$ with $r < s \leq n+1$) which are in the same interval $[(k-1)/n, k/n)$. But then the fractional part of $(s-r)\theta$ lies in $[0,1/n)$. Therefore, each $[(m-1)/n, m/n]$ contains the fractional part of some $d\theta$ where d is a multiple of $s-r$. As every subinterval (x,y) of $(0,1)$ contains an interval of the form $[(m-1)/n, m/n]$ for some m, n, the claim asserted follows.

Using this, one may extend any given digits to produce powers as follows.

Lemma 1. Let $a > 1$ be not a power of 10 and let A be any given natural number. Then, one may add digits to the right end of the digits of A to obtain some power of a.

Proof. For any a as above, $\log_{10}(a)$ is irrational because, if it is u/v, then $10^u = a^v$ which implies by uniqueness of prime decomposition that a must be a power of 10, a contradiction of the hypothesis. So, it follows by the above observation that each interval $(x,y) \subseteq (0,1)$ contains some fractional part $\{n \log_{10}(a)\}$. Now, suppose A has $d+1$ digits; that is, $10^d \leq A < 10^{d+1}$. Then, we consider $x \in (0,1)$ such that $10^x = A/10^d$. Choosing some large n so that $10^{1/n} < 1 + \frac{1}{A}$ (as $\lim_{n\to\infty} 10^{1/n} = 1$), we consider the point $y \in (x,1)$ with $10^y = \frac{10^{1/n}A}{10^d}$. Note that $y < 1$ because $10^{1/n}A < A + 1 \leq 10^{d+1}$. If the fractional part $\{r \log_{10}(a)\} \in (x,y)$, we have

$$x < r \log_{10}(a) - k < y$$

for some positive integer k. Taking 10-th powers, we have

$$10^x < \frac{a^r}{10^k} < 10^y$$

which gives

$$10^{k-d}A < a^r < 10^{k-d}10^{1/n}A < 10^{k-d}A + 10^{k-d}.$$

Thus, a^r has been obtained by adding $k-d$ digits to the right of the base 10 expansion of A.

Illustration. Let us see how to demonstrate the above lemma for a small number. Let us begin with $A = 4$ and $a = 2$. Of course A itself is a power of 2 but let us see what we get from the above lemma. In the above notation, $d = 0$ and $x = \log_{10}(4)$. The choice $n = 16$ is large enough so that $10^{1/n} < 1 + 1/4 = 1.25$. Then $y = x + 1/16$ and the choice of r, k such that

$$10^x = 4 < \frac{2^r}{10^k} < 10^y = 4 + \frac{1}{16}$$

can be taken to be $r = 12, k = 3$. Hence 4 can be extended to $2^{12} = 4096$.

3. Primes with a Given Beginning

Now, we consider the problem of extending given digits on the right to get a prime. Here, we will need the following property of prime numbers which is a weak consequence of the so-called prime number theorem:

There exists n_0 so that for $n \geq n_0$, there is always a prime strictly between n and $n + \frac{n}{\log n}$.

Lemma 2. Let A be any given natural number. Then, one may add digits to the right end of the digits of A to obtain a prime number.

Proof. As our purpose is to add digits to the right end, we may assume that $A \geq n_0$ where n_0 is as above. Now, let $r > \frac{A}{\log_e(10)}$ and consider a prime p between $10^r A$ and $10^r A + \frac{10^r A}{\log_e(10^r A)}$. Thus, $p = 10^r A + d$ where $d < \frac{10^r A}{\log_e(10^r A)} < 10^r$ since $A < \log_e(10^r) = r \log_e(10)$ by the choice of r.

Finally, note that the last lemma implies the following:

COROLLARY 1.

The fractional parts of $\log_{10}(p)$, as p runs over primes, is dense in $(0, 1)$.

Proof. Let n be arbitrary and divide $(0, 1)$ into the intervals $(0, 1/n)$, $[1/n, 2/n), \cdots, [(n-1)/n, 1)$. Consider the numbers $10^{(m-1)/n}, 10^{m/n} \in [1, 10)$. By lemma 2, for each $m < n$, there is a prime p and some integer d so that

$$10^{(m-1)/n} < \frac{p}{10^d} < 10^{m/n}.$$

Thus, $(m-1)/n < \log_{10}(p/10^k) < m/n$ which means the fractional part of $\log_{10}(p)$ lies in $((m-1)/n, m/n)$. This completes the proof of the corollary as m, n are arbitrary.

We remark that using a weak version of the prime number theorem for arithmetic progressions, one may similarly prove that given any string of beginning digits and any string of end digits which end in $1, 3, 7$ or 9, one may introduce digits in between to get a prime.

4. Some Exponential Functions Producing Primes

The so-called Bertrand postulate (which was discussed in an earlier chapter) tells us that there is a prime between N and $2N$ for each $N > 1$. Using this, one can write down a function which produces infinitely many primes. Let us first discuss this 1951 result due to E M Wright [1]. This asserts:

Lemma 3. There exists a real number $s > 0$ such that the sequence $a_0 = s, a_1 = 2^s, a_2 = 2^{2^s}, \cdots, a_{n+1} = 2^{a_n}$ produces primes $[a_n] = [2^{2^{2^{\cdot^{\cdot^{\cdot}}}}}]$ (s times) for all $n > 0$.

Proof. Let $p_1 = 2, p_2 = 3$ and choose primes p_n for $n > 2$ such that

$$2^{p_n} < p_{n+1} < p_{n+1} + 1 < 2^{p_n+1}.$$

Look at the sequences b_n and c_n defined as follows. Define $b_n = \log_2 \log_2 \cdots \log_2(p_n)$ and $c_n = \log_2 \log_2 \cdots \log_2(p_n + 1)$ where there are n logarithms to the base 2. Then, we have

$$p_n < \log_2 p_{n+1} < \log_2(p_{n+1} + 1) < p_n + 1.$$

This means $b_n < b_{n+1} < c_{n+1} < c_n$ which ensures that the sequence $\{b_n\}$ converges to some real number s as $n \to \infty$. Notice that for this number s, the sequence $a_n = 2^{2^{2^{\cdot^{\cdot^{\cdot^{s}}}}}}$ satisfies $p_n < a_n < p_n + 1$. Hence $p_n = [a_n]$. This completes the proof.

Remarks.

(i) The above formula is not a practical one. Since there is a choice of p_n's allowed, the real number s is not unique. One possible value of s is $1.9287800\cdots$ and the primes p_n defined by the lemma grow much too fast. For example, p_4 has 5000 digits.

(ii) A result earlier to Wright's result above (in fact, the result which motivated Wright's theorem) is due to W H Mills [2] in 1947. This uses a result on primes which is considerably deeper than Bertrand's postulate. This deeper result alluded to is due to the British mathematician A E Ingham; he derived in 1937 (see [3]) the following concrete consequence of the prime number theorem:

There is a positive number c such that $p_n + cp_n^{5/8} > p_{n+1}$ for all n, where $p_1 < p_2 < p_3 < \cdots$ is the sequence of all primes.

Lemma 4. There exists a real number $t > 0$ such that $[t^{3^n}]$ is a prime for every n.

Proof. Start with Ingham's result and choose a large $N > c^8$. Look at the prime p_n such that $p_n < N^3 < p_{n+1}$. Then, we have

$$p_n < N^3 < p_{n+1} < p_n + cp_n^{5/8} < N^3 + cN^{15/8} < N^3 + N^2 < (N+1)^3 - 1.$$

Take for N, a prime $p > c^8$. Thus, we have a sequence of primes $p_{r_0} = p < p_{r_1} < p_{r_2} < \cdots$ such that

$$p_{r_n}^3 < p_{r_{n+1}} < (p_{r_n} + 1)^3 - 1 \cdots (\heartsuit)$$

Then the sequences $u_n = p_{r_n}^{3^{-n}}$ and $v_n = (p_{r_n} + 1)^{3^{-n}}$ satisfy

$$v_n = (p_{r_n}+1)^{3^{-n}} > (p_{r_{n+1}}+1)^{3^{-n-1}} = v_{n+1} > p_{r_{n+1}}^{3^{-n-1}} = u_{n+1} > p_{r_n}^{3^{-n}} = u_n.$$

Indeed, the inequality $v_n > v_{n+1}$ is simply the second inequality in ♡; the inequality $u_{n+1} > u_n$ is the first inequality of ♡ and the inequality $v_{n+1} > u_{n+1}$ is obvious. Hence, the sequence $\{u_n\}$ is a bounded, monotonically increasing sequence and must have a limit t. Clearly, $t = \lim_{n\to\infty} u_n$ satisfies $u_n \leq t < v_n$. Thus,

$$p_{r_n} \leq t^{3^n} < p_{r_n} + 1.$$

This proves that $[t^{3^n}] = p_{r_n}$ for all n.

Remarks on Mills's Constant

Mills proved only the existence of a constant t as above. Later, others showed that there are uncountably many choices for t but it is still not possible to produce a value of t which can be proven. Under the Riemann hypothesis, one can prove that there is a value of t which is between 1.3 and 1.31 for which the sequence $[t^{3^n}]$ gives primes.

References

[1] E M Wright, A prime-representing function, *Amer. Math. Monthly*, **Vol. 58**, No. 9, pp. 616–618, 1951.

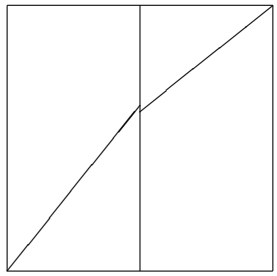
[2] W H Mills, A prime-representing function, *Bull. Amer. Math. Soc.*, **53**, pp. 604, 1947.

[3] A E Ingham, On the difference between consecutive primes, *Quart. J. Math. Oxford Ser.*, **Vol. 8**, pp. 255–266, 1937.

An Irrational Walk and Why 1 is Not Congruent

1. Introduction

The subject of Diophantine equations is an area of mathematics where solutions to very similar-looking problems can vary from the elementary to the deep. Problems are often easy to state, but it is usually far from clear whether a given one is trivial to solve or whether it must involve deep ideas. Fermat showed that the equations $X^4 + Y^4 = Z^4$ and $X^4 - Y^4 = Z^4$ do not have nontrivial solutions in integers. He did this through a method now known as the method of descent. In fact, he discovered this while working on a Diophantine problem called the congruent number which we discuss below. There are other situations where these equations arise naturally. One such problem we discuss is the following.



Suppose we start walking from a corner of a unit square to reach the diagonally opposite corner. The rule is to walk on a straight line to some point of the middle vertical line as in the figure and, on reaching that point, walk towards the opposite corner along a straight line. Thus, we have a path as in the figure consisting of one segment until the middle line is reached and the other from that point to the opposite corner of the square. The question is whether we can follow such a path where both the segments we walked can be rational in lengths. This was asked (and answered!) by Roy Barbara in Article 93.21, Vol. 93 (2009), *The Mathematical Gazette*. We discuss this problem also.

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 17, No. 1, pp. 76–82, January 2012.

2. The Congruent Number Problem

A natural number d is said to be a *congruent number* if there is a right-angled triangle with rational sides and area d.

(Equivalently:) Can we have an *arithmetic progression* of three terms which are all squares of rational numbers and the common difference d?

That is, x^2-d, x^2, x^2+d comprised of squares of rational numbers where x is rational?

Indeed, Let $u \leq v < w$ be the sides of a right-triangle with rational sides. Then $x = w/2$ is such that $(v-u)^2/4, w^2/4, (u+v)^2/4$ form an arithmetic progression.

Conversely, if $x^2 - d = y^2, x^2, x^2 + d = z^2$ are three rational squares in arithmetic progression, then $z - y, z + y$ are the legs of a right angled triangle with rational legs, area $(z^2 - y^2)/2 = d$ and rational hypotenuse $2x$ because $2(y^2 + z^2) = 4x^2$.

- For example, $5, 6, 7$ are congruent numbers.
  To see these, consider the following three right-angled triangles:
  with sides $3/2, 20/3, 41/6$ with area 5,
  with sides $3, 4, 5$ with area 6,
  with sides $35/12, 24/5, 337/60$.
- $1, 2, 3$ are not congruent numbers.

The fact that $1, 2$ are not congruent numbers is essentially equivalent to Fermat's last theorem for the exponent 4.

Indeed, if $a^2 + b^2 = c^2$, $\frac{1}{2}ab = 1$ for some rational numbers a, b, c then $x = c/2, y = |a^2 - b^2|/4$ are rational numbers satisfying $y^2 = x^4 - 1$.

Similarly, if $a^2 + b^2 = c^2$, $\frac{1}{2}ab = 2$ for rational numbers a, b, c, then $x = a/2, y = ac/4$ are rational numbers satisfying $y^2 = x^4 + 1$.

These equations reduce to the equation $x^4 \pm z^4 = y^2$ over integers which was proved by Fermat using the method of descent not to have nontrivial solutions.

The unsolvability of $y^2 = x^4 \pm 1$ in rational numbers are exactly equivalent to showing $1, 2$ are not congruent.

In fact $y^2 = x^4 - 1$ for rational x, y gives a right-angled triangle with sides $y/x, 2x/y, (x^4 + 1)/xy$ and area 1.

Similarly, $y^2 = x^4 + 1$ for rational x, y gives a right-angled triangle with sides $2x, 2/x, 2y/x$ and area 2.

Here is an amusing way of using the above fact that 1 is not a congruent number to show that $\sqrt{2}$ is irrational!

Indeed, consider the right-angled triangle with legs $\sqrt{2}, \sqrt{2}$ and hypotenuse 2. If $\sqrt{2}$ were rational, this triangle would exhibit 1 as a congruent number!

Though it is an ancient problem to determine which natural numbers are congruent, it is only in late 20th century that substantial results were

obtained and progress has been made which is likely to lead to its complete solution.

The rephrasing in terms of arithmetic progressions of squares emphasizes a connection of the problem with rational solutions of the equation $y^2 = x^3 - d^2x$.

Such equations define *elliptic curves.*

It turns out that:

d is a congruent number if, and only if, the elliptic curve $E_d : y^2 = x^3 - d^2x$ has a solution with $y \neq 0$.

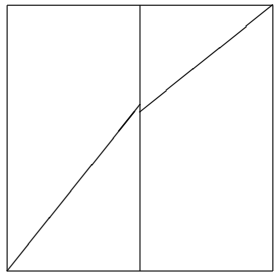
In fact, $a^2 + b^2 = c^2, \frac{1}{2}ab = d$ implies $bd/(c-a), 2d^2/(c-a)$ is a rational solution of $y^2 = x^3 - d^2x$.

Conversely, a rational solution of $y^2 = x^3 - d^2x$ with $y \neq 0$ gives the rational, right-angled triangle with sides $(x^2 - d^2)/y, 2xd/y, (x^2 + d^2)/y$ and area d.

In a nutshell, here is the reason we got this elliptic curve. The real solutions of the equation $a^2 + b^2 = c^2$ defines a surface in 3-space and so do the real solutions of $\frac{1}{2}ab = d$. The intersection of these two surfaces is a curve whose equation in suitable co-ordinates is the above curve.

A Rational Walk Which is Impossible

Now, we discuss a problem which, on the face of it, is very different, but leads to the same impossibility problem as above. Recall the figure we started with in the introduction.



Recall that the rule is to walk on a straight line to some point of the middle vertical line as in the figure and, on reaching that point, walk towards the opposite corner along a straight line. Thus, we have a path as in the figure consisting of one segment of length r until the middle line is reached and the other of length s from that point to the opposite corner. The question is whether we can follow such a path with both the distances r, s rational numbers. Suppose such a 'rational' path is possible. Let us call the vertical distance x on the middle line from the bottom to the point we

reach on it. Of course, the rest of the vertical distance is $1 - x$. Now,

$$\begin{aligned} r^2 - \frac{1}{4} &= x^2 \\ s^2 - \frac{1}{4} &= (1-x)^2 \end{aligned}$$

This gives $2x = 1 + r^2 - s^2$, which is then rational. Then, writing $r = p/q$ and $s = u/v$, we have two equations

$$\frac{\sqrt{4p^2 - q^2}}{2q} = x$$

$$\frac{\sqrt{4u^2 - v^2}}{2v} = 1 - x$$

Therefore, since the above square-roots are rational, they must be integers and so, $q = 2Q$ (if q were odd, the number $4p^2 - q^2$ would be -1 modulo 4 which cannot be a square).

Thus,

$$x = \frac{\sqrt{p^2 - Q^2}}{2Q} = \frac{l}{2Q}$$

for some l with $(l, Q) = 1$.

Similarly, $v = 2V$ and

$$1 - x = \frac{\sqrt{u^2 - V^2}}{2V} = \frac{m}{2V}$$

with $(m, V) = 1$.

Thus,

$$1 = \frac{l}{2Q} + \frac{m}{2V}$$

gives $2QV = lV + mQ$.

As $(l, Q) = 1 = (m, V)$, we get $Q|V, V|Q$; that is, $Q = V$ as both are positive integers.

Hence, we have obtained $l^2 + Q^2 = p^2, m^2 + Q^2 = u^2, l + m = 2Q$ with $(l, Q) = 1 = (m, Q)$.

We show that this set of equations does not have any integral solutions. We could try to use a characterization of primitive Pythagorean triples and proceed but we take another approach. Now, the trivial identity $(l+m)^2 + (l-m)^2 = 2(l^2 + m^2)$ gives, on multiplication by $(l + m)^2$ that

$$(l+m)^4 + (l^2 - m^2)^2 = 2(l+m)^2(l^2 + m^2).$$

The reason to do this is that we have an expression in terms of p, u and Q as follows. Indeed, putting $l + m = 2Q$, $l^2 - m^2 = p^2 - u^2$ and $l^2 + m^2 = p^2 + u^2 - 2Q^2$, we have

$$16Q^4 + (p^2 - u^2)^2 = 8Q^2(p^2 + u^2 - 2Q^2).$$

In other words,

$$4Q^4 - (p^2 + u^2)Q^2 + \frac{(p^2 - u^2)^2}{8} = 0.$$

This means that the discriminant $(p^2+u^2)^2-2(p^2-u^2)^2 = 6p^2u^2-p^4-u^4$ must be a perfect square, say d^2. But then the general algebraic identity

$$(p^2 + u^2)^4 - (6p^2u^2 - p^4 - u^4)^2 = (4pu(p^2 - u^2))^2$$

tells us that $(p^2 + u^2, d, 4pu(p^2 - u^2))$ is an integer solution of the equation $X^4 - Y^4 = Z^2$. As we already saw, this has only the trivial solution when Y is 0. Note that $d = (p^2 + u^2)^2 - 2(p^2 - u^2) \neq 0$ since $\sqrt{2}$ is irrational. Therefore, we have shown that a rational walk as above is impossible for the same reason that 1 is not a congruent number; viz., that the Fermat equation $X^4 - Y^4 = Z^2$ does not have integral solutions with $Y \neq 0$. It would be interesting to directly relate the above 'rational walk' problem to the congruent number problem for 1!

Covering the Integers

Let $f : \mathbf{N} \to \mathbf{C}$ be an arithmetic function. Then, f can be recovered back from the function (its Möbius transform) $\widehat{f}(n) = \sum_{d|n} f(d)$ by the Möbius inversion formula

$$f(n) = \sum_{d|n} \mu(d)\widehat{f}(n/d),$$

where the Möbius function is defined $\mu(n) = 1$ if $n = 1$, $\mu(n) = (-1)^r$ if $n = p_1 p_2 \cdots p_r$ for distinct primes $p_1, \cdots, p_r$ and $\mu(n) = 0$ if not. Here is an elementary observation (in the spirit of the uncertainty principle as made by Paul Pollack):

Lemma. Let f be any non-zero arithmetic function such that the support

$$\{n : \widehat{f}(n) \neq 0\},$$

is a finite set. Then, the support

$$\{n : f(n) \neq 0\},$$

of f is infinite.

Proof. Suppose f is non-zero and that $\{n : f(n) \neq 0\}$ is finite. Then, $F(z) := \sum_{n\geq 1} \widehat{f}(n)z^n$ is a non-zero polynomial. But, if $M = Max(|f(n)| : n \geq 1)$, then for $|z| < 1$, we have

$$|F(z)| = |\sum_n (\sum_{d|n} f(d))z^n| \leq \sum_n \sum_{d|n} |f(d)||z|^n$$

$$\leq \sum_n (\sum_{d|n} M)|z|^n \leq M \sum_n n|z|^n = \frac{m|z|}{1-|z|^2} < \infty.$$

Therefore, we can interchange the summations to obtain

$$F(z) = \sum_r \sum_{d|n} f(d)z^{rd} = \sum_r \sum_{d|n} f(d)\frac{z^d}{1-z^d}.$$

Now, if $N = \text{Max}(n : f(n) \neq 0)$, then $F(z)$ clearly has a pole at $z = e^{2i\pi/N}$ which contradicts the fact that F is an entire function.

This gives a proof of the infinitude of primes as follows.

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 17, No. 3, pp. 284–290, March 2012.

Note that $\widehat{\mu}(n) = \sum_{d|n} \mu(d) = 0$ for $n > 1$. So, $\widehat{\mu}$ has finite support. So, if there were only finitely many primes, μ would have finite support contradicting the 'uncertainty' result proved above.

The above type of argument has interesting applications to what are known as covering congruences. These can be described as follows.

Just as every natural number is either odd or even, one can see that for any k, the congruences

$x \equiv 1 \pmod 2$, $x \equiv 1 \pmod 4$, $\cdots$, $x \equiv 1 \pmod{2^k}$, $x \equiv 0 \pmod{2^k}$

cover the set of all integers. In other words, every integer satisfies at least one of these congruences. Similarly, for any positive integer N, the set of congruences $x \equiv i \pmod N$ for $i = 0, 1, \cdots, N-1$ covers the integers.

Thus, these are called sets of 'covering congruences'. The general definition is the following.

Let $a_1, \cdots, a_k$ be integers and let $n_1, \cdots, n_k$ be positive integers. The set of congruences $x \equiv a_i \pmod{n_i}$ for $i = 1, \cdots, k$ is called a set of *covering congruences* if $\mathbf{Z} = \bigcup_{i=1}^{k} (a_i + n_i \mathbf{Z})$. We write the set in short as $a_1(n_1), a_2(n_2), \cdots,$
$a_k(n_k)$.

Note that in both the cases above, the 'moduli' $n_1, \cdots, n_k$ of the congruences have the property that $\sum_{i=1}^{k} \frac{1}{n_i} = 1$.

A set of covering congruences $a_1(n_1), \cdots, a_k(n_k)$ is called a *disjoint covering system* if every integer satisfies exactly one of the congruences $x \equiv a_i \pmod{n_i}$.

Note that the two sets of covering congruences above, viz.,

$$1(2), 1(2^2), \cdots, 1(2^k), 0(2^k)$$

and

$$0(N), 1(N), \cdots, N-1(N)$$

are disjoint covering systems. Note also that at least two of the moduli are the same. That this must always be true is the assertion of the following proposition whose proof follows the method we started the article with.

PROPOSITION

Let $a_1(n_1), a_2(n_2), \cdots, a_k(n_k)$ be a disjoint system of covering congruences where $n_1 \le n_2 \le \cdots \le n_k$. Then, $n_{k-1} = n_k$. Moreover $\sum_{j=1}^{k} \frac{1}{n_j} = 1$.

Proof. We may assume without loss of generality that $0 \le a_j < n_j$ for each $j \le k$. By the hypothesis, we have for $|z| < 1$,

$$\sum_{j=1}^{k} \frac{z^{a_j}}{1 - z^{n_j}} = \sum_{j=1}^{k} \sum_{r=0}^{\infty} z^{a_j + r n_j} = \sum_{n \ge 0} z^n = \frac{1}{1-z}.$$

Thus, this function has a pole at the point $z = 0$. But, if $n_i < n_k$ for all $i < k$, then this function has a pole at $z = e^{2i\pi/n_k}$, a contradiction. This proves the first assertion.

Let $n = LCM(n_1, \cdots, n_k)$. Then, we have

$$1 - z^n = \prod_{j=1}^{k} (1 - e^{2i\pi a_j/n_j} z^{n/n_j}),$$

as each n-th root of unity is a simple root of the polynomial on the left hand side. This can be rewritten as

$$1 - z^n = \sum_{I \subset \{1,\cdots,k\}} (-1)^{|I|} z^{\sum_{j\in S} n/n_j} e^{2i\pi \sum_{j\in I} a_j/n_j}.$$

Comparing degrees gives us $\sum_{j=1}^{k} \frac{n}{n_j} = n$ which is the second assertion.

This leaves the question of the existence of a covering system (necessarily not disjoint by the above proposition) with distinct moduli. The first set of covering congruences for which the moduli are distinct was given by A Schinzel. This is the set

$$0(2), 0(3), 1(4), 5(6), 7(12).$$

Here are two famous conjectures due to Erdös and others which are still open.

Conjecture 1. (Erdös-Selfridge). There is no finite system of covering congruences where all the moduli are distinct and odd.

Conjecture 2. (Erdös) For any $M > 0$, there exists a system of covering congruences where all the moduli are distinct and $> M$.

Erdös mentioned in 1995 that the last conjecture is perhaps his favourite problem!

We finish with a number-theoretic application which originally motivated the study of covering congruences. This is the following beautiful result due to (who else but!) Erdös.

Theorem. (Erdös, 1950). *There are infinitely many odd integers which are not expressible as the sum of a prime and a power of* 2.

Proof. Consider a covering system of congruences $a_i(n_i)$ with $1 \leq i \leq k$ where $p_1, \cdots, p_k$ are distinct odd primes and n_i the least positive number satisfying $2^{n_i} \equiv 1 \bmod p_i$.

Erdös constructed such covering systems explicitly; one such is

$$0(2), 0(3), 1(4), 3(8), 7(12), 23(24)$$

Note that the n_i's here – $2, 3, 4, 8, 12, 24$ – are the orders of 2 modulo the primes $3, 7, 5, 17, 13, 241$.

Given any such system, the Chinese remainder theorem provides a common solution to the congruences

$x \equiv 2^{a_i} \pmod{p_i}$; $1 \leq i \leq k$ and $x \equiv 1 \pmod{2}$.

Such a solution x is unique modulo $2\prod_{i=1}^{k} p_i$. Consider the smallest positive integer solution, say x_0. Now, for each integer r, there exists some i such that $r \equiv a_i \pmod{m_i}$.

So, if $n \equiv n_0 \pmod{2p_1 \cdots p_k}$, then

$n - 2^r \equiv n_0 - 2^{a_i} \equiv 0 \pmod{p_i}$.

Thus, if $n - 2^r > p_i$, then it must be composite.

This proves that all n not of the form $2^r + p_i$ for some r and some $i \leq k$ are inexpressible in the form asserted. To dispose of the exceptional cases, we may impose extra congruence conditions.

An example (taking the above covering system $0(2), 0(3), 1(4), 3(8), 7(12), 23(24)$ of Erdös) gives us:

No integer $\equiv 7629217$ *(*mod 1184810*) is a sum of a power of* 2 *and an odd prime.*

Z-W Sun has done substantial work in the subject of covering congruences and revealed connections with zero-sum problems. We finish with a following amazing application completed by Sun of the above work by Erdös and later work of Cohen, Selfridge on covering congruences.

Consider the 29*-digit number*

$$\begin{aligned} M &= 664830849615885101240106915 90 \\ &= 2.3.5.7.11.13.17.19.31.37.41.61.73.97.109.151.241.257.331. \end{aligned}$$

Then, the solutions of the congruence

$$x \equiv 47867742232066880047611079 \mod M$$

cannot be expressed as $\pm p^a \pm q^b$ *where* p, q *are primes and* a, b *are non-negative integers.*

As can be readily imagined, simple questions for integers arising out of covering systems of congruences have many interesting analogues for groups where the congruences are replaced by cosets of subgroups. That will be a topic to discuss on another occasion.

S Chowla and S S Pillai: The Story of Two Peerless Indian Mathematicians[1]

Ramanujan may be a household name
in our country, but it is a shame
that not much is known about who later came.
Here, we talk about Chowla and Pillai
whose names in the mathematical landscape will lie
right at the top Any doubts? Illai Illai!

Sarvadaman Chowla (1907–1995) and S S Pillai (1901–1950) were two of the foremost mathematicians to emerge from India in the generation immediately after Ramanujan. The Mathematics Geneology Project lists both Ramanujan and Chowla among the students of Littlewood! This article specially features Chowla and Pillai. As a matter of fact, the June 2004 issue of *Resonance* journal had already featured Pillai [1] but we shall see that a discussion of Chowla is necessarily intertwined with one of Pillai. It has been mentioned by G H Hardy that after Ramanujan, the greatest Indian mathematician was Pillai. We journey through some of the very interesting and illuminating correspondences between Chowla and S S Pillai which reveals also other personal and historical aspects. Apart from that, we talk about Chowla's and Pillai's mathematical works. In a book of this type, it is essential to select only those topics which are more elementary or easy to describe while conveying some of the beauty and depth of the ideas. Fortunately, in the works of Chowla and Pillai, we can find a veritable treasury which is accessible at a level which can be enjoyed by even the non-expert. Each of their works has an element of surprise and an element of elegance and simplicity. They worked on a wide spectrum of areas of number theory. We select some of their more elementary gems and discuss their proofs. In fact, we attempt to retain as much of the original ideas in the arguments as possible.

It is an enigma that even a layman may ask a question in elementary number theory which turns out to be nontrivial. The fact that several old problems in elementary number theory remain unsolved to this day, has been referred to in different ways by people. To quote Professor K Ramachandra,

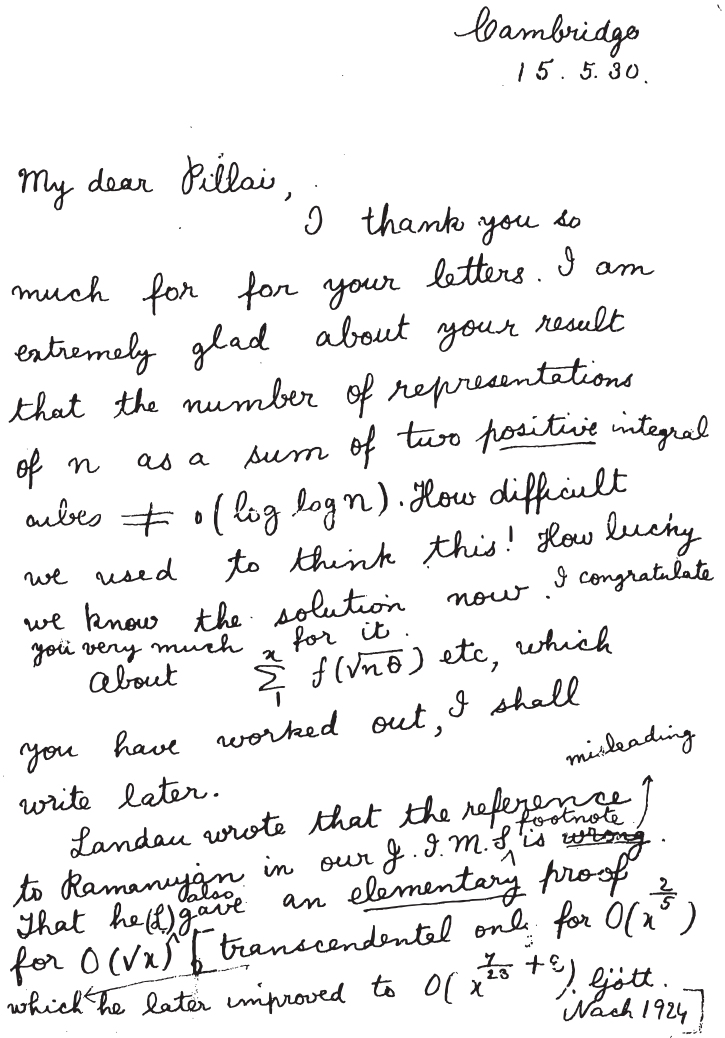
The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 17, No. 9, pp. 855–883, September 2012.

[1]This chapter was part of an article written in collaboration with R Thangadurai.

"*in figurative terms, what has been solved can be likened to an egg-shell, and what remains to be solved to the infinite space surrounding it.*"

2. Chowla to Pillai Correspondence

Starting in the late 1920s, and up to one month before Pillai's death, Chowla and Pillai maintained regular correspondence. They published joint papers starting in 1930 with a famous piece of work on the Euler's totient function. Some other themes that they collaborated on were concerned with solutions to the Brahmagupta–Pell equation and the Waring problem. The correspondence between these two stalwarts is mathematically illuminating to read. It also reveals the intellectual honesty they possessed and the joy each drew from the other's successes.



Cambridge
15. 5. 30.

My dear Pillai,

I thank you so much for for your letters. I am extremely glad about your result that the number of representations of n as a sum of two positive integral cubes $\neq o(\log\log n)$. How difficult we used to think this! How lucky we know the solution now. I congratulate you very much for it.

About $\sum_1^x f(\sqrt{n}\theta)$ etc, which you have worked out, I shall write later.

Landau wrote that the reference (footnote) to Ramanujan in our J. I. M. S. is misleading. That he (also) gave an elementary proof for $O(\sqrt{x})$ [transcendental only for $O(x^{\frac{2}{5}})$ which he later improved to $O(x^{\frac{7}{23}+\varepsilon})$ Göttinger Nach 1924].

I am sorry for my mistake
If there any misprints in
our J. London M. S. paper please
write to me. I could not find any
I hope there are ~~are~~ not too many
faults in it. Please tell them to me.

The ~~letter~~ pages I sent you on Waring's
~~theorem~~ ~~was~~ were for you. It has
appeared in J. L. M. S. I am sorry
I did not write to you before. But
I hope Mr. Narasinga Rao will excuse
me if they are also going to
publish it

Walfisz sent some matter that
proves that

$$\sum_{1}^{R} E(x) = \frac{3}{2\pi^2} R^2 + O(R^{\frac{5}{3}});$$

can you improve it? I hope
I shall soon send his proof.
(I have been doing Landau's
1912 Gött. Nach. paper lately, ~~so I had~~ I hope you have in Madras Univ. Library)

I only state a few results in this letter.

$$(1) \qquad \sum_{1}^{\sqrt{R}} \sqrt{R - x^2} = \frac{\pi}{4} R - \frac{1}{2}\sqrt{R} + O(R^{\frac{1}{4}})$$

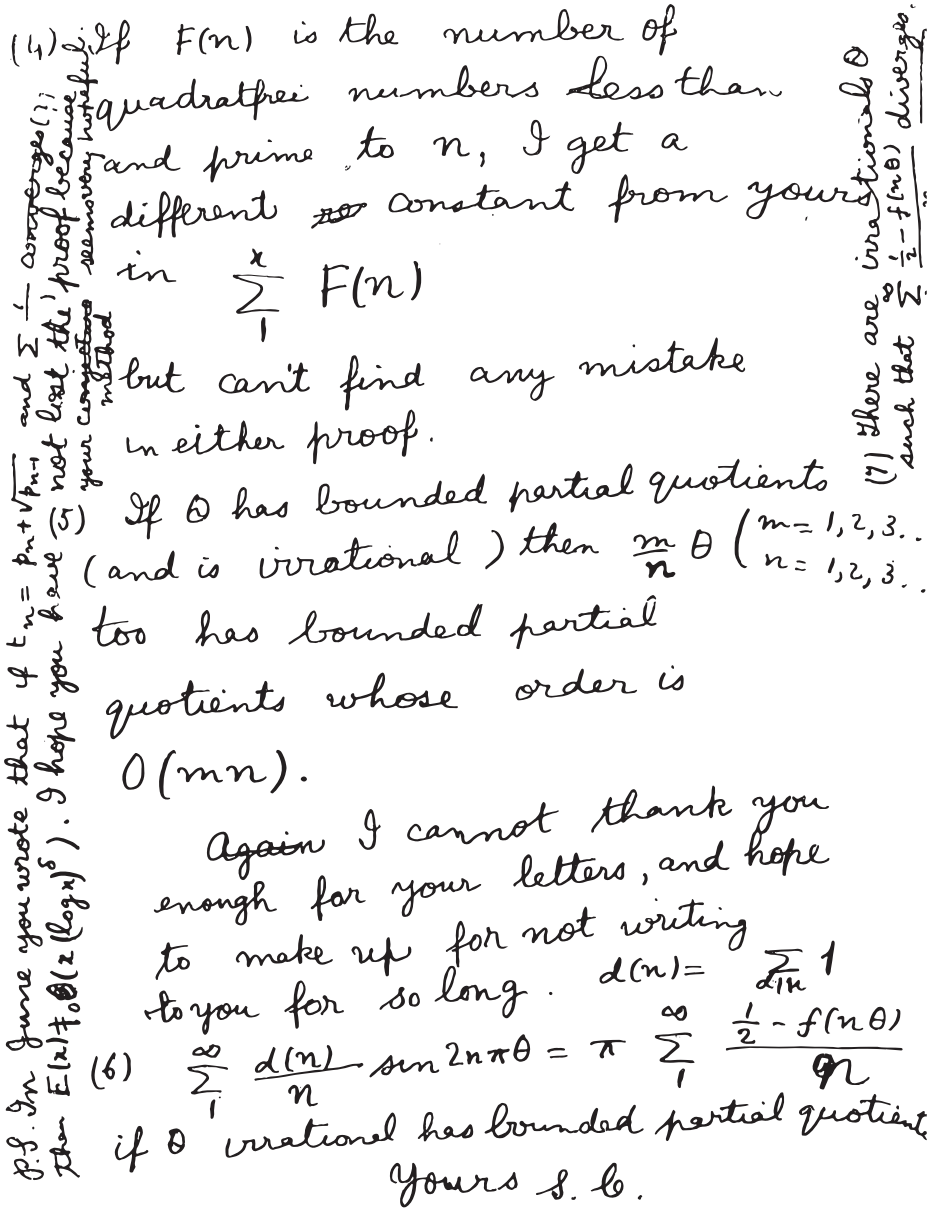
It helps in Lattice points of circle $\odot\ x^2 + y^2 = R$. The first term is known from Integral Calculus. The error term is "best possible".

(2) $f(x)$ the fractional part of x;

$$\sum_{1}^{x} f\left(\log(n)\right) = \frac{1}{2} x + o(x)$$

$$(3) \qquad \sum_{n=1}^{R^{\frac{1}{k}}} \left(R - n^k\right)^{\frac{1}{k}} = A R^{\frac{2}{k}} - \frac{1}{2} R^{\frac{1}{k}} + O(R^{\frac{1}{k} - \frac{1}{k^2}})$$

I believe that the error is "best possible", but cannot prove except when $k = 2$ [$k = 2, 3, 4, 5$ in Theorem by Bessel Fns.



(4) If $F(n)$ is the number of squadratfrei numbers less than and prime to n, I get a different constant from yours in $\sum_1^x F(n)$ but can't find any mistake in either proof.

(5) If θ has bounded partial quotients (and is irrational) then $\frac{m}{n}\theta$ $\begin{pmatrix} m=1,2,3.. \\ n=1,2,3.. \end{pmatrix}$ too has bounded partial quotients whose order is $O(mn)$.

Again I cannot thank you enough for your letters, and hope to make up for not writing to you for so long. $d(n) = \sum_{d|n} 1$

(6) $\sum_1^\infty \frac{d(n)}{n} \sin 2n\pi\theta = \pi \sum_1^\infty \frac{\frac{1}{2} - f(n\theta)}{n}$ if θ irrational has bounded partial quotients

Yours S. C.

(7) there are irrationals θ such that $\sum \frac{\frac{1}{2} - f(n\theta)}{n}$ diverges.

P.S. In June you wrote that if $t_n = p_n + \sqrt{p_{n-1}}$ and $\sum \frac{1}{t_n}$ converges (1) then $E(x) \neq O(x(\log x)^5)$. I hope you have not lost the proof because your comparison seems very useful method

---

The letter shows the reluctance on Chowla's part to be a co-author of some result where he felt he had not contributed enough. The letter is written by Chowla after he joined St.Stephen's College in Delhi. Through the years, Chowla consistently expresses almost in every letter his gladness for the correspondence between them!

The number theorist K Ramachandra spoke of his first meeting with Chowla at the Institute for Advanced Study in Princeton during the

former's first visit there. After discussing mathematics, Chowla got them both bottles of 'pepsi' from a vending machine. After the meeting, Ramachandra says that he ran around the premises muttering that he drank pepsi with Chowla!

Chowla's fertile imagination earned him the sobriquet of 'poet of mathematics' from his associates. Chowla passed away in the U.S. in 1995 at the age of 88. On the other hand, Pillai died tragically at the age of 49 in 1950. Pillai was invited to visit the Institute for Advanced Study in Princeton for a year. The flight which he boarded to participate in the 1950 International Congress of Mathematicians tragically crashed near Cairo on the 31st of August. The readers are directed to Pillai's collected works which have appeared recently.

3. Mathematical Gems from Chowla and Pillai

Waring's Problem

A discussion of Pillai's mathematical work must start with Waring's problem and vice versa! However, since this has been written about in detail in the June 2004 issue, we mention this problem in passing and refer the readers to the above-mentioned *Resonance* article by C S Yogananda [2].

Waring's problem asks for the smallest number $g(k)$ corresponding to any $k \geq 2$ such that every positive integer is a sum of $g(k)$ numbers each of which is the k-th power of a whole number. Hilbert had shown that such a finite number $g(k)$ does exist. The ideal Waring's conjecture predicts a particular value of $g(k)$. Indeed, if 3^k is divided by 2^k, the quotient is $[(3/2)^k]$, and some remainder r, where $[t]$ denotes the greatest integer less than or equal to t. Now, the number

$$2^k[(3./2)^k] - 1 = ([(3/2)^k] - 1)2^k + (2^k - 1)1^k$$

is a sum of $2^k + [(3/2)^k] - 2$ numbers which are k-th powers and is not the sum of a smaller number of k-th powers. Hence,

$$g(k) \geq 2^k + [(3/2)^k] - 2.$$

This ideal Waring conjecture asserts that this lower bound is the correct bound also. Pillai proved, among other things, that this ideal Waring conjecture holds good under the condition on k that the remainder r on dividing 3^k by 2^k satisfies $r \leq 2^k - [(3/2)^k] - 2$ (chapter 21 of [3]). This is known to hold for all $k \leq 471600000$. At this time, the ideal Waring conjecture is known to hold for all large enough k.

4. The Least Prime Quadratic Residue

Chowla's lifelong pre-occupation with class number of binary quadratic forms led him to discover some rare gems on the way, so to speak! An interesting problem, useful in cryptography, for instance, is to find for a given prime p, the smallest prime q which is a quadratic residue (that is, a square) modulo p. For example, the quadratic reciprocity law tells us that if $p \equiv \pm 1$ modulo 8, then 2 is the least quadratic residue mod p. Chowla [4] proved the following beautiful result:

Let $p > 3$ be a prime such that $p \equiv 3$ mod 8. Let $l(p)$ denote the least prime which is a quadratic residue mod p. If the number $h(-p)$ of classes of binary quadratic forms of discriminant $-p$ is at least 2, then $l(p) < \sqrt{\frac{p}{3}}$. If $h(-p) = 1$, then $l(p) = \frac{p+1}{4}$ (and, therefore, $\frac{p+1}{4}$ is prime!).

Remarks. (i) The theorem implies, in particular, that for primes $p > 3$, $p \equiv 3 \bmod 8$, we have $l(p) = \frac{p+1}{4}$ if and only if $h(-p) = 1$ because $\sqrt{\frac{p}{3}} < \frac{p+1}{4}$ for $p > 3$.

(ii) The proof of the theorem is easy and uses Minkowski's reduction theory of quadratic forms which produces in each equivalence class of positive-definite forms, a unique one $ax^2 + bxy + cy^2$ which is 'reduced' in the sense that $|b| \leq a \leq c$.

5. Chowla's Counter-examples to a Claim of Ramanujan and a Disproof of Chowla's Conjecture

Among Ramanujan's numerous astonishing results, there are also occasional lapses. One such was his 'proof' (in his very first paper of 1911) that the numerators of Bernoulli numbers are primes. This is false; for instance, denoting by B_n the Bernoulli number defined by

$$\frac{z}{e^z - 1} = \sum_{n \geq 0} B_n \frac{z^n}{n!},$$

and by N_n, the numerator of B_n/n, the numbers N_{20}, N_{37} are composite. In 1930, Chowla showed [5] that Ramanujan's claim has infinitely many counter-examples. Surprisingly, Chowla returns to this problem 56 years later(!) in a joint paper with his daughter [6] and poses as an unsolved problem that N_n is always square-free. In a recent article, Dinesh Thakur [7] points out that Chowla's question has infinitely many negative answers. Indeed, Thakur shows:

For any fixed irregular prime p less than 163 million, and any arbitrarily large k, there exists a positive integer n such that N_n is divisible by p^k.

If we observe (from the existing tables) that 37^2 divides N_{284}, Chowla's question has a negative answer. The proof of the more general assertion uses the so-called Kummer congruences which essentially assert that the value of $\frac{(p^{n-1}-1)B_n}{n}$ modulo p^k depends (for even n) only on n modulo $p^{k-1}(p-1)$, if $p-1$ does not divide n. Using this as well as certain functions called p-adic L-functions, the general assertion of arbitrarily large powers can also be obtained.

6. Problem on Consecutive Numbers

Pillai proved in 1940 that any set of n consecutive positive integers where $n \leq 16$, contains an integer which is relatively prime to all the others. However, there are infinitely many sets of 17 consecutive integers where the above fact fails. For instance, $N+2184, N+2185, \cdots, N+2200$ is such a set whenever N is a multiple of $2.3.5.7.11.13 = 30,030$. Moreover, Pillai also proved [8] that for any $m \geq 17$, there are infinitely many blocks of m consecutive integers for which the above property fails. Now, generalizations to arithmetic progressions instead of consecutive numbers are known.

7. How Spread-out are Perfect Powers?

Look at the sequence of all perfect powers of positive integers:

$$1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, \cdots .$$

We observe that differences between consecutive terms can be: 1 $(9-8)$, $2 = (27-25)$, 3 $(4-1)$, 4 $(36-32)$, 5 $(32-27)$ etc.

Pillai conjectured that consecutive terms can be arbitrarily far apart [9]. In other words, given any number, one can find consecutive terms whose difference is larger than that given number. Equivalently, the conjecture asserts:

Given a positive integer k, the equation $x^p - y^q = k$ has only finitely many solutions in positive integers $x, y, p, q \geq 2$.

This is unproved as yet even for one value of $k > 1$ although it is known now that if one of these 4 parameters is fixed, the finiteness holds.

8. Independent Values of the Cotangent Function

A typical aspect of Chowla's works has been to come back to an old result after several years and applying it in an unexpected manner. On 9.2.1949, Chowla had written to Carl Ludwig Siegel about a certain non-vanishing of a particular type of series. Three days later, he received a reply from Siegel, improving the result. In 1970, Chowla, while wondering about relations between the roots of a certain polynomial, realized that not only could he

re-prove Siegel's improved version in a simpler fashion [10], he could use this old result to prove what he wanted about the roots! Let us discuss it briefly.

If p is a prime number, consider the values $x_r = \cot(r\pi/p)$ of the cotangent function, for $0 < r < p$. Evidently, $x_r + x_{p-r} = 0$. Also, $\sum_{r=1}^{p-1} x_r = 0$ but this is easily deduced from the earlier relations. So, a natural question is:

Are all the linear relations of the form $\sum_{i=1}^{p-1} a_r x_r = 0$ *with* $a_i \in \mathbf{Q}$, *consequences of the relations* $x_r + x_{p-r} = 0$ *for* $1 \leq r < p$*?*

Indeed, x_r's are the roots of an irreducible polynomial over $\mathbf{Q}$, of degree $p-1$ and, one may ask for possible linear relations among the roots of any irreducible polynomial over $\mathbf{Q}$. Chowla's theorem asserts:

Let p *be a prime number and* $x_r = \cot(\pi r/p)$ *for* $r = 1, \cdots, \frac{p-1}{2}$. *If* $a_i \in \mathbf{Q}$ *such that* $\sum_{i=1}^{\frac{p-1}{2}} a_i x_i = 0$, *then* $a_i = 0$ *for all* $i \leq (p-1)/2$.

Chowla uses some very basic Galois theory to deduce that, under the assumption $\sum_{i=1}^{\frac{p-1}{2}} a_i x_i = 0$ above, there are $(p-1)/2$ such linear relations, viz.,

$$a_1 x_1 + a_2 x_2 + \cdots + a_{\frac{p-3}{2}} x_{\frac{p-3}{2}} + a_{\frac{p-1}{2}} x_{\frac{p-1}{2}} = 0$$

$$a_1 x_2 + a_2 x_3 + \cdots + a_{\frac{p-3}{2}} x_{\frac{p-1}{2}} + a_{\frac{p-1}{2}} x_1 = 0$$

$$\vdots$$

$$a_1 x_{\frac{p-1}{2}} + a_2 x_1 + \cdots + a_{\frac{p-1}{2}} x_{\frac{p-3}{2}} = 0.$$

If the a_i's are not all 0, this leads to the vanishing of the 'cirulant' determinant

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_{(p-1)/2} \\ x_2 & x_3 & \cdots & x_1 \\ & \ddots & \ddots & \\ x_{(p-1)/2} & x_1 & \cdots & x_{(p-3)/2} \end{pmatrix}.$$

At this point, Chowla quotes the well-known value of this determinant and proceeds.

What is the value of this determinant?

In the 3×3 case

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \\ x_3 & x_1 & x_2 \end{pmatrix},$$

has determinant $3x_1x_2x_3 - x_1^3 - x_2^3 - x_3^3$.

Let $1, \omega, \omega^2$ be the cube roots of unity.

If x_1, x_2, x_3 are replaced by $\omega x_1, \omega^2 x_2, x_3$ or by $\omega^2 x_1, \omega x_2, x_3$, the expression remains the same. As $x_3 = -x_1 - x_2$ leads to $3x_1x_2x_3 - x_1^3 - x_2^3 - x_3^3 = 0$,

the three expressions $x_1 + x_2 + x_3, \omega x_1 + \omega^2 x_2 + x_3, \omega^2 x_1 + \omega x_2 + x_3$ are factors. In other words, the determinant in the 3×3 case is given as:

$$\det \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \\ x_3 & x_1 & x_2 \end{pmatrix} = -(x_1+x_2+x_3)(\omega x_1+\omega^2 x_2+x_3)(\omega^2 x_1+\omega x_2+x_3).$$

Similarly, in general, the determinant of $\begin{pmatrix} x_1 & x_2 & \cdots & x_{(p-1)/2} \\ x_2 & x_3 & \cdots & x_1 \\ & \ddots & \ddots & \\ x_{(p-1)/2} & x_1 & \cdots & x_{(p-3)/2} \end{pmatrix}$ equals the product (up to sign) of

$$\omega^r x_1 + \omega^{2r} x_2 + \cdots + \omega^{\frac{r(p-1)}{2}} x_{\frac{p-1}{2}}$$

as r varies from 1 to $\frac{p-1}{2}$ where $\omega = e^{\frac{4i\pi}{p-1}}$, $(p-1)/2$-th root of unity.

Here, Chowla realizes with surprise that the above factors are (up to certain non-zero factors) none else other than the special value at $s = 1$ of certain functions $L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}$ called Dirichlet L-functions corresponding to Dirichlet characters χ modulo p which satisfy $\chi(-1) = -1$. The non-vanishing of these are the older result mentioned above and show, thus, that the determinant is non-zero. Hence, the linear independence of the $\cot(r\pi/p)$ for $1 \leq r \leq (p-1)/2$ is established.

Remarks. (i) Kai Wang closely followed Chowla's proof to generalize his theorem to non-primes and to derivatives of the cotangent function [11] by showing:

For any $s \geq 0$ and an arbitrary natural number k, the $\frac{\phi(k)}{2}$ real numbers $\frac{d^s}{dx^s} \cot\left(x + \frac{r\pi}{k}\right)_{x=0}$ (where $r \leq \frac{\phi(k)}{2}$ and $(r, k) = 1$) are linearly independent over $\mathbf{Q}$.

(ii) The non-vanishing at $s = 1$ of $L(s, \chi)$ for nontrivial Dirichlet characters is the key fact used in the proof of Dirichlet's famous theorem on existence of infinitely many primes in any arithmetic progression $an + b$ with $(a, b) = 1$.

(iii) Kenkichi Iwasawa (see [12]) showed later in 1975 that the above result has connections with the so-called "regular" primes. The definition of regular primes is not needed here and, we merely recall that Kummer had proved that the Fermat equation $x^p + y^p = z^p$ has no non-zero solutions in integers if p is a 'regular prime'. It is unknown yet whether there are infinitely many regular primes (although Fermat's last theorem has been proved completely) – surprisingly, it has been known for a long time that there are infinitely many irregular primes! The connection of the above result of Chowla with regular primes is the following.

The linear independence of the $(p-1)/2$ cotangent values ensures that there exist rational numbers $t_1, \cdots, t_{\frac{p-1}{2}}$ so that

$$2\sin\frac{2\pi}{p} = \sum_{r=1}^{\frac{p-1}{2}} t_r \cot(2r\pi/p).$$

Iwasawa shows the prime p is regular if and only if, none of the t_r's have denominators which is a multiple of p and, at least one t_r has numerator also not divisible by p.

9. On the Number of Permutations of a Given Order

Chowla wrote a series of papers on generating functions for the number of permutations of a given order etc. In the permutation group S_n, let $A_n(d)$ denote the number of permutations σ satisfying $\sigma^d = Id$. In collaboration with Herstein and Scott, he showed ([13]):

$$\sum_{n=0}^{\infty} \frac{A_n(d)x^n}{n!} = exp(\sum_{k|d} \frac{x^k}{k}).$$

Here, convenience of notation, one takes $A_0(n) = 1$. Let us prove this beautiful, useful fact.

We look for a recursive relation for $A_n(d)$ in terms of $A_k(d)$ for $k < n$. Look at what happens to the symbol n under any permutation contributing to $A_n(d)$. If the symbol is fixed, then the rest of the $n-1$ symbols can be permuted in $A_{n-1}(d)$ ways. Now, suppose the symbol n is a part of a k-cycle for some $1 < k \leq n$. Note that any permutation contributing to $A_n(d)$ has some order dividing d; thus, if it has a k-cycle in its decomposition, then $k|d$. Now, each k-cycle contributes $A_{n-k}(d)$ elements. As there are $(n-1)(n-2)\cdots(n-k+1)$ ways to choose such k-cycles, we get

$$A_n(d) = A_{n-1}(d) + \sum_{k|d;1<k\leq n} (n-1)\cdots(n-k+1)A_{n-k}(d).$$

This can be rewritten as

$$\frac{A_n(d)}{n!} = \sum_{k|d;1\leq k\leq n} \frac{A_{n-k}(d)}{(n-k)!}.$$

Therefore, the generating function $f(x) = \sum_{n\geq 0} \frac{A_n(d)}{n!}$ satisfies

$$xf'(x) = \sum_{i\geq 1} \frac{A_i(d)x^i}{i!} = \sum_{i\geq 1} \left(\sum_{k|d,1\leq k\leq i} \frac{A_{i-k}(d)}{(i-k)!} \right) x^i,$$

on using the recursion above.

Combining the terms corresponding to a particular $A_j(d)$, we have therefore

$$xf'(x) = \sum_{j\geq 0} \frac{A_j(d)}{j!} \sum_{k|d} x^{j+k} = f(x) \sum_{k|d} x^k.$$

This is a differential equation

$$\frac{f'(x)}{f(x)} = \sum_{k|d} x^{k-1}$$

whose general solution is obtained by integration as

$$f(x) = c.exp\left(\sum_{k|d} \frac{x^k}{k} \right)$$

for some constant c. Since $f(0) = A_0(d) = 1 = c$, we get the assertion

$$\sum_{n\geq 0} \frac{A_n(d)}{n!} = \exp\left(\sum_{k|d} \frac{x^k}{k} \right).$$

This formula is useful in a number of ways. For instance, one can get an asymptotic estimate of how fast $A_n(d)$ grows with n (for any fixed d). Moreover, for $d = p$, a prime, this gives a simple-looking closed formula for $A_n(p)$ for any n.

9.1 *Closed Form for the Prime Case*

In the above identity

$$\sum_{n\geq 0} \frac{A_n(d)}{n!} = \exp\left(\sum_{k|d} \frac{x^k}{k} \right).$$

take $d = p$, a prime and note that

$$\sum_{n\geq 0} \frac{A_n(p)}{n!} = e^x e^{x^p/p} = \sum_{i\geq 0} \frac{x^i}{i!} \sum_{j\geq 0} \frac{x^{pj}}{p^j j!}.$$

Comparing the coefficients of x^n, we obtain

$$A_n(p) = \sum_{i+pj=n} \frac{n!}{p^j j! i!}.$$

In particular, this number is a positive integer for each $n \geq p$(!)
This is an exclamation mark, not a factorial!

Also, a classical theorem in the theory of groups, due to Frobenius, asserts that in any finite group G, the number of elements satisfying x^d =identity (for any divisor d of the order of G) is a multiple of d. Thus, we have $A_n(d)$ is a multiple of d for each $n \geq d$.

This statement for $A_n(p)$ gives, therefore, that $\sum_{i+pj=n} \frac{n!}{p^j j! i!}$ is a multiple of p for every $n \geq p$ and, the special case $n = p$ is known as Wilson's theorem.

9.2 *Applications to Finite Groups*

Apart from being useful in its own right, the study of the numbers $A_n(d)$ has connections to some counting problems in groups. Notice that the number $A_n(d)$ of permutations in S_n which satisfy x^d = identity, is nothing else than the number of group homomorphisms from a cyclic group of order d to S_n – each homomorphism associates a permutation σ satisfying σ^d = Identity, to a fixed 'generator' of the cyclic group. For *any* group G (not necessarily cyclic), knowledge of the numbers h_n of group homomorphisms from G to S_n for various n, allows us to find a recursive expression for the number of subgroups of G which have a given index in it. In fact, if s_n is the number of subgroups of index n in G, then

$$s_n + \frac{h_1}{1!}s_{n-1} + \frac{h_2}{2!}s_{n-2} + \cdots + \frac{h_{n-1}}{(n-1)!}s_1 = \frac{h_n}{(n-1)!}.$$

10. Convenient Numbers and Class Number

Euler observed that $18518809 = 197^2 + 1848(100)^2$ is a prime. In fact, Euler was interested in producing large primes of the form $x^2 + ny^2$ for various values of n. It happens (and is easy to prove) that a number which has a unique expression of the form $x^2 + y^2$ is prime. Thus, one may hope this is true for expressions of the form $x^2 + ny^2$ also for any n. However, as Euler noted [14], this holds only for a certain set of values of n. He constructed explicitly a set of 65 positive integers for which this is true (the largest of which is 1848) – he called such numbers 'idonean' or 'convenient'. To this day, it is not proven that Euler's list is complete [15]. However, a beautiful result of Chowla shows at least that the list of idonean numbers is finite! To explain how it is done, we very briefly define and discuss binary quadratic forms – another name for expressions of the form $ax^2 + bxy + cy^2$.

A binary, integral quadratic form is a polynomial $f(x, y) = ax^2+bxy+cy^2$ where a, b, c are integers. It is primitive if $(a, b, c) = 1$. The integer $b^2 - 4ac$ is known as the *discriminant*.

As

$$4af(x, y) = (2ax + by)^2 + (4ac - b^2)y^2 = (2ax + by)^2 - dy^2,$$

when $d < 0$ and $a > 0$, $f(x, y)$ takes only positive values (excepting the value 0 at $x = y = 0$). Thus, when $a > 0$, and the discriminant is negative, the form is positive-definite.

For example, $x^2 + ny^2$ is a positive-definite form with discriminant $-4n$.

Two forms $f(x, y)$ and $g(x, y)$ are said to be *equivalent* or, said to be in the same *class* if $f(\alpha x+\beta y, \gamma x+\delta y)) = g(x, y)$ where $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL(2, \mathbf{Z})$, an integer matrix of determinant 1.

The motivation behind this definition is:

Equivalent forms take the same sets of values as x, y vary over integers.

This is clear because one may also write

$$g(x, y) = f(\alpha x + \beta y, \gamma x + \delta y))$$

in the form

$$f(x, y) = g(\delta x - \beta y, -\gamma x + \alpha y)).$$

Notice that the matrix $\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$ is simply the inverse of the matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$.

Moreover, equivalent forms have the same discriminant. Gauss showed:

For $d < 0$, the number $h(d)$ of classes of primitive, positive-definite binary quadratic forms of discriminant d is finite.

Gauss conjectured that $h(d) \to \infty$ as $-d \to \infty$. This was proved by Heilbronn. By a modification of Heilbronn's argument, Chowla proved the following fact which was another conjecture of Gauss [16]:

$\frac{h(d)}{2^t} \to \infty$ as $-d \to \infty$ where t is the number of primes dividing d.

This interesting fact is useful in a totally different context which we indicate briefly now.

Euler obtained the following list of 65 numbers called 'Numerus idoneus' (or 'convenient' numbers):

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21,
22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58,
60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130,
133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280,
312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848.

Consider any odd number m co-prime to n which is expressible as $m = x^2 + ny^2$ with $(x, ny) = 1$. If each such m which has a unique expression of the form $x^2 + ny^2$ in positive integers x, y is necessarily prime, the number n is said to be idonean.

As mentioned in the beginning of this section, Euler observed that $18518809 = 197^2 + 1848(100)^2$ is a prime by showing 1848 is idonean.

Firstly, it is not even clear whether the list of idonean numbers is finite or not. This can be analyzed (and was analyzed by Gauss) using the theory of quadratic forms.

Firstly, we recall one more notion – the genus.

Two primitive, positive-definite forms of discriminant d are said to be in the same *genus* if they take the same set of values modulo d. As forms in the same class take the same set of values, they are in the same genus. Each genus, therefore, consists of finitely many classes.

Gauss proved (modulo some gaps which were filled later by Grübe):

A positive integer n is idonean if and only if, for forms of discriminant $-4n$, every genus consists of a single class.

Chowla's theorem $\frac{h(d)}{2^t} \to \infty$ as $-d \to \infty$ where t is the number of primes dividing d, which was quoted above, implies that for large enough $-d$, each genus has more than one class of forms. Therefore, by Chowla's theorem, the set of idonean numbers is finite!

As a matter of fact, Euler's list is expected to be a complete one (this has been proved to be so under the assumption of a deep conjecture known as the generalized Riemann hypothesis).

11. Matrices and Quadratic Polynomials

As we saw earlier, the equivalence classes of integral, binary quadratic forms are related to the group $SL_2(\mathbf{Z})$ of integral matrices of determinant 1. Recall also that equivalent forms take the same sets of integer values as x, y vary over integers. The following result of Chowla with J Cowles and M Cowles [17] shows that the relation is an intimate one. We recall that two matrices A, B are said to be *conjugate* if there is an invertible matrix P such that $B = PAP^{-1}$. The *trace* of a matrix is the sum of its diagonal entries. Then:

For all integers $t \neq \pm 2$, the number of conjugacy classes of matrices in $SL_2(\mathbf{Z})$ with trace t, equals the number of equivalence classes of integral, binary quadratic forms with discriminant $t^2 - 4$.

Recall the discriminant of a quadratic form $ax^2 + bxy + cy^2$ was defined in the last section to be the number $b^2 - 4ac$. Here is the easy proof of the above theorem.

Associate to each matrix $M := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$, the quadratic form

$$m(x, y) := bx^2 + (d - a)xy - cy^2.$$

Note that if the trace of M is t, then $a + b = t$ and, therefore, the discriminant of $m(x, y)$ is

$$(d - a)^2 + 4bc = (d + a)^2 - 4(ad - bc) = t^2 - 4.$$

For a conjugate matrix $N := AMA^{-1}$ where $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbf{Z})$, write N as $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Then, the form $n(x, y) = b'x^2 + (d' - a')xy - c'y^2$ is easily seen to be $m(x', y')$ where

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A^t \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha x + \gamma y \\ \beta x + \delta y \end{pmatrix}.$$

In other words, under the above association, conjugate matrices of trace t correspond to equivalent forms of discriminant $t^2 - 4$.

Conversely, associate to a quadratic form $f(x, y) = px^2 + qxy + ry^2$ with discriminant $t^2 - 4$ (so, $q^2 - 4pr = t^2 - 4$), the matrix

$$F := \begin{pmatrix} \frac{t-q}{2} & p \\ -r & \frac{t+q}{2} \end{pmatrix} \in SL_2(\mathbf{Z}).$$

Note that indeed, $\det F = \frac{t^2-q^2}{4} + pr = 1$ and $\operatorname{trace} F = t$.

Further, look at any equivalent form $f'(x, y) = f(ax + by, cx + dy)$ with $M := \begin{pmatrix} a & b \\ c & d \in SL_2(\mathbf{Z}) \end{pmatrix}$.

Write $f'(x, y) = p'x^2 + q'xy + r'y^2$.

Then, we compute and see that

$$M^t F (M^t)^{-1} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} \frac{t-q}{2} & p \\ -r & \frac{t+q}{2} \end{pmatrix} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = \begin{pmatrix} \frac{t'-q'}{2} & p' \\ -r' & \frac{t'+q'}{2} \end{pmatrix},$$

which shows that the corresponding matrices are conjugate in $SL_2(\mathbf{Z})$.

The above associations are inverse to each other and proves the proposition.

Remarks. The above association is also useful in deciding if two matrices are conjugate in $SL_2(\mathbf{Z})$ or not. For instance, the matrices $\begin{pmatrix} 1 & 3 \\ 3 & 10, \end{pmatrix}$ $\begin{pmatrix} 1 & 1 \\ 9 & 10 \end{pmatrix}$ which have trace 11 are associated to the quadratic forms

$$3x^2 + 9xy - 3y^2 \ , x^2 + 9xy - 9y^2,$$

respectively. However, they are evidently in-equivalent because the first one takes only multiples of 3 as values whereas the second one takes values like 1 at $(x, y) = (1, 0)$.

12. Average of Euler's ϕ-function

Euler's ϕ-function, denoted by $\phi(n)$ is an arithmetic function defined on natural numbers that counts the number of natural numbers $1 \leq m \leq n$ with $(m, n) = 1$. Euler gave a formula which can be proved using inclusion – exclusion principle as follows.

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

where the product varies over all the distinct prime divisors. This formula shows that the functional value fluctuates a lot.

In analytic number theory, to study such fluctuating arithmetical functions, one often looks at their *average behaviour*. One can prove that the average value from 1 to x is $\frac{3}{\pi^2}x$ but the interesting part is to have an idea of the error which would be introduced if we take this value. In analytic number theory, this methodology of '*determining the main term and estimating the error term*' is fundamental because we cannot deduce anything concrete if the error term is of the same order as the main term! One has

$$\sum_{1 \leq n \leq x} \phi(n) = \frac{3}{\pi^2}x^2 + E(x),$$

where $E(x)$ is the remainder or error term in the average.

Dirichlet showed that for any given $\epsilon > 0$, there is a constant $C > 0$ so that $|E(x)| \leq Cx^{1+\epsilon}$ for all $x > 0$. Later, this was improved to $|E(x)| \leq C'x \log x$ for all $x > 0$ by Mertens.

Sylvester prepared a table of values for $\sum_{n \leq x} \phi(n)$ and $\frac{3}{\pi^2}x^2$ for all $x = 1, 2, \cdots, 1000$. However, he failed to notice that $E(820) < 0$ and made a conjecture that $E(x) \geq 0$ for all x. In 1929, Chowla wrote a letter to Pillai where he predicted that $E(x) > 0$ for infinitely many values of x and $E(x) < 0$ for infinitely many values of x.

In order to prove an error term, say $|E(x)| \leq cg(x)$, is tight for some non-negative function $g(x)$, one needs to produce a positive constant c_0 and infinitely many x's such that $|E(x)| > c_0 g(x)$.

Such a result is called an *'omega'-result* in analytic number theory; *we write* $E(x) = \Omega(g(x))$.

Chowla and Pillai showed that $E(x) = \Omega(x \log\log\log x)$.

Such a result took many years to generalize. There is a conjecture by Montgomery that

$$E(x) = O(x \log\log x) \text{ and } E(x) = \Omega_{\pm}(x \log\log x),$$

which is still open.

13. A Variant of Tic-Tac-Toe!

In 1933, Pillai studied a variant of Tic-Tac-Toe game as follows. Let $n \geq 3$ be an integer and $t \leq n$ be another integer. Suppose $n \times n$ grid with n^2 squares is given in the plane. Let P and Q be two players playing. By turns each mark a square. The rule of playing the game is as follows. Suppose P is the starter and, let P_r and Q_r be the squares marked respectively by P and Q during their r-th turns. After P's (or Q's) s-th turns, whoever marked t squares in a straight line wins the game.

Pillai proves that when $t = n$ and the game is carefully played, then it will end always in a draw. However, if $t < n$, then for a given t, there is a function $f(n)$ depending on n such that if $t \geq f(n)$, then the game ends in a draw. When $t < f(n)$, he proved that the player who starts will win. Also, he proved that $f(n) \leq n + 1 - \sqrt{n/6}$ and $f(n) = n$ for all $n = 3, 4, 5,$ and 6. For large values of n, the correct order of $f(n)$ is still unknown!

14. Smooth Numbers

Smooth numbers are numbers which have only 'small' prime factors. For example, 1,620 has prime factorization $2^2 \times 3^4 \times 5$; therefore 1620 is 5-smooth because none of its prime factors is greater than 5. Smooth numbers have a number of applications to cryptography. For example, the very smooth hash functions are used constructively to get a provably secure design. They also play a role in music theory apparently (Longuet–Higgins, H C, Letter to a musical friend, *Music Review* (August: 244-248), 1962!)

For other applications, the interested reader may also consult [18] and [19].

For any real numbers $x, y > 1$ with $y \leq x$, we define $\psi(x, y)$ to be the number of positive integers $t \leq x$ such that if a prime $p|t$, then $p \leq y$. In other words, $\psi(x, y)$ counts all the y-smooth numbers up to x. Ramanujan (in a letter to Hardy) was the first to study these smooth numbers when $y = 3$(!)

He obtained a nice asymptotic formula for $\psi(x, 3)$.

In the 7-th conference of Indian Mathematical Society during 3–5, April, 1931 at Trivandrum, Pillai extended the above result of Ramanujan which implies an asymptotic formula for $\psi(x, y)$ if $y > 1$ is a fixed real number. This is technical to state but we mention it here in passing, for the interested reader:

If $p_1, p_2, \cdots, p_r \leq y$ are all the prime numbers less than y, then

$$\frac{\psi(x,y) - \frac{(\log x)^r}{r! \prod_{i=1}^r \log p_i} + \frac{(\log x)^{r-1} \log(p_1 \cdots p_r)}{2(r-1)! \prod_{i=1}^r \log p_i})}{\log^{r-1} x} \to 0$$

when $x \to \infty$.

Around that time, Dickman obtained an asymptotic result for $\psi(y^u, y)$ for any fixed $u > 0$. The word 'asymptotic' here refers to an assertion of the form 'what is the limit of $\frac{\psi(y^u,y)}{y^u}$ as $u \to \infty$'?

A more rigorous proof of Dickman's result, in modern standards, was supplied by Chowla and T Vijayaraghavan in 1947 where they used an unpublished result of Pillai which is more general than the above result of Pillai!

It should be mentioned that Ramanujan – see page 337 of S Ramanujan, *The lost notebook and other unpublished papers*. Narosa Publishing House, (1988) – had the following entry. We write in the standard notations as above:

$$\psi(x, x^c) \sim x\left(1 - \int_c^1 \frac{du}{u}\right) \text{ if } 1/2 \le c \le 1;$$

$$\psi(x, x^c) \sim x\left(1 - \int_c^1 \frac{du}{u} + \int_c^{1/2} \frac{dv}{v}\int_v^{1-v} \frac{du}{u}\right) \text{ if } 1/3 \le c \le 1/2;$$

$$\psi(x, x^c) \sim x\left(1 - \int_c^1 \frac{du}{u} + \int_c^{1/2} \frac{dv}{v}\int_v^{1-v} \frac{du}{u} - \int_c^{1/3} \frac{dz}{z}\int_z^{(1-z)/2} \frac{dv}{v}\int_v^{1-v} \frac{du}{u}\right)$$

if $1/4 \le c \le 1/3$*; and so on.*

This is nothing else than Dickman's asymptotic formula for $\psi(x, y)$!

15. Chowla's Argument and the Langlands Conjecture

In this last section, we mention how an argument due to Chowla plays a role in the famous Langlands conjectures. The cognoscenti would know that the latter conjectures drive much of the contemporary research in number theory [20].

This section is mostly taken from a lecture of Professor Ram Murty at Kerala School of Mathematics, Calicut – thanks go to Professor Ram Murty for allowing inclusion of the contents in this write up.

For each integer $n \ge 1$, define $d(n)$ is the number of positive divisors of n. In his famous paper on 'highly composite numbers', Ramanujan gave an upper bound for the function $d(n)$ as follows:

$$d(N) \le 2^{\frac{\log N}{\log\log N}} \text{ for all } N \ge 2$$

and he produced infinitely many integers N for which the above bound is attained.

For any given $\epsilon > 0$, we can deduce from the above upper bound that there is a constant N_0 depending on ϵ so that

$$d(N) \le N^\epsilon \text{ for all } N \ge N_0.$$

Chowla proved this deduction using another argument involving Dirichlet series.

Let $r \geq 1$ be any integer and let

$$L_r(s) = \sum_{n=1}^{\infty} \frac{d^r(n)}{n^s} \text{ where } s \in \mathbf{C} \text{ with } \Re(s) > 1.$$

Chowla observed that the series

$$L_r(s) = \prod_p \left(1 + \frac{2^r}{p^s} + \frac{3^r}{p^{2s}} + \cdots\right)$$

(where the product runs over all the prime numbers) converges absolutely for $\mathrm{Re}(s) > 1$ for all $r \geq 1$. In particular, when $s = 2$, this series converges. So,

$$\sum_{n=1}^{\infty} \frac{d(n)^r}{n^2} < \infty \text{ for all integers } r \geq 1.$$

Therefore, the n-th term which is $\dfrac{d(n)^r}{n^2}$ tends to zero. In particular, it is bounded for all large enough n's. Thus, we get

$$d(n)^r \leq cn^2 \text{ for all } n \geq M$$

for some $M > 0$ and $c > 0$ constants and this is true for all $r \geq 1$.

Thus, for all $n \geq M$, we get $d(n) \leq c^{1/r} n^{2/r}$. Also, note that $c^{1/r} \to 1$ as $r \to \infty$.

Given $\epsilon > 0$, we can find r_0 such that $2/r < \epsilon$ for all $r \geq r_0$ and we get $d(n) \leq n^{\epsilon}$.

To show how this sort of argument plays a role in the famous Langlands conjectures, we describe such a conjecture. This can be done through the famous Ramanujan delta function. Ramanujan studied the following q-series

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} \text{ where } z \in \mathbf{C} \text{ with } \Im(z) > 0; q = e^{2\pi i z}$$

which is often called Ramanujan's delta function because of his fundamental contribution to it although it was already studied by Jacobi and others.

The delta function satisfies the following property:

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $\in SL_2(\mathbf{Z})$ *(that is, for integers* a, b, c, d *with* $ad - bc = 1$*),*

$$\Delta\left(\frac{az + b}{cz + d}\right) = (cz + d)^{12} \Delta(z).$$

Since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbf{Z})$ and by the above relation, we see that $\Delta(z+1) = \Delta(z)$ and hence Δ function is a periodic function.

Therefore, it has a Fourier expansion. It can be proved that the Fourier expansion of $\Delta(z)$ is

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n) e^{2i\pi nz},$$

where $\tau(n)$ is the Fourier coefficients which are integers.

Traditionally, one writes $q = e^{2i\pi z}$ so that $\Delta(z) = \sum_{n=1}^{\infty} \tau(n) q^n$.

Ramanujan computed the initial τ values and conjectured the following relations.

1. $\tau(mn) = \tau(m)\tau(n)$ whenever $(m, n) = 1$.
2. $\tau(p^{a+1}) = \tau(p)\tau(p^a) - p^{11}\tau(p^{a-1})$ for all primes p and $a \geq 1$.
3. $|\tau(p)| < 2p^{11/2}$ for every prime p.

The first two conjectures were proved by Mordell in 1917 and the third one was proved by P Deligne in 1975 using deep algebraic geometry.

Note that the third conjecture of Ramanujan is equivalent to the assertion:

$$\tau(n) = O(n^{\frac{11}{2}+\epsilon})$$

for any given $\epsilon > 0$.

Our interest is in this version of Ramanujan's conjecture.

Let us define for each integer $n \geq 1$,

$$\tau_n = \tau(n)/n^{11/2}.$$

Then Ramanujan's conjecture is equivalent to $\tau_n = O(n^{\epsilon})$ for any given $\epsilon > 0$. Define the L-series attached to Δ function as

$$L(s, \Delta) = \sum_{n=1}^{\infty} \frac{\tau_n}{n^s},$$

where $s \in \mathbf{C}$ with $\Im(s) > 0$.

Since $\tau(n)$ is a multiplicative function (the first conjecture of Ramanujan mentioned above and proved by Mordell), we see that τ_n^r is also a multiplicative function and hence we get

$$L(s, \Delta) = \prod_p \left(1 + \frac{\tau_p}{p^s} + \frac{\tau_{p^2}}{p^{2s}} + \cdots\right).$$

Using the second conjecture of Ramanujan, one notes that for all primes p, we have

$$\sum_{a=0}^{\infty} \tau_{p^a} X^a = \frac{1}{1 - \tau_p X + X^2} = \frac{1}{(1 - \alpha_p X)(1 - \beta_p X)},$$

where α_p and β_p are the complex roots of $X^2 - \tau_p X + 1$. Note that $\alpha_p + \beta_p = \tau_p$ and $\alpha_p \beta_p = 1$.

$$L(s,\Delta) = \prod_p \left(1 - \frac{\alpha_p}{p^s}\right)^{-1} \left(1 - \frac{\beta_p}{p^s}\right)^{-1} = \prod_p \prod_{m=0}^{1} \left(1 - \frac{\alpha_p^{1-m}\beta_p^m}{p^s}\right)^{-1}.$$

For any $r \geq 1$, Langlands defined the function:

$$L_r(s,\Delta) = \prod_p \prod_{m=0}^{r} \left(1 - \frac{\alpha_p^{r-m}\beta_p^m}{p^s}\right)^{-1}.$$

He conjectured that for every $r \geq 1$, $L_r(s,\Delta)$ defines a series which is absolutely convergent for $\Re(s) > 1$.

Note that the Dirichlet series

$$S_r := \sum_{n=1}^{\infty} \frac{\tau_n^{2r}}{n^s}$$

can be written as a product of the $L_k(s,\Delta)$ for $k \leq r$. Therefore, if the conjecture of Langlands is true, then S_r converges absolutely for $\Re(s) > 1$ for every $r \geq 1$. This implies, by Chowla's argument, that

$$\frac{\tau_n^{2r}}{n^2} \leq C \iff \tau_n \leq C^{1/2r} n^{1/r}$$

for all $n \geq n_0$. Thus, we arrive at $\tau_n = O(n^\epsilon)$ for any given $\epsilon > 0$ (!). However, at present Langlands's conjecture is known only for all $r \leq 9$.

Collected works of Chowla and of Pillai:

The collected works of Chowla and of Pillai contain unpublished papers also. The interested readers can look at:

- *Collected works of S Chowla*, Vol.1,2,3, Edited by James G Huard and Kenneth S Williams, CRM Univ. de Montreal, 1999.
- *Collected works of S S Pillai*, Edited by R Balasubramanian and R Thangadurai, Ramanujan Mathematical Society Collected Works Series, 2010.

References

[1] B Sury, Box 1, *Resonance*, **Vol. 9**, No. 6, 2004.
[2] Waring's problem and the circle method, *Resonance*, **Vol. 9**, No. 6, pp.51–55, 2004.

[3] G H Hardy and E M Wright, *An introduction to the theory of numbers,* Oxford Univ. Press, third ed., 1954.

[4] S Chowla, The least prime quadratic residue and the class number, *J. Number Theory*, **22**, 1–3, 1986.

[5] S Chowla, On a conjecture of Ramanujan, *Tohoku Math. J.* **33**, 1–2, 1930.

[6] S Chowla and P Chowla, Some unsolved problems, *Norske Vid. Selsk. Forth.* (Trondheim), p.7, 1986.

[7] D Thakur, A note on numerators of Bernoulli numbers, *Proc. Amer. Math. Soc.*, Electronically published on 24.02.2012.

[8] S S Pillai, On a linear diophantine equation, *Proc. Indian Acad. Sci.* A, **12**, pp.199–201, 1940.

[9] S S Pillai, On the inequality $0 < a^x - b^y \leq n$, *Journal Indian M. S.,* **19**, pp. 1–11, 1931.

[10] S Chowla, The nonexistence of nontrivial linear relations between the roots of a certain irreducible equation, *J. Number Theory*, **2**, 120–123, 1970.

[11] Kai Wang, On a theorem of Chowla, *J. Number Theory*, **15**, 1–4, 1982.

[12] Raymond Ayoub, On a theorem of Chowla, *J. Number Theory*, **7**, 108–120, 1975.

[13] S Chowla, I N Herstein and W R Scott, The solutions of $x^d = 1$ in symmetric groups, *Norske Vid. Selsk. Forth.* (Trondheim) **25**, 29–31, 1952.

[14] L Euler, De Formulis specei $mxx + nyy$ ad numeros primos explorandos idoneis earumque mirabilis proprietatibus, *Opera Omnia* I, **v. 4**, Teubner, pp. 269–289, 1916.

[15] G Frei, Leonhard Euler's convenient numbers, *Math. Intell.*, **7**, No. 3, 55–58, 64, 1985.

[16] S Chowla, An extension of Heilbronn's class-number theorem, *Quart. J. Math.*, **5**, 304–307, 1934.

[17] S Chowla, J Cowles and M Cowles, *J.Number Theory*, **12**, 372–377, 1980.

[18] A Granville, Smooth numbers: Computational number theory and beyond, *Proceedings of an MSRI workshop*, 2004.

[19] A Hildebrand and G Tenenbaum, Integers without large prime factors, *J. Theor. Nombres Bordeaux*, **5**, No. 2, 411–484, 1993.

[20] Ram Murty, *Topics in Number Theory*, Mehta Research Institute Lecture Note No. 1, 1993.

Multi-variable Chinese Remainder Theorem

1. Introduction

The Chinese remainder theorem (CRT) seems to have originated in the 3rd century AD in the work of Sun-Tsu. There are also versions in Indian 5th century mathematics of Aryabhata. The classical versions dealt with coprime moduli. Oystein Ore proved a version [1] for non-coprime moduli in 1952 in the *American Mathematical Monthly* but, this does not seem to be well-known because a paper published 50 years later by Howard [2] proves the same result! However, a multi-variable version does not seem to be known. We present such a version and point out that there are still many questions open for investigation.

2. Classical CRT

A variant of a folklore tale goes as follows. Three thieves steal a number of gold coins and go to sleep after burying the loot. During the night, one thief wakes up and digs up the coins and, after distributing into 6 equal piles, finds 1 coin left over which he pockets quietly after burying the rest of the coins. He goes back to sleep and after a while, a second thief wakes up and digs up the coins. After making 5 equal piles, he again finds 1 coin left over which he pockets and buries the rest and goes to sleep. The 3rd thief wakes up and finds the rest of the coins make 7 equal piles excepting a coin which he pockets. If the total number of coins they stole is not more than 200, what is the exact number?

With a bit of hit and trial, one can find that 157 is a possible number. The Chinese remainder theorem gives a systematic way of solving this in general.

In the above problem, the sought-for natural number N is so that $N-1$ is a multiple of 6, $N-2$ is a multiple of 5 and $N-3$ is a multiple of 7. This means that N leaves *remainders* $1, 2, 3$ on division by $6, 5, 7$ respectively.

Let us consider two coprime natural numbers m_1, m_2 and suppose, we are looking for a natural number N which leaves remainders a_1, a_2 on division by m_1, m_2 respectively. Then, the Euclidean division algorithm tells us that

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 20, No. 3, pp. 206–216, March 2015.

the smallest positive integer of the form $m_1k_1 + m_2k_2$ (for integers k_1, k_2) is the greatest common divisor (GCD) of m_1 and m_2 (which is 1 in this case). Therefore, we have integers (of opposite signs) k_1, k_2 such that

$$m_1k_1 + m_2k_2 = 1.$$

The number

$$N = a_1m_2k_2 + a_2m_1k_1$$

has the property that $(N-a_1)$ is a multiple of m_1 and $(N-a_2)$ is a multiple of m_2. We have not yet got a number as sought since N could be negative. However, we may add a suitable multiple of m_1m_2 to N and that will satisfy the requirements.

More generally, suppose there are r natural numbers $m_1, \cdots, m_r$ which are pairwise coprime. We seek a natural number N leaving given remainders $a_1, \cdots, a_r$ on divisions by $m_1, \cdots, m_r$ respectively. An appropriate generalization of the above argument for two numbers is the following. If M_i denotes the product of all the m_j's excepting m_i, then the GCD of m_i and M_i is 1 for each $i = 1, \cdots, r$. As above, the Euclidean algorithm gives integers n_i, k_i such that

$$n_iM_i + k_im_i = 1,$$

for each $i = 1, \cdots, r$.

We have therefore, $a_in_iM_i - a_i$ is a multiple of m_i for each $i \leq r$.

As m_i divides M_j for each $j \neq i$, the integer

$$N = a_1n_1M_1 + a_2n_2M_2 + \cdots + a_rn_rM_r,$$

is such that $(N - a_i)$ is a multiple of m_i for each $i \leq r$. Adding a suitable multiple of $m_1m_2 \cdots m_r$, we can get a natural number N such that N leaves the remainder a_i on division by m_i for each $i \leq r$.

Note that any other natural number N_0 satisfying the same property must differ from N by a multiple of each m_i and hence, of the product $m_1m_2 \cdots m_r$.

In other words, there is a unique solution for N in the range $[1, m_1m_2 \cdots m_r]$.

Here is a nice exercise.

If $m_1, \cdots, m_r$ are natural numbers which are not necessarily pairwise coprime, then there is a natural number N yielding given remainders a_i on division by m_i if, and only if, the GCD of m_i and m_j divides $a_i - a_j$ for each i, j.

2.1 Gauss and Congruences

The great mathematician C F Gauss defined the algebraic notion of 'congruence' which generalizes the notion of equality of numbers and

dramatically simplifies the proofs of several number-theoretic results. Given a natural number m, one says two integers x and y are '*congruent modulo* m' – written $x \equiv y \mod m$ – if $x - y$ is an integral multiple of m.

Not surprisingly, the notation is also due to Gauss! Congruences to a fixed modulus behave much like equality. For instance, it is very easy to verify:

$$x_1 \equiv y_1 \mod m \ , \ x_2 \equiv y_2 \mod m$$

implies

$$x_1 + x_2 \equiv y_1 + y_2 \mod m \ , x_1 x_2 \equiv y_1 y_2 \mod m.$$

Further, we note that negative numbers are dealt with on equal footing; a statement such as x leaves a remainder 3 on division by 4 can be written as $x \equiv -1 \bmod 4$ as well. Note that if x leaves a remainder 3 on division by 4, then x^{2013} leaves the same remainder and, this is easier to see via congruences because

$$x \equiv -1 \bmod 4 \Rightarrow x^{2013} \equiv (-1)^{2013} = -1 \equiv 3 \bmod 4.$$

The argument that for two coprime integers m, n, $1 = mu + nv$ for integers u, v from the Euclidean division algorithm, can also be rephrased as asserting that '*Each of the two integers has a multiplicative inverse modulo the other*'. That is, there exists an integer u (unique mod n – meaning unique up to adding multiples of n) such that $mu \equiv 1 \bmod n$ and, similarly, there is an integer v (unique mod m) such that $nv \equiv 1 \bmod m$.

We call u '*the* multiplicative inverse of m mod n' keeping in mind that it is defined only up to addition of multiples of n.

The calculus of congruences is highly efficient in formulating and solving problems in elementary number theory. For instance, given a number with the digits $d_1 d_2 \cdots d_k$ in base 10, its remainder on division by 9 is simply that of the sum $\sum_{i=1}^{k} d_i$. Note that the given number could be as large as 10^{r-1} while the sum of its digits is at the most $9r$ which is much smaller for large r; this reduces computation drastically.

In the language of congruences, the classical Chinese remainder theorem we proved above can be recast as follows:

(Explicit) Chinese Remainder Theorem: *Let $m_1, \cdots, m_r$ are pairwise coprime natural numbers, and a_i $(1 \leq i \leq r)$ be arbitrary integers. Write $M_i = \prod_{j \neq i} m_j$. Let n_i be the multiplicative inverse of M_i* mod*ulo m_i. Then, the unique solution N* mod *$m_1 m_2 \cdots m_r$ to the system of congruences $N \equiv a_i \bmod m_i$ for all $i \leq r$ is given by*

$$N = a_1 n_1 M_1 + a_2 n_2 M_2 + \cdots + a_r n_r M_r.$$

3. Many Variable CRT

Let us observe first that if c is an integer coprime to m and d is its multiplicative inverse modulo m, then $x = da$ is a solution to a congruence $cx \equiv a \bmod m$. Therefore, the classical CRT can be formulated also as a system of congruences of the form $c_i x \equiv a_i \bmod m_i$ $(1 \leq i \leq r)$ where $(c_i, m_i) = 1$ for each i; the solution above changes to $N = \sum_{i=1}^{r} d_i a_i n_i M_i$ where $c_i d_i \equiv 1 \bmod m_i$. Thus, it is easy to formulate a multivariable version where the left hand sides are linear polynomials in several variables x_i's instead of a single one. However, we soon realize that a necessary and sufficient condition of the existence of a solution in general is far from obvious. We formulate and prove the following multivariable version and analyze later what else needs to be done.

Theorem. *Let k, n be arbitrary positive integers and suppose a_{ij} are integers (for $1 \leq i \leq k, 1 \leq j \leq n$). Suppose $m_1, \cdots, m_k$ are pairwise coprime integers and $b_1, \cdots, b_r$ be arbitrary integers. Then, the k simultaneous congruences*

$$\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &\equiv b_1 \pmod{m_1},\\
a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &\equiv b_2 \pmod{m_2},\\
&\cdots\cdots\cdots\cdots\\
a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n &\equiv b_k \pmod{m_k}
\end{aligned}$$

have a solution in integers $x_1, \cdots, x_n$ if and only if, for each $i \leq k$, the GCD of $a_{i1}, a_{i2}, \cdots, a_{in}, m_i$ divides b_i.

Proof. We apply induction on k to prove the theorem. The proof is constructive modulo the Euclidean division algorithm (which is also constructive).

Consider first the case $k = 1$.

If the integers $x_1, \cdots, x_n$ satisfy the congruence

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 \pmod{m_1},$$

we have $\sum_{j=1}^{n} a_{1j}x_j - b_1 = m_1 t$ for some integer t. Thus, the greatest common divisor of $a_{11}, a_{12}, \cdots, a_{1n}$ and m_1 divides b_1. This condition is also sufficient by the Euclidean division algorithm. For, if $b_1 = sd$ where $d = \mathrm{GCD}(a_{11}, \cdots, a_{1n}, m_1)$, then writing

$$d = \sum_{j=1}^{n} a_{1j}y_j + m_1 t,$$

we have a solution $x_1 = sy_1, \cdots, x_n = sy_n$ of the congruence

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \equiv b_1 \pmod{m_1}.$$

Therefore, for a general k, a necessary condition for a common solution is that, for each $i \leq k$, the GCD of $a_{i1}, a_{i2}, \cdots, a_{in}, m_i$ divides b_i.

This condition also ensures that each individual congruence has a solution.

Now, we suppose that the GCD condition holds and that we have already arrived at a common solution $x_1, \cdots, x_n$ in integers for the first r congruences ($1 \leq r < k$):

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n \equiv b_i \pmod{m_i} \quad \forall \quad 1 \leq i \leq r.$$

Now, we first choose a solution $y_1, \cdots, y_n$ of the $(r+1)$-th congruence

$$a_{r+1,1}x_1 + a_{r+1,2}x_2 + \cdots + a_{r+1,n}x_n \equiv b_{r+1} \pmod{m_{r+1}}.$$

For each $j \leq n$, choose X_j such that

$$m_1 m_2 \cdots m_r X_j \equiv y_j - x_j \pmod{m_{r+1}}.$$

These choices are possible because $m_1 m_2 \cdots m_r$ and m_{r+1} relatively prime. We observe that for the new choices

$$x'_j = x_j + m_1 m_2 \cdots m_r X_j \quad (1 \leq j \leq n),$$

the first r congruences continue to hold. Moreover,

$$\begin{aligned} \sum_{j=1}^{n} a_{r+1,j} x'_j &\equiv \sum_{j=1}^{n} a_{r+1,j}(x_j + m_1 m_2 \cdots m_r X_j) \\ &\equiv \sum_{j=1}^{n} a_{r+1,j} y_j \equiv b_{r+1} \pmod{m_{r+1}}. \end{aligned}$$

Therefore, the theorem is proved by induction.

Remarks.

(i) The classical Chinese remainder theorem can be thought of as the special case when the matrix $\{a_{ij}\}$ has only a single column which is non-zero.

(ii) If the matrix $\{a_{ij}\}$ has a left inverse (that is an $n \times k$ integer matrix $\{b_{ij}\}$ such that $BA = I_n$, then clearly the necessary condition of the theorem holds for any choice of $b_1, \cdots, b_k$.

In particular, if $k = n$ and $\{a_{ij}\}$ is in $GL(n, \mathbf{Z})$, each system of n linear congruences in n variables with pairwise co-prime moduli has a solution.

(iii) A special case of the above theorem which is of interest as it produces a solution for arbitrary b_i's, is the following one. In the theorem above,

if, for each $i \leq k$, there is some j for which a_{ij} is coprime to m_i, then the necessary condition obviously holds.

(iv) In the classical case of one variable, there is a unique solution modulo $m_1 m_2 \cdots m_k$. In the multivariable case, there is no natural uniqueness assertion possible. The point is that homogeneous congruences in more than one variable have many solutions. So, uniqueness can be asked for only after specifying a box (more precisely, an n-dimensional parallelotope) in which we seek solutions.

For example, both $(1, 4)$ and $(0, -1)$ are simultaneous solutions of the congruences

$$x - y \equiv 1 \pmod{2},$$

$$x + y \equiv 2 \pmod{3}.$$

(v) The Euclidean division algorithm is the principal reason behind these classical versions of the Chinese remainder theorem. In particular, it holds good over the polynomial ring in one variable over a field. If n elements are coprime, then there is a linear combination which gives 1. This is no longer if we consider, for instance, polynomials in two variables.

For example, in the polynomial ring $\mathbf{C}[X, Y]$, consider the congruences

$$t \equiv 0 \pmod{X},$$

$$t \equiv 1 \pmod{Y}.$$

Here, of course, by a congruence $f(X, Y) \equiv g(X, Y) \bmod h(X, Y)$, we mean that there is a polynomial $k(X, Y)$ so that

$$h(X, Y)k(X, Y) = f(X, Y) - g(X, Y).$$

There is no common solution of the two congruences mentioned above as there do not exist polynomials f, g for which $Xf + Yg = 1$!.

(vi) The Chinese remainder theorem has been generalized to rings and modules. But, none of the versions is an analogue of the many variable case proved above.

4. General Moduli for Multivariable CRT

Here, we point out a criterion which is sufficient to ensure the existence of a solution when the moduli m_i's are general (that is, not necessarily pairwise coprime).

The case of general moduli is equivalent to a system of congruences for prime power moduli. By the above theorem, we need to look at only the case when all the moduli are powers of a single prime p. If we can get a necessary

and sufficient criterion for these cases, we will get such a criterion for the general case. In this section, we fix a prime p and moduli $m_i = p^{t_i}$. We further consider only the special case of n congruences in n variables. That is, let us look at an $n \times n$ integer matrix $A = \{a_{ij}\}$ and at the corresponding system of congruences

$$\sum_{j=1}^{n} a_{ij}x_j \equiv b_i \pmod{p^{t_i}} \quad \forall \quad i \leq n.$$

We write $b_i = p^{\beta_i}u_i'$ and $\det(A) = p^{\delta}d$ where u_i', d are not divisible by p. A sufficient criterion is the following one:

Lemma. If $\delta \leq \beta_i \leq t_i$ for all $i \leq n$, then the simultaneous system of congruences above has a common solution.

Proof. The proof is straight forward.

Write the system of congruences as an equality $Ax = b + mu$ for some $u_1, \cdots, u_n$, where we have written x, b, m as columns and where x, u need to be shown to exist. Here m is the column $(p^{t_1}, p^{t_2}, \cdots, p^{t_n})^t$.

If $B = adj(A)$, the adjoint matrix of A, then multiplying the matrix equation on the left by $B = \{b_{ij}\}$, we have $\det(A)x = B(b + mu)$ i.e.

$$p^{\delta}dx_i = \sum_{j=1}^{n} b_{ij}(p^{\beta_j}u_j' + p^{t_j}u_j) \ \forall \ i \leq n.$$

By the hypothesis, the equality below has all entries to be integers:

$$dx_i = \sum_{j=1}^{n} b_{ij}(p^{\beta_j-\delta}u_j' + p^{t_j-\delta}u_j) = \sum_{j=1}^{n} b_{ij}p^{\beta_j-\delta}(u_j' + p^{t_j-\beta_j}u_j) \quad \forall \quad i \leq n.$$

As $(p, d) = 1$, we may choose u_j's satisfying

$$p^{t_j-\beta_j}u_j \equiv -u_j' \pmod{d} \quad \forall \quad j.$$

Write $u_j' + p^{t_j-\beta_j}u_j = dy_j$ for $j \leq n$; then, we have

$$x_i = \sum_{j=1}^{n} b_{ij}p^{\beta_j-\delta}y_j \quad \forall \quad i \leq n.$$

Hence, we have a simultaneous solution to the congruences.

5. A Question for Investigation

Although sufficient conditions such as the one above can be formulated, it is not clear (unlike the single variable case) how to formulate a general necessary and sufficient condition for the multivariable Chinese remainder theorem when the moduli are not necessarily pairwise coprime.

References

[1] Oystein Ore, The general Chinese remainder theorem, *The American Mathematical Monthly*, **Vol. 59**, No. 6, 1952.

[2] Fredric T Howard, A Generalized Chinese Remainder Theorem, *The College Mathematics Journal*, **Vol. 33**, No. 4, pp. 279–282, September 2002.

Which Positive Integers are Interesting?

To Ramanujan, each number was a personal friend
in whose company, a lifetime he did spend.
Let us too begin this quest
to befriend numbers of interest.
A friend of a friend is a friend, may we not pretend?!

Much has been written about the numbers π and e (which are themselves related by the beautiful identity $e^{i\pi} = -1$). However, if we are to think of only those interesting numbers which are positive integers, each of us comes with her or his own list. Indeed, the question "which positive integers are interesting?" is not well-defined for, if n were the smallest uninteresting positive integer, it is interesting for that reason! Be that as it may, we identify some positive integers which have certain unique characteristics. In some of these examples, this number is unique with those characteristics and, in other cases, it is the smallest or the largest positive integer encountered where a pattern changes, although there may be other numbers with those characteristics. We also use our discussion as an excuse to unveil interesting mathematics behind some of these phenomena. The numbers are not necessarily arranged according to size.

30031

We are exposed to a beautiful thought process in school when we learn Euclid's proof of the infinitude of primes. Recall that the argument proceeds by observing that once we have gotten hold of the first few prime numbers, the number obtained by adding 1 to their product must have a prime factor which must necessarily be larger than the previous ones. As this large number leaves remainder 1 on division by any of these primes, any of its prime factors is larger than the previous primes (and hence gives a new prime). The '*hope*' (if one may call it that) that this new number is itself a prime, leads quickly to disillusionment. The first example is $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031$. I leave it to the reader to find the prime factors of this number. The intriguing question as to whether we do get primes infinitely often in this process is still open! The largest known prime P for which the product of all the primes until P is 1 less than a prime number is 42209.

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 20, No. 8, pp. 680–698, August 2015.

In the above proof of infinitude of primes, we used the sequence of numbers of the form $2 \times 3 \times \cdots p_n + 1$. One could as well have used the sequence $2 \times 3 \times \cdots p_n - 1$ instead. In that case, $2 \times 3 \times 5 \times 7 - 1 = 11 \times 19$ is composite. Once again, it is unknown whether there are infinitely many primes of this form.

Let us pause for a moment to mull over an irony – *among all numbers of the form* $2 \times 3 \times \cdots p_n + 1$*, it is certain that either we have infinitely many primes or infinitely many composite numbers but, we do not know the answer to either of these at present!*

561

In cryptography, one of the recurring themes is the employment of the so-called Fermat little theorem – *If* p *is a prime number and* a *is an integer which is not a multiple of* p*, the number* $a^{p-1} - 1$ *is a multiple of* p.

The thought that this property might characterize all primes perishes soon. There are composite positive integers n such that every positive integer a co-prime to n possesses the property that $a^{n-1} - 1$ is a multiple of n. Such numbers – now known as Carmichael numbers – have a characterizing property. This is the property:

n is a Carmichael number if and only if it is square-free and each prime divisor p of n satisfies $p - 1$ divides $n - 1$.

Look at 'Prime ordeal', *Resonance*, pp.866-881, September 2008, for a proof.

The smallest Carmichael number is 561. Indeed, $561 = 3 \times 11 \times 17$ and $560 = 16 \times 5 \times 7$.

If a is relatively prime to 561, then $a^{560} - 1$ has factors $a^2 - 1, a^{10} - 1, a^{16} - 1$ which are multiples of $3, 11, 17$ respectively, by Fermat's little theorem.

15

For an integer $n > 1$, look at all its divisors including 1 and n. Let $s(n)$ denote the sum of all digits of all the divisors.

For example, $s(10) = 1 + 2 + 5 + (1 + 0) = 9$.

Let us iterate this process, that is, look at $s_2(n) = s(s(n)), s_3(n) = s(s_2(n))$ etc. In general, $s_{k+1}(n) = s(s_k(n))$.

For instance

$$\begin{aligned} s_2(10) &= s(9) = 1 + 3 + 9 = 13, \\ s_3(10) &= s(13) = 1 + 1 + 3 = 5, \\ s_4(10) &= s(5) = 1 + 5 = 6, \\ s_5(10) &= s(6) = 1 + 2 + 3 + 6 = 12, \end{aligned}$$

$$\begin{aligned}
s_6(10) &= s(12) = 1+2+3+4+6+(1+2) = 19,\\
s_7(10) &= s(19) = 1+(1+9) = 11,\\
s_8(10) &= s(11) = 1+(1+1) = 3,\\
s_9(10) &= 1+3 = 4,\\
s_{10}(10) &= s(4) = 1+2+4 = 7,\\
s_{11}(10) &= 1+7 = 8,\\
s_{12}(10) &= 1+2+4+8 = 15,\\
s_{13}(10) &= 1+3+5+(1+5) = 15.
\end{aligned}$$

Therefore, after 12 iterations, 10 leads to 15; note that 15 is a fixed point for the function s. The beautiful thing that happens is that *every* positive integer $n > 1$ leads to 15 (so, 15 is like a black hole!).

The proof is very simple. The integer n has less than $2\sqrt{n}$ divisors (for each divisor $d < \sqrt{n}$, the divisor n/d is a divisor $> \sqrt{n}$). Any positive integer m has $[\log_{10}(m)]+1$ digits (if it has d digits, then $10^{d-1} \leq m < 10^d$ which gives, on taking logs to the base 10 what is asserted). As each digit is at most 9, the sum of the digits of m is at most $9(\log_{10}(m)]+1)$. Therefore, n is a positive integer, for any divisor m of n, the sum of digits of m is at most $9([\log_{10}(n)]+1)$ which gives

$$s(n) < 18\sqrt{n}([\log_{10}(n)]+1).$$

Using this, we get $s(n) < n$ if $n \geq 10^4$.

For $n < 10^4$, we can use a better upper bound for the number of divisors of n to again deduce $s(n) < n$ if $n > 15$. We leave it to the ingenuity of the reader to complete by herself the argument for proving $s(n) < n$ when $n > 15$. In fact, it turns out that $s(n) < n$ excepting the six values $16, 18, 24, 28, 36, 48$. For these six values, we have $s_2(n) < n$ excepting 18 for which $s_4(18) < 18$. Thus, by descending, it follows that one needs to check only the numbers 2 to 15. This can be done by hand. In fact, for large n, the argument shows that $s_k(n) = 15$ where k is of the order of $\log\log n$.

15 **again!**

The number 15 has a claim to fame for another reason too. To motivate it, we recall a few things. Lagrange proved that every positive integer is expressible as a sum of four squares of integers. On the other hand, Gauss proved that a natural number n is expressible as a sum of three squares of integers if and only if it is NOT of the form $4^k(8r+7)$. Indeed, Gauss was so excited about this discovery which he noted in his mathematical diary as:

"EYPHKA! $\Delta + \Delta + \Delta = n$."

It is said that this was the single discovery that turned Gauss's mind into taking up mathematics as a career although he was a great philologist as well. Fermat stated the result that a positive integer > 1 is a sum of two squares of integers if and only if, in its prime decomposition, every prime of the form $4k + 3$ appears with an even power. Ramanujan wrote down a list of 55 such 'positive forms' $ax^2 + by^2 + cz^2 + dw^2$ for positive integers a, b, c, d which he claimed were the only ones of this form which take ANY positive integer value as the variables take integer values. His list was almost perfect – the one exception $x^2 + 2y^2 + 5z^2 + 5w^2$ takes all values excepting the value 15(!)

The mathematician and puzzlist John Conway came up with the following general observation which he proved along with his student William Alan Schneeberger. Consider

$$q(x_1, x_2, \cdots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$$

in n variables which takes only strictly positive values for all real values of the variables other than $x_i = 0$ for all i (one calls it *positive-definite*), where all a_{ij}'s are integers and $a_{ij} = a_{ji}$ for $i \neq j$. They proved the remarkable theorem that if this function takes all the integer values from 1 to 15 when we consider integer values for the variables x_i, then it takes ALL integer values! Conway–Schneeberger's proof was very involved and the mathematician Manjul Bhargava who received a Fields medal in 2014 (not for this work though) came up with a much simpler proof of this result and, what is more, vastly generalized the result. Thus, 15 is special for the reason that:

If $\sum_{i,j=1}^{n} a_{ij} x_i x_j$ is positive-definite, and a_{ij} are integers such that $a_{ij} = a_{ji}$, and if all integer values from 1 *to* 15 *occur as values of the form when evaluated at suitable integers $x_1, x_2, \cdots, x_n$ then ALL positive integers occur as values. Moreover,* 15 *is the smallest such number.*

1729

Any list of interesting positive integers is likely to include the taxicab number 1729. The story of Ramanujan coming up with the observation that 1729 is the smallest positive integer which is the sum of two perfect cubes in two different ways

$$10^3 + 9^3 = 1729 = 12^3 + 1^3,$$

is too well-documented to repeat here. However, what may not be so well-known is that 1729 is also a Carmichael number! Indeed, $1729 = 7 \times 13 \times 19$ and $1728 = 2^6 \times 3^3$. If a is coprime to 1729, then $a^{1728} - 1$ has factors

$a^6-1, a^{12}-1, a^{18}-1$ which are multiples of $7, 13, 19$ respectively. So, by the criterion for Carmichael numbers mentioned during the discussion on 561 tells us that 1093 is a Carmichael number as well.

1806

This number has a very curious origin. It turns out to be the unique solution to the following problem.

Find all the even numbers n which satisfy $n = \prod_{p\ prime,(p-1)|n} p$.

Note that this means n includes ALL possible primes p for which $p-1$ divides n. Thus, numbers like $n = 2, 6$ are ruled out.

Note that n must be square-free. One easily sees that $2, 3, 6, 7, 43$ divide n. Moreover, any such n must be divisible by these numbers (and perhaps others). Because of the hypothesis that a prime $p|n$ if, and only if, $(p-1)|n$, if a new prime factor of n arises, it must be one more than a product of smaller prime factors of n. However, the above numbers cannot give a new prime because the numbers

$$2 \times 43 + 1, 2 \times 3 \times 43 + 1, 2 \times 7 \times 43 + 1, 2 \times 3 \times 7 \times 43 + 1$$

are all composite. Therefore, the unique answer to the problem is the number $2. \times 3 \times 7 \times 43 = 1806$.

The discovery/appearance of this number is due to Kellner and is in the context of Bernoulli numbers – the numerator of the n-th Bernoulli number is the above product. Thus, 1806 is the unique number n for which the numerator of B_n equals n.

6174

This was a discovery by D Kaprekar in the 1940's. Starting with any 4-digit number (other than those with identical digits), apply the following transformation. Arrange the digits in the descending order, say $a > b > c > d$. Subtract the number with the digits *dcba* from *abcd* to obtain a 4-digit number (even if it is a 3-digit number, it should be regarded as a 4-digit number with 0 in the beginning). This transformation produces after finitely many iterations (at the most 7), the number 6174 which has come to be known as the Kaprekar constant. Note that 6174 is invariant under this transformation.

Before proving that every 4-digit number leads to 6174, we should first look for such constants among 2-digit and 3-digit numbers.

It is immediately seen that any 2-digit number (other than those with identical digits) leads to the cycle

$$09 \to 81 \to 63 \to 27 \to 45 \to 09.$$

The unique 3-digit Kaprekar constant is 495. So, 495 has at least as much claim to fame as 6174 (!)

Indeed, if abc is a 3-digit number with $a \geq b \geq c$ and $a > c$, and if we write

$$abc - cba = pqr,$$

then

$$10 + c - a = r, 10 - 1 + b - b = q, a - 1 - c = p.$$

Thus, $q = 9$ and $p + r = 9$. Hence, we need to check only the numbers

$$990, 891, 792, 695, 594$$

each of which is seen to lead to 495 which is fixed by the iteration.

For a 4-digit number $abcd$ with $a \geq b \geq c \geq d$ and $a > d$, write the first iteration as $abcd - dcba = pqrs$.

Then, $10 + d - a = s$.

Now, if $b = c$, we have $r = 9+c-b = 9, q = 9+b-c = 9$ and $a-1-d = p$.

Thus, if $b = c$, we get $q = r = 9$ and $p + s = 9$ which leaves us to check only the five numbers $9990, 8991, 7992, 6993, 5994$. Each of these is easily seen to lead to 6174 which is fixed by the Kaprekar iteration.

Finally, in case $b > c$, we have

$$10 + d - a = s, 10 - 1 + c - b = r, b - 1 - c = q, a - d = p.$$

These imply $q + r = 8$ and $p + s = 10$. This means that one needs to check only the 25 numbers

$$p80s, p71s, p62s, p53s, p44s$$

for

$$(p, q) = (9, 1), (8, 2), (7, 3), (6, 4), (5, 5).$$

Each of these leads to 6174.

After this, we could go in two different directions – look at a general number d of digits or/and a general base b in place of 10. We mention a few results and leave it to the interested reader to investigate further.

For instance, if the base $b = 2r$, then the only 3-digit Kaprekar constant in base b has the digits $r - 1, 2r - 1$ and r – the proof of this generalization is the same as that of 495 in base 10.

It can be proved that there are no odd bases b admitting a 3-digit Kaprekar constant.

As for 4-digit Kaprekar constants, there is one in base 5 which is 3032 – so, once again this has as much claim to be of interest as 6174 has!

The other bases where 4-digit Kaprekar constants exist are of the form $b = 4^k \times 10$. In this base, the 4-digit Kaprekar constant has digits $6 \times 4^k, 2(4^k - 1) + 1, 8(4^k - 1) + 7$ and 4×4^k.

This can be proved similarly to the case of base 10.

There is no 5-digit Kaprekar constant in base 10.

On the other hand, base 15 has the Kaprekar constant with the 5 digits

$$10, 4, 14, 9, 5.$$

There exist 5-digit Kaprekar constants in each base of the form $b = 6k + 3 \geq 15$; this is left to the interested reader to determine.

3435

This is sometimes known as the Ramachandra number. An eminent number theorist K Ramachandra observed when he was in college that his Professor's car number 3435 has the property

$$3435 = 3^3 + 4^4 + 3^3 + 5^5.$$

This is the only number > 1 with this property. However, this remains just a curiosity and does not seem to unveil any serious mathematics.

1848

We will see that 1848 is the largest of 65 numbers written down by Euler with a certain property. It is known that there could be at the most two larger numbers with that property. It is easy to show that if an odd number has a unique expression as a sum of two squares of positive integers $n = x^2 + y^2$ and, if x, y are coprime, then n must be a prime number. Euler generalized this property in order to obtain a primality criterion. He defined a positive integer m to be '*Idoneal*' or '*convenient*' ('Idoneus Numerus' in Latin) if it satisfies the property:

If an odd positive integer n admits a unique expression $n = x^2 + my^2$ with $x, y > 0$ and if, in addition, the GCD $(x, my) = 1$, then n must be prime.

Euler wrote down a list of 65 convenient numbers (the smallest 'inconvenient' number is 11) based on a criterion he obtained. The largest in his list is 1848. Until date, no bigger convenient number has been found. S Chowla was the first to prove in 1934 that there are only finitely many convenient numbers. This is based on deep methods (coming under the umbrella of class field theory) outside the scope of our discussion. Later, in 1973, it has been shown by Weinberger that Euler could have missed at most two other convenient numbers. Indeed, assuming the truth of a deep unsolved

problem known as the generalized Riemann hypothesis, it follows that there could be at the most one number missing in Euler's list.

Using the fact that 1848 is idonean, Euler observed that $18518809 = 197^2 + 1848(100)^2$ is a prime.

8191

We know that every positive integer can be represented in binary form (that is, in base 2) in terms of 0's and 1's. There is nothing sacrosanct (mathematically) about base 2 and, one may represent numbers in any base one wants to use. Notice that the number 31 has the base 2 expansion

$$(11111)_2$$

and the base 5 expansion

$$(111)_5.$$

So, it is natural to ask which natural numbers have all their digits to be equal to 1 with respect to *two different* bases > 1.

It was observed by Goormaghtigh nearly a century ago that 8191 has this property;

$$(111)_{90} = (1111111111111)_2.$$

In usual decimal (base 10) notation, this number is 8191.

The question can be posed in another form as follows. If $b_1 \neq b_2$ are two positive integers > 1, then the number with m ones in base b_1 is $1 + b_1 + b_1^2 + \cdots + b_1^{m-1} = \frac{b_1^m - 1}{b_1 - 1}$. Therefore, we are asking if this number can consist of n one's in another base b_2.

This is equivalent to solving

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1}$$

in natural numbers $x, y > 1$ for some $m, n > 2$.

The largest known solution is 8191 mentioned above. It is still unknown whether there are only finitely many solutions in all variables x, y, m, n. In fact,

1093

Fermat's last 'theorem' – asserting that the equation $x^n + y^n = z^n$ has no solutions in positive integers x, y, z when $n > 2$ – took 350 years to be justifiably called a theorem. However, there were several subjective results from the old times. One of them due to Wieferich showed that the first case of Fermat's last theorem holds good for a prime p for which $2^{p-1} - 1$ is not a multiple of p^2. That is, for such a prime p, the equation $x^p + y^p = z^p$

has no solutions in positive integers x, y, z coprime to p. If there were no such 'Wieferich primes', we would have a relatively elementary proof of (the first case of) Fermat's last theorem. However, there are Wieferich primes and 1093 is the smallest. The next is 3511. To this day, no others are known although on probabilistic grounds one expects asymptotically $\log\log(x)$ Wieferich primes until x as $x \to \infty$.

The relation of congruence modulo a positive integer is a very convenient way to express many divisibility statements. If m is a fixed positive integer, one calls two integers a and b to be congruent modulo m, if $a - b$ is a multiple of m (meaning $a - b = mc$ for some integer c). The notation $a \equiv b \mod m$ is due to the great mathematician C-F Gauss who also discussed the notion in the first place. Congruence relation generalizes equality and, it is an easy exercise to check that it satisfies natural properties like:

$a \equiv b \mod m$; $c \equiv d \mod m$ implies

$$a + c \equiv b + d \mod m \ , \ ac \equiv bd \mod m.$$

Fermat's little theorem can be re-stated as the assertion:

$a^{p-1} \equiv 1 \mod p$ if p is a prime $a \not\equiv 0 \mod p$.

Then, Wieferich's congruences are $2^{p-1} \equiv 1 \mod p^2$ for $p = 1093, 3511$.

If 2 is replaced by some other positive integers, there are other examples when analogous congruences hold; viz.,

$$\begin{aligned} 3^{10} &\equiv 1 \mod 11^2 \\ 7^4 &\equiv 1 \mod 5^2 \\ 31^6 &\equiv 1 \mod 7^2 \end{aligned}$$

To see that $2^{1092} - 1$ is a multiple of 1093^2, we proceed as follows.

Now $3^7 = 2187 = (2 \times 1093) + 1 = 2p + 1$, say.

Then $3^{14} \equiv 4p + 1 \mod p^2$.

Also, $2^{14} = 16384 = 15p - 11$ which gives $2^{28} \equiv -330p + 121 \mod p^2$.

So, $3^2 \times 2^{28} \equiv -1876p - 4 \mod p^2$.

On dividing by 4, we have

$$3^2 \times 2^{26} \equiv -469p - 1 \mod p^2.$$

Raising to the 7-th power, we have:

$3^{14} \times 2^{26\times 7} \equiv -(1 + 469p)^7 \equiv -(1 + 7 \times 469p) \mod p^2$

$\equiv -(1 + 3283p) \equiv -(1 + 4p) \equiv -3^{14} \mod p^2$ as observed above.

Hence $2^{26\times 7} \equiv -1 \mod p^2$ which gives $2^{1092} = 2^{26\times 7\times 6} \equiv (-1)^6 \equiv 1 \mod p^2$.

On the other hand, we show that a prime p which is either of the form $b^N + 1$ or of the form $1 + b + b^2 + \cdots + b^n$ for some b, *cannot* satisfy $b^{p-1} \not\equiv 1 \mod p^2$.

In particular, we have the observation:

Neither Mersenne primes (that is, primes of the form $1 + 2 + 2^2 + \cdots + 2^{n-1}$*), nor Fermat primes (that is, primes of the form* $2^n + 1$*) can be Wieferich primes.*

More generally, we prove:

Let p *be a prime whose expression in a base* $b > 1$ *is of the form*

$$1 + b^k + b^{2k} + \cdots + b^{nk}$$

for some $n, k \geq 1$*. Then,*

$$b^{p-1} \equiv 1 + \frac{p-1}{(n+1)k}(b^k - 1)p \not\equiv 1 \mod p^2.$$

Here is the proof.

Now $p = 1 + b^k + \cdots + b^{nk} = \frac{b^{(n+1)k}-1}{b^k-1}$.

Now, p and $b^k - 1$ are relatively prime because p is a prime and

$$p \geq b^k + 1 > b^k - 1.$$

Since p divides $b^{(n+1)k} - 1$, the order of b mod p is a divisor of $(n+1)k$. If it were smaller, say mr, with $m|(n+1)$ and $r|k$, then either $m < n + 1$ or $r < k$.

If $r < k$, then the assertion $b^{(n+1)r} \equiv 1 \mod p$ means p divides

$$(1 + b^r + \cdots + b^{nr})(b^r - 1).$$

Now, p and $b^r - 1$ are relatively prime because p is a prime and $p \geq b^k + 1 > b^r - 1$.

Hence $p = 1 + b^k + \cdots + b^{nk}$ divides $1 + b^r + \cdots + b^{nr}$, which is impossible as p is the bigger number.

Now, if $m < n + 1$, then the condition $b^{mk} \equiv 1$ means p divides $1 + b^k + \cdots + b^{(m-1)k} = \frac{b^{(mk}-1}{b^k-1}$ as p and $b^k - 1$ are relatively prime because p is a prime and $p \geq b^k + 1 > b^k - 1$.

This is impossible, as $p = 1 + b^k + \cdots + b^{nk}$ is larger than $1 + b^k + \cdots + b^{(m-1)k}$.

We have shown that the order of b mod p is $(n+1)k$; hence, this order $(n+1)k$ divides $p - 1$.

Now, raise $b^{(n+1)k} = 1 + p(b^k - 1)$ to the $\frac{p-1}{(n+1)k}$-th power. We have

$$b^{p-1} \equiv 1 + p(b^k - 1)\frac{p-1}{(n+1)k} \mod p^2.$$

Now, again the observation that p is relatively prime to $b^k - 1$ implies that p does not divide $(b^k - 1)\frac{p-1}{(n+1)k}$.

This completes the proof.

In view of the observation above, *an elementary proof of the first case of Fermat's last theorem exists (thanks to Wieferich's criterion) for Mersenne primes and Fermat primes.*

Wieferich's criterion can be proved with a bit of knowledge of the Eisenstein reciprocity law which generalizes the so-called quadratic reciprocity law of Gauss (again!). This is somewhat outside the scope of our discussion. However, we can fortunately give an elementary result which is in the spirit of (but weaker than) Wieferich's criterion and gives a sufficient criterion for Fermat's last theorem to hold good.

Let p be an odd prime and let x, y, z be integers such that $(p, xyz) = 1$ and $x^p + y^p \equiv z^p \ mod\ p^2$. Then, there exists a positive integer $a \leq (p-1)/2$ such that $(a+1)^p - a^p - 1 \equiv 0 \ mod\ p^2$. In particular, if none of the $(p-1)/2$ congruences hold, the first case of Fermat's last theorem holds.

Proof. By Fermat's little theorem, $z \equiv z^p = x^p + y^p \equiv x + y \bmod p$.

As $(p, x) = 1$, there is an integer x' such that $xx' \equiv 1 \bmod p$ (viz., write $1 = pu + xx'$ for some x').

Note that since $z \equiv x + y \bmod p$, we have $zx' \equiv 1 + yx' \bmod p$.

Consider the integer $a \equiv yx' \bmod p$ with $1 \leq a \leq (p-1)/2$. Writing $a = yx' + pt$ and applying the binomial expansion, we have

$$a^p \equiv y^p (x')^p \mod p^2.$$

Also, $a + 1 \equiv yx' + 1 \bmod p$ which gives, on raising to the p-th power and applying binomial theorem as before, that

$$(a+1)^p \equiv (yx')^p + 1 \equiv a^p + 1 \mod p^2.$$

This proves the assertion.

Note that if the $(p-1)/2$ congruences in the statement above are replaced by the single congruence corresponding to $a = 1$, we have Wieferich criterion.

71

John Conway discovered an amazing fact. Start with any positive integer other than 22. Let us start with 1 say. Define the sequence which just reads out the number of times each chain of digits is repeated in turn. That is, after 1, we have 11 (meaning one 1) and after that we have 21 (to mean two 1's) and 1211 (to mean one 2, one 1) and 111221 (meaning one 1, one 2, two 1's) etc. In general, if $a_1^{k_1} a_2^{k_2} \cdots a_r^{k_r}$ with $a_i \neq a_{i+1}$, then the next term

of the sequence is defined to be

$$k_1 a_1 k_2 a_2 \cdots k_r a_r.$$

For example, the sequence starting from 1 is:

$$1, 11, 21, 1211, 111221, 312211, 13112221, 1113213211, 31131211131221, \cdots$$

If d_n is the number of digits in the n-th term, then Conway discovered the remarkable fact that the ratio d_{n+1}/d_n approaches a constant λ (called Conway's constant) which is the unique real root of the polynomial

$$x^{71} - x^{69} - 2x^{68} - x^{67} + 2x^{66} + 2x^{65} + x^{64} - x^{63} - x^{62} - x^{61} - x^{60} - x^{59} + 2x^{58} + 5x^{57} + 3x^{56} - 2x^{55} - 10x^{54} - 3x^{53} - 2x^{52} + 6x^{51} + 6x^{50} + x^{49} + 9x^{48} - 3x^{47} + 7x^{46} - 8x^{45} - 8x^{44} + 10x^{43} + 6x^{42} + 8x^{41} - 5x^{40} - 12x^{39} + 7x^{38} - 7x^{37} + 7x^{36} + x^{35} - 3x^{34} + 10x^{33} + x^{32} - 6x^{31} - 2x^{30} - 10x^{29} - 3x^{28} + 2x^{27} + 9x^{26} - 3x^{25} + 14x^{24} - 8x^{23} - 7x^{22} - 7x^{21} + 9x^{20} - 3x^{19} - 4x^{18} - 10x^{17} - 7x^{16} + 12x^{15} + 7x^{14} + 2x^{13} - 12x^{12} - 4x^{11} - 2x^{10} - 5x^9 + x^7 - 7x^6 + 7x^5 - 4x^4 + 12x^3 - 6x^2 + 3x - 6$$

of degree 71. If this is remarkable, it is even more remarkable that every starting number (other than 22) leads to this same constant λ of degree 71. The proof is very involved and comes under the umbrella of what is now known as the cosmological theorem.

I give a very rough explanation of this phenomenon for the sake of the more mathematically precocious reader among high school students. Some experimentation will tell us that all the numbers in this sequence from the 8th one onwards arise from certain basic strings of elements – 92 of them. In effect, these 92 'atoms' can be written down explicitly and all elements of the Conway sequence can be described in a sense through these 92 elements. Thus, each element of the sequence is a word in the 92 basic elements and *the number of digits* can be described recursively. This amounts to having a 92×92 matrix which describes the recursion. A well-known technique on recursion shows that the n-th term is expressible in terms of 'eigenvalues' of the matrix. These eigenvalues are solutions of a polynomial equation which is obtained from the matrix. In the case above, the polynomial has degree 71 and the ratios d_{n+1}/d_n approach the only positive real root of this polynomial – this is the λ mentioned above!

Skewes's constants

The great mathematician C F Gauss conjectured at the age of 15, what is now called the prime number theorem. He conjectured that the number $\pi(x)$ of primes not exceeding a number x is asymptotically given by the logarithmic integral function $li(x) = \int_2^x \frac{dt}{\log\ t}$. Here, by 'asymptotically', we mean that the ratio $\pi(x)/li(x)$ approaches 1 as x grows unboundedly large. However, the inequality $\pi(x) < li(x)$ was seen to hold for values of

x when these functions could be calculated. J E Littlewood proved in 1914 that the difference actually changes signs infinitely often. Hence, there is indeed a smallest natural number n for which $\pi(n) \geq li(n)$. But, this was an existential proof. Littlewood had a doctoral student named Skewes who, one day in 1933, presumably said "(Ex)Skewes me! Assuming the Riemann Hypothesis, I can show that there is a number N no larger than $10^{10^{10^{34}}}$ such that $\pi(N) \geq li(N)$". Twenty years later, Skewes himself showed without assuming the Riemann Hypothesis, that there is a number M no larger than $10^{10^{10^{964}}}$ such that $\pi(M) \geq li(M)$. These two numbers have come to be known as Skewes's constants. The latest developments have brought the constants down to e^{728} although no explicit value of n is known for which $\pi(n) \geq li(n)$. In the above, we have used the phrase Riemann Hypothesis for an (perhaps the most important) open problem in mathematics.

Graham's constant G

The number is so gigantic that additional notation is needed to write it down. This number arose as follows.

Consider a hypercube in n dimensions. This is the generalization of a square in 2 dimensions and a cube in 3 dimensions; it has 2^n vertices. If we join every vertex to every other one, we get what is known as a complete graph. R L Graham and B L Rothschild considered the following problem. If we colour each edge with one of two available colours, is it always true that there must exist a complete subgraph containing four coplanar vertices such that all its six edges are of the same colour?

This is not necessarily true for 3-dimensional cubes – we leave it to the reader to construct an example. On the other hand, Graham and Rothschild proved the existence of a complete, monochromatic subgraph containing four coplanar vertices in any colouring, if the dimension n is large enough. Until now, one does not know the minimal possible value of n with this property but the proof of Graham and Rothschild showed the existence of an n which is at the most a constant G known as Graham's constant. To define what G is, we introduce Knuth's up-arrow notation.

For positive integers a, b we already know the usual exponentiation a^b as a shorthand notation for multiplying a to itself b times. Knuth introduces the up-arrow notation as: $a \uparrow b$ for a^b. Next, define

$$a \uparrow\uparrow b = \underbrace{a \uparrow (a \uparrow (a \uparrow (\cdots)))}_{b \text{ times}}.$$

For example, $4 \uparrow\uparrow 3 = 4^{(4^4)}$ while $3 \uparrow\uparrow 4 = 3^{(3^{(3^3)})} = 3^{(3^{27})}$ a much larger number. In fact, the former has about 154 digits whereas the latter has

more than 10^{12} digits.

Now, the next stage is easy to define.

For positive integers a, b define

$$a \uparrow\uparrow\uparrow b = \underbrace{a \uparrow\uparrow (a \uparrow\uparrow (a \uparrow\uparrow (\cdots)))}_{b \text{ times}}.$$

More generally,

$$a \uparrow^n b = \underbrace{a \uparrow^{n-1} (a \uparrow^{n-1} (a \uparrow^{n-1} (\cdots)))}_{b \text{ times}}$$

where $\uparrow^k$ stands for $\underbrace{\uparrow\uparrow \cdots \uparrow}_{k \text{ times}}$.

In terms of these notations, Graham's constant $G = g_{64}$ where

$$g_1 = 3 \uparrow^4 3, g_2 = 3 \uparrow^{g_1} 3, \cdots, g_n = 3 \uparrow^{g_{n-1}} 3.$$

We cannot even have a reasonable comprehension of how big this number is but it has appeared in a mathematical proof; such is the *power* of the human mind!

Counting, Recounting and Matching

Counting problems are teeny-weeny
and don't require a magical genie
until we encounter a count
that seems impossible to surmount.
But then there is always Fubini!

1. Introduction

Although we start our mathematical education by learning to count, it is this very thing which is one of the most difficult things to carry out in practice. In this article, we discuss a very simple method which is available in a very general form under the name of Fubini's principle. In its simplest form, it is the obvious observation that counting in two different ways produces the same sum. However, the various examples we discuss will hopefully convince the reader that the principle is surprisingly effective.

2. Hare and Tortoise

Let us start with a simple example.

Suppose, we wish to find the length of the longest possible sequence of real numbers such that the sum of every 7 consecutive terms is positive and the sum of every 11 consecutive terms is negative.

How do we analyze this problem?

Consider such a possible sequence of length at least 17 (if one exists), say $a_1, \cdots, a_{17}, \cdots$.

The trick is to write the following array made up from these numbers, viz.:

$$\begin{array}{ccccccc} a_1 & a_2 & a_3 & \cdots & \cdots & a_7 \\ a_2 & a_3 & a_4 & \cdots & \cdots & a_8 \\ \vdots & & \vdots & & & \\ a_{11} & a_{12} & a_{13} & \cdots & \cdots & a_{17} \end{array}$$

Each row sum is positive while each column sum is negative, which is impossible as seen by considering the sum of ALL these numbers. Hence, the maximal possible length is less than 17.

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 21, No. 4, pp. 353–368, April 2016.

Let me leave as an exercise the task of finding a sequence of 16 numbers with the required property (turn to the last page if you cannot work it out).

The principle we have been discussing is sometimes known as Fubini's principle. In its simplest form, it is the obvious observation that counting in two different ways produces the same sum. To further convince ourselves that such a simple principle can indeed be powerful, here are some more examples:

3. Valuable Tiles

Tile the plane by unit squares with vertices at integer lattice points. Inside each unit square, fill in some real number and call it the value of that unit square. Let A be a finite collection of unit squares having the property that the total value of the 'translate' $A + (i, j)$ is positive for each lattice point (i, j). Here, by translate $A + (i, j)$, we mean the set $\{(x + i, y + j) : (x, y) \in A\}$. Then, we claim that for each finite collection B of unit squares, *some translate of B must have positive value.*

The solution depending on the Fubini principle goes as follows:

Denote by $[i, j]$, the unit square whose lower left corner has co-ordinates (i, j) and let $v(i, j)$ denote its value. Write

$$A = \{[i_1, j_1], \cdots, [i_r, j_r]\}$$

$$B = \{[k_1, l_1], \cdots, [k_s, l_s]\}.$$

Now, for each $1 \leq m \leq s$, the total value of the translate $A + (k_m, l_m)$ is $\sum_{n=1}^{r} v(i_n + k_m, j_n + l_m)$ which is known to be positive. Hence,

$$\sum_{m=1}^{s} \sum_{n=1}^{r} v(i_n + k_m, j_n + l_m) > 0$$

which gives

$$\sum_{n=1}^{r} (\sum_{m=1}^{s} v(i_n + k_m, j_n + l_m)) > 0.$$

Therefore, we must have some $n \leq r$ for which $\sum_{m=1}^{s} v(i_n + k_m, j_n + l_m) > 0$; hence, the translate $(i_n, j_n) + B$ has total positive value.

4. Partitions

A well-known application of the Fubini principle is the following stunning fact about partitions of a number. Recall that the number $p(n)$ of partitions of n is the number of ways of partitioning n objects into smaller collections. For instrance $p(4) = 5$ because there are 5 ways to partition 4 objects:

all 4, $3+1$, $2+2$, $2+1+1$, $1+1+1+1$. This number of partitions of n grows extremely fast as n grows. The fact alluded to asserts:

The number of partitions of n into m parts equals the number of partitions of n in which the largest part is m.

The proof is by plotting an array of points corresponding to a partition in the following manner:

For a partition $n_1 + n_2 + \cdots + n_r = n$ where $n_1 \leq n_2 \leq \cdots n_r$, draw an array consisting of dots with n_1 dots in the first row, n_2 dots in the second row (centered to the left) etc.

Now, count column-wise; for instance, $8 = 2 + 2 + 4$ gives the conjugate array corresponding to the partition $8 = 3 + 3 + 1 + 1$.

5. Regular Solids

Here is yet another striking example of the Fubini principle:

There are exactly five platonic solids.

In a platonic solid, the faces meeting at a vertex are regular polygons with the same number of sides, the number of faces meeting at each vertex is the same, and the solid angles at each vertex is the same.

If there are v vertices, e edges and f faces in the solid, and the faces are regular polygons with p sides, then let us count the edges by counting faces.

We get pf edges but we have counted each edge twice as it is the edge of exactly two faces.

Hence, the Fubini principle implies $2e = pf$.

Similarly, counting the edges by means of the two end point vertices, this number also equals qv where q is the number of faces meeting at any vertex.

Hence,

$$qv = 2e = pf.$$

Rewrite it as

$$\frac{v}{1/q} = \frac{e}{1/2} = \frac{f}{1/p}.$$

Now, we use the famous formula of Euler: $v - e + f = 2$; see, for instance Example 9 on p.601 of the article '*Invariants*' by B V Rajarama Bhat in the July 2010 issue of *Resonance*. So,

$$\frac{v}{1/q} = \frac{e}{1/2} = \frac{f}{1/p} = \frac{v - e + f}{1/q - 1/2 + 1/p}.$$

This is equal to

$$\frac{2}{1/q - 1/2 + 1/p} = \frac{4pq}{2p - pq + 2q} = \frac{4pq}{(4 - (p-2)(q-2)}.$$

We had shown $qv = 2e = pf = \frac{4pq}{(4-(p-2)(q-2)}$.

Therefore, $(p-2)(q-2) < 4$ which gives exactly five solutions

$$(3,3), (3,4), (3,5), (4,3), (5,3).$$

These are the five Platonic solids – tetrahedron, octahedron, icosahedron, cube and dodecahedron respectively.

6. Fubini for Bounds

Even when it is not possible to count precisely, the Fubini principle can be useful to get lower bounds for the actual count. Here is one problem which looks simple but proves to be deceptively difficult unless we think of Fubini.

Consider n points on a line and look at the sequence of $\binom{n}{2}$ possible pairwise distances. Suppose each pairwise distance appears at the most twice. Then, there are at least $[n/2]$ numbers which appear exactly once as pairwise distances.

Let us view the points from left to right on a horizontal line and denote them by $P_1, P_2, \cdots, P_n$ respectively. Let a distances appear exactly once and b distances appear exactly twice; then $a + 2b = \binom{n}{2}$.

The distances P_1P_i for $1 < i \leq n$ are $n-1$ distinct numbers.

The distances P_2P_j for $2 < j \leq n$ are $n-2$ distinct numbers,

The distance P_1P_i can equal P_2P_j at the most for one choice (i,j); for, if $P_1P_k = P_2P_l$, then

$$P_1P_2 = P_iP_j = P_kP_l,$$

which leads to a contradiction.

Thus, we have at least $n-3$ distances P_2P_j not occurring as P_1P_i.

In this manner, P_3P_r for $3 < r \leq n$ gives at least $(n-3)-2 = n-5$ distances not occurring as some P_1P_i or some P_2P_j.

Thus, we have a lower bound $a + b \geq (n-1) + (n-3) + \cdots = [n^2/4]$.

So, $a \geq [n^2/2] - \binom{n}{2} = [n/2]$.

7. Teachers with Designs

Here is a problem which seems like a scenario which could happen. We discuss it and solve it using the Fubini principle. However, we point out after the discussion that this scenario cannot occur! We will also give an example of a similar situation which can occur in practice.

Here is the situation.

In a school, suppose there are a total of 50 teachers and s students. Suppose, it happens that each teacher teaches a total of exactly 57 students

and each pair of students has exactly one common teacher. Then, can we determine the total number of students?

Let us suppose t is the total number of teachers (in our case $t = 50$) and that the total number of students is s. Suppose each teacher teaches a total of exactly s_0 students (we have $s_0 = 57$) and that each pair of students has exactly t_0 common teachers (we have $t_0 = 1$).

We will find the relations between t, t_0, s, s_0.

Let us look at any teacher T and a pair of students S_i, S_j taught by her. Count the number of triples (T, S_i, S_j) as T varies over teachers and S_i, S_j vary over pairs of students such that T teaches both S_i and S_j. As a teacher teaches exactly s_0 students, there are exactly $\binom{s_0}{2}$ triples (T, S_i, S_j) containing any particular teacher T. Therefore, the total number of triples is $t\binom{s_0}{2}$.

On the other hand, for each pair of students S_i, S_j there are exactly t_0 common teachers which means there are t_0 triples (T, S_i, S_j) containing the pair S_i, S_j. As there are $\binom{s}{2}$ ways to select the pair of students S_i, S_j, the total number of triples is $t_0\binom{s}{2}$.

By Fubini's principle, we get

$$t\binom{s_0}{2} = t_0\binom{s}{2}.$$

In our example, $t = 50, t_0 = 1, s_0 = 57$. So, we have $\frac{50\times 57\times 56}{2} = \frac{s(s-1)}{2}$. Solving this quadratic equation, we obtain $s = 400$.

Now, what is wrong with it? Nothing excepting the fact that this situation cannot occur! Indeed, a necessary condition for the scenario to arise is given by Fisher's inequality which does not hold good here. Indeed, if there are v students and b teachers such that each teacher k students and any pair of students have λ common teachers, then *turns out that* there exists a constant r such that each student is taught by exactly r teachers and r satisfies

$$bk = rv \ , \ r(k-1) = \lambda(v-1).$$

In this standard notation, (b, v, r, k, λ) is called a block design. There is an inequality due to population geneticist and statistician Ronald Fisher (the doctoral supervisor of the well known Indian statistician C R Rao) which asserts that $b \geq v$; this is not satisfied in our situation.

Let us give an example of a similar scenario which can actually occur. We recall in passing the famous quote by John von Neumann in 1947: '*If people do not believe that mathematics is simple, it is only because they do not realize how complicated life is.*'

Suppose there are a certain number b of teachers in a school who offer to supervise a project each on different subjects. The projects are offered

to an exclusive group of the 9 most talented students each of whom can work on more than one project. Each teacher supervises exactly 3 students. Every pair of students works on exactly one common project. Is this possible? If so, what is the total number of teachers, and what is the (common) number of teachers supervising each student (the number r predicted above)?

The answer turns out to be yes, the situation can arise and the numbers b and r can be found. Just as in the earlier problem, let us count the triples:

(T, S_1, S_2) where T varies over the b teachers and S_1, S_2 are two students supervised by T.

For each teacher, there are $\binom{3}{2}$ choices for (S_1, S_2) so that the total number of triples is $t\binom{3}{2}$. On the other hand, for any fixed pair (S_1, S_2) among the 9 students, there is exactly one common supervisor so that the number of triples is $\binom{9}{2}$. By Fubini's principle,

$$t\binom{3}{2} = \binom{9}{2}.$$

Hence $t = 12$. Moreover, the constraints $bk = rv\ ,\ r(k-1) = \lambda(v-1)$ along with the values $b = 12, k = 3, v = 9$ give $r = 4$. A situation when this happens is represented by the following 9×12 ($v \times b$) matrix consisting of 0's and 1's. In this matrix, each row represents a student, each column a teacher, and the number of 1's in each row is 4 ($r = 4$); there are exactly three 1's in each column ($k = 3$), and each pair of rows has 1's in exactly one column ($\lambda = 1$). How is such a matrix (equivalently (b, v, r, k, λ) block design) constructed? This is tricky, and the essentially unique such matrix turns out to be

$$\begin{pmatrix}
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}.$$

In general, if M is a $v \times b$ matrix consisting of 1's and 0's, then it corresponds to a (b, v, r, k, λ) block design if, and only if, $MM^t = \lambda J_v + (r-\lambda)I_v$ and $u_v M = k u_b$, where u_v, u_b are vectors comprised of 1's and J_v is the $v \times v$ matrix all of whose entries are 1's.

8. Sperner's Theorem from Fubini

A striking application of the Fubini principle is a proof of the Sperner theorem on antichains which asserts:

If $|S| = n$, then no antichain can contain more than $\binom{n}{[n/2]}$ subsets in its collection.

Here, a collection of its subsets is said to be antichain no subset in this collections contains another in the collection.

Let us first look at an application.

Let $a_1, \cdots, a_n$ be n real numbers satisfying $|a_i| \geq 1$ for all i. Look at the 2^n numbers of the form $\sum_{i=1}^n \epsilon_i a_i$ where each ϵ_i is ± 1. Then, any interval of length less than 2 contains at the most $\binom{n}{[n/2]}$ of these 2^n numbers. Here is a proof. We may assume without loss of generality that each $a_i \geq 1$.

For $\epsilon_1, \cdots, \epsilon_n \in \{1, -1\}$, put $E(\epsilon) = \{i \leq n : \epsilon_i = 1\}$. If $\epsilon'_1, \cdots, \epsilon'_n \in \{1, -1\}$, then let us look at $\sum_{i=1}^n \epsilon_i a_i - \sum_{i=1}^n \epsilon'_i a_i$.

If $E(\epsilon') \subset E(\epsilon)$, then the above difference is simply

$$2 \sum_{i \in E(\epsilon) \setminus E(\epsilon')} a_i \geq 2|E(\epsilon) \setminus E(\epsilon')| \geq 2.$$

Hence, only one of the sums can be in an interval length < 2.

As the sums inside an interval of length < 2 correspond to antichains, Sperner's theorem immediately implies our assertion that there are at the most $\binom{n}{[n/2]}$ sums as above in such an interval.

Here is a proof of Sperner's theorem using the Fubini principle.

Let $|S| = n$; any maximal chain

$$\emptyset \neq S_1 \subset S_2 \subset \cdots \subset S_n = S,$$

evidently has $|S_i| = i$. Also, clearly there are $n!$ maximal chains. If T is any subset of S (with i elements say), then there are $i!(n-i)!$ maximal chains which contain T as a term. Let $T_1, T_2, \cdots, T_m$ be an antichain; let $C_1, C_2, \cdots, C_{n!}$ be all the maximal chains in S.

Consider the set Σ of pairs (C_i, T_j) where T_j occurs in C_i.

Write a matrix M whose (i, j)-th entry is 1 if C_i contains T_j as a term; write the entry 0 if not.

Then, the sum of j-th column is $k_j!(n-k_j)!$ where T_j has k_j elements; so, the sum of all entries is $\sum_{j=1}^m k_j!(n-k_j)!$. On the other hand, two different T_j's cannot occur in the same C_i (as $T_1, T_2, \cdots, T_m$ is an antichain) which means each row sum is at the most 1. Thus, sum of all entries is $\leq n!$; hence

$$\sum_{j=1}^m k_j!(n-k_j)! \leq n!$$

In other words, $\frac{1}{\sum_{j=1}^{m}\binom{n}{k_j}} \leq 1$.

Since any $\binom{n}{r} \leq \binom{n}{[n/2]}$, we have $m \leq \binom{n}{[n/2]}$.

9. Counting Leads to Identities

Counting is likely to involve expressions in terms of binomial coefficients; so, there are situations when the Fubini principle will provide us with beautiful identities involving binomial coefficients.

We start with some simple, well-known identities which arise in this manner.

A class contains g girls and b boys, where we write $b \leq g$ to fix notation. Suppose one wants to choose s students from the class for the school quiz team.

Let us see how many ways they can be chosen.

The first naive way says $\binom{g+b}{s}$ ways.

Now, let us look at a choice involving r boys and $s-r$ girls; there are $\binom{b}{r}\binom{g}{s-r}$ choices.

As r can vary from 0 to b, we have the total $\sum_{r=0}^{b}\binom{b}{r}\binom{g}{s-r}$.

By Fubini's principle, we get

$$\sum_{r=0}^{b}\binom{b}{r}\binom{g}{s-r} = \binom{b+g}{s}.$$

We usually rewrite it in the symmetric form

$$\sum_{u,v\geq 0, u+v=s}\binom{b}{u}\binom{g}{v} = \binom{b+g}{s}$$

where it is understood that a binomial coefficient $\binom{n}{d} = 0$ if $n < d$.

Note the particular case

$$\sum_{u\geq 0}\binom{g}{u}^2 = \binom{2g}{g}.$$

Here is a more complicated example. Look at all paths from $(0,0)$ of length $2n+1$ where each step is of unit length either to the east or to the west or to the south or to the north, and which ends on the Y-axis.

We wish to count the number of such paths.

As we begin and end on the same vertical line, the total number of east moves and west moves are equal; if this is r each, we have $\binom{2n+1}{2r}\binom{2r}{r}$ choices. As the rest of the $2n+1-2r$ steps are vertical (up or down), there are $2^{2n+1-2r}$ choices.

Therefore, the total number of paths of length $2n+1$ is $\sum_r 2^{2n+1-2r}\binom{2n+1}{2r}\binom{2r}{r}$.

On the other hand, if we only look at the set of paths on the X-axis, which start and end at $(0,0)$ and go by unit distance east or west, there are $\binom{4n+2}{2n+1}$ paths.

Calling the latter steps as e_x, w_x, and the earlier steps E, W, S, N, the correspondence

$$E \mapsto e_x e_x, W \mapsto w_x w_x, N \mapsto e_x w_x, S \mapsto w_x e_x$$

is a bijection.

Hence, we obtain

$$\binom{4n+2}{2n+1} = \sum_r 2^{2n+1-2r}\binom{2n+1}{2r}\binom{2r}{r}.$$

10. Counting Tiles of Different Shapes

Now, we discuss a very interesting example coming from tiling. Suppose we have a board of dimension 1 foot $\times n$ feet.

We have white and black 'tiles' which are unit squares in dimension; we also have grey tiles (dominos) of dimension 1×2.

Let us tile the board (that is, fill the board with these with these three types of tiles without overlapping).

For instance, if $n = 1$, there are two possible ways to tile – one using the white square and the other using the black square.

If $n = 2$, then there are five ways to tile (black-black, white-white, white-black, black-white, grey).

So, if t_n denotes the number of ways to tile the $1 \times n$ board, we have $t_1 = 2, t_2 = 5$.

Let us also put $t_0 = 1$ for convenience. Here is an observation:

$t_{2n+1} = 2\sum_{r=0}^{n} t_{2r}$.

Indeed, note that every tiling of a $1 \times (2n+1)$ board must contain an odd number of squares (hence, at least one square).

Look at the right-most square in a tiling.

Since all the tiles to its right are the 1×2 dominos, the right-most square occurs at an odd-numbered place, say $(2r+1)$-th place.

Then, the number of tilings with the right-most square at the $(2r+1)$-th place is $2t_{2r}$ because the left-most $2r$ tiles can be tiled in t_{2r} with the $(2r+1)$-th tile being white or black.

Hence, the assertion $t_{2n+1} = 2\sum_{r=0}^{n} t_{2r}$ is proved.

We also have:

$t_{n+1} = 2t_n + t_{n-1}$; in particular, t_{n+1} and t_{n-1} are of the same parity.

Indeed, the first term $2t_n$ counts the number of tilings of the $1 \times (n+1)$-board with the last tile a square, and t_{n-1} counts those for which the last tile is a domino.

We make a divisibility observation now:

t_n divides t_{2n+1} as well as $\sum_{r=0}^{n} t_{2r}$.

In fact, look at the two possibilities for a tiling – one in which the n-th and $(n+1)$-th places are filled by a domino or not.

If they are not occupied by a domino, the board is "breakable" at the n-th place, and there are $t_n t_{n+1}$ such tilings.

If a domino occupies the n-th and $(n+1)$-th squares, the number of tilings is $t_{n-1}t_n$.

Hence, we have

$$t_{2n+1} = t_n t_{n+1} + t_{n-1}t_n = t_n(t_{n+1} + t_{n-1})$$

which is evidently a multiple of t_n.

Note also that since t_{n+1}, t_{n-1} have the same parity, $t_{n+1}/2$ is a multiple of t_n which means that t_n divides $t_{2n+1}/2 = \sum_{r\geq 0} t_{2r}$.

On the other hand, in any tiling of the $1 \times n$ board, consider the number d of dominos.

They occupy $2d$ squares, and in the rest of the $n-2d$ squares, one can have a black or white square which gives 2^{n-2d} possibilities.

Now, the number of tiles here is $n-d$ (because there are d dominos and $n-2d$ unit squares).

So, the number of ways to choose d dominos from these $n-d$ tiles is $\binom{n-d}{d}$.

Hence, we get:

$$t_n = \sum_{d\geq 0} 2^{n-2d} \binom{n-d}{d}.$$

In particular, the divisibility properties above give divisibility properties for the integers $\sum_{d\geq 0} 2^{n-2d}\binom{n-d}{d}$.

I leave it as interesting exercises to discover other such relations by counting tiles rather than using algebra; for instance, prove the following:

$$t_{n-1} + t_n = \sum_{r\geq 0} 2^r \binom{n+1}{2r}.$$

$$(t_{2n-1} + t_{2n})^2 = \sum_{r=0}^{4n} t_r.$$

I also leave it to the interested person to discover such identities when we count tilings by squares of a different colours and dominos of b different colours.

11. A Higher Congruence by Counting

Counting in two different ways, we can prove the following beautiful congruence:

For a prime $p > 3$, and $n \geq r$, $\binom{pn}{pr} \equiv \binom{n}{r} \bmod p^3$.

Proof. Consider a $n \times p$ grid of squares from which we select pr squares. We may either choose r entire rows; otherwise, there are at least two rows from which between 1 and $p-1$ squares are chosen. Cyclically shifting the squares in each row divides the choices into equivalence classes out of which $\binom{n}{r}$ classes are singletons; the other classes are all of cardinalities multiples of p^2. Thus, we have, first of all,

$$\binom{pn}{pr} \equiv \binom{n}{r} \bmod p^2.$$

We refine this argument now.

If a choice of pr squares has less than $r-2$ entire rows, the corresponding equivalence class has cardinality a multiple of p^3. Therefore, the asserted congruence mod p^3 reduces to showing the special case $\binom{2p}{p} \equiv 2 \bmod p^3$ when $p \geq 5$. To see this, note

$$\binom{2p}{p} = \sum \binom{p}{k}^2 \equiv 2 + p^2 \sum_{k=1}^{p-1} k^{-2} \mod p^3.$$

The latter sum is clearly $\equiv \sum_{k=1}^{p-1} k^2 \equiv 0 \bmod p$ when $p > 3$.

12. Macaulay Expansion by Counting

We finish with a beautiful number-theoretic statement for with a Fubini-type proof [1]. For each natural number r, denote by S_r, the set of all r-digit numbers in some base b whose digits are in strictly decreasing order of size. Evidently, S_r is non-empty if and only if $b \geq r$; in this case, S_r has $\binom{b}{r}$ elements.

Let us now write the elements of S_r in increasing order. For instance, in base 10, the first few of the 120 members of S_3 are:

$$(2,1,0), (3,1,0), (3,2,0), (3,2,1), (4,1,0), (4,2,0), (4,2,1), (4,3,0), \cdots .$$

Then, we have:

Given any positive integer n, and any base b such that $\binom{b}{r} > n$, the $(n+1)$-th member of S_r is $(a_r, \cdots, a_2, a_1)$ where $n = \binom{a_r}{r} + \binom{a_{r-1}}{r-1} + \cdots + \binom{a_1}{1}$. In particular, for each n, the Diophantine equation $\binom{a_r}{r} + \binom{a_{r-1}}{r-1} + \cdots + \binom{a_1}{1} = n$ has a unique solution in positive integers $a_r > a_{r-1} > \cdots > a_1 \geq 0$.

We leave the proof as an exercise.

The expression $n = \binom{a_r}{r} + \binom{a_{r-1}}{r-1} + \cdots + \binom{a_1}{1}$ is known as Macaulay's expansion and can simply be proved by the greedy algorithm but the above statement gives a combinatorial interpretation.

Here are a couple of examples to illustrate the statement.

(i) Let $r = 3$ and $n = 12$.

We may take any base b so that $\binom{b}{3} > 12$. For example, $b = 6$ is allowed because $\binom{6}{3} = 20$.

Among the 20 members in S_3, the 13-th member is $(5, 2, 1)$.

Note that

$$\binom{5}{3} + \binom{2}{2} + \binom{1}{1} = 12.$$

(ii) Let $r = 3, n = 74$.

We may take $b = 10$ as $\binom{10}{3} = 120$. The 75-th member of S_3 is $(8, 6, 3)$. Note that

$$\binom{8}{3} + \binom{6}{2} + \binom{3}{2} = 74.$$

Remark. Informally, Fubini's theorem gives conditions under which a function f of two variables satisfies the property that the integral of f under the product measure equals

$$\int (\int f(x, y)dy)dx = \int (\int f(x, y)dx)dy.$$

An example to show this subtlety is the function

$$f(x, y) = \frac{x^2 - y^2}{(x^2 + y^2)^2} \ \forall\ 0 < x, y < 1.$$

Then,

$$\int (\int f(x, y)dy)dx = \pi/4 \neq -\pi/4 = \int (\int f(x, y)dx)dy.$$

Answer to the Puzzle

A sequence of 16 numbers with each subsequence of 7 consecutive terms adding to a positive number and every subsequence of 11 consecutive terms adding to a negative number is:

$$-5, -5, 13, -5, -5, -5, 13, -5, -5, 13, -5, -5, -5, 13, -5, -5.$$

References

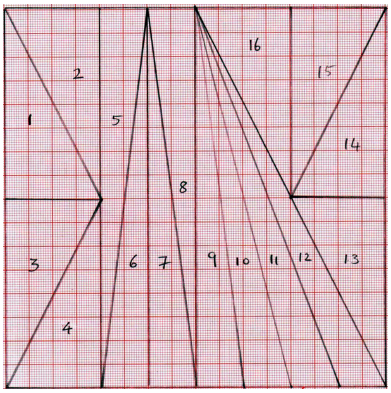
[1] B Sury, Macaulay expansion, *Amer. Math. Monthly*, **Vol. 121**, 2014.

Odd if it isn't an Even Fit! Lighting up Tiling

There was a chap who could tile a square
whom I was perfectly willing to hire.
"Used triangles – all of areas same,
and needed but eleven for this game",
he said, and I knew he was a liar!

Tiling Squares by Triangles of Given Area

Try to cut a square into finitely many triangles (possibly of different shapes) of equal area. You would find that – no matter what the shapes are – the number of triangles is always even. Here is an example.



There is some interesting history behind the discovery of the above fact. In 1965, Fred Richman from the university of New Mexico had decided to pose this in an examination in the master's programme. He had observed this in some cases but when he tried to prove it in general prior to posing it in the exam, he was unsuccessful. So, the problem was not posed in the exam. His colleague and bridge partner John Thomas tried for a long time and finally came up with a proof that it is impossible to break the unit square with corners at $(0,0),(1,0),(0,1)(1,1)$ cannot be broken into an odd number of triangles when the vertices of all the triangles have rational co-ordinates with odd denominators. He sent the paper to the *Mathematics Magazine* where the referee thought the result may be fairly easy (but could

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 20, No. 1, pp. 23–33, January 2015.

not find a proof himself) and perhaps known (but could not find a reference to it). On the referee's suggestion, Richman and Thomas posed this as a problem [1] in the *American Mathematical Monthly* which nobody could solve. Subsequently, Thomas's paper appeared in the *Mathematics Magazine* [2] in 1968. Finally, in 1970, Paul Monsky proved the complete version in a paper [3] in the *American Mathematical Monthly* removing the restriction imposed in Thomas's paper.

We shall discuss Monsky's proof of this beautiful fact presently. Amazingly, it uses some nontrivial mathematical objects called 2-adic valuations.

In fact, one may consider generalizations of squares like cubes and hypercubes of higher dimensions. If an n-dimensional cube is cut into simplices (generalizations of triangles like tetrahedra etc. in higher dimensions) of equal volumes, it turns out that the number of simplices must be a multiple of $n!$

One also says that a region like the interior of a square is 'tiled' by triangles if the square can be broken into triangular pieces.

There is also a generalization of the result on tiling by triangles of squares to the (so-called) polyominos. Polyominos are just unions of unit squares.

Connected subsets of the square lattice tiling of the plane are called special polyominos. That is, they have standard edges – edges of the unit squares are parallel to the co-ordinate axes. The generalization alluded to is due to S K Stein [4] and asserts:

Consider a special polyomino which is the union of an odd number of unit squares. If this polyomino is a union of triangles of equal areas, then the number of triangles is even.

We discuss the proof of this statement after discussing the solution by Paul Monsky of the first problem we started with. It can be noticed that the proof uses crucially that the number of unit squares in the polyomino is odd. Interestingly, this question is still unanswered when the number of unit squares in the polyomino is even.

The proof of Monsky as well as Stein's result above use the so-called '2-adic valuation function'. The 2-adic valuation is a function from the set of non-zero rational numbers to the set of integers; it simply counts the power of 2 dividing any integer or, more generally, any rational number. What is meant by the power of 2 dividing a rational number? Writing any non-zero rational number as p/q with p, q having no common factors, one may look at the power of 2 dividing p or q. If p, q are both odd, this is simply 0. If p is even, then the 2-adic valuation of p/q is defined to be the power of 2 dividing p. If q is even, then the 2-adic valuation of p/q is defined to be the negative of the power of 2 dividing q, Formally, we write:

$$\phi : \mathbf{Q}^* \to \mathbf{Z}$$

defined by $\phi(\frac{2^a b}{c}) = a$ where b, c are odd; define also $\phi(0) = \infty$ so that ϕ is defined for all rational numbers. We keep in mind that 0 has larger 2-adic value than any other rational number.

Colour a point $(x, y) \in \mathbf{Q} \times \mathbf{Q}$ by the colour:

$$\begin{gathered}\text{red, if } \phi(x), \phi(y) > 0,\\ \text{blue, if } \phi(x) \leq 0; \phi(x) \leq \phi(y),\\ \text{green, if } \phi(x) > \phi(y) \text{ and } \phi(y) \leq 0.\end{gathered}$$

In this manner, all points of $\mathbf{Q} \times \mathbf{Q}$ are coloured by these three colours.

For example:

$(2, 0)$ is red, $(1, 3)$ is blue and $(1, 1/2)$ is green. Also, $(0, 0)$ is red while $(1, 0)$ is blue and $(0, 1)$ is green.

Now, we proceed to assert something which is easy to believe but not that easy to prove. The assertion is that it is possible to extend the above function to a function on the whole of real numbers (but the values can be non-integers). In our further discussion, we assume without further ado, the existence of an extension

$$\phi : \mathbf{R} \to \mathbf{R}$$

which satisfies:

ϕ restricts to the 2-adic valuation on $\mathbf{Q}$;

$\phi(xy) = \phi(x) + \phi(y)$;

$\phi(x + y) \geq min(\phi(x), \phi(y))$.

This is important to have such an extension because we would really like to colour **all** *points in a square.*

For instance, as $\phi(3/4) = \phi(2^{-2}3) = -2$, the second property above implies that

$$\phi(3/4) = 2\phi(\sqrt{3}/2) = -2.$$

Hence $\phi(\sqrt{3}/2) = -1$.

Let us start Monsky's proof by first considering the unit square with a left lower corner at $(0, 0)$ and making a few easy observations:

(i) *If a point a is red, then any point x and $x + a$ have the same colour.*

(ii) *On any line, there are at the most two colours.*

(iii) *The boundary of the square has an odd number of segments which have a red end and a blue end.*

(iv) *If a triangle is not 'complete' (that is, has vertices only of one or two colours), then it has* 0 *or* 2 *red-blue edges.*

Proof. Recall

$$\begin{aligned} \phi(xy) &= \phi(x) + \phi(y) \\ \phi(x+y) &\geq min(\phi(x), \phi(y)) \end{aligned}$$

In particular, if $\phi(x) > \phi(y)$, then $\phi(x+y) = \phi(y)$.

In particular, if (x, y) is blue, then $\phi(x) \leq \phi(y)$ and so, $\phi(y/x) \geq 0$ and, if (x, y) is green, then $\phi(x) > \phi(y)$ and so, $\phi(y/x) < 0$.

Let us prove (i) now.

As a is red, its co-ordinates have positive ϕ and it is easy to check in each of the three cases of colouring for a point x that x and $x + a$ have the same colour.

For (ii), without loss of generality, we may assume that the line passes through the origin. But two other points $(x_i, y_i); i = 1, 2$ on the line $y = tx$ have colours blue and green respectively, say.

But then $\phi(y_1/x_1) = \phi(y_2/x_2) = \phi(t)$ is impossible as the former is ≥ 0 while the latter is < 0.

To prove (iii), note that (ii) implies that such segments on the boundary must be on the segment from $(0, 0)$ to $(1, 0)$ which are red and blue respectively. But, this is clear.

The proof of (iv) is completely clear by considering the various possibilities RRB,RBB,RGG,RRG,BBG,BGG.

Now, we are ready to prove:

Let a square be tiled by n triangles of equal areas. Then, n is even.

Proof (Monsky). Counting the red-blue edges on the square, we are counting the interior edges twice and the boundary edges once.

Thus, (iii) above would be contradicted unless there is a complete triangle. But then a complete triangle has area A with $\phi(A) < 0$ – let us check this now.

Firstly, note that the triangle can be moved so that the vertices are at $(0, 0), (a, b)$ and (c, d) where (a, b) is blue and (c, d) is green. Thus, the area is $(ad - bc)/2$.

As (a, b) is blue, $\phi(a) \leq \phi(b)$ and as (c, d) is green, $\phi(c) > \phi(d)$.

Therefore, $\phi(ad) = \phi(a) + \phi(d) < \phi(b) + \phi(c) = \phi(bc)$ which gives $\phi(ad - bc) = \phi(ad) = \phi(a) + \phi(d) \leq 0$.

Hence $\phi(A) = \phi((ad - bc)/2) \leq -1$.

So, if there are n triangles, then $\phi(A) = \phi(1/n) < 0$; that is, n is even.

This completes Monsky's wonderful proof.

Let us now prove the more general version on polyominos mentioned above:

Consider a polyomino which is the union of an odd number of unit squares. If it is tiled by triangles of equal areas, then the number of triangles is even.

Proof. It can be seen that if a line segment made up of segments parallel to the axes has a blue end and a green end, then each of the individual segments has ends only coloured blue or green and, an odd number of them have both colours as ends.

The key observation is:

If a polyomino made up of standard squares as above is made up of n triangles of equal areas and, if an odd number of standard edges on its boundary have ends coloured blue and green, then $\phi(2A) \leq \phi(n)$, where A is the area of the polyomino.

The proof of this in turn depends on the following fact:

Let (x_i, y_i); $i = 0, 1, 2$ be the vertices of a triangle T where $(x_i, y_i) \in S_i$ with
$S_0 = \{(x, y) : \phi(x), \phi(y) > 0\}$,
$S_1 = \{(x, y) : \phi(x) \leq 0, \phi(y)\}$,
$S_2 = \{(x, y) : \phi(y) < \phi(x), \phi(y) \leq 0\}$.
Then, $\phi(area(T) \leq -\phi(2)$.

Proof. As translation by $(-x_1, -y_1)$ does not change areas, and $P_i - P_0 \in S_i$ for any $P_i \in S_i$, we may assume that $(x_0, y_0) = (0, 0)$.
Then, area$(T) = \frac{1}{2}|x_1 y_2 = x_2 y_1|$.
Now $\phi(x_1) \leq 0, \phi(y_1)$. Also $\phi(y_2) \leq 0$ and $\phi(y_2) < \phi(x_2)$.
Thus, $\phi(x_1 y_2) < \phi(x_2 y_1)$ and $\phi(x_1 y_2) \leq 0$.
Hence $\phi($ area of $T) = \phi(1/2) + \phi(x_1 y_2) \leq \phi(1/2) = -\phi(2)$.

Next, we observe:

If a polyomino made up of standard squares as above is made up of n triangles of equal areas and, if an odd number of standard edges on its boundary have ends coloured blue and green, then $\phi(2A) \leq \phi(n)$, where A is the area of the polyomino:

Look at a triangle of the dissection which has all three colours and let B denotes its area.
Note that points in S_0, S_1, S_2 have different colours.
Now, $nB = A$ and $\phi(B) \leq -\phi(2)$; that is, $\phi(A) - \phi(n) \leq -\phi(2)$. Therefore,

$$\phi(n) \geq \phi(2A).$$

We now proceed to show that a special polyomino which is the union of an odd number of unit squares and is a union of triangles of equal areas, then the number of triangles is even.

We note that a standard (unit) edge with a blue end and a green end must be parallel to the X-axis and lies on a line whose height is odd.

Therefore, on the border of each standard square, there is an edge with a blue end and a green end.

Edges in the interior of the polyomino are adjacent to two standard squares whereas those on the boundary are adjacent to one standard square of the polyomino.

As there is an odd number of standard squares, the above observation applies and, implies that $\phi(2A) \leq \phi(n)$. But, $\phi(2A) \geq 1$; so n must be a multiple of 2.

2. Tiling Rectangles by Rectangles

Let us discuss tiling integer rectangles with integer rectangles now. Can we tile a rectangle of size 28×17 by rectangles of size 4×7?

At least, the area of the smaller rectangle divides that of the larger one (a necessary requirement for tiling). But, in fact, we don't have a tiling. Why?

Look at each row of the big rectangle. If we have managed to tile as required, then 17 would be a positive linear combination of 4 and 7. This is impossible.

Thus, two necessary conditions for tiling an $m \times n$ rectangle with $a \times b$ rectangles are:

(i) ab divides mn and,
(ii) each of m, n should be expressible as positive linear combinations of a, b.

Are these conditions sufficient for tiling?

Look at a 10×15 rectangle which we wish to tile with copies of a 1×6 rectangle.

The two necessary conditions mentioned clearly hold true in this case. However, a tiling is obviously impossible. Let us see why.

In fact, more generally, we claim that for copies of an $a \times b$ rectangle to tile an $m \times n$ rectangle, a third condition that is also necessary is that a must divide either m or n and b also must divide m or n.

To demonstrate this, look at a possible tiling.

We may suppose $a > 1$ (if $a = b = 1$, there is nothing to prove).

We colour the unit squares of the $m \times n$ rectangle with the different a-th roots of unity $1, \zeta, \zeta^2, \cdots, \zeta^{a-1}$ as follows.

Think of the rectangle as an $m \times n$ matrix of unit squares and colour the (i, j)-th unit square by ζ^{i+j-2}. Here is a suggestive figure:

a $a+1$

1	ζ	ζ^2	$\cdots$	$\cdots$	$1/\zeta$	1	ζ	$\cdots$	
ζ	ζ^2	ζ^3	$\cdots$						
ζ^2	ζ^3	$\cdots$							
$\vdots$									

Since each tile (copy of the smaller rectangle used) contains all the a-th roots of unity exactly once, and as the sum $1 + \zeta + \cdots + \cdots \zeta^{a-1} = 0$, the sum of all the entries of the $m \times n$ rectangle must be 0.

Therefore, $\sum_{i=1}^{m} \sum_{j=1}^{n} \zeta^{i+j-2} = 0$.

But this sum is the same as $(\sum_{i=1}^{m} \zeta^{i-1})(\sum_{j=1}^{n} \zeta^{j-1}) = 0$ which means one of these two sums must be 0.

But $\sum_{i=1}^{m} \zeta^{i-1} = 0$ if, and only if, $\zeta^m - 1 = 0$; that is, $a|m$. Similarly, the other sum is 0 if, and only if, $a|n$.

Thus, this condition that a divides m or n is necessary and, by the same reasoning it is necessary for tiling that b divides m or n.

Looking at the above proof, it is also easy to see how to tile when these conditions hold good. That is, we have the necessary and sufficient criterion:

Proposition. *An $m \times n$ rectangle can be tiled with copies of $a \times b$ rectangles if, and only if,*

(i) *ab divides mn,*
(ii) *m and n are expressible as non-negative linear combinations of a and b,*
(iii) *a divides m or n and b divides m or n.*

This generalizes in an obvious way to any dimension and we leave it to the reader to investigate this.

We discuss now the following result for which several proofs are available.

If a rectangle is tiled by rectangles each of which has at least one of its sides integral, then the big rectangle must also have a side of integral length.

We place the co-ordinate system such that all the sides of the rectangles have sides parallel to the co-ordinate axes.

Consider the function $f(x, y) = e^{2i\pi(x+y)}$ for $(x, y) \in \mathbf{R}^2$.

For a rectangle defined by $[a,b] \times [c,d]$, we have

$$\int\int f(x,y) = \int_a^b e^{2i\pi x} dx \int_c^d e^{2i\pi y}$$
$$= \left(\frac{e^{2i\pi b} - e^{2i\pi a}}{2i\pi}\right)\left(\frac{e^{2i\pi d} - e^{2i\pi c}}{2i\pi}\right).$$

Thus, the integral of f over a rectangle is zero if and only if it has at least one integer side is zero; hence, in case of a tiling by such rectangles, the integral is zero which means that the big rectangle has an integer side.

One of the beautiful results proved by Max Dehn using methods from topology (outside our scope here) is:

A rectangle of size $l \times b$ is tileable by squares if and only if l/b is a rational number.

He proved more generally:

Let R be a rectangle which has at least one side of rational length. If R is tiled by rectangles each of which has rational ratio of length to breadth. Then, all the sides of all the rectangles (including R) are of rational lengths.

Interestingly, this result of Dehn was re-proved by Brooks by associating an electrical network consisting of currents, voltages and resistances with the tiling and using well known properties of such networks. The discussions in this article would convince the reader that the subject draws from several areas of mathematics. However, we have mostly included only proofs which involve some simple algebra and basic number theory. Topological arguments require a more detailed discussion. In the next part of the article, we hope to discuss such aspects.

References

[1] F Richman and J Thomas, Problem 5471, *The American Mathematical Monthly*, **74**, p. 329, 1967.

[2] J Thomas, A dissection problem, *The Mathematics Magazine*, **41**, pp. 187–190, 1968.

[3] P Monsky, On dividing a square into triangles, *The American Mathematical Monthly*, **77**, pp. 161–164, 1970.

[4] S K Stein and S Szabo, Algebra & Tiling, *The Carus Mathematical Monographs* 25, Published by the Mathematical Association of America, 1994.

Polya's One Theorem with 100 pages of Applications

Believe me, Mathematics is an asset
in counting (it can aid and abet)
of different isomers even stereo.
We'd have bid it cheerio
but for this magic PET!

In 1937, George Polya wrote a paper which is considered one of the most significant papers in 20th-century mathematics [1]. The article contained one theorem and 100 pages of applications. It introduced a combinatorial method and led to hitherto unexpected applications to diverse problems in science. Very interestingly, we mention in passing that it was noticed and pointed out to the mathematical community only as late as 1960 by Frank Harary that Polya's work had already been anticipated in 1927 by J H Redfield [2].

Polya's theory of enumeration was discussed in detail in an earlier issue of *Resonance* by Shriya Anand [3], a summer student of the author. In what follows, we recall briefly some of this theory and complement the earlier article by adding some other applications not discussed there.

Let us start with an example. Consider the problem of painting the faces of a cube either black or white. How many such distinct coloured cubes are there? Since the cube has 6 faces, and we have 2 colours to choose from, the total number of possible coloured cubes is 2^6. But, painting the top face white and all the other faces black produces the same pattern as painting the bottom face white and all the other faces black as we can simply invert the cube and it looks the same! The answer to the above question is not so obvious. To find the various possible colour patterns which are inequivalent, we shall exploit the fact that the rotational symmetries of the cube have the structure of a group.

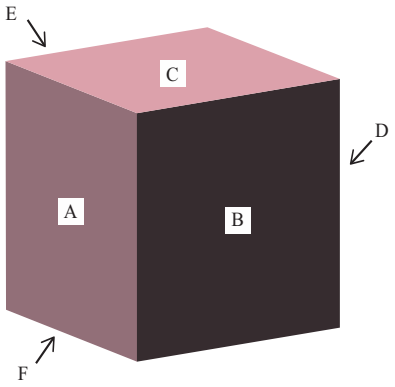
Before explaining how the above problem is dealt with by Polya's theory in more precise terms, we mention that the scope of Polya's theory is extraordinarily wide because of its very simple and very general expression. This theory deals with enumeration of mathematical configurations which can be thought of as placement of shapes in receptacles. More abstractly, we have mappings from a set D of receptacles to a set R of shapes. Thus, in a configuration, two elements of D may have the same image in R; that is, the

The chapter is a modified version of an article that first appeared in *Resonance*, Vol. 19, No. 4, pp. 338–346, April 2014.

same shape can be placed in more than one receptacle. Each shape is given a value and the value of a configuration is the total value of all the shapes. A typical problem would be to determine the number of configurations with a given value. Those permutations of the receptacles which yield another configuration which is equivalent to the original one, give rise to a group and the theory is stated in terms of this group. For instance, in the cube-colouring problem, let D be the set of 6 faces of the cube and R is the set of two colours black and white. A configuration here is a colouring of the faces by the two colours; that is, a mapping $\phi : D \to R$.

The group of rotations of the 6 faces has 24 elements (see the figure):

(i) the identity element;
(ii) rotating clockwise by 90 degree about the line through the centers of opposite faces like A and D (there are three such rotations);
(iii) rotating by 180 degrees about the line through the centers of opposite faces like A and D (there are three such);
(iv) rotating anti-clockwise by 90 degrees about the line through the centers of opposite faces like A and D (there are three such);
(v) rotating by 180 degrees about lines through the centers of diagonally opposite edges like the edge of the faces A and B and the edge of the faces D and E (there are six such);
(vi) rotating clockwise by 120 degrees about the line connecting diagonally opposite vertices like the vertex where A,B,C meet and the vertex where D,E,F meet (there are four such);
(vii) rotating anti-clockwise by 120 degrees about the line connecting diagonally opposite vertices like the vertex where A,B,C meet and the vertex where D,E,F meet (there are four of these).



Returning to the cube-colouring problem, let X be the set of all colourings. With respect to the group G of permutations of D, we can define an equivalence of elements in X as follows:

$\phi_1 \sim \phi_2$ if, and only if, there exists some $g \in G$ such that $\phi_1 g = \phi_2$.

As G is a group, $\sim$ is an equivalence relation on X. So, it partitions X into disjoint equivalence classes. It is clear that the orbits of the action i.e., the equivalence classes under $\sim$ are precisely the different colour patterns. Therefore, we need to find the number of orbits of the action of G on X. Polya's theorem has as its starting point a lemma known popularly as Burnside's lemma although it was already known due to Cauchy and Frobenius. That lemma says that for a group G of transformations on a set X, the number of orbits is $\frac{1}{|G|}\sum_{g\in G}|X^g|$ where X^g is the set of points of X fixed by g. In the problem of colouring cubes with two colours, this lemma suffices to find the number of configurations. We will describe this now. Finer information like how many configurations have 2 white faces and 4 black faces need the force of Polya's theorem.

In the cube-colouring problem with two colours, X has 2^6 elements. Let us see how the above mentioned 24 transformations affect X. The identity, of course, does not change anything; that is, fixes all the 2^6 elements of X. The rotation mentioned in (ii) above fixes all those colourings where the faces B,C,E,F have the same colour and A,D could be arbitrarily coloured. The description for transformations in (iv) is similar. For the transformation in (iii), the colours of B and E should match and so should the colours of C and F. The transformation described in (v) fixes those colourings where A and B have the same colour, D and E have the same colour and C and F have the same colour. Under the transformations of type (vi) and (vii), a colouring which is fixed must have three 'top' faces of the same colour and the 'bottom' three of the same colour. Thus, the sum $\sum_{g\in G}|X^g|$ equals

$$2^6 + 6\cdot 2^3 + 8\cdot 2^2 + 3\cdot 2^2\cdot 2^2 + 6\cdot 2^2\cdot 2 = 240.$$

Therefore, Cauchy–Frobenius–Burnside lemma gives the number of orbits to be $240/24 = 10$.

To describe Polya's theorems, we shall consider only finite sets D, R like in the example of the cube. For a group G of permutations on a set of n elements and variables $s_1, s_2, \ldots, s_n$, one defines a polynomial expression (called the cycle index) for each $g \in G$. If $g \in G$, let $\lambda_i(g)$ denote the number of i-cycles in the disjoint cycle decomposition of g. Then, the cycle index of G, denoted by $z(G; s_1, s_2, \ldots, s_n)$ is defined as the polynomial expression

$$z(G; s_1, s_2, \ldots, s_n) = \frac{1}{|G|}\sum_{g\in G} s_1^{\lambda_1(g)} s_2^{\lambda_2(g)} \ldots s_n^{\lambda_n(g)}.$$

For instance,

$$z(S_n; s_1, s_2, \ldots, s_n) = \sum_{\lambda_1+2\lambda_2+\ldots+k\lambda_k=n} \frac{s_1^{\lambda_1} s_2^{\lambda_2} \ldots s_k^{\lambda_k}}{1^{\lambda_1}\lambda_1! 2^{\lambda_2}\lambda_2! \ldots k^{\lambda_k}\lambda_k!}$$

We may view the above-mentioned configurations obtained by placing a set R of shapes in D receptacles also as a colouring problem – viz., the shapes can be thought of as colours and the receptacles as various objects to be coloured. Polya's theorem asserts:

Suppose D is a set of m objects to be coloured using a range R of k colours. Let G be the group of symmetries of D. Then, the number of colour patterns $= \frac{1}{|G|} z(G; k, k, \ldots, k)$.

The cycle index of the group G of symmetries of the 6 faces of the cube turns out to be

$$z(G; s_1, \cdots, s_6) = \frac{1}{24}(6s_1^2 s_4 + 3s_1^2 s_2^2 + 8s_3^2 + 6s_2^3 + s_1^6).$$

So, in our example of the cube, the number of distinct coloured cubes

$$= \frac{1}{24}\left(2^6 + 6 \cdot 2^3 + 8 \cdot 2^2 + 3 \cdot 2^2 \cdot 2^2 + 6 \cdot 2^2 \cdot 2\right) = 10.$$

There are 10 distinct coloured cubes in all, using two colours, as we saw above.

Incidentally, if we look at a regular octahedron, then the group of symmetries of the 6 *vertices* is the same group above of symmetries of the 6 *faces* of the cube.

A 'Valuable' Version of Polya's Theorem

The above version of Polya's theorem gives us the total number of configurations but we can retrieve finer information from other versions. We look at one example before proceeding to some other applications of Polya's theorem. As mentioned earlier, one could assign a value for each shape/ colour in R and enumerate the number of configurations with a given value. It is convenient to give values of shapes to be non-negative integers. One forms the generating function

$$c(x) = c_0 + c_1 x + c_2 x^2 + c_3 x^3 + \cdots$$

which is a polynomial where c_k is the number of shapes which have the value k. The finer version of Polya's theorem we are alluding to asserts that if a_k is the number of configurations whose total value is k, then the generating function

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$$

is obtained by substituting $c(x^r)$ for s_r in the cycle index.

For simplicity, suppose R has two elements Black and white which have values 0 and 1. Then, the generating polynomial above is simply $1 + x$.

Let us discuss the example of chlorination of Benzene where some hydrogen atoms get substituted by Chlorine atoms. Give the values 0 and 1 to Cl and H, and note that the group of symmetries of the Benzene molecule is the group of rotations of the regular hexagon, which is the so-called dihedral group D_6 of order 12. The cycle index of D_6 is

$$z(D_6) = \frac{1}{12}\left(s_1^6 + 4s_2^3 + 2s_3^2 + 3s_1^2 s_2^2 + 2s_6\right).$$

Substituting $1 + x^r$ for s_r's, we obtain the polynomial

$$\frac{1}{12}\left((1+x)^6 + 4(1+x^2)^3 + 2(1+x^3)^2 + 3(1+x)^2(1+x^2)^2 + 2(1+x^6)\right)$$
$$= 1 + x + 3x^2 + 3x^3 + 3x^4 + x^5 + x^6.$$

Therefore, the number of configurations which have 2 chlorine atoms is the coefficient of 4 which is 3. These are the ortho dichlorobenzenes, meta dichlorobenzenes and para dichlorobenzenes where the gap between the vertices corresponding to the carbon atoms to which the two chlorine atoms are attached are $1, 2$ and 3 edges respectively.

More general weighted versions of Polya's theorem as well as the immediate applications to enumerating isomers of chemical compounds have been discussed in detail in the earlier article in 2002.

Graph Enumeration

A key application of Polya's theorem is to the enumeration of graphs. Indeed, the introduction of Polya's paper begins with the words (as translated by Read):

"*This paper presents a continuation of work done by Cayley. Cayley has repeatedly investigated combinatorial problems regarding the determination of the number of certain trees. Some of his problems lend themselves to chemical interpretation: the number of trees in question is equal to the number of certain theoretically possible chemical compounds.*"

Indeed, a chemical compound with no multiple bonds corresponds to a tree where different types of vertices correspond to different atoms. In case of multiple bonds, one may regard different kinds of edges also.

A tree consists of vertices and edges and is a connected graph where each edge connects two vertices. There can be several edges meeting at a vertex. There is no closed path. Therefore, the number of edges is one less than the number of vertices. A vertex is called r-edged if there are exactly r edges originating there.

Consider an alkane – this has a formula C_nH_{2n+2}. The carbon atoms are usually assumed to have valency 4 which means that the structure of the alkane is determined (that is the positions of the hydrogen atoms are uniquely determined) by the structure formed by the carbon atoms. Topologically different trees with n four-edged vertices and $2n+2$ one-edged vertices correspond to the different isomers with the molecular formula C_nH_{2n+2}.

Thus, the enumeration of isomers as above is equivalent to the enumeration of trees as above. Interestingly, in Polya's paper, he describes the groups of symmetries for certain chemical compounds as so-called wreath products. Polya calls wreath products as coronas. As far as one can ascertain, this is the first introduction and study of finite wreath products as permutation groups.

Polya's theorem was generalized by de Bruijn in a way which allows one to permute the shapes in R also.

Musings on Music

Polya's theorem has been applied to the theory of music. One may determine the number of chords. To define this, one takes the n-scale to be the integers from 0 to $n-1$ under addition modulo n. There are translations $a \mapsto a+i$, where $0 \leq i < n$. An equivalence class (that is an orbit) is called a chord and, one wishes to determine for each $r < n$, the number of r-chords; that is, the number of orbits consisting of r elements. This is equivalent to colouring the n-notes by two colours – we choose the notes in the chord by colouring them by one colour and those which are not in it by the other colour. The group is simply the cyclic group of order n whose cycle index is:

$$z(C_n; s_1, \cdots, s_n) = \frac{1}{n} \sum_{d|n} \phi(d) s_d^{n/d}.$$

In this, we substitute $1+x^d$ for s_d and obtain the generating function whose coefficient of x^r is the number of r-chords.

We obtain the number of r-chords to be

$$\frac{1}{n} \sum_{d|(n,r)} \phi(d) \binom{n/d}{r/d}.$$

Sometimes, one allows for a bigger group of transformations of the scale by allowing inversion $a \mapsto -a$ also. Then, the group becomes the dihedral group D_n of order $2n$ formed by the translations and the transposition above. In this case, as we have the cycle index of D_n to be

$$z(D_n; s_1, \cdots, s_n) = \frac{1}{2n} \sum_{d|n} \phi(\frac{n}{d}) s_{n/d}^d + \frac{1}{4}(s_1^2 s_2^{\frac{n}{2}-1} + s_2^{\frac{n}{2}})$$

if n is even and

$$z(D_n; s_1, \cdots, s_n) = \frac{1}{2n} \sum_{d|n} \phi(\frac{n}{d}) s_{n/d}^d + \frac{1}{2} s_1 s_2^{\frac{n-1}{2}}$$

if n is odd, we may determine the number of r-chords in this dihedral case to be:

$$\frac{1}{2n} \sum_{d|(n,r)} \phi(d) \binom{n/d}{r/d} + \frac{1}{2} \binom{[n/2]}{[r/2]}$$

if n is odd;

$$\frac{1}{2n} \sum_{d|(n,r)} \phi(d) \binom{n/d}{r/d} + \frac{1}{2} \binom{n/2}{r/2}$$

if n, r are even and;

$$\frac{1}{2n} \sum_{d|(n,r)} \phi(d) \binom{n/d}{r/d} + \frac{1}{2} \binom{\frac{n}{2}-1}{[r/2]}$$

if n is even and r is odd.

For instance, in 12-tone music with dihedral symmetry, the number of pentachords is computed to be 38.

For more details, the interested reader may see the paper [4] by Reiner.

The paper of Polya was in German and was translated by RC Read and this appears in a book now (see[5]). Also, several interesting generalizations and applications have been discussed by Krishnamurthy in the book [6] available in an Indian edition.

References

[1] G Polya, Kombinatorische Anzahlbestimmungen fur Gruppen, Graphen und chemische Verbindungen, *Acta Mathematica*, **Vol. 68**, pp. 145–254, 1937.

[2] J H Redfield, The theory of group reduced distributions, *Amer. J.Math.*, **49**, pp. 433–455, 1927.

[3] Shriya Anand, How to count – an exposition of Polya's theory of enumeration, *Resonance*, pp. 19–35, September 2002.

[4] David L Reiner, Enumeration in music theory, *The American Mathematical Monthly*, pp. 51–54, January 1985.

[5] G Polya and R C Read, *Combinatorial enumeration of groups, graphs, and chemical compounds*, Springer-Verlag, 1987.

[6] V Krishnamurthy, *Combinatorics – Theory and Applications*, Affiliated East-West Press Private Limited, 1985.