



© 1997–2009, Millennium Mathematics Project, University of Cambridge.

Permission is granted to print and copy this page on paper for non-commercial use. For other uses, including electronic redistribution, please contact us.

May 2003

Features



A whirlpool of numbers

by Nick Mee



Jeserac sat motionless within a whirlpool of numbers. The first thousand primes, expressed in the binary scale that had been used for all arithmetical operations since electronic computers were invented, marched in order before him. Endless ranks of 1's and 0's paraded past, bringing before Jeserac's eyes the complete sequences of all those numbers that possessed no factors except themselves and unity. There was a mystery about the primes that had always fascinated Man, and they held his imagination still.

Jeserac was no mathematician, though sometimes he liked to believe he was. All he could do was to search among the infinite array of primes for special relationships and rules which more talented men might incorporate in general laws. He could find how numbers behaved, but he could not explain why. It was his pleasure to hack his way through the arithmetical jungle and sometimes he discovered wonders that more skilful explorers had missed.

He set up the matrix of all possible integers, and started his computer stringing the primes across its surface as beads might be arranged at the intersections of a mesh. Jeserac had done this a hundred times before and it had never taught him anything. But he was fascinated by the way in which the numbers he was studying were scattered, apparently according to no laws, across the spectrum of the integers. He knew the laws of distribution that had already been discovered, but always hoped to discover more.

from

The City and the Stars by Arthur C. Clarke (1956)

The building blocks of arithmetic



Carl Friedrich Gauss

In the words of the great German mathematician Carl Friedrich Gauss: "Mathematics is the Queen of the Sciences and Arithmetic is the Queen of Mathematics." The modern name for the branch of mathematics that Gauss was referring to as Arithmetic is Number Theory – the study of the properties of the positive whole numbers or integers. The 19th century mathematician Kronecker famously claimed that "God made the integers, all the rest is the work of man."

The fundamental building blocks of Number Theory are the primes. These are the numbers: 2, 3, 5, 7, 11, 13,... defined as the whole numbers that cannot be divided exactly by any other whole number, excluding the trivial division by the number 1. Primes cannot be broken down into simpler components; they play a role in mathematics that is similar to the role of the elements in chemistry. From the 100 or so chemical elements it is possible to synthesize the millions of compounds that are studied by chemists. The Fundamental Theorem of Arithmetic, which was proved by Euclid, states that

All positive whole numbers are either primes or they can be uniquely decomposed into a product of primes.

For instance:

$$\begin{array}{rcl} 84 & = & 2 \times 2 \times 3 \times 7, \\ 85 & = & 5 \times 17, \\ 86 & = & 2 \times 43, \\ 87 & = & 3 \times 29, \\ 88 & = & 2 \times 2 \times 2 \times 11, \\ 89 & & \text{is prime,} \end{array}$$

A whirlpool of numbers

$$\begin{aligned}90 &= 2 \times 3 \times 3 \times 5, \\91 &= 7 \times 13\end{aligned}$$

If we take all the primes less than 300, we find that there are just 62 of them:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29,
31, 37, 41, 43, 47, 53, 59, 61, 67, 71
73, 79, 83, 89, 97, 101, 103, 107, 109, 113,
127, 131, 137, 139, 149, 151, 157, 163, 167, 173,
179, 181, 191, 193, 197, 199, 211, 223, 227, 229,
233, 239, 241, 251, 257, 263, 269, 271, 277, 281,
283, 293.

25 of these primes are below 100, 21 are between 100 and 200 and 16 are between 200 and 300. It looks as though the primes become more spread out as their size increases. If we look further we find that between 10,000 and 10,100 there are just 11 primes, between 100,000 and 100,100 there are just 6. This seems to confirm that the primes become rarer as they become bigger, but do they eventually die out altogether? We know that there are no naturally occurring elements on Earth beyond number 92 – Uranium. But is the same true of the primes? What is the biggest prime number?

There is no biggest prime

The properties of prime numbers have been studied by mathematicians since antiquity. It was the Ancient Greeks who first proved that there are infinitely many primes, so there is not, in fact, a biggest prime number. Euclid's *Elements* provides the oldest known proof. The proof works by showing that if we assume that there is a biggest prime number, then there is a contradiction. We can number all the primes in ascending order, so that $P_1 = 2$, $P_2 = 3$, $P_3 = 5$ and so on. If we assume that there are just n primes, then the biggest prime will be labelled P_n . Now we can form the number Q by multiplying together all these primes and adding 1, so

$$Q = (P_1 \times P_2 \times P_3 \times P_4 \dots \times P_n) + 1.$$

Now we can see that if we divide Q by any of our n primes there is always a remainder of 1, so Q is not divisible by any of the primes. But we know that all positive integers are either primes or can be decomposed into a product of primes. This means that either Q must be prime or Q must be divisible by primes that are larger than P_n . Our assumption that P_n is the biggest prime has led us to a contradiction, this assumption must therefore be false, so there is no biggest prime.

How are primes distributed?

We now know that the primes become sparser as they become bigger, but they don't dwindle away completely. So the next question is, can we understand how the primes are distributed? Can the primes be fitted into a pattern in the way that the elements can be organised in the Periodic Table? This is one of the most important problems in the whole of mathematics.

The spacing between primes seems quite irregular, but there does appear to be a tendency for the spacing to increase, as we noted above. The Prime Number Theorem states that the function $x / \ln(x)$, where $\ln(x)$ is the natural logarithm of x , gives a reasonable approximation for the number of primes less than x , which we will

A whirlpool of numbers

represent as $\pi(x)$. As x increases, this approximation becomes ever more accurate. The following table compares these two functions:

x	$\text{Pi}(x)$	$x/\ln(x)$	$\text{Pi}(x)/(x/\ln(x))$
1000	168	145	1.159

There is no simple formula that will generate all the primes, but Euler showed that the formula

$$f(n) = n^2 - n + 41$$

is remarkable because it is equal to a prime for every integer value of n up to 40. The primes generated by the formula are:

41, 43, 47, 53, 61, 71, 83, 97, 113, 131,
 151, 173, 197, 223, 251, 281, 313, 347, 383, 421,
 461, 503, 547, 593, 641, 691, 743, 797, 853, 911,
 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601.

The formula necessarily fails to produce a prime when $n = 41$, because in this case $f(n) = n^2 - n + 41 = 41^2 - 41 + 41 = 41^2$.

Euler also devised a much more important function that is now known as the *zeta function*:

$$\zeta(s) = \sum(1/n^s) = 1^{-s} + 2^{-s} + 3^{-s} + 4^{-s} + \dots$$

Euler showed that the zeta function is equal to an infinite product

$$z(s) = \prod \frac{1}{(1 - 1/p^s)} = \frac{1}{(1 - 1/2^s)(1 - 1/3^s)(1 - 1/5^s)(1 - 1/7^s)\dots}$$

where the product is over all the primes p . This is a remarkable result: when the zeta function is expressed as the sum of an infinite number of terms, the sum includes a term that takes a value for every positive integer, but when expressed as an infinite product the only terms that are included are those that take a value for a prime.

The zeta function, as defined by Euler, is only valid for values of s that are greater than 1. For these values of s the zeta function can be summed to a finite value, even though the number of terms is infinite. However, if s is equal to or less than 1, the series diverges, so the function is not well defined. For instance, taking $s = -2$ gives

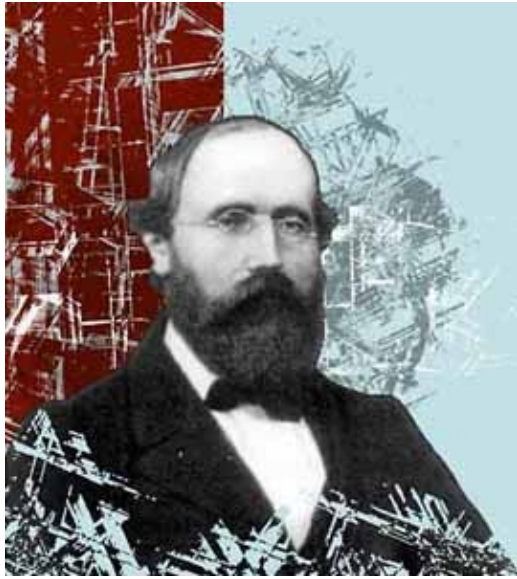
$$\sum(1/n^{-2}) = \sum n^2 = 1 + 4 + 9 + 16 + \dots,$$

a series which increases without end. By comparison, when $s = 2$,

$$\zeta(2) = \sum(1/n^2) = 1^{-2} + 2^{-2} + 3^{-2} + 4^{-2} + \dots = 1 + 1/4 + 1/9 + 1/16 + \dots$$

This series can be summed to give $\zeta(2) = \pi^2/6$.

The Riemann Zeta Function



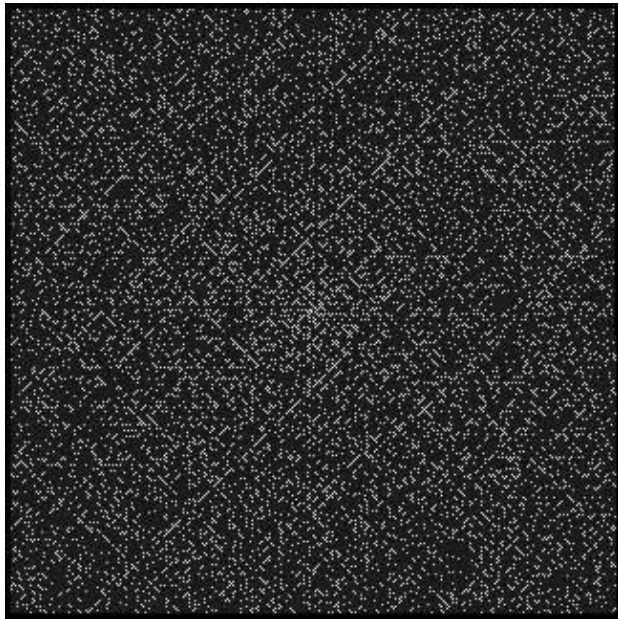
Georg Friedrich Bernhard Riemann

In 1859 Georg Friedrich Bernhard Riemann published his only paper on Number Theory. In this paper Riemann found a function that is identical to Euler's zeta function for values of s that are greater than 1, but that is well defined for all real numbers. The Riemann zeta function is actually defined for **complex values** of s , where $s = a + bi$ and $i^2 = -1$. Riemann proved that there were many deep connections between his analytically continued zeta function and the distribution of primes. Riemann's intuition was quite remarkable in connecting the properties of a continuous function of a complex variable to the properties of the primes which are real and discrete. More specifically, Riemann showed that $\pi(x)$, the number of primes less than x , is related to the points at which the zeta function is equal to zero – these points are known as the *zeroes of the function*. Riemann found that when s is a real number the zeta function only equals zero when s is equal to a negative even integer, that is at the points $s = -2, -4, -6, \dots$ But Riemann also found other zeroes of the zeta function, all of which appeared to be on the line $s = 1/2 + bi$. The approximate value for the first of these is at $b = 14.134725$. Riemann conjectured that all the non-real zeroes of the zeta function lie on the line $s = 1/2 + bi$, although he was unable to prove this. The conjecture has become known as the *Riemann Hypothesis* and it is the key to understanding the distribution of the primes. Recent computer-based calculations have shown that at least the first 100 billion zeroes, with non-real s , all fall on Riemann's line. But, as yet, there is still no proof that there are no exceptions to this pattern.

The British number theorist G.H. Hardy relates in his book "A mathematician's apology" that before setting out on his return voyage over the North Sea from Denmark in the 1920s, expecting the crossing to be treacherous, he posted a note to a colleague to say that he had proved the Riemann Hypothesis. Although a staunch and proselytizing atheist, Hardy explained that he had sent the note in order to guarantee that God would not allow him to drown. Because if he had drowned that would mean that proofs had been claimed for both of the two most famous problems in mathematics: Fermat's Last Theorem and the Riemann Hypothesis, but that the mathematician making the claim had died before communicating the proof to anyone else. Fermat's Last Theorem had achieved legendary status amongst mathematicians, because, in the 17th century, the French civil servant and amateur mathematician Pierre de Fermat, one of the greatest figures in the history of Number Theory, had scribbled in the margin of a book that he had a wonderful proof of the theorem, but the margin was too small for him to write it down. The book was a 17th century edition of the classic Greek text on Number Theory written in the first century A.D., Diophantus' *Arithmetica*. Fermat subsequently died,

leaving mathematicians to search for 350 years for a proof of the theorem.

The hardest problem in all of mathematics?



Ulam's Prime number spiral

In the 150 years since Riemann's paper nobody has ever been able to prove or disprove his conjecture, but Fermat's Last Theorem was finally proved by Andrew Wiles in 1994. The Riemann Hypothesis is now the most famous outstanding problem in mathematics. But the Riemann Hypothesis has far more important consequences for mathematics than Fermat's Last Theorem. In fact, there are areas of mathematics that have been developed by mathematicians on the assumption that the Riemann Hypothesis is true. The Riemann Hypothesis also appears to be an even more difficult problem than Fermat's Last Theorem.

Any implicit regularity in the primes that is encoded in the zeta function has still not been explicitly deciphered. However, there is a much simpler pattern exhibited in the distribution of primes. In 1963 the Polish mathematician Stanislaw Ulam, who worked on the American nuclear programme, the Manhattan Project, during the Second World War was doodling abstractedly in the interval between two seminars at a conference. He drew a grid of squares, then he wrote the number 1 at the centre of the grid and continued to write out the sequence of all the positive integers in ascending order spiralling out from the centre. Ulam noticed to his great surprise that when the integers were organised in this way, there was a tendency for the primes to be lined up along diagonal lines in the grid. The result was so unexpected that a picture of the Prime Number Spiral was featured on the cover of the March 1964 issue of *Scientific American* which included an article by Martin Gardner about the spiral: "Mathematical Recreations: The Remarkable Lore of the Prime Number." *Sci. Amer.* 210, 120–128, March 1964.

A whirlpool of numbers

265	264	263	262	261	260	259	258	257	256	255	254	253	252	251
210	209	208	207	206	205	204	203	202	201	200	199	198	197	250
211	162	161	160	159	158	157	156	155	154	153	152	151	196	249
212	163	122	121	120	119	118	117	116	115	114	113	150	195	248
213	164	123	90	89	88	87	86	85	84	83	112	149	194	247
214	165	124	91	66	65	64	63	62	61	82	111	148	193	246
215	166	125	92	67	50	49	48	47	60	81	110	147	192	245
216	167	126	93	68	51	42	41	46	59	80	109	146	191	244
217	168	127	94	69	52	43	44	45	58	79	108	145	190	243
218	169	128	95	70	53	54	55	56	57	78	107	144	189	242
219	170	129	96	71	72	73	74	75	76	77	106	143	188	241
220	171	130	97	98	99	100	101	102	103	104	105	142	187	240
221	172	131	132	133	134	135	136	137	138	139	140	141	186	239
222	173	174	175	176	177	178	179	180	181	182	183	184	185	238
223	224	225	226	227	228	229	230	231	232	233	234	235	236	237

Primes along the diagonal of a spiral

The picture above shows the spiral for the first 100,000 integers. The composite numbers are shown as black dots and the primes are shown as white dots. In the grid numerous long diagonal white lines can clearly be seen. If numbers other than 1 are taken as the starting number of the spiral, the general appearance of the grid is the same. No-one has come up with a clear explanation of why this should be the case. But it implies that there are long sequences of primes that can be generated by formulae such as $f(n)=an^2+bn+c$, where a , b and c are integers.

If we start with the number 41 at the centre of the spiral, we find that the numbers on the diagonal form the sequence $f(n)=n^2-n+41$, which is the formula discovered by Euler that takes prime values for all integer values of n up to 40.

In the illustration the number 41 is situated at the centre and the numbers continue in an anti-clockwise spiral. The squares of the grid that contain composite numbers are coloured yellow and the squares that contain primes are coloured white. The first 15 numbers generated by the formula $f(n)=n^2-n+41$ appear along one of the main diagonals of the square.

A whirlpool of numbers



A whirlpool of numbers

Although Stanislaw Ulam is generally credited with the discovery of the Prime Number Spiral, it appears that Ulam might not have been the first person to make this discovery. Chapter 6 of Arthur C. Clarke's classic 1956 novel "The City and the Stars" opens with the hero Jeserac analysing a "whirlpool" of integers on his computer monitor and seeing the primes strung out "across its surface as beads might be arranged at the intersections of a mesh". It looks as though Arthur C. Clarke had already discovered the Prime Number Spiral seven years before it was found by Ulam. I recently asked Sir Arthur C. Clarke about the inspiration for his discussion of the primes in "The City and the Stars". He told me that

After half a century I have no idea what made me think of this. I never had a computer until 1970 when H.P. gave me HAL Jr (HP9001), the direct ancestor of the palmtop. But I was impressed by the unfinished Babbage machine, which I must have seen in the Science Museum soon after I moved to London in 1936.

Mathematicians study the properties of primes for their own intrinsic interest. But prime numbers also have modern scientific applications, especially in cryptography. The United States Government Intelligence Agency, the NSA, is the world's biggest employer of pure mathematicians. Whenever you make a transaction on the internet, such as a credit card purchase, the security of the transaction is ensured by the use of public key encryption using a method based on some subtle Number Theory devised by Ron Rivest, Adi Shamir and Len Adleman, also known as RSA. RSA encryption utilises a numerical key that is formed by multiplying together two very large primes. The security of the system is dependent on the difficulty of factorizing very large numbers. The number of steps that are necessary to factorize a large number using all known algorithms increases exponentially with the size of the number. This means that the cryptographer can always stay one step ahead of the computer. If computer processors become fast enough to factorize the 128 digit numbers that are used for encipherment, we can start to use 512 digit numbers. However, if a mathematician were to find a new more efficient factorization algorithm the security of our enciphered transactions might be under threat. Cryptographers feel safe, because, although leading mathematicians have searched for such an algorithm for many centuries none has ever been found.

A whirlpool of numbers

Last year three Indian mathematicians – Prof. Manindra Agrawal and two of his graduate students, Neeraj Kayal and Nitin Saxena – published an algorithm for testing whether a number is prime or composite (see [Prime time](#) from Issue 22 of *Plus*). The algorithm employs quite elementary arithmetic and is stated by the authors in just 13 lines. The important new feature of the algorithm is that the time taken to test the primality of a number N increases polynomially with the size of N rather than exponentially. In fact, it increases as the twelfth power of N . Following this revelation, perhaps we shouldn't be too hasty to rule out the possibility that there is also a simple algorithm for factorization that has similarly been overlooked. Maybe cryptographers should be worried.

Further Reading

- The City and the Stars – Arthur C. Clarke (1956)
 - Fermat's Last Theorem – Simon Singh (1997)
 - Life, the Universe and Mathematics CD-ROM by Nick Mee (1998)
 - The Code Book on CD-ROM by Simon Singh and Nick Mee (2002)
-

About this article



Nick Mee studied mathematics at the University of Cambridge, was Senior Wrangler in 1985 and went on to complete a Ph.D. with the title "Supersymmetric Quantum Mechanics and Geometry".

He recently developed [The Code Book](#) on CD-ROM with Simon Singh and is currently developing software for [Connections in Space](#) with Professor John Barrow, the Director of the Millennium Mathematics Project. Details about his other software projects are available at the [Virtual Image](#) website.

This article was written with the valuable help and inspiration of Sir Arthur C. Clarke, who is currently writing a novel entitled "The Last Theorem" about Fermat's Last Theorem.



Plus is part of the family of activities in the Millennium Mathematics Project, which also includes the [NRICH](#) and [MOTIVATE](#) sites.