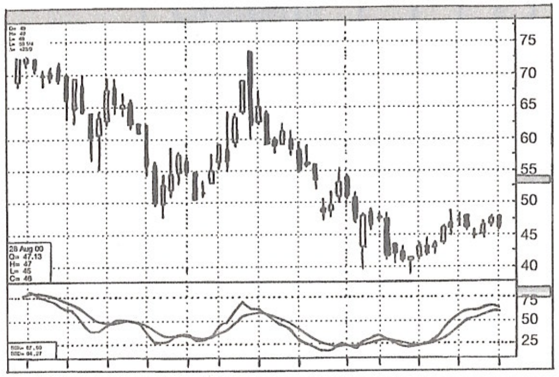
What coordinates do for us

We continue to use coordinates for maps, but another common use of coordinate geometry occurs in the stock market, where the fluctuations of some price are recorded as a curve. Here the *x*-coordinate is time, and the *y*-coordinate is the price. Enormous quantities of financial and scientific data are recorded in the same way.



Stock market data represented in coordinates

CHAPTER 7

Patterns in Numbers

The origins of number theory

Despite becoming ever more fascinated by geometry, mathematicians did not lose their interest in numbers. But they did start asking deeper questions, and answered many of them. A few had to wait for more powerful techniques. Some remain unanswered to this day.

Number theory

There is something fascinating about numbers. Plain, unadorned whole numbers, 1, 2, 3, 4, 5, ... What could possibly be simpler? But that simple exterior conceals hidden depths, and many of the most baffling questions in mathematics are about apparently straightforward properties of whole numbers. This area is known as *number theory*, and it turns out to be difficult precisely because its ingredients are so basic. The very simplicity of whole numbers leaves little scope for clever techniques.

The earliest serious contributions to number theory – that is, complete with proofs, not just assertions – are found in the works of Euclid, where the ideas are thinly disguised as geometry. The subject was developed into a distinct area of mathematics by the Greek, Diophantus, some of whose writings survive as later copies. Number theory was given a big boost in the 1600s by Fermat, and developed by Leonhard Euler, Joseph-Louis Lagrange and Carl Friedrich Gauss into a deep and extensive branch of mathematics which touched upon many other areas, often seemingly unrelated. By the end of the 20th century these connections had been used to answer some – though not all – of the ancient puzzles, including a very famous conjecture made by Fermat around 1650, known as his Last Theorem.

For most of its history, number theory has been about the internal workings of mathematics itself, with few connections to the real world. If ever there was a branch of mathematical thought that lived in the heady reaches of the ivory towers, it was number theory. But the advent of the digital computer has changed all that. Computers work with electronic representations of whole numbers, and the problems and opportunities raised by computers frequently lead to number theory. After 2500 years as a purely intellectual exercise, number theory has finally made an impact on everyday life.

Primes

Anyone who contemplates the multiplication of whole numbers eventually notices a fundamental distinction.

Many numbers can be broken up into smaller pieces, in the sense that the number concerned arises by multiplying those pieces together. For instance, 10 is 2 × 5, and 12 is 3 × 4. Some numbers, however, do not break up in this manner. There is no way to express 11 as the product of two *smaller* whole numbers; the same goes for 2, 3, 5, 7 and many others.

The numbers that can be expressed as the product of two smaller numbers are said to be *composite*. Those that cannot be so expressed are *prime*. According to this definition, the number 1 should be considered prime, but for good reasons it is placed in a special class of its own and called a *unit*. So the first few primes are the numbers

2 3 5 7 11 13 17 19 23 29 31 37 41

As this list suggests, there is no obvious pattern to the primes (except that all but the first are odd). In fact, they seem to occur somewhat irregularly, and there is no simple way to predict the next number on the list. Even so, there is no question that this number is somehow *determined* – just test successive numbers until you find the next prime.

Despite, or perhaps because of, their irregular distribution, primes are of vital importance in mathematics. They form the basic building blocks for all numbers, in the sense that larger numbers are created by multiplying smaller ones. Chemistry tells us that any molecule, however complicated, is built from atoms – chemically indivisible particles of matter. Analogously, mathematics tells us that any number, however big it may be, is built from primes – indivisible numbers. So primes are the atoms of number theory.

This feature of primes is useful because many questions in mathematics can be solved for all whole numbers provided they can be solved for the primes, and primes have special properties that sometimes make the solution of the question easier. This dual aspect of the primes – important but ill-behaved – excites the mathematician's curiosity.

Euclid

Euclid introduced primes in Book VII of the *Elements*, and he gave proofs of three key properties. In modern terminology, these are:

(i) Every number can be expressed as a product of primes.

(ii) This expression is unique except for the order in which the primes occur.

(iii) There are infinitely many primes.

What Euclid actually stated and proved is slightly different. Proposition 31, Book VII tells us that any composite number is measured by some prime – that is, it can be divided exactly by that prime. For example, 30 is composite, and it is exactly divisible by

Why Uniqueness of Prime Factors is not Obvious

Since the primes are the atoms of number theory, it might seem obvious that the *same* atoms always turn up when a number is broken into primes. After all, atoms are the indivisible pieces. If you could break a number up in two distinct ways, wouldn't that involve splitting an atom? But here the analogy with chemistry is slightly misleading.

To see that uniqueness of prime factorization is *not* obvious, we can work with a restricted set of numbers:

1 5 9 13 17 21 25 29

and so on. These are the numbers that are one greater than a multiple of 4. Products of such numbers also have the same property, so we can build such numbers up by multiplying smaller numbers of the same type. Define a 'quasiprime' to be any number in this list that is not the product of two smaller numbers *in the list*. For instance, 9 is quasiprime: the only smaller numbers in the list are 1 and 5, and their product is not 9. (It is still true that $9 = 3 \times 3$, of course, but the number 3 is not in the list.)

It is obvious – and true – that every number in the list is a product of quasiprimes. However, although these quasiprimes are the atoms of the set, something rather strange happens. The number 693 breaks up in two different ways: $693 = 9 \times 77 = 21 \times 33$, and all four factors, 9, 21, 33 and 77, are *quasiprime*. So uniqueness of factorization fails for this type of number.

several primes, among them 5 – in fact, $30 = 6 \times 5$. By repeating this process of pulling out a prime divisor, or *factor*, we can break any number down into a product of primes. Thus, starting from $30 = 6 \times 5$, we observe that 6 is also composite, with $6 = 2 \times 3$. Now $30 = 2 \times 3 \times 5$, and all three factors are prime.

If instead we had started from $30 = 10 \times 3$, then we would break down 10 instead, as $10 = 2 \times 5$, leading to $30 = 2 \times 5 \times 3$. The same three primes occur, but multiplied in a different order – which of course does not affect the result. It may seem obvious that however we break a number into primes, we always get the same result except for order, but this turns out to be tricky to prove. In fact, similar statements in some related systems of numbers turn out to be *false*, but for ordinary whole numbers the statement is true. Prime factorization is *unique*. Euclid proves the key fact needed to establish uniqueness in Proposition 30, Book VII of the *Elements*: if a prime divides the product of two numbers, then it must divide at least one of those numbers. Once we know Proposition 30, the uniqueness of prime factorization is a straightforward consequence.

Proposition 20, Book IX states that: 'Prime numbers are more than any assigned multitude of prime numbers.' In modern terms, this

The Largest Known Prime

There is no largest prime, but the largest *known* prime as of May 2009 is $2^{43,112,609} - 1$, which has 12,978,189 decimal digits. Numbers of the form $2^p - 1$, with p prime, are called Mersenne primes, because Mersenne conjectured in his *Cogitata Physica-Mathematica* of 1644 that these numbers are prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ and 257, and composite for all other whole numbers up to 257.

There are special high-speed methods for testing such numbers to see if they are primes, and we now know that Mersenne made five mistakes. His numbers are composite when $p = 67$ and 257, and there are three more primes with $p = 61, 89, 107$. Currently 44 Mersenne primes are known. Finding new ones is a good way to test new supercomputers, but has no practical significance.

means that the list of primes is infinite. The proof is given in a representative case: suppose that there are only three prime numbers, a, b and c. Multiply them together and add one, to obtain $abc + 1$. This number must be divisible by some prime, but that prime cannot be any of the original three, since these divide abc exactly, so they cannot also divide $abc + 1$, since they would then divide the difference, which is 1. We have therefore found a new prime, contradicting the assumption that a, b, c are all the primes there are.

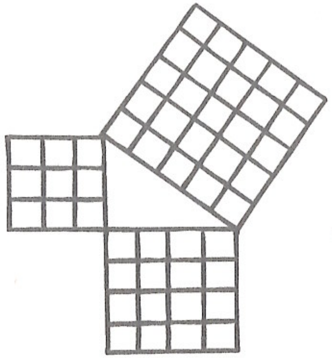
Although Euclid's proof employs three primes, the same idea works for a longer list. Multiply all primes in the list, add one and then take some prime factor of the result; this always generates a prime that is not on the list. Therefore no finite list of primes can ever be complete.

Diophantus

We have mentioned Diophantus of Alexandria in connection with algebraic notation, but his greatest influence was in number theory. Diophantus studied general questions, rather than specific numerical ones, although his *answers* were specific numbers. For example: 'Find three numbers such that their sum, and the sum of any two, is a perfect square.' His answer is 41, 80 and 320. To check: the sum of all three is $441 = 21^2$. The sums of pairs are $41 + 80 = 11^2$, $41 + 320 = 19^2$ and $80 + 320 = 20^2$.

One of the best known equations solved by Diophantus is a curious offshoot of Pythagoras's Theorem. We can state the theorem algebraically: if a right triangle has sides a, b, c with c being the longest, then $a^2 + b^2 = c^2$. There are some special right triangles for which the sides are whole numbers. The simplest and best known is when a, b, c are 3, 4, 5, respectively; here $3^2 + 4^2 = 9 + 16 = 25 = 5^2$. Another example, the next simplest, is $5^2 + 12^2 = 13^2$.

In fact, there are infinitely many of these *Pythagorean triples*. Diophantus found all possible whole number solutions of what we now write as the equation $a^2 + b^2 = c^2$. His recipe is to take any two whole numbers, and form the difference between their squares, twice their product and the sum of their squares. These three numbers always form a Pythagorean triple, and all such triangles arise in this manner provided we also allow all three numbers to be multiplied by some constant. If the numbers are 1 and 2, for example, we get the famous 3-4-5 triangle. In particular, since there are infinitely many ways to choose the two numbers, there exist infinitely many Pythagorean triples.



The 3-4-5 right-angled triangle

Fermat

After Diophantus, number theory stagnated for over a thousand years, until it was taken up by Fermat, who made many important discoveries. One of his most elegant theorems tells us exactly when a given integer n is a sum of two perfect squares: $n = a^2 + b^2$. The solution is simplest when n is prime. Fermat observed that there are three basic types of prime:

(i) The number 2, the only even prime.

(ii) Primes that are 1 greater than a multiple of 4, such as 5, 13, 17 and so on – these primes are all odd.

(iii) Primes that are 1 less than a multiple of 4, such as 3, 7, 11 and so on – these primes are also odd.

He proved that a prime is a sum of two squares if it belongs to categories (i) or (ii), and it is not a sum of two squares if it belongs to category (iii).

For instance, 37 is in category (ii), being 4 × 9 + 1, and $37 = 6^2 + 1^2$, a sum of two squares. In contrast, $31 = 4 \times 8 - 1$ is in category (iii), and if you try all possible ways to write 31 as a sum of two squares, you will find that nothing works. (For instance, 31 = 25 + 6, where 25 is a square, but 6 is not.)

What We Don't Know about Prime Numbers

Even today, the primes still have some secrets. Two famous unsolved problems are the Goldbach Conjecture and the Twin Primes Conjecture.

Christian Goldbach was an amateur mathematician who corresponded regularly with Euler. In a letter of 1742, he described evidence that every whole number greater than 2 is the sum of three primes. Goldbach viewed 1 as a prime, which we no longer do; as a consequence, we would now exclude the numbers $3 = 1 + 1 + 1$ and $4 = 2 + 1 + 1$. Euler proposed a stronger conjecture: that every even number greater than 2 is the sum of two primes. For example, $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 5 + 5$ and so on. This conjecture implies Goldbach's. Euler was confident that his conjecture was true, but could not find a proof, and the conjecture is still open. Computer experiments have shown it to be true for every even number up 10^{18}. The best known result was obtained by Chen Jing-Run in 1973 using complicated techniques from analysis. He proved that every sufficiently large even number is the sum of two primes, or a prime and an almost-prime (the product of two primes).

The twin prime conjecture is much older, and goes back to Euclid. It states that there are infinitely many *twin primes* p and $p + 2$. Examples of twin primes are 5, 7 and 11, 13. Again, no proof or disproof is known. In 1966, Chen proved that there are infinitely many primes p, such that $p + 2$ is either prime or almost-prime. Currently, the largest known twin primes are $2{,}003{,}663{,}613 \times 2^{195{,}000} \pm 1$, found by Eric Vautier, Patrick McKibbon and Dmitri Gribenko in 2007.

The upshot is that a number is a sum of two squares if and only if every prime divisor of the form $4k - 1$ occurs to an even power. Using similar methods, Joseph-Louis Lagrange proved in 1770 that every positive integer is a sum of four perfect squares (including one or more 0s if necessary). Fermat had previously stated this result, but no proof is recorded.

One of Fermat's most influential discoveries is also one of the simplest. It is known as Fermat's Little Theorem, to avoid confusion with his Last (sometimes called Great) Theorem, and it states that if p is any prime and a is any whole number, then $a^p - a$ is a multiple of p. The corresponding property is *usually* false when p is composite, but not always.

Fermat's most celebrated result took 350 years to prove. He stated it around 1640, and he claimed a proof, but all we know of his work is a short note. Fermat owned a copy of Diophantus's *Arithmetica*, which inspired many of his investigations, and he often wrote down his own ideas in the margin. At some point he must have been thinking about the Pythagorean equation: add two squares to get a square. He wondered what would happen if instead of squares you tried cubes, but found no solutions. The same problem arose for fourth, fifth or higher powers.

In 1670 Fermat's son Samuel published an edition of Bachet's translation of the *Arithmetica*, which included Fermat's marginal notes. One such note became notorious: the statement that if $n \geq 3$, the sum of two nth powers is never an nth power. The marginal note states 'To resolve a cube into the sum of two cubes, a fourth power into two fourth powers or, in general, any power higher than the second into two of the same kind is impossible; of which fact I have found a remarkable proof. The margin is too small to contain it.'

It seems unlikely that his proof, if it existed, was correct. The first,

Pierre de Fermat

1601–1665

Pierre Fermat was born at Beaumont-de-Lomagne in France in 1601, son of the leather merchant Dominique Fermat and Claire de Long, the daughter of a family of lawyers. By 1629 he had made important discoveries in geometry and the forerunner of the calculus, but he chose law as a career, becoming a Councillor at the parliament of Toulouse in 1631. This entitled him to add the 'de' to his name. As an outbreak of plague killed off his superiors, he advanced rapidly. In 1648 he became a King's Councillor in the local parliament of Toulouse, where he served for the rest of his life, reaching the most senior level of the Criminal Court in 1652.

He never held an academic position, but mathematics was his passion. In 1653 he contracted plague, was rumoured to be dead, but survived. He carried out extensive correspondence with other intellectuals, notably the mathematician Pierre de Carcavi and the monk Marin Mersenne.

He worked in mechanics, optics, probability and geometry, and his method for locating the maximum and minimum values of a function paved the way for calculus. He became one of the world's leading mathematicians, but published little of his work, mainly because he was not willing to spend the time required to bring it into publishable form.

His most long-lasting influence was in number theory, where he challenged other mathematicians to prove a series of theorems and solve various problems. Among these was the (misnamed) 'Pell equation' $nx^2 +1 = y^2$, and the statement that the sum of two non-zero perfect cubes cannot be a perfect cube. This is a special case of a more general conjecture, 'Fermat's Last Theorem', in which cubes are replaced by nth powers for any $n \geq 3$.

He died in 1665, just two days after concluding a legal case.

and currently only, proof was derived by Andrew Wiles in 1994; it uses advanced abstract methods that did not exist until the late 20th century.

After Fermat, several major mathematicians worked in number theory, notably Euler and Lagrange. Most of the theorems that Fermat had stated but not proved were polished off during this period.

Gauss

The next big advance in number theory was made by Gauss, who published his masterpiece, the *Disquisitiones Arithmeticae* (*Investigations in Arithmetic*) in 1801. This book propelled the theory of numbers to the centre of the mathematical stage. From then on, number theory was a core component of the mathematical mainstream. Gauss mainly focused on his own, new, work, but he also set up the foundations of number theory and systematized the ideas of his predecessors.

The most important of these foundational changes was a very simple but powerful idea: *modular arithmetic*. Gauss discovered a new type of number system, analogous to integers but differing in one key respect: some particular number, known as the **modulus**, was identified with the number zero. This curious idea turned out to be fundamental to our understanding of divisibility properties of ordinary integers.

Here is Gauss's idea. Given an integer m, say that a and b are **congruent to the modulus** m, denoted

$$a \equiv b(\text{mod } m)$$

if the difference $a - b$ is exactly divisible by m. Then arithmetic to the modulus m works exactly the same as ordinary arithmetic, except that we may replace m by 0 anywhere in the calculation. So, any multiple of m can be ignored.

The phrase 'clock arithmetic' is often used to capture the spirit of Gauss's idea. On a clock, the number 12 is effectively the same as 0 because the hours repeat after 12 steps (24 in continental Europe and military activities). Seven hours after

Carl Friedrich Gauss
1777–1855

Gauss was highly precocious, allegedly correcting his father's arithmetic when aged three. In 1792, with financial assistance from the Duke of Brunswick-Wolfenbüttel, Gauss went to Brunswick's Collegium Carolinum. There he made several major mathematical discoveries, including the law of quadratic reciprocity and the prime number theorem, but did not prove them. From 1795–98 he studied at Göttingen, where he discovered how to construct a regular 17-sided polygon with ruler and compass. His *Disquisitiones Arithmeticae*, the most important work in number theory to date, was published in 1801.

Gauss's public reputation, however, rested on an astronomical prediction. In 1801 Giuseppe Piazzi discovered the first asteroid: Ceres. The observations were so sparse that astronomers were worried that they might not find it again when it reappeared from behind the Sun. Several astronomers predicted where it would reappear; so did Gauss. Only Gauss was right. In fact, Gauss had used a method of his own invention, now called the 'method of least squares', to derive accurate results from limited observations. He did not reveal this technique at the time, but it has since become fundamental in statistics and observational science.

In 1805 Gauss married Johanna Ostoff, whom he loved dearly, and in 1807 he left Brunswick to become director of the Göttingen observatory. In 1808 his father died, and Johanna died in 1809 after giving birth to their second son. Soon after, the son died too.

Despite these personal tragedies, Gauss continued his research, and in 1809 he published his *Theoria Motus Corporum Coelestium in Sectionibus Conicis Solem Ambientium*, a major contribution to celestial mechanics. He married again, to Minna, a close friend of Johanna's, but the marriage was more out of convenience than love.

Around 1816 Gauss wrote a review of deductions of the parallel axiom from the other axioms of Euclid, in which he hinted at an opinion he had probably held since 1800, the possibility of a logically consistent geometry that differed from Euclid's.

In 1818 he was placed in charge of a geodetic survey of Hanover, making serious contributions to the methods employed in surveying. In 1831, after the death of Minna, Gauss began working with the physicist Wilhelm Weber on the Earth's magnetic field.

They discovered what are now called Kirchhoff's laws for electrical circuits, and constructed a crude but effective telegraph. When Weber was forced to leave Göttingen in 1837, Gauss's scientific work went into decline, though he remained interested in the work of others, notably Ferdinand Eisenstein and Georg Bernhard Riemann. He died peacefully in his sleep.

6 o'clock is not 13 o'clock, but 1 o'clock, and in Gauss's system $13 \equiv 1 \pmod{12}$. So modular arithmetic is like a clock that takes m hours to go full circle. Not surprisingly, modular arithmetic crops up whenever mathematicians look at things that change in repetitive cycles.

The *Disquisitiones Arithmeticae* used modular arithmetic as the basis for deeper ideas, and we mention three.

The bulk of the book is a far-reaching extension of Fermat's observations that primes of the form $4k + 1$ are a sum of two squares, whereas those of the form $4k - 1$ are not. Gauss restated this result as a characterization of integers that can be written in the form $x^2 + y^2$, with x and y integers. Then he asked what happens if instead of this formula we use a general *quadratic form*, $ax^2 + bxy + cy^2$. His theorems are too technical to discuss, but he obtained an almost complete understanding of this question.

Another topic is the law of quadratic reciprocity, which intrigued and perplexed Gauss for many years. The starting point is a simple question: what do perfect squares look like to a given modulus?

For instance, suppose that the modulus is 11. Then the possible perfect squares (of the numbers less than 11) are

$$0 \quad 1 \quad 4 \quad 9 \quad 16 \quad 25 \quad 36 \quad 49 \quad 64 \quad 81 \quad 100$$

which, when reduced (mod 11), yield

$$0 \quad 1 \quad 3 \quad 4 \quad 5 \quad 9$$

with each non-zero number appearing twice. These numbers are the *quadratic residues*, mod 11.

The key to this question is to look at prime numbers. If p and q are primes, when is q a square (mod p)? Gauss discovered that while there is no simple way to answer that question directly, it bears a remarkable relation to another question: when is p a square (mod q)? For example, the list of quadratic residues above shows that $q = 5$ is a square modulo $p = 11$. It is also true that 11 is a square modulo 5 – because $11 \equiv 1 \pmod 5$ and $1 = 1^2$. So here both questions have the same answer.

Gauss proved that this law of reciprocity holds for any pair of odd primes, except when both primes are of the form $4k - 1$, in which case the two questions always have opposite answers. That is: for any odd primes p and q,

$$q \text{ is a square (mod } p) \text{ if and only if } p \text{ is a square (mod } q),$$

unless both p and q are of the form $4k - 1$, in which case

$$q \text{ is a square (mod } p) \text{ if and only if } p \text{ is } \textit{not} \text{ a square (mod } q).$$

Initially Gauss was unaware that this was not a new observation: Euler had noticed the same pattern. But unlike Euler, Gauss managed to prove that it is always true. The proof was very difficult, and it took Gauss several years to fill one small but crucial gap.

A third topic in the *Disquisitiones* is the discovery that had convinced Gauss to become a mathematician at the age of 19: a geometric construction for the regular 17-gon (a polygon with 17 sides). Euclid provided constructions, using unmarked ruler and compass, for regular polygons with three, five and 15 sides; he also knew that those numbers could be repeatedly doubled by bisecting angles, yielding regular polygons with four, six, eight and 10 sides, and so on. But Euclid gave no constructions for 7-sided polygons, 9-sided ones, or indeed any other numbers than the ones just listed. For some two thousand years, the mathematical world assumed that Euclid had said the last word, and no other regular polygons were constructable. Gauss proved them wrong.

It is easy to see that the main problem is constructing regular p-gons when p is prime. Gauss pointed out that such a construction is equivalent to solving the algebraic equation

$$x^{p-1} + x^{p-2} + x^{p-3} + \cdots + x^2 + x + 1 = 0$$

Now, a ruler-and-compass construction can be viewed, thanks to coordinate geometry, as a sequence of quadratic equations. If a construction of this kind exists, it follows (not entirely trivially) that $p - 1$ must be a power of 2.

The Greek cases $p = 3$ and 5 satisfy this condition: here $p - 1 = 2$ and 4, respectively. But they are not the only such primes. For instance $17 - 1 = 16$ is a power of 2. This does not yet prove that the 17-gon is constructable, but it provides a strong hint, and Gauss managed to find an explicit reduction of his 16th degree equation to a series of quadratics. He stated, but did not prove, that a construction is possible whenever $p - 1$ is a power of 2 (still requiring p to be prime), and it is impossible for all other primes. The proof was soon completed by others.

These special primes are called *Fermat primes*, because they were studied by Fermat. He observed that if p is a prime and $p - 1 = 2^k$, then k must itself be a power of 2. He noted the first few Fermat primes: 2, 3, 5, 17, 257 and 65,537. He conjectured that numbers of the form $2^{2^m} + 1$ are always prime, but this was wrong. Euler

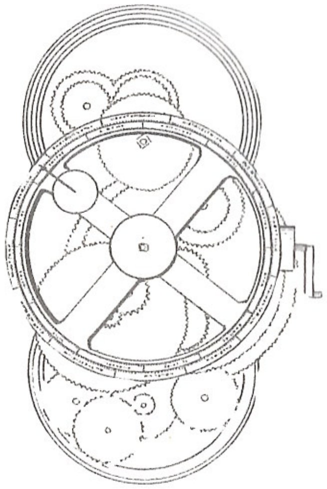
What number theory did for them

One of the earliest practical applications of number theory occurs in gears. If two cogs are placed together so that their teeth mesh, and one cog has *m* teeth, the other *n* teeth, then the movement of the cogs is related to these numbers. For instance, suppose one cog has 30 teeth and the other has 7. If I turn the big cog exactly once, what does the smaller one do? It returns to the initial position after 7, 14, 21 and 28 steps. So, the final 2 steps, to make 30, advance it by just 2 steps. This number turns up because it is the remainder on dividing 30 by 7. So the motion of cogs is a mechanical representation of division with remainder, and this is the basis of modular arithmetic.

Cogwheels were used by ancient Greek craftsmen to design a remarkable device, the Antikythera mechanism. In 1900 the sponge diver Elias Stadiatis found a formless lump of corroded rock in a wreck of 65 BC near the island of Antikythera, some 40 metres (140 feet) down. In 1902 the archaeologist Valerios Stais noticed that the rock contained a gear wheel, and was actually the remains of a complicated bronze mechanism. It was inscribed with words in the Greek alphabet.

The mechanism's function has been worked out from its structure and its inscriptions, and it turns out to be an astronomical calculator. There are more than 30 gear wheels – the latest reconstruction, in 2006, suggests there were originally 37. The numbers of cogs correspond to important astronomical ratios. In particular, two cogs have 53 teeth – a difficult number to manufacture – and this number comes from the rate at which the Moon's furthest point from the Earth rotates. All the prime factors of the numbers of teeth are based on two classical astronomical cycles, the Metonic and Saros cycles. X-ray analysis has revealed new inscriptions and made them readable, and it is now certain that the device was used to predict the positions of the Sun, the Moon and probably the then-known planets. The inscriptions date to around 150–100 BC.

The Antikythera mechanism is of a sophisticated design, and appears to incorporate Hipparchus's theory of the motion of the Moon. It may well have been built by one of his students, or at least with their aid. It was probably an executive toy for a royal personage, rather than a practical instrument, which may explain its exquisite design and manufacture.



A reconstruction of the Antikythera mechanism

discovered that when m = 5 there is a factor 641.

It follows that there must also exist ruler-and-compass constructions for the regular 257-gon and 65,537-gon. F.J. Richelot constructed the regular 257-gon in 1832, and his work is correct. J. Hermes spent ten years working on the 65,537-gon, and completed his construction in 1894. Recent studies suggest there are mistakes.

Number theory started to become mathematically interesting with the work of Fermat, who spotted many of the important patterns concealed in the strange and puzzling behaviour of whole numbers. His annoying tendency not to supply proofs was put right by Euler, Lagrange and a few less prominent figures, with the sole exception of his Last Theorem, but number theory seemed to consist of isolated theorems – often deep and difficult, but not very closely connected to each other.

Marie-Sophie Germain

1776–1831

Sophie Germain was the daughter of the silk merchant Ambroise-François Germain and Marie-Madelaine Gruguelin. At age 13 she read of the death of Archimedes, killed by a Roman soldier while contemplating a geometric diagram in the sand, and was inspired to become a mathematician. Despite her parents' well-meaning efforts to deter her – mathematics was not then considered a suitable vocation for a young lady – she read the works of Newton and Euler, wrapped in a blanket while her mother and father were sleeping. When her parents became convinced of her commitment to mathematics, they relented and started to help her, giving her financial support throughout her life.

She obtained lecture notes from the École Polytechnique, and wrote to Lagrange with some original work of her own under the name 'Monsieur LeBlanc'. Lagrange, impressed, eventually discovered that the writer was a woman, and had the good sense to encourage her and become her sponsor. The two worked together, and some of her results were included in a later edition of Legendre's 1798 *Essai sur le Théorie des Nombres*.

Her most celebrated correspondent was Gauss. Sophie studied the *Disquisitiones Arithmeticae*, and from 1804 to 1809 she wrote a number of letters to its author, again concealing her gender by using the name LeBlanc. Gauss praised LeBlanc's work in letters to other mathematicians. In 1806 he discovered that LeBlanc was actually female, when the French occupied Braunschweig. Concerned that Gauss might suffer the same fate as Archimedes, Sophie contacted a family friend who was a senior officer in the French Army, General Pernety. Gauss learned of this, and discovered that LeBlanc was actually Sophie.

Sophie need not have worried. Gauss was even more impressed, and wrote to her: 'But how to describe to you my admiration and astonishment at seeing my esteemed correspondent Monsieur Le Blanc metamorphose himself into this illustrious personage ... When a person of the sex which, according to our customs and prejudices, must encounter infinitely more difficulties than men to familiarize herself with these thorny researches, succeeds nevertheless in surmounting these obstacles and penetrating the most obscure parts of them, then without doubt she must have the noblest courage, quite extraordinary talents and superior genius.'

Sophie obtained some results on Fermat's Last Theorem, the best available until 1840. Between 1810 and 1820 she worked on the vibrations of surfaces, a problem posed by the Institut de France. In particular, an explanation was sought for 'Chladni patterns' – symmetric patterns that appear if sand is sprinkled on a metal plate, which is then caused to vibrate using a violin bow. On her third attempt she was awarded a gold medal, although for unknown reasons, possibly a protest about the unfair treatment of women scientists, she did not appear at the award ceremony.

In 1829 she developed breast cancer, but continued to work on number theory and the curvature of surfaces until her death two years later.

All that changed when Gauss got in on the act and devised general conceptual foundations for number theory, such as modular arithmetic. He also related number theory to geometry with his work on regular polygons. From that moment, number theory became a major strand in the tapestry of mathematics.

Gauss's insights led to the recognition of new kinds of structure in mathematics – new number systems, such as the integers mod n, and new operations, such as the composition of quadratic forms. With hindsight, the number theory of the late 18th and early 19th centuries led to the abstract algebra of the late 19th and 20th

What number theory does for us

Number theory forms the basis of many important security codes used for Internet commerce. The best known such code is the RSA (Ronald Rivest, Adi Shamir and Leonard Adleman) cryptosystem, which has the surprising feature that the method for putting messages into code can be made public without giving away the reverse procedure of decoding the message.

Suppose Alice wants to send a secret message to Bob. Before doing this, they agree on two large primes p and q (having at least a hundred digits) and multiply them together to get $M = pq$. They can make this number public if they wish. They also compute $K = (p - 1)(q - 1)$, but keep this secret.

Now Alice represents her message as a number x in the range 0 to M (or a series of such numbers if it's a long message). To encode the message she chooses some number a, which has no factors in common with K, and computes $y \equiv x^a (\text{mod } M)$. The number a must be known to Bob, and can also be made public.

To decode messages, Bob has to know a number b such that $ab \equiv 1$ mod K. This number (which exists and is unique) is kept secret. To decode y, Bob computes

$$y^b (\text{mod M}).$$

Why does this decode? Because

$$y^b \equiv (x^a)^b \equiv x^{ab} \equiv x^1 \equiv x (\text{mod } M),$$

using a generalization of Fermat's Little Theorem due to Euler.

This method is practical because there are efficient tests to find large primes. However, there are no known methods for finding the prime factors of a large number efficiently. So telling people the product pq does not help them find p and q, and without those, they cannot work out the value of b, needed to decode the message.

centuries. Mathematicians were starting to enlarge the range of concepts and structures that were acceptable objects of study. Despite its specialized subject matter, the *Disquisitiones Arithmeticae* marks a significant milestone in the development of the modern approach to the whole of mathematics. This is one of the reasons why Gauss is rated so highly by mathematicians.

Until the late 20th century, number theory remained a branch of pure mathematics – interesting in its own right, and because of its numerous applications within mathematics itself, but of little real significance to the outside world. All that changed with the invention of digital communications in the late 20th century. Since communication then depended on numbers, it is hardly a surprise that number theory came to the fore in those areas of application. It often takes time for a good mathematical idea to acquire practical importance – sometimes hundreds of years – but eventually most topics that mathematicians find significant for their own sake turn out to be valuable in the real world too.