S Chowla and S S Pillai

The Story of Two Peerless Indian Mathematicians

B Sury and R Thangadurai

Ramanujan's story has been well-chronicled and it is well-known that generations of mathematicians in India have been inspired by it. However, not much has been written about the period immediately following Ramanujan's. Two of the most famous Indian mathematicians of this period are Sarvadaman Chowla and S S Pillai. We journey through some of the very interesting and illuminating correspondences between Chowla and Pillai. We also attempt to convey some of the beauty and depth of their mathematical work.

B Sury (left) introduces this article as:

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"!

R Thangadurai (right) is with the Harish-Chandra Research Institute in Allahabad. His main area of interest is number theory.

1. Introduction

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 Genealogy Project lists both Ramanujan and Chowla among the students of Littlewood! This article specially features Chowla and Pillai. The journal *Resonance* had already featured Pillai [1]; however, 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 Pillai which reveals also other personal and historical aspects. Apart from that, we discuss Chowla's and Pillai's mathematical works. We select only those topics which are more elementary or easy to describe

Keywords
Chowla–Pillai correspondence, Waring's problem, binary quadratic forms, class number, error asymptotics for Euler's function, Langlands conjectures.

S Chowla

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 that 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. While discussing their proofs, 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 non-trivial. 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, "*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–Pillai Correspondence

Starting in the late 1920s, and up to one month before Pillai's demise in 1950, Chowla and Pillai maintained a regular correspondence. Interestingly, in the earliest available letter dated 8th of January, 1929, Chowla mentions among other things that the number 175,95,9000 is the smallest integer that can be expressed as sum of two positive cubes in three different ways. He goes on to express the hope that now they can "begin their proper work". 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 (See *Box* 1).

S S Pillai

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 $\sum^{x}_{1} f(\sqrt{n}\,\theta)$ 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 $O(\sqrt{x})$ which he later improved to $O(x^{\frac{7}{29}+\varepsilon})$. [transcendental only for $O(x^{\frac{2}{5}})$ Gött. Nach 1924]

Box 1. Continued...

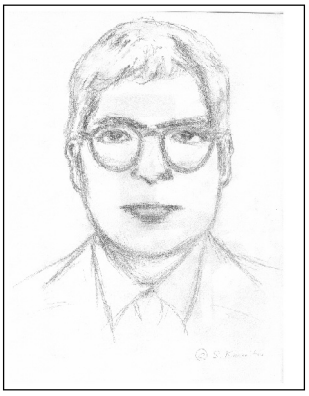
Box 1. Continued...

I am sorry for my mistake.
If there any misprints in
our G. 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 it in Madras Univ. Library)

The correspondence also reveals the intellectual honesty they possessed and the joy each drew from the other's successes. One of the letters written by Chowla after he joined St.Stephens College in Delhi expresses his reluctance to be a coauthor of some result where he felt he had not contributed enough. Through the years, he expresses almost in every letter his gladness for the correspondence between them!



Sketch of S S Pillai by mathematician Kanemitsu.

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 US 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.

3. 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 [2], we mention this problem in passing.

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

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.

power of a whole number. Hilbert had shown that such a finite number $g(k)$ does exist. The ideal Waring 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 actually an equality. 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 present, the ideal Waring conjecture is known to hold for all large enough k.

4. 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:

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*.

Theorem. *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 $l(p) < \sqrt{p/3}$. If $h(-p) = 1$, then $l(p) = (p+1)/4$ (and, therefore, $(p+1)/4$ is prime!).

Remarks.

• The theorem implies, in particular, that for primes $p > 3, p \equiv 3 \bmod 8$, we have $l(p) = (p+1)/4$ if and only if $h(-p) = 1$, because $\sqrt{p/3} < (p+1)/4$ for $p > 3$.

• 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] pointed out that Chowla's question has infinitely many negative answers by showing: *For any fixed irregular prime p less than*

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.

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

$$\frac{(p^{n-1}-1)B_n}{n} \mod p^k$$

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.

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.

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 $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030$. 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:

$$1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, 121, 125, 128, \cdots .$$

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:

Conjecture. *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 has not been proved 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.

This conjecture has not been proved 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 Cotangent Function

A typical aspect of Chowla's works has been to come back to an old result after several years and apply 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 this 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:

Theorem. *Let p be a prime number and $x_r = \cot(\pi r/p)$ for $r = 1, \cdots, (p-1)/2$. If $a_i \in \mathbf{Q}$ are such that $\sum_{i=1}^{(p-1)/2} a_i x_i = 0$, then $a_i = 0$ for all $i \leq (p-1)/2$.*

Chowla uses some very basic Galois theory to deduce that, under the assumption

$$\sum_{i=1}^{(p-1)/2} a_i x_i = 0,$$

there are $(p-1)/2$ such linear relations which may be captured by the matrix relation,

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_{(p-1)/2} \\ x_2 & x_3 & \cdots & x_1 \\ & \ddots & \ddots & \\ x_{(p-1)/2} & x_1 & \cdots & x_{(p-3)/2} \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{(p-3)/2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

If the a_i's are not all 0, this leads to the vanishing of the 'circulant' 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. That is, the determinant in the 3×3 case is given as:

$$\begin{vmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \\ x_3 & x_1 & x_2 \end{vmatrix} =$$

$$-(x_1 + x_2 + x_3)(\omega x_1 + \omega^2 x_2 + x_3)(\omega^2 x_1 + \omega x_2 + x_3).$$

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

$$\omega^r x_1 + \omega^{2r} x_2 + \cdots + \omega^{r(p-1)/2} x_{(p-1)/2}$$

as r varies from 1 to $(p-1)/2$, where $\omega = e^{4\pi i/(p-1)}$, a $(p-1)/2$-th root of unity.

Here, Chowla realizes with surprise that the above factors (up to certain non-zero factors) are none other than the special values at $s = 1$ of certain functions $L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)/n$ called Dirichlet L-functions corresponding to Dirichlet characters χ modulo p which satisfy $\chi(-1) = -1$. The non-vanishing of these are the older

Chowla realizes with surprise that the factors (up to certain non-zero factors) are none other than the special values at $s = 1$ of certain functions $L(s, \chi) = \sum_{n=1}^{\infty} \chi(n)/n$ called Dirichlet L-functions corresponding to Dirichlet characters χ modulo p which satisfy $\chi(-1) = -1$.

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!

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.

• 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* $\phi(k)/2$ *real numbers*

$$\frac{\mathrm{d}^s}{\mathrm{d}x^s} \cot\left(x + \frac{r\pi}{k}\right)_{x=0}, \quad r \leq \frac{\phi(k)}{2}, \ (r,k) = 1,$$

are linearly independent over $\mathbf{Q}$.

• The non-vanishing at $s = 1$ of $L(s, \chi)$ for non-trivial 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 $(a, b) = 1$.

• Kenkichi Iwasawa [12] showed 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 Kummer's result: 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 $\frac{p-1}{2}$ cotangent values ensures 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 showed that 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. 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. In the permutation group S_n, let $A_n(d)$ denote the number of permutations σ satisfying $\sigma^d = I$, the identity permutation. In collaboration with Herstein and Scott, he showed [13]:

$$\sum_{n=0}^{\infty} \frac{A_n(d)x^n}{n!} = \exp(\sum_{k|d} \frac{x^k}{k}).$$

For 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

$$xf'(x) = \sum_{j \geq 0} \frac{A_j(d)}{j!} \sum_{k|d} x^{j+k} = f(x) \sum_{k|d} x^k \ .$$

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

$$\sum_{n \geq 0} \frac{A_n(d)}{n!} = \exp\left(\sum_{k|d} \frac{x^k}{k} \right) \qquad (*)$$

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 $(*)$, 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 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 $\sigma^d =$ 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

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.

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 $18518809 = 197^2 + 1848 \cdot 100^2$ 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 a 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 its *discriminant.* Since

$$4af(x, y) = (2ax+by)^2+(4ac-b^2)y^2 = (2ax+by)^2-dy^2,$$

A beautiful result of Chowla shows at least that the list of idonean numbers is finite!

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 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 the following: *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]: *$h(d)/2^t \to \infty$ 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.

For $d < 0$, the number $h(d)$ of classes of primitive, positive-definite binary quadratic forms of discriminant d is finite.

Euler obtained the following list of 65 numbers called 'Numerus idoneus' ('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,

Euler observed that $18518809 = 197^2 + 1848 \cdot 100^2$ is a prime by showing 1848 is idonean.

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 coprime to n and 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 $18518809 = 197^2 + 1848 \cdot 100^2$ is a prime by showing 1848 is idonean.

It is not clear whether the list of idonean numbers is finite or not. This can be analyzed (and was done 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 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 $h(d)/2^t \to \infty$ 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 complete[1].

[1] Euler's list of idonean numbers has been proved to be complete 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. 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, and the discriminant of a quadratic form $ax^2 + bxy + cy^2$ is the number $b^2 - 4ac$. Then:

Theorem. *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 $t^2 - 4$.*

Here is an easy proof. 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

$$F := \begin{pmatrix} (t-q)/2 & p \\ -r & (t+q)/2 \end{pmatrix} \in SL_2(\mathbf{Z}).$$

Note that indeed, $\det F = (t^2-q^2)/4 + pr = 1$ and trace $F = t$.

Further, consider any equivalent form $f'(x,y)$ $= f(ax+by, cx+dy)$ with $M := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$. 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

$$3x^2 + 9xy - 3y^2, \quad x^2 + 9xy - 9y^2$$

respectively. However, they are evidently inequivalent because the first one takes only multiples of 3 as values whereas the second one takes values such as 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 the 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 $3x^2/\pi^2$ for all $x = 1, 2, \cdots, 1000$. However, he failed to notice that $E(820) < 0$ and made a conjecture that

In analytic number theory, to study such fluctuating arithmetical functions, one often looks at their *average behaviour*.

$E(x) \geq 0$ 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 that an error estimate, 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 $E(x) = \Omega(x \log\log\log x)$.

This result took many years to generalize. A conjecture by Montgomery which is still open, asserts:

$$E(x) = O(x \log\log x) \text{ and } E(x) = \Omega_{\pm}(x \log\log x).$$

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 an $n \times n$ grid with n^2 squares is given in the plane. Let P and Q be two players competing. By turns each marks a square. Whoever marks t squares in a straight line first, 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, 1620 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 in 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[2]. For other applications, the interested reader may consult [18] and [19].

[2] H C Longuet-Higgins, Letter to a musical friend, *Music Review*, pp.244–248, August 1962.

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 7th 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:

Theorem 1. *If $p_1, p_2, \cdots, p_r \leq y$ are all the prime numbers less than y, then when $x \to \infty$,*

$$\frac{\psi(x,y) - \frac{(\log x)^r}{r!\prod_{i=1}^r \log p_i} + \frac{(\log x)^{r-1}\log(p_1 \cdots p_r)}{2(r-1)!\prod_{i=1}^r \log p_i})}{\log^{r-1} x} \longrightarrow 0.$$

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 $\psi(y^u, y)/y^u$ as $u \to \infty$'?

A more rigorous proof of Dickman's result, by 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!

[3] See p.337 of S Ramanujan, *The Lost Notebook and Other Unpublished Papers*, Narosa Publishing House, 1988.

It should be mentioned that Ramanujan[3] has the following entry in his notes. We write in the standard notations as above:

$$\psi(x,x^c) \sim x\left(1-\int_c^1 \frac{\mathrm{d}u}{u}\right) \quad \text{if } 1/2 \leq c \leq 1;$$

$$\sim x\left(1-\int_c^1 \frac{\mathrm{d}u}{u}+\int_c^{1/2}\frac{\mathrm{d}v}{v}\int_v^{1-v}\frac{\mathrm{d}u}{u}\right) \quad \text{if } 1/3 \leq c \leq 1/2;$$

$$\sim x\left(1-\int_c^1 \frac{\mathrm{d}u}{u}+\int_c^{1/2}\frac{\mathrm{d}v}{v}\int_v^{1-v}\frac{\mathrm{d}u}{u}- \int_c^{1/3}\frac{\mathrm{d}z}{z}\int_z^{(1-z)/2}\frac{\mathrm{d}v}{v}\int_v^{1-v}\frac{\mathrm{d}u}{u}\right) \quad \text{if } 1/4 \leq c \leq 1/3;$$

and so on.

This is nothing else than Dickman's asymptotic formula for $\psi(x,y)$!

15. Chowla and the Langlands Conjecture

[4] This section is mostly taken from the lecture of Professor Ram Murty at Kerala School of Mathematics, Calicut where the second author was present. He is thankful to Professor Ram Murty for allowing him to include the contents in this write-up.

In this last section[4], 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].

For each integer $n \geq 1$, define $d(n)$ as 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:

$$d(N) \leq 2^{\frac{\log N}{\log\log N}} \text{ for all } N \geq 2$$

and he produced infinitely many integers N for which this 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

$$d(N) \leq N^{\epsilon} \text{ for all } N \geq N_0.$$

Chowla proved this deduction using another argument involving Dirichlet series. Let $r \geq 1$ be any integer and let

$$L_r(s) = \sum_{n=1}^{\infty} \frac{d(n)^r}{n^s} \text{ where } s \in \mathbb{C} \text{ with } \mathrm{Re}(s) > 1.$$

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 $r \geq 1$. Here, $\mathrm{Re}(s)$ denotes the real part of s. 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 constants $M > 0$ and $c > 0$ 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

$$\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24}, \text{ where } z \in \mathbb{C} \text{ with } \mathrm{Im}(z) > 0,$$

where $\mathrm{Im}(z)$ denotes the imaginary part of z and $q = e^{2\pi iz}$. This is often called *Ramanujan's delta function* because of his fundamental contribution to it, though it was already studied by Jacobi and others.

The delta function satisfies the following property: *for all* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ (*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 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Z})$ 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 $\tau(n)$ are 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.

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 $s \in \mathbb{C}$ with $\mathrm{Im}(s) > 0$.

Since $\tau(n)$ is a multiplicative function (the first conjecture of Ramanujan mentioned earlier 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, we have, for all primes p,

$$\sum_{a=0}^{\infty} \tau_{p^a} X^a = \frac{1}{1 - \tau_p X + X^2} = \frac{1}{(1-\alpha_p X)(1-\beta_p X)},$$

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*, Edited by James G Huard and Kenneth S Williams, CRM Univ. de Montreal, Vols 1,2,3, 1999.
- *Collected works of S. S. Pillai*, Edited by R Balasubramanian and R Thangadurai, Ramanujan Mathematical Society Collected Works Series, 2010.

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 $\mathrm{Re}(s) > 1$.

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 $\mathrm{Re}(s) > 1$ 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 $r \leq 9$.

Suggested Reading

[1] B Sury, 'S S Pillai', *Resonance*, Vol.9, No.6, pp.2–3, 2004.

[2] C S Yogananda, 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, 3rd Ed., 1954.

[4] S Chowla, The least prime quadratic residue and the class number, *J. Number Theory*, Vol.22, pp.1–3, 1986.

[5] S Chowla, On a conjecture of Ramanujan, *Tohoku Math. J.*, Vol.33, pp.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, Vol.12, pp.199–201, 1940.

[9] S S Pillai, On the inequality $0 < a^x - b^y \leq n$, *Journal Indian M. S.*, Vol.19, pp.1–11, 1931.

[10] S Chowla, The non-existence of non-trivial linear relations between the roots of a certain irreducible equation, *J. Number Theory*, Vol.2, pp.120–123, 1970.

[11] Kai Wang, On a theorem of Chowla, *J. Number Theory.*, Vol.15, pp.1–4, 1982.

[12] R Ayoub, On a theorem of Chowla, *J. Number Theory*, Vol. 7, pp.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) Vol.25, pp.29–31, 1952.

[14] L Euler, De Formulis specei $mxx+nyy$ ad numeros primos explorandos idoneis earumque mirabilis proprietatibus, *Opera Omnia* I, Vol.4, Teubner, pp.269–289, 1916.

[15] G Frei, Leonhard Euler's convenient numbers, *Math. Intell.*, Vol.7, No.3, pp.55–58, 64, 1985.

[16] S Chowla, An extension of Heilbronn's class-number theorem, *Quart.J.Math.*, Vol.5, pp.304–307, 1934.

[17] S Chowla, J Cowles and M Cowles, On the number of conjugacy classes in *SL* (2, Z), *J. Number Theory*, Vol.12, pp.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*, Vol.5, No.2, pp.411–484, 1993.

[20] Ram Murty, Topics in Number Theory, *Mehta Research Institute Lecture Note* No.1, 1993.

Address for Correspondence
B Sury
Stat-Math Unit, Indian Statistical Institute
8th Mile Road
Bangalore 560 059
Email: sury@isibang.ac.in

R Thangadurai
Harish-Chandra Research Institute, Chhatnag Road, Jhusi, Allahabad 211019
Email: thanga@hri.res.in