A Promising Approach to the Twin Prime Problem

Bhaskar Bagchi

Bhaskar Bagchi is with the Indian Statistical Institute since 1971, first as a student and then as a member of the faculty. He is interested in diverse areas of mathematics like combinatorics, elementary and analytic number theory, functional analysis, combinatorial topology and statistics.

The famous twin prime conjecture asserts that there are infinitely many pairs of primes differing by 2. More generally, it is conjectured that for any even number h, there are infinitely many pairs of primes differing by h. (This is obviously false for odd h.) Indeed, in a famous paper, G H Hardy and J E Littlewood made the following (much stronger) conjecture.

Let $\pi_h(x)$ denote the number of primes $p \leq x$ for which $p+h$ is also prime. Clearly the twin prime conjecture amounts to saying that $\lim_{x \to \infty} \pi_h(x) = \infty$ for any even h. Hardy and Littlewood hazarded the guess:

$$\pi_h(x) \sim C_h \frac{x}{(\log x)^2} \text{ as } x \to \infty. \quad [1]$$

Recall that the symbol $\sim$ means that the functions on its two sides are 'asymptotically equal'. That is, their ratio converges to 1 in the indicated limit. The constant C_h which occurs in [1] is a very strange one! It is explicitly given by the (conjectured) formula

$$C_h = \left(\prod_{p \mid h} \left(1 + \frac{1}{p-1} \right) \right) \left(\prod_{p \nmid h} \left(1 - \frac{1}{(p-1)^2} \right) \right). \quad (1)$$

The products in (1) are over primes p. The first product is over the (finitely many) primes dividing h while the second product is over all the other primes. Notice that when h is odd, $1 - \frac{1}{(2-1)^2} = 0$ occurs as a factor in the second product, so that $C_h = 0$ for odd h, as it ought to be. But whence came the strange formula (1) for even values of h? It arose in a 'heuristic proof' of [1] given by Hardy and Littlewood. Mathematicians talk of a heuristic proof when they have a 'proof', which looks 'essentially correct' to them – despite having seri-

Keywords
Twin primes, Ramanujan sum.

ous technical gaps in it, which bar them from calling it a genuine proof.

The heuristic proof of Hardy and Littlewood is probabilistic in nature. Its technical gap consists in the untenable assumption that divisibility by two or more distinct primes are independent random events! While every number theorist 'knows' in her heart that God is playing dice with the primes, this is of course absurd. The primes arise out of a totally deterministic process. There is nothing random in the Sieve of Eratosthenes!

While every number theorist 'knows' in her heart that God is playing dice with the primes. The primes arise out of a totally determinstic process. There is nothing random in the Sieve of Eratosthenes!

Following the lead of Hardy and Littlewood, number theory now abounds in probabilistic 'heuristics'. They are notoriously difficult to rigorise, even while they carry great conviction to the cognoscenti. A whole new branch of number theory called 'sieve theory' has been created in the attempt to justify them. Unfortunately, as of now, this theory works within a very narrow range of the relevant parameters. This is why the present author was (and still is) excited when two Indian mathematicians – H Gopalkrishna Gadiyar and R Padma [2] – came up in 1999 with an entirely new heuristics in support of [1]. Unlike the original argument, this new argument is analytic. What remains is to justify the interchange of two limits, the bread and butter of analytic number theory. However, one should remember that if interchange of limits could be allowed without proper justification then proving the famous Riemann hypothesis would have been a trivial matter!

One should remember that if interchange of limits could be allowed without proper justification then proving the famous Riemann hypothesis would have been a trivial matter!

Recall that an arithmetic function is a complex-valued function on the set of natural numbers (i.e. positive integers, excluding zero). Such a function f is called multiplicative if $f(mn) = f(m)f(n)$; whenever m and n are relatively prime. Notice that the values of a multiplicative function f are determined everywhere once one knows their values at prime powers (i.e., numbers of the form p^k, p prime, $k \geq 1$). In the presence of ap-

The main players in the Gadiyar–Padma 'proof' are the arithmetic functions $C_q(\cdot)$ of Ramanujan, many familiar arithmetic functions can be written as infinite linear combinations of these C_q's.

propriate convergence assumptions, this fact translates into the famous Euler product identity:

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} \sum_{k \geq 0} f(p^k). \qquad (2)$$

This holds, for instance, when the left hand side is absolutely convergent. If, further, f vanishes at all 'genuine powers' (i.e., $f(p^k) = 0$ for p prime, $k \geq 2$), then (2) simplifies to

$$\sum_{n=1}^{\infty} f(n) = \prod_{p} (1 + f(p)). \qquad (3)$$

The main players in the Gadiyar–Padma 'proof' are the arithmetic functions $C_q(\cdot)$ of Ramanujan. For any positive integer q, $C_q(\cdot)$ is defined by

$$C_q(n) = \sum_{w} w^n, \qquad (4)$$

where the sum is over all primitive qth roots of unity (i.e., complex numbers w such that $w^q = 1$ but $w^r \neq 1$ for $1 \leq r < q$). These functions have a number of remarkable properties. The first and most obvious property is periodicity: $C_q(n+q) = C_q(n)$. This property will play no role here. But this is the property which makes Ramanujan's discovery (that many familiar arithmetic functions can be written as infinite linear combinations of these C_q's) so enchanting. For instance, in Ramanujan's self-explanatory notation for periodic functions, the first few C_q's are given by

$$\begin{aligned}
C_1 &= \overline{1};\ C_2 = \overline{-1,1};\ C_3 = \overline{-1,-1,2};\\
C_4 &= \overline{0,-2,0,2};\ C_5 = \overline{-1,-1,-1,-1,4};\\
C_6 &= \overline{1,-1,-2,-1,1,2};\ C_7 = \overline{-1,-1,-1,-1,-1,-1,6};\\
C_8 &= \overline{0,0,0,-4,0,0,0,4};\ C_9 = \overline{0,0,-3,0,0,-3,0,0,6};\\
C_{10} &= \overline{1,-1,1,-1,-4,-1,1,-1,1,4}.
\end{aligned}$$

Recall that the arithmetic function $\sigma(\cdot)$ is given by: $\sigma(n)$ = sum of all divisors of n (including 1 and n).

Here is Ramanujan's fabulous expansion for the related function $\frac{\sigma(n)}{n}$:

$$\frac{\sigma(n)}{n} = \frac{\pi^2}{6}\sum_{k=1}^{\infty}\frac{c_k(n)}{k^2},$$

which not only indicates (correctly) that the 'mean value' of $\frac{\sigma(n)}{n}$ is $\frac{\pi^2}{6}$, but also shows how $\frac{\sigma(n)}{n}$ oscillates 'almost periodically' around this mean value. Alas, this formula too plays no role in what follows.

For us the most important property of the Ramanujan sums is their orthogonality.

The second important property of $c_q(\cdot)$ (which plays a minor role) is multiplicativity in the index. For each fixed n, $c_q(n)$ is a multiplicative function of q:

$$c_{qr}(n) = c_q(n)c_r(n) \text{ for } (q,r) = 1.$$

Its proof is immediate from the observation that every primitive (qr)th root of unity can be written uniquely as the product of a primitive qth root and a primitive rth root – provided q and r are relatively prime.

From our view point, the most important property of the Ramanujan function [3] is the following 'orthogonality' relation:

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}c_q(n)c_r(n+h) = \begin{cases} c_q(h) & \text{if } q = r \\ 0 & \text{if } q \neq r. \end{cases} \quad (5)$$

But the proof of (5) is easy – it is safely left to the reader.

Three more arithmetic functions will be important for our purpose. These are: Euler's totient function $\phi(\cdot)$, Möbius function $\mu(\cdot)$ and von Mangoldt's function $\Lambda(\cdot)$. Recall that $\phi(n)$ is the number of integers in $[1,n]$, which are relatively prime to n. $\mu(n) = (-1)^k$ if n is the product of k distinct primes (for some k) and $\mu(n) = 0$ otherwise. Finally $\Lambda(n) = \log p$ if n is a power of some prime p, and $\Lambda(n) = 0$ otherwise. Both $\phi(\cdot)$ and $\mu(\cdot)$ are multiplicative. In consequence, for each fixed h, the function $f(q) := (\frac{\mu(q)}{\phi(q)})^2 c_q(h)$ is also multiplicative. Applying Euler's formula (3) to this particular function f, and noticing the triviality

$$c_p(h) = \begin{cases} p-1 & \text{if } p|h \\ -1 & \text{if } p \nmid h; \end{cases}$$

we obtain the alternative formula

$$\sum_{q=1}^{\infty} \left(\frac{\mu(q)}{\phi(q)} \right)^2 c_q(h) = C_h \tag{6}$$

for the constants C_h (see (1)) of Hardy and Littlewood.

The last input in the Gadiyar–Padma heuristics is a Ramanujan expansion formula due to Hardy:

$$\sum_{q=1}^{\infty} \frac{\mu(q)}{\phi(q)} c_q(n) = \frac{\phi(n)}{n} \Lambda(n). \tag{7}$$

Now, to get to the heart of the 'proof', replace the index q in (6) by a new index r, replace n by $n+h$, and call the resulting identity (6'). Multiply (6) by (6'), getting one identity for each n. Add these identities for $1 \le n \le N$, divide the result by N and then take limit as $N \to \infty$. If all go well, we should get:

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} \frac{\phi(n)}{n} \Lambda(n) \frac{\phi(n+h)}{n+h} \Lambda(n+h)$$
$$= \sum_{q=1}^{\infty} \sum_{r=1}^{\infty} \frac{\mu(q)\mu(r)}{\phi(q)\phi(r)} \lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} c_q(n) c_r(n+h). \tag{8}$$

Now using the orthogonality relation (4) and the formula (5), the right hand side of (7) evaluates to C_n, yielding

$$\sum_{n=1}^{N} \frac{\phi(n)}{n} \Lambda(n) \frac{\phi(n+h)\Lambda(n+h)}{n+h} \sim C_h N \text{ as } N \to \infty. \tag{9}$$

Now (8) is really (equivalent to) the conjecture (1). At any rate, if there were only finitely many primes p for which $p+h$ were a prime, then $\Lambda(n)\Lambda(n+h) = 0$ for 'most' values of n and hence the left hand side of (8) would be at most a constant times $N^{1/2}(\log N)$? On the other hand, for even h; $C_h \neq 0$ (obvious from the formula (1)) and hence (8) is contradicted. This contradiction clearly shows that the formula (8) (equivalently (7)) implies the twin prime conjecture. In fact, the deduction of (1) from (8) is an easy technical step (summation by parts) which we leave out of this discussion. The problem that remains is to justify the deduction of (7) from (6). Any takers?

Suggested Reading

[1] G H Hardy and J E Littlewood, Some problems of partitio numerorum; III: On the expansion of a number as a sum of primes, *Acta Math.*, 44, 1922.

[2] H G Gadiyar and R Padma, Ramanujan – Fourier series, the Wiener – Khintchine formula and the distribution of twin primes, *Physica*, A 269, 1999.

[3] S Ramanujan, On certain trigonometric sums and their applications in the theory of numbers, *Trans. Camb. Phil. Soc.*, 22, 1918.

[4] G H Hardy, Note on Ramanujan's trigonometric function $C_q(n)$ and certain series of arithmetic functions, *Proc. Camb. Phil. Soc.*, 20, 1921.

Address for Correspondence
Bhaskar Bagchi
Math. Stat. Unit
Indian Statistical Institute
Bangalore 560 059, India.
Email:bbagchi@isibang.ac.in

The mind likes a strange idea as little as the body likes a strange protein and resists it with similar energy. It would not perhaps be too fanciful to say that a new idea is the most quickly acting antigen known to science. If we watch ourselves honestly we shall often find that we have begun to argue against a new idea even before it has been completely stated.

Wilfred Batten Lewis Trotter
(1872-1939) English Surgeon

Twin Primes and the Pentium Chip

It is an old maxim of mine that when you have excluded the impossible, whatever remains, however improbable, must be the truth.

– Sherlock Holmes

If p is a prime such that $p+2$ is also a prime then $p, p+2$ are known as twin primes. One of the outstanding unsolved problems in number theory is to prove (or disprove) that there are infinitely many twin primes. Euler had proved the infinitude of primes by showing that the series of reciprocals of primes diverges (see *Resonance*, Vol.1(3), pp.78-95, 1996). Guided by this some mathematicians considered the series of reciprocals of twin primes. If this series had been divergent then we could have concluded that there are infinitely many twin primes. But to make matters interesting, in 1919, V Brun proved that it converged to a value that has been calculated to be approximately 1.90216.

So the series of reciprocals of twin primes is of interest. Thomas Nicely, a number theorist, was compiling and extending the list of twin primes and computing the sum of their reciprocals using computers; this sort of exercise is referred to as number crunching. In 1994 when he was checking his calculations he discovered that there were errors:

I encountered erroneous results which were related to this bug as long ago as June, 1994, but it was not until 19 October 1994 that I felt I had eliminated all other likely sources of error (software logic, compiler, chipset, etc.)…

Through trial and error and finally a binary search, the discrepancy was isolated to the pair of twin primes 824633702441 and 824633702443, which were producing incorrect floating point reciprocals (the ultra-precision reciprocals were also in error, by a lesser amount, evidently due to a minor dependency on floating point arithmetic in Lenstra's original integer arithmetic code).

Finally the source of the error was traced to the division algorithm implemented on the Pentium chip. The bug relates to operations that convert floating point numbers into integer numbers. Intel withdrew the defective chips from the market and re-released corrected pentiums. This instance should be enough to convince sceptics that number crunching has its uses! Apparently, the Pentium III family has a flaw that slows down the boot process in a small number of chips! I suppose 'eternal vigilance is the price of computing power!'

(In a different context, it seems, a launch failure of the Ariane 5 rocket, which happened less than a minute into the launch, was traced to behavior around an overflow condition in one of the softwares used in it! One of the computers on board had a floating point to integer conversion that overflowed, but because the overflow was not handled by the software the computer did a dump of its memory. Unfortunately, this memory dump was interpreted by the rocket as instructions to its rocket nozzles. Apparently, even a failure of an ISRO rocket was traced to one such programming error.)

Moral: If you are interested in number crunching just go ahead without worrying about its utility. The world may be grateful to you some day!

C S Yogananda
Department of Mathematics, IISc, Bangalore 560 012, India.