Problems with PRIMES

TIM MELROSE & PAUL SCOTT

Introduction

A prime number is an integer greater than 1 that is divisible by only itself and 1.

For example the first ten primes are:

2, 3, 5, 7, 11, 13, 17, 19, 23 and 29.

A positive integer greater than 1 that is not a prime is called composite.

The number 1 itself is considered neither prime nor composite. In fact Ernst Gabor Strauss (1922–1983) was said to have replied to a student's question about why 1 is not a prime:

> The primes are the building bricks for arithmetic, and 1 is just not a brick!

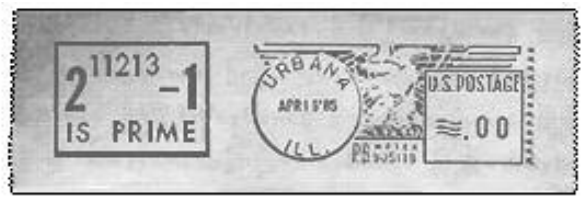
One of the few things we know about primes is that there are infinitely many of them. This was proved by the ancient Greeks, and Euclid in particular, in about 350 B.C.

The largest prime known today is

$$2^{25\,964\,951}-1$$

which was announced on 18 February 2005.

The discovery of a new prime used to be celebrated with a glass of wine or a postage stamp:



Nowadays it is boasted about by computer manufacturers or software companies to seek publicity.

Primes certainly would occupy a less central position in number theory were it not for a result known as the *Fundamental Theorem of Arithmetic* which states:

> Any positive integer (other than 1) can be written uniquely as the product of prime numbers.

As the name suggests it is one of the most basic but important propositions in all of mathematics.

Primes, once associated exclusively with pure mathematics, have recently found an unexpected application in the areas of national security, and in particular public-key cryptography. This uses the principle that it is very difficult to find the factors of a given product of two very large primes.

Mersenne's work

The French priest Marin Mersenne (1588–1648) played an important role in 17th century number theory and also more general mathematics. Scholars inquisitive about mathematics or stumped by a difficult problem would often write to Mersenne who could direct them to a likely authority, if he did not know the answer himself. Today Mersenne's name is mainly associated with numbers of the form $2^n - 1$; that is, numbers one less than a power of 2. To honour Mersenne these are called *Mersenne numbers*. It is clear that all such numbers are odd but more importantly some of them are prime; as

is the case with $2^{13466917} - 1$.

Mersenne immediately understood that if n is composite then $2^n - 1$ must also be composite. For example taking $n = 33$, then

$2^{33} - 1 = 8\,589\,934\,591 = 7 \times 1\,227\,133\,513$

is not a prime. However when n is prime, the situation becomes less clear. Letting $p = 2$, 3, 5, and 7 yields the "Mersenne primes"

$2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$,
and $2^7 - 1 = 127$

respectively. But if we take $p = 11$ as the exponent we get $2^{11} - 1 = 2047 = 23 \times 89$. Mersenne was also fully aware that a prime p was not enough to guarantee $2^p - 1$ to also be prime. In fact he made the following assertion in his book *Cognitata Physica-Mathematica*:

> The only primes between 2 and 257 for which $2^p - 1$ is prime are $p = 2$, 3, 5, 7, 9, 11, 13, 17, 19, 31, 67, 127 and 257.

Unfortunately Mersenne missed the fact that the numbers $2^{61} - 1$, $2^{89} - 1$ and $2^{107} - 1$ are in fact prime. But conversely $2^{67} - 1$ and $2^{257} - 1$ turned out not to be prime at all. We can forgive Mersenne for these errors as he lived in the pre-computer age. The case of $2^{67}-1$ was proved by Edouard Lucas (1842–1891) in 1876 who used an argument which did not explicitly yield any of the factors. It was not until the following century that Frank Nelson Cole did find its factors.

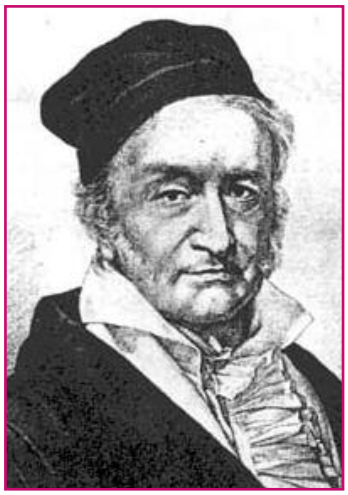
$2^{67} - 1$ is composite!

In 1903 at a meeting of the American Mathematical Society, among the speakers on the agenda was Frank Nelson Cole. When it came Cole's turn, he purposefully walked to the front of the room and without saying anything, proceeded to multiply 2 by itself 67 times under his breath. He then subtracted 1 and finally arrived at the enormous result of

147 573 952 588 676 412 927.

Having witnessed this wordless calculation, the bemused audience then watched as he wrote on the blackboard

Marin Mersenne
(1588–1648)



Carl Friedrich Gauss
(1777–1855)

193 707 721 × 761 838 257 287

which he also computed silently. The product was none other than

147 573 952 588 676 412 927.

Cole then took his seat without uttering a word. Those in the audience, having just witnessed the explicit factorisation of Mersenne's number $2^{67} - 1$ into its two huge factors, then burst into unanimous applause for Cole and gave him a standing ovation.

It was not until a while after the meeting that Cole admitted he had been working on the calculation for the previous two decades!

In spite of Cole's factorisation, Mersenne numbers remain a plentiful source of primes. In fact the five largest primes known today are Mersenne primes. For more information on the current search for primes see www.utm.edu/research/primes/largest.html.

Gauss's contribution

In his article 329 *Disquisitiones Arithmeticae* (1801), the German mathematician Carl Friedrich Gauss (1777–1855) wrote:

> The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern

> geometers to such an extent that it would be superfluous to discuss the problem at length... Further, the dignity of science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated.

One of the most intriguing aspects of primes is that there is no obvious pattern governing their distribution among the positive integers. In fact all attempts to find a formula that will produce only primes, or even predict their exact distribution, have so far failed. But Gauss switched his attention from finding individual primes to finding their average distribution.

In 1792, at the age of 15, Gauss examined a table of prime numbers compiled by the German-Swiss Mathematician Johann Heinrich Lambert (1728–1777). Gauss was seeking a rule which governs the number of primes less than or equal to some integer x. We denote this number by $\pi(x)$. For example since there are 6 primes smaller than 14, we have $\pi(14) = 6$. A closer examination indicates that on average the gaps between primes becomes larger and larger. Gauss asked whether for large x the behaviour of $\pi(x)$ could be approximated by a known function. Gauss then made a bold conjecture which he scribbled on the back of his table of logarithms. It read

> primzahlem unter a $(= \infty)$ $a/\ln a$.

This can be interpreted as saying

> $\pi(a) \sim a/\ln a$ for large values of a.

Gauss did not attempt to prove his conjecture, he merely got a sense of what he thought the answer should be. The proof (of the more precise result involving limits) eluded many great minds including Georg Friedrich Bernhard Riemann (1826–1866), himself a student of Gauss, who published a paper on the subject in 1859. Success finally came in 1896 when Jacques Salomon Hadamard (1865–1963) of France and Charles de la Vallée-Poussin (1866–1962) of Belgium independently proved Gauss's conjecture. Today this result is known as *The Prime Number Theorem*.

Other facts about primes

The answer to the question of how many prime numbers exist is given by the fundamental theorem:

> There exist infinitely many prime numbers.

Euclid was the first to prove this (c 350 BC). His proof is also one of the simplest.

Euclid's Proof. Suppose that

$p_1 = 2 < p_2 = 3 < \ldots < p_r$

are all the primes. Let

$P = p_1 p_2 \ldots p_r + 1$

and let p be a prime dividing P. Then p cannot be any of $p_1, p_2, \ldots p_r$, otherwise p would divide the difference $P - p_1 p_2 \ldots p_r = 1$, which is impossible. So this prime p is still another prime, and $p_1, p_2, \ldots p_r$ would not be all the primes.

However the proof of Euclid's theorem does not give us a way of producing new primes since, for example,

$$2 \times 3 \times \ldots \times 13 + 1 = 30031 = 59 \times 509.$$

One of the ways to find all primes less than or equal to N is to list all numbers less than or equal to N and then cross out all multiples of primes. Those numbers left must be primes. This method is called the *Sieve of Eratosthenes*, named after Eratosthenes (who lived in the third century BC), but is obviously not practical for larger numbers. For example if we take $N = 100$, and we cross off all multiples of primes, then the remaining numbers (in white, below) are all the primes.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Some known results about primes

- In 1845 Bertrand (1822–1900) investigated experimentally the properties of $\pi(x)$, the number of primes less than or equal to x. As a result, he conjectured:

  For $n > 1$, between n and $2n$ there is always a prime number.

  This was proved by Tschebycheff in 1852.

- In 1837, Dirichlet (1805–1859) proved that an arithmetic progression $\{a + nb\}$, where a and b are relatively prime, contains an infinite number of primes.

- There exist arbitrarily long stretches of numbers which do not contain a prime. For example
  1000! +2, 1000! +3, ... 1000! +1000
  is a stretch of 999 consecutive composite numbers.

Unproved conjectures

Primes have a tendency to arrange themselves in pairs of the form $(p, p+2)$: for example 3 and 5, 5 and 7, 17 and 19. This is also evident among much larger numbers such as 29 879 and 29 881. Such primes are called twin primes or prime pairs, and it is not known whether there are infinitely many of these twin primes. However most mathematicians believe the answer is, "Yes".

A more famous conjecture regarding primes is the *Goldbach Conjecture*, named after Christian Goldbach (1690–1764), a German mathematician who later became Russia's foreign affair minister. In a letter to Euler (1742) he conjectured:

1. Every even number greater than or equal to 4 is the sum of two primes; for example
   $4 = 2 + 2$, $6 = 3 + 3$, $8 = 3 + 5$,
   $10 = 5 + 5$, $12 = 5 + 7$.

(It is easy to verify that this conjecture fails for odd numbers, 11 for example.)

In the letter Goldbach also expressed the following belief:

2. Every integer n greater than or equal to 5 is the sum of three primes.

As far as is known, Euler did not prove (1), but neither Euler nor anyone else has been able to find a counter-example. This conjecture has since been tested for all even numbers up to at least 1010 and found to be true. This still remains one of the great unsolved conjectures of mathematics.

Pierre de Fermat (1601–1655)

Pierre de Fermat (1601–1655) conjectured that

$$F_n = 2^{2^n} + 1$$

is prime for any non-negative integer n. The conjecture was proven to be incorrect in 1732, when Euler showed that

$$F_5 = 4\,294\,967\,297 = 6\,700\,417 \times 641.$$

More recently analysis of these so-called Fermat numbers have found no other primes above F_4. However no-one has yet proved that F_4 is the largest Fermat prime.

References

Caldwell, C. (n.d.). *The Primes Pages*. Accessed at http://www.utm.edu/research/primes/largest.html.

Dunham, W. (1994). *The Mathematical Universe*. New York: John Wiley & Sons.

Maor E. (1994). *The Story of a Number*. Princeton: Princeton University Press.

Mollin, R. A. (1998). *Fundamental Number Theory with Applications*. New York: CRC Press.

Ribenboim, P. (1996). *The New Book of Prime Number Records*. New York: Springer-Verlag.

Ribenboim. P. (2000). *My Numbers, My Friends*. New York: Springer-Verlag.

Tim Melrose
Wynn Vale, SA
timmelrose@hotmail.com

Paul Scott
Wattle Park, SA
mail@paulscott.info