# Some Unsolved Problems in Number Theory

## Progress Made in Recent Times

*K Ramachandra*

The beauty of the theory of numbers is that it poses so many simple-looking problems most of which remain unsolved even today. Many of these problems have come down to us from ancient times, indicating the age-old fascination that human beings have felt for numbers. We list a few of these problems below, describing some known results and indicating the progress made in recent times.

## The Infinitude of Primes

It is easy to show that the list 2, 3, 5, 7, 11, ... of primes does not terminate. The biggest prime known explicitly today has more than $10^5$ digits! Now consider pairs of primes that differ by 2, for instance $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, .... These are the so-called *twin primes*. It is not known as of today whether the list of twin primes terminates or not. It *is* known that the sum $1/3 + 1/5 + 1/11 + 1/17 + \cdots = \sum 1/p$ taken over all primes $p$ such that $p+2$ is prime is finite (indeed, the sum, known as *Brun's constant*, can be computed to a fair degree of accuracy), but this does not prove that there are only finitely many such primes. (It is clearly possible for a sum of infinitely many positive numbers to be finite; for instance, this happens with the sets $\left\{\frac{1}{1}, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \cdots\right\}$ and $\left\{\frac{1}{1}, \frac{1}{4}, \frac{1}{9}, \frac{1}{16}, \frac{1}{25}, \ldots,\right\}$. Ancient Greeks believed this was impossible. The well-known paradoxes of Zeno are related to this observation.) The best that we know today is that the list of pairs $(p,q)$ of primes with

$$0 < p - q < c \ln p \qquad (c = 1/4)$$

does not terminate. This is a very deep result due to H Maier of Germany. (Actually his constant $c$ is slightly less than $1/4$.) We are very far from this result for, say, $c = 1/100$.

Another question deals with the number $\pi(x)$ of primes $p$ below $x$. It was noticed by Legendre, Gauss, Riemann and others that $\pi(x)$ is roughly equal to $x/\ln x$; this is equivalent to saying that the $n^{\text{th}}$ prime is roughly equal to $n \ln n$. Chebychev showed that there exist constants $a, b$ such that

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

for all $x$. Using the methods of complex variables, Hadamard and de la Vallee Poussin proved independently in the 1890's that

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

Instead of $\pi(x)$, it is nicer to deal with the function $Q(x)$ which counts the prime $p$ with the weight $\ln p$; that is, $Q(x) = \sum_{p \le x} \ln p$. It was proved around the turn of the century that

$$|Q(x) - x| < x\left(e^{\sqrt{\ln x}}\right)^{-h}$$

for all $x > 10^{100}$ and a certain absolute positive constant $h$. The precise value of

$h$ is not important. One of the deepest results in prime number theory is the theorem that the term $e^{\sqrt{\ln x}}$ can be replaced by

$$e^{(\ln x)^{3/5}(\ln \ln x)^{-1/5}}.$$

This result is due to the Soviet mathematician I M Vinogradov.

## Additive Prime Number Theory

In 1742 Goldbach asked, in a letter to Euler, whether every even number from 6 onwards can be expressed as a sum of two odd primes. The answer to this question is unknown even today! The achievements in this problem have a very long history. Using the so-called 'circle method' pioneered by Ramanujan–Hardy, Hardy and Littlewood showed that if the hypothesis formulated below holds true, then every odd number from some point onwards can be expressed as a sum of 3 odd primes. The hypothesis is stated in terms of the following function $\mu$ defined on the set of positive integers:

$$\mu(n) = \begin{cases} 1, & \text{for } n = 1; \\ 0, & \text{if } n \text{ is divisible by the square of a prime;} \\ (-1)^k, & \text{if } n \text{ is the product of } k \text{ distinct primes.} \end{cases}$$

Let $a, b$ be positive integers, and let $h > 3/4$ be a constant. The hypothesis then states that the following inequality holds for all $x > N(a,b,h)$, where $N$ is some function that depends only on $a, b, h$:

$$\left|\sum \mu(an+b)\right| \leq x^h.$$

(The 'circle method' was developed by Ramanujan and Hardy while they were working on the partition problem. The problem is to find an asymptotically accurate formula for $p(n)$, the number of partitions of $n$ or the number of ways that $n$ can be written as an unordered sum of positive integers ($p(1) = 1$, $p(2) = 2$, $p(3) = 3$, $p(4) = 5$, ...). It has been known from the time of Euler that

$$\prod_{j=1}^{\infty}\left(1 - z^j\right)^{-1} = \sum_{n=1}^{\infty} p(n) z^n.$$

Let $f(z)$ denote the infinite product on the left side. The singularities of $f(z)$ are the roots of unity and lie densely on the unit circle $|z| = 1$; thus $f(z)$ has the unit circle as its circle of convergence. Using Cauchy's residue theorem, we obtain

$$p(n) = \frac{1}{2\pi i} \oint_{|z|=r} \frac{f(z)}{z^{n+1}} dz,$$

for $0 < r < 1$. Thus the problem of estimating $p(n)$ has been converted into one of estimating an integral. The beautiful and amazingly productive idea pioneered by Ramanujan and Hardy was to estimate the integral by identifying the points where 'most' of the contribution comes from; these are clearly the points on $|z| = r$ that lie 'close' to the poles of $f(z)$. The practical details are formidable, but what is of significance is that the method, originally conceived to tackle the partition problem, has turned out to be applicable to a large class of related problems—for instance, Waring's problem.)

s

This hypothesis is open as of today. It is considered very difficult to prove, even in the special case $a = b = 1$, $h = 1 - 10^{-100}$.

However, in 1937 Vinogradov proved the same result without having to use any unproved hypothesis. A recent result in the direction of Goldbach's conjecture is the one by O Ramare: *Every positive even number can be expressed as a sum of not more than 6 primes.* Another result by the author and his colleagues A Sankarayanan and K Srinivas is the following: let $g_n$ denote the $n^{\text{th}}$ even number expressible as a sum of 2 odd primes ($g_1 = 6, g_2 = 8, g_3 = 10, \ldots$). We do not know whether the range of $g$ exhausts the even numbers beyond 6, but the following is now known:

$$(g_{n+1} - g_n)^{37} < k g_n \qquad \text{for all } n,$$

where $k$ is a positive constant independent of $n$.

## Waring's Problem

Let $k$ be any natural number greater than 1. More than two centuries back, E Waring conjectured the following. *Let $g(k) = 2^k + [1.5^k] - 2$ and write $g$ for $g(k)$. Then every positive integer $n$ can be expressed as a sum of $g$ or fewer positive $k^{\text{th}}$ powers; that is, for all $n \in \mathbf{N}$ there exist non-negative integers $x_1, x_2, \ldots, x_g$ such that $n = x_1^k + x_2^k + \cdots + x_g^k$.* It is not too hard to check that the number $q = 2^k[1.5^k] - 1$ cannot be expressed as a sum of fewer than $g$ positive $k^{\text{th}}$ powers; that is, the equation

$$x_1^k + x_2^k + \cdots + x_{g-1}^k = q$$

has no solution in non-negative integers $x_i$. (*Example*: Let $k = 3$; then $g = 8 + 3 - 2 = 9$ and $q = (8 \times 3) - 1 = 23$. Since $23 < 3^3$, to express 23 as a sum of positive cubes we must use only the summands 1 and 8, and since $23 = (2 \times 8) + (7 \times 1)$, we require at least 9 such summands. Thus 23 cannot be expressed as a sum of fewer than 9 positive cubes.) Thus $g$ is the most economical number of summands.

The current status of the problem is as follows: *There exists an absolute positive constant $C$ such that Waring's conjecture is true for all $k > C$.* The proof derives from the ideas of Ramanujan, Hardy, Littlewood, Vinogradov, Dickson, Ridout and Mahler and is very complicated, running to hundreds of pages. It should be mentioned that the proof only establishes the existence of $C$ and gives no clue as to its magnitude; no $C$, however large, can be calculated by the method of proof.

## Problems on Irrationality

Consider the zeta function $\zeta(t)$ defined for real numbers $t > 1$ as follows: $\zeta(t) = \sum_{n \geq 1} 1/n^t$. One of the grand achievements of the century is the proof that

$$\zeta(3) = 1 + \frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{4^3} + \cdots$$

is irrational. (An *irrational number* is one that is not expressible as a ratio of two non-zero integers. Related to the idea of irrationality is the notion of transcendence. A number is *algebraic* if it is the root of a polynomial with integral coefficients; else it is *transcendental*. Examples of algebraic irrationals are $\sqrt{2}$, $\sqrt[3]{2}$

and $\sqrt[3]{10} + \sqrt[5]{21}$, and examples of transcendental numbers are $\pi$, $e$ and $\ln 2$ (here $e = 2.71828\ldots$ is Euler's number). The proof that a given number is transcendental can be extremely difficult.) The proof is due to R Apery. What happens when $t$ is an odd positive integer greater than 3 is open. Strangely, a great deal is known when $t$ is an even positive integer. Indeed, it is known that the value of $\zeta(t)$ is a rational multiple of $\pi^t$ whenever $t$ is an even positive integer. (This has been known since the time of Euler.) This immediately implies that $\zeta(t)$ is irrational, indeed transcendental, when $t$ is an even positive integer. The paucity of positive conclusions for the case when $t$ is an odd positive integer is extremely curious.

Much the same can be said for Euler's constant $\gamma$, defined thus:

$$\gamma = \lim_{n\to\infty}\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right) - \ln n.$$

Amazingly, it is not known whether $\gamma$ is rational or not.

The transcendency of numbers such as $\pi + \ln 2$ was first proved by A Baker. These are deep results.

## Concluding Remarks

It appears that there is no dearth of attractive problems. What is needed are solutions! What has been solved is very little and what remains to be solved is vast. 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.

**K Ramachandra, Honorary Visiting Professor, National Institute of Advanced Studies, Indian Institute of Science Campus, Bangalore 560 012, India.**