Journal and Proceedings of
The Royal Society of New South Wales

Volume 119 pts 1-2 [*Issued December, 1986*]

pp.95-101

Return to CONTENTS

The Love of Numbers*

John H. Loxton

[Presidential Address, April 1986]

It is now well known that the answer to the ultimate question of life, the universe and everything is 42. [1.] So we see that numbers are the fundamental elements of civilisation as we know it. Numbers such as telephone numbers and car licenses serve to whip our activities into some sort of order. Numbers are turned to good account by the Gas Board and the Taxation Office. Numbers, especially big round ones, fuel the arguments of economists and politicians. Numbers have mystical properties: 7 is a nice friendly number, while 13 is an unlucky one, particularly on Fridays. Although we would not rationally except to get anything significant by adding Margaret Thatcher's telephone number to Bob Hawke's this is still a very popular method of prophecy. For example, in the prophecy of Isaiah, the lion proclaims the fall of Babylon because the numerical equivalents of the Hebrew words for "lion" and "Babylon" have the same sum. [2.] Numbers are ubiquitous. All this was much more pithily expressed by Leopold Kronecker in 1880: "God created the integers – all else is the work of man".

Mathematics is the numbers game par excellence. This is not to say that mathematicians are better than anybody else at reconciling their bank statements. In fact, Isaac Newton, who was Master of the Mint, employed a book-keeper to do his sums. Rather, mathematicians are the keepers of the odd numbers and the even numbers [3], the square numbers and perfect numbers, the complex numbers and the irrational numbers. So there has grown up the study of the theory of numbers. Ever since Pythagoras, mathematicians have been intrigued, delighted and frustrated by the wonderful world of numbers. To Pythagoras, numbers were the absolute and ultimate foundation of nature, the source of music and, through the music of the spheres, the explanation for the motion of the planets. [4] Some of the most inspired work of such great mathematicians as Euler, Laqrange. Gauss. Dirichlet and their successors has dealt with the theory of numbers. However, in these more rational times. such elegant pursuits have seemed to some to be merely dilletantism. Fourier was one such critic. Jacobi, in 1840, complained that "Fourier had the opinion that the principal object of mathematics was public use and the explanation of natural phenomena, but a philosopher like him ought to know that the sole object of the science is the honour of the human spirit and that under this view a problem of the theory of numbers is worth as much as a problem on the system of the world".

The most intriguing, delightful and frustratinq of all numbers are the prime numbers. Prime numbers are numbers which cannot be factorised as a product of smaller numbers.[5] Thus the first few prime numbers are

2, 3, 5. 7, 11, 13. 17, 19, 23, 29, 31, 37. 41, 43, 47, 53, 59, 61, ...

The prime numbers are the atoms of arithmetic because, as the ancient Greeks knew, every number can be factorised uniquely as a product of prime numbers. For example

666 = (2 x 333 = 2 x 3 x 111 =) 2 x 3 x 3 x 37.

There are infinitely many primes. This also was discovered by the Greeks and the argument is simple, elegant and compelling. Let 2, 3, 5, ... P be a list of all the primes up to some particular prime P. Consider the number

N = 2 x 3 x 5 x ... x P + 1.

This number is not divisible by 2: in fact, we are left with a remainder of 1 after dividing by 2. In the same way, N is not divisible by 3, or by 5. or by any of the primes up to P. However. N is divisible by some prime which might be N itself if N is prime. This prime is different from any of the primes 2, 3, 5, ... P, and so is greater than P. Consequently, the series of primes never comes to an end. Of course, only a finite number of primes have ever been seen, but some of them are pretty big. These big primes are all Mersenne primes, that is primes which are 1 less then a power of 2 [6]. It so happens that there is a very efficient method of testing whether $2^n - 1$ is prime, the amount of calculation being proportional to n^3. The known Mersenne primes are listed in Table 1 with their discoverers and computation times. They serve to underline the spectacular growth in computing power in recent years. Lehmer's primes were found on the first generation of electronic computers. while Slowinski's monsters have been found on the Cray supercomputer. Since n has increased by a factor of about 400 in this time, the amount of calculation has increased by a factor of about $400^3 = 64 \times 10^6$, so we might conclude that today's computers are about a million times faster than the early machines.

Table 1. Mersenne Primes

Value of n for which 2^n-1 is prime	When proved to be prime	Discoverer	Computation time
2, 3, 5, 7	antiquity	mentioned by Euclid	
13	1461	in codex Lat. Monac. 14908	
17, 19	1588	Pietro Antonio Cataldi	
31	1772	Euler	
61, 89, 107, 127	1876	Lucas	
521, 607, 1279, 2203, 2281	1952	Lehmer, Robinson	1 min–1 hr
3217	1957	Riesel	5½ hrs
4253, 4423	1961	Hurwitz	50 min
9689, 9941, 11213	1963	Gillies	2 hrs
19937	1971	Tuckerman	35 min
21701, 23209	1978	Noll, Nickel	8 hrs
44497	1979	Slowinski, Nelson	8 min
86243	1983	Slowinski	
132049	1984	Slowinski	

216091	1985	Slowinski

Table 2. Values of $\pi(x)$

x	$\pi(x)$	$\pi(x)/x/\log x$
10	4	0.92
100	25	1.15
1 000	168	1.15
10 000	1 229	1.14
100 000	9 952	1.11
1 000 000	78 498	1.09
10 000 000	664 579	1.08
100 000 000	5 761 455	1.06
1 000 000 000	50 847 534	1.05
10 000 000 000	455 052 512	1.04

To our present knowledge, the detailed behaviour of the prime numbers is unpredictable. There is no useful formula for calculating the n-th prime. This is part of the fascination of the search for bigger and bigger primes. In fact, we have no certain knowledge about where the next Mersenne prime will appear or even if there are any more of them at all. There is more suspense in the prime numbers than in the whole of the "HitchHikers Guide to the Galaxy".[1]

On the other hand. the distribution of the primes exhibits stunning regularity. This can be seen in the behaviour of the function R(x) which counts the number of primes up to x. As Table 2 reveals, $\pi(x)$ is approximately x/log x. To put it another way, the probability that a randomly chosen number n is prime is about l/log n. This is the famous prime number theorem. It was discovered experimentally around 1800 by Gauss and Legendre and eventually proved in 1896 by Hadamard and de la Val1ée Poussin with the aid of new and powerful analytic methods. However. x/log x is only a reasonably good approximation to $\pi(x)$ and it is natural to ask for a better one. This question was explored by Riemann in 1860 and he saw that the prime numbers are intimately connected with a function now called the Riemann zeta function. Riemann obtained what is essentially an exact formula for n(x) in terms of the zeros of his zeta function. It is therefore crucial to know where the zeros of the zeta function are. This is what the infamous Riemann Hypothesis does.[7] The Riemann Hypothesis is supported by an impressive amount of experimental evidence. For example, if we make a list of the zeros of the zeta function, we find that the first 200 million zeros or so are exactly where Riemann predicted However, there are infinitely many zeros and every one of them is important, so the ultimate answer to the question of the distribution of the prime numbers is still a long way off. The story continues: the latest attempts to settle the Riemann Hypothesis uncovered connections between prime numbers and quantum electrodynamics.

What then are we to make of this theory of numbers? It seems to be a very private science and there are those who will ask why the serious study of these matters is really worth-while. I have tried to illustrate how the theory of numbers captures the essence of mathematics: beauty, inevitability, unexpectedness and depth. Here the interplay of ideas is at its most dazzling. For this reason, the work of the great men of this subject is permanent. For example, Riemann wrote only one paper on the theory of numbers and the Riemann Hypothesis is not much more than a throwaway line, but it will always be the Riemann Hypothesis even after it is settled. There is a further twist to this argument. The theory of numbers is harmless. The point is beautifully made in “A mathematician’s apology” by G.H. Hardy.[8] “A good deal of elementary mathematics, which includes, for example, a fair working knowledge of the differential and integral calculus, has considerable practical utility. These parts of mathematics are, on the whole, rather dull: they are just the parts which have the least aesthetic value. The real mathematics of the real mathematicians, the mathematics of Fermat and Euler and Gauss and Abel and Riemann, is almost wholly useless. Mathematicians may be justified in rejoicing that there is one science at any rate, and that their own, whose very remoteness from ordinary human activities should keep it gentle and clean. It is the dull and elementary parts of mathematics that work for good or ill. Real mathematics has no effects on war, No one has yet discovered any warlike purpose to be served by the theory of numbers or relativity and it seems very unlikely that anyone will do so for many years”. Despite its contradictions, it seems to me that this sums up the motives of real mathematicians. But the world is a funny place and, sooner or later, much real mathematics finds a public use.

In recent times, the hazards of space travel and electronic banking have spawned exciting developments in secret codes. Much of this involves the theory of numbers. The work is so important that the Defence Establishment in the United States made strenuous efforts to have the study of prime numbers classified. One species of code is the error-correcting code. Signals from the depths of space, say, are transmitted as strings of zeros and ones. When a 0 is sent, usually a 0 is received, but occasionally, because of noise, a 1 is received instead. A 1 is usually received as a 1, but occasionally as a 0. We could guard against these occasional errors by sending each symbol several times, but this is very inefficient. Space satellites and compact disc players use subtle error-correcting codes which rely on ideas from algebraic number theory and geometry. Another species of code is the public-key code which makes it possible to send signed electronic mail. This is what I will try to describe next.[9]

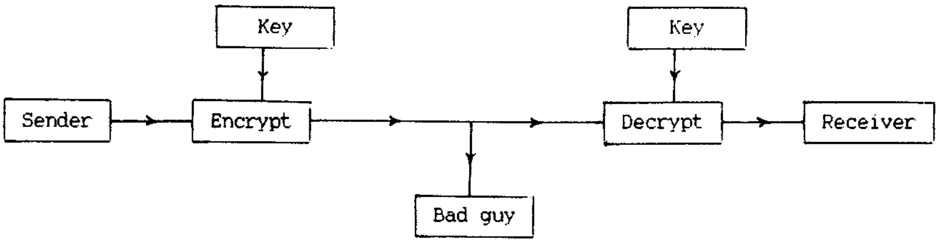

Figure 1. Conventional cryptography

Conventional cryptography makes use of a secret key known to the sender and the receiver. but not to the “bad guy”. (See Figure l.)

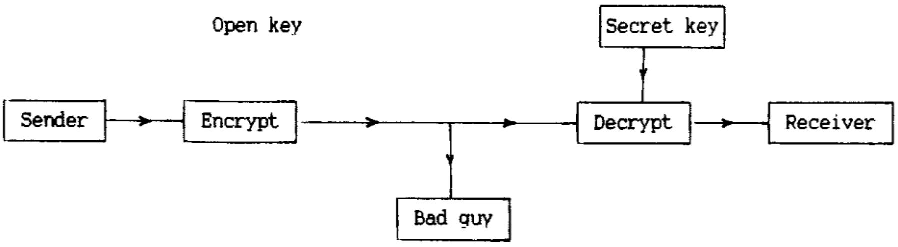

Figure 2. Public-key cryptography

This is the stuff of trench warfare and spy stories. The main problem is to exchange a sufficient amount of key between sender and receiver and to keep it secret, because once the key is compromised at either end the “bad guy” can read the message. Public-key cryptography, by contrast, looks like this. (See Figure 2.)

The code requires two different keys, one for encrypting and one for decrypting and depends on the fact that knowledge of the encrypting key is no help in decrypting. The mechanism is a trapdoor function. This is a function E for encryption

$$\text{message } X \;\; E\Rightarrow \;\text{cipher } EW$$

which has an inverse D for decryption

$$\text{cipher } E(X) \;\; D\Rightarrow \;\text{message } D(E(X)) = X.$$

with the essential property that the inverse D cannot be discovered by studying E. So E is a trapdoor through which messages vanish and they can only be recovered by a different route with the aid of the special key D. If we have a supply of one-way functions, we can set up a cryto-net. Suppose a group of people wish to talk to each other privately. Each person i chooses a trapdoor function E_i with an inverse D_i. The functions E_1, E_2 ... are listed in a public directory, while each person keeps his inverse function D_i secret. When i wants to send a message X to j, he encrypts the message X as

$$Y = E_j(D_i(X))$$

and sends it to j. Now j can recover the message by calculating

$$E_i(D_j(Y)) = E_i(D_j(E_j(D_i(X)))) = E_i(D_i(X)) = X.$$

Only j can read the message because only j knows D_j. This ensures privacy. Moreover. only i could have sent the message because only i knows D_i, so the scheme provides authentication as well.[10]

Do these marvellous trap-door functions exist? They are, of course, logically impossible and it will therefore take a little time to construct one. The first ingredient is the modular arithmetic invented by Gauss around 1800. If a number n when divided by the modulus m leaves the remainder r. we say n is congruent to r modulo m and write $n \equiv r(\text{mod } m)$. This means that m divides n - r exactly with no remainder. For example, $37 \equiv 1 \pmod 9$ because $37 = 4 \times 9 + 1$: $37 \equiv 4 \pmod{11}$ because $37 = 3 \times 11 + 4$. The notation is meant to suggest that arithmetic works with these remainders according to the usual rules. For example.

$$37 \times 41 = 1517$$

can be written as $(3 \times 11 + 4) \times (3 - 11 + 8) = (137 \times 11 + 10)$ and on taking remainders modulo 11 this yields the correct equation

$$4 \times 8 \equiv 10 \pmod{11}.$$

Arithmetic modulo 9 makes a useful check on computation. For example,

$$123456789 \times 987654321 \neq 121932631212635269$$

because the left side is 0 x 0 (mod 9) and the right side is 1 (mod 9) as you may easily cheek.[ll]

The second ingredient is Fermat's little theorem.[12] Fermat discovered in 1640 that if p is a prime and b is any integer not divisible by p, then

$$b^{p-1} \equiv 1 \text{ (mod p).}$$

that is b^{p-1} is exactly divisible by p. For example, 2^6 -1 = 63 is indeed divisible by 7, that is $2^6 \equiv 1$ (mod 7). On the other hand, $2^{322} \equiv 123$ (mod 323) and we see that 323 cannot be a prime. This is the prototype for the fast methods of testing for primality. The proof of Fermat's little theorem is another gem of the theory of numbers. Observe that the possible remainders modulo p are 0,1,2, ..., p - 1. The numbers b, 2b, 3b, ... (p - 1)b have distinct non-zero remainders modulo p, so these remainders must be 1,2, ... p - 1 in some mixed up order. If we multiply these two sets of numbers together, we must get the same result modulo p, that is

$$b.2b.3b....(p - 1)b \equiv 1.2.3.... (p - 1) \text{ (mod p).}$$

Cancelling 1.2,3. ... (p - 1) on both sides gives $b^{p-1} \equiv 1$ (mod p). Actually, we need a little more. If p and q are distinct primes and b is any integer not divisible by either prime, then

$$b^{(p-1)(q-1)} \equiv 1 \text{ (mod pq).}$$

For example, 323 = 17 x 19, 288 = 16 x 18 and $2^{288} \equiv 1$ (mod 323). This extension follows from Fermat's little theorem because

$$b^{(p-1)(q-1)} \equiv 1^{(q-1)} = 1 \text{ (mod p).}$$

i.e. p divides $b^{(p-1)(q-1)}$ - 1, and

$$b^{(p-1)(q-1)} \equiv 1^{(p-1)} = 1 \text{ (mod q),}$$

i,e. q divides $b^{(p-l)(q-1)}$ - 1,

whence pq divides $b^{(p-1)(q-1)}$ - 1 as required.

Here is the trapdoor function devised by Rivest, Shamir and Adleman in 1978. Choose two large secret prime numbers p and q about 50 digits long. Their product r = pq is the encypting modulus. Also choose the encrypting exponent S, making sure that s has no common factor with either p - 1 or q - 1. The numbers r and s define the public key and go in the telephone book of encrypting functions. Before encryption, a written message is converted into a string of digits, say by A = 01, B = 02, C = 03, ... We break the resulting string into blocks of 100 digits. Each block X is then encrypted by the function

$$E(X) \equiv X^s \text{ (mod r).}$$

To decrypt, find the decrypting exponent t by solving the congruence st ≡ 1 (mod(p - 1)(q -)) and then use the decrypting function D given by

$$D(Y) \text{ a } y^t \text{ (mod r).}$$

This works because st = 1 + k(p -)(q - 1) and so

$$D(E(X)) \equiv E(X)^t \equiv X^{st} = X^{l+k(p-l)(q-1)}$$

$$= X.(X^{(p-1)(q-1)k} . \equiv X(\text{mod } r).$$

(The last step depends on $X^{(p-Mq-1)} \equiv 1$ (mod pq).) For a simple and therefore utterly useless example, take r = 187 = 11 x 17 and s = 7. The message X = 003 is encrypted as

$$Y \equiv X^s = 3^7 = 2187 \equiv 3 \ (\text{mod } 187).$$

The decrypting exponent comes from solving 7t ≡ 1 (mod 160) which gives t = 23. So we can decrypt Y = 130 by calculating

$$y^t = 130^{23} \equiv 3 \ (\text{mod } 187).$$

Despite initial appearances, all these calculations are very easy on a computer. The point to notice is that this really is a trapdoor because the decrypting exponent cannot be calculated from the public information r and a. We must factorise r = pq first before we can calculate t.[13] But r is a 100 digit number and it appears to be essentially impossible to factorise such large numbers. The strength of the scheme depends on the fact that it is easy to find large primes but it is very difficult at the moment to factorise large numbers. However, there is no guarantee that some one will not invent a revolutionary method of factorising tomorrow and unhinge this trapdoor in the process. There is now more incentive for trying to understand the mysteries of the primes than ever.

I have tried to defend my science by appealing to public use and base motives. I have also tried to illustrate the private face, the incorruptible beauty and fascination of the subject. I have neither the time nor the knowledge to explain how the ideas of the theory of numbers permeate the whole of science. Consider this Platonic dialogue [14]:

> Corbeiller: "In the last 60 years, however, a new revolution has taken place, and everywhere we look we find that what seems to be continuous is really composed of atoms."
> Empeiros, "But are not modern mathematicians interested in such things?"
> Corbeiller: "They are, but they give them other names. They call them Number Theory and the Theory of Discontinuous Groups. Actually, they have found much more then we can use yet in physics, but we have in crystals illustrations of some of their simpler theorems".

Again, here is the great Russian mathematician Yu. I. Manin [15]:

> "It is remarkable that the deepest ideas of number theory reveal a far-reaching resemblance to the ideas of modern theoretical physics. Like quantum mechanics, the theory of numbers furnishes completely non-obvious patterns of relationship between the continuous and the discrete (the technique of Dirichlet series and trigonometric sums, p-adic numbers, nonarchimedean analysis) and emphasizes the role of hidden symmetries (classfield theory. which describes the relationship between prime numbers and the Galois groups of algebraic number fields). One would like to hope that this resemblance is no accident. and that we are already learning new words about the World in which we live, but we do not yet understand their meaning".

Numbers, then, are the key to knowledge. The last word, as is only proper, belongs to Winston Churchill, who saw the great importance of this subject and how he might have been a really great man but for one sma11 thing:

> "I had a feeling once about Mathematics – that I saw it all. Depth beyond depth was revealed to me – Byss and the Abyss. I saw – as one might see the transit of Venus or even the Lord Mayor's Show – a quantity passing infinity and changinq its sign from plus to minus. I saw exactly why it happened and why the tergiversation was inevitable – but it was after dinner and I let it go".[16]

Notes

1. D. Adams, "The Hitch-Hikers Guide to the Galaxy". (Pan, 1979). The apotheosis of Deep Thought is revealed in chapter 27.
2. Isaiah 21 : 8, 9.
3. No mathematician could have been so crass as the Minister in the New South Wales Government who declared during a petrol strike that, for the purposes of petrol rationing, car number plates ending in 0 were to be considered even.
4. For a modern opinion, see D. Adams, "Life, the universe and everything" (Pan, 1982, chapter 7). "It is now realised that numbers are not absolute, but depend on the observer's movement in restaurants".
5. By convention and convenience, 1 is not a prime. So the Prime Minister, despite his ego, is not prime. Neither, in most cases. are prime ribs of beef.
6. They are named after Marin Mersenne who corresponded with mathematicians of the day, provoking them with his execrable hand-writing and conjectures in number theory. In 1644, he gave a list of the Mersenne primes up to 10^{79} which was only correct up to 10^{18}, so he is perhaps fortunate to be commemorated in this way.
7. The Riemann zeta function is defined by the formula

   $\zeta(s) = 1^{-s} + 2^{-s} + 3^{-s} + \ldots$

   Here $s = \sigma + it$ is a complex variable. The Riemann Hypothesis asserts that the solutions of the equation $\zeta(\sigma + it) = 0$ all have $\sigma = ½$ (except for "trivial" zeros of ζ at -2, -4, -6, ...).
8. It is worth noting that this delightful little book was written in 1940 and that its rhetoric is the distillation of years of high table conversation in Oxbridge Colleges.
9. The prehistory of cryptography up to 1967 is described breathlessly in "The Codebreakers" by David Kahn (Macmillan. 1967). For later developments, see the article by N.J.A. Sloane on "Error-correcting codes and cryptography" in "The mathematical Gardner", edited by D.A. Klarner (Wadsworth, 1981).
10. Devise a protocol by which two potentially dishonest players can play a fair game of poker without using any cards, for example, over the telephone. See "Mental Poker" by Shamir, Rivest and Adleman in "The Mathematical Gardner" (ibid).
11. This trick called "casting out nines" is almost obsolete now. Should you have forgotten your 987654321 times tables, all you need recall is that 987654321 x 81 = 80000000001. so multiply 123456789 by 80000000001 and divide the result by 81 to get 121932631112635269.
12. Not to be confused with the infamous Fermat's last theorem which is neither a theorem nor the last thing he did and which there is no space to explain here.
13. At least, this is the current position. if s is chosen carefully, the only way to crack the code is to solve the congruence for the decrypting exponent. It is perfectly possible that

someone will discover a better method. This is exactly what happened recently to another "trapdoor" based on the knapsack problem, None of the modern schemes for cryptography have been proved to be secure.

14. Philippe Le Corbeiller, "Crystals and the future of physics", Scientific American, January 1953, 50-56.
15. Yu. I. Manin, "Mathematics and Physics", translated by Ann and Neal Koblitz (Birkhauser, 1981).
16. Quoted in "The Mathematical Magpie" by C. Fadiman (Simon and Schuster, 1962, page 255).

Return to Top