This is the last preprint. The final paper appeared in "Mathematics and Culture, I", ed. by M. Emmer, Springer 2003.

This is a translation, performed by the editors of the mentioned book, of a paper by the same authors written in Italian. The authors did not approve such a version. I am inserting some corrections, but the paper should be rewritten to get rid of such an amateurish translation. A. Languasco

Prime Numbers and Cryptography

ALESSANDRO LANGUASCO, ALBERTO PERELLI

On the one hand, the study of numbers – and especially of prime numbers – has fascinated mathematicians since ancient times; on the other hand, humans have always felt the need for security in the transmission of information. In the last twenty years, thanks to the discovery of new mathematical methods and the remarkable progress in computing, a strict relationship has gradually developed between the two disciplines. At present, the most secure methods for the transmission of information that have recently been boosted by the development of e-commerce, are based on algorithms that depend on remarkable properties of prime numbers. In this article, we will briefly outline the development of the theory of prime numbers; then we will describe an application to the problem of security during data transmission, that is cryptography.

Prime Numbers

First of all, let us remember that a natural number $n > 1$ is said to be a *prime number* if it is divisible only by 1 and by itself: for instance, the numbers 2, 3, 5, 7, 11, 13, 17 and 19 are prime numbers.

Already the ancient Greeks had taken an interest in the determination of prime numbers. A technique developed in that period is the well-known *Sieve of Eratosthenes*: this method allows the calculation of all prime numbers between 2 and x, where x is any fixed real number. After writing down all natural numbers between 2 and x, one should take the number 2 and cross off every multiple of that prime number; the same should be done for the next non-crossed out number on the list (3) and so on. One proceeds this way (the next step involves considering the number 5 and crossing out all its multiples) up to the biggest natural number smaller than $\sqrt{x}$. Since, by the end of this procedure, we have crossed out all natural numbers with proper divisors smaller than $\sqrt{x}$, the remaining natural numbers are all prime numbers in the interval $[2,x]$.

Another problem that interested the Greeks is whether prime numbers are infinite. The answer is affirmative and several proofs of this are known. Here we will present Euclid's arithmetic proof:

Theorem (Euclid): *The number of primes is infinite*.

Proof. This proof uses the method of contradiction. Let us suppose that there exist a finite number of prime numbers p_1 to p_k such that $p_1 < p_2 < \ldots < p_k$. Let us now consider the number

$$N = p_1 p_2 \ldots p_k + 1$$

N clearly cannot be a prime number in that it is greater than p_k. On the other hand, N is not divisible by any p_j and therefore N is a prime number, which contradicts what above. The theorem is thereby proved. ■

At this point, one might wonder: *why are prime numbers interesting?* The most immediate reply to this question is that prime numbers are, in some way, the building blocks with which all integers are built. Formally, this statement is expressed by the well-known following theorem:

Fundamental Theorem of Arithmetic: *Every integer N > 1 can be written uniquely as a product of finitely many prime numbers.*

Observations:
(1) The proof of the Fundamental Theorem of Arithmetic consists of two parts:
a) existence of factorisation (direct consequence of the definition of prime number) trivial
b) uniqueness of factorisation (simple but not wholly ~~banal~~).
As to b), we recall that Hilbert's example shows how it is possible to build simple "numeric systems" in which the *uniqueness of factorisation does not hold*. Let us consider the integers of the form $4k + 1$, $k = 0, 1, \ldots$, that constitute a closed system with respect to multiplication. It can be easily verified that

$$693 = 9 \cdot 77 = 21 \cdot 33$$

provides two distinct factorisations of 693 as product of "primes" in this system: in fact, 9, 77, 21 and 33 do not allow a non-trivial factorisation as product of natural numbers of the form $4k + 1$.
(2) From the Fundamental Theorem of Arithmetic, it follows that

Corollary: $\sqrt{2}$ *is irrational.*

Proof. Let us suppose that $\sqrt{2} = \frac{m}{n}$. Then $n\sqrt{2} = m$ and therefore

$$2n^2 = m^2$$

Let us observe now that the factor 2 on the left side of the last equation has an odd exponent, whereas it has an even exponent on the right hand side, which contradicts the Fundamental Theorem of Arithmetic. ■

~~By and large~~, we can group problems relating to prime numbers into two distinct major categories:

- *algebraic problems* – concerning mainly the behaviour of prime numbers in algebraic extensions of rational numbers;
- *analytic problems* – concerning mainly distribution of primes among natural numbers.

In this article, we only deal with analytic problems.

It is natural to wonder: *how many prime numbers are there?* We already know that there are infinite primes, but what we are asking here is what is the order of magnitude of the quantity

$$\pi(x) = \text{number of primes between 1 and } x \,.$$

The first attempt to solve such problem was made by Gauss towards the end of the XVIII century. Using tables of primes he himself had calculated, Gauss conjectured that the number of primes not exceeding x is asymptotic to $x/\log x$:

$$\frac{\pi(x)}{x/\log x} \to \text{for } x \to \infty$$

As we will see later, Gauss's conjecture turned out to be correct and is nowadays know as the *Prime Numbers Theorem* (PNT).

The first steps towards proving Gauss's conjecture were made by Chebyshev towards the mid-nineteenth century.

Theorem (Chebyshev): *There exist two constants* $0<c<1<C$ *such that, for a sufficiently large* x:

$$c\frac{x}{\log x} \le \pi(x) \le C\frac{x}{\log x} \,.$$

The proof of Chebyshev's Theorem is based on an elementary but clever technique involving some properties of binomial coefficients.

The decisive step towards proving the PNT was taken by Riemann just a few years after Chebyshev. The fundamental novelty of Riemann's method was that of studying the function $\pi(x)$ using *complex analysis* (hence the "analytical" adjective used for such type of research).

Riemann introduced the function of the *complex* variable s

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad \text{Re}(s) > 1,$$

that is nowadays known as the *Riemann zeta function*. The Riemann zeta function is connected to prime numbers by means of *Euler's identity:*

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \quad \mathrm{Re}(s) > 1,$$

where the product is extended to all prime numbers. Euler's identity is a simple consequence of the Fundamental Theorem of Arithmetic and is actually considered to be the *analytical equivalent* of the unique factorisation of integers.

The crucial point about Euler's identity is that prime numbers explicitly appear on the right hand side, while the left hand side is defined independently of them. Riemann's method therefore paves the way for the possibility to obtain information about prime numbers through the study of the analytical properties of the function ζ(s). For instance, by taking advantage of the fact that

$$\lim_{s \to 1^+} \zeta(s) = +\infty$$

it is possible to easily obtain an analytical proof of Euclid's Theorem on the infinity of prime numbers.

Such analytical proof is owed to Euler, who considered ζ(s) as a function of the *real* variable *s*. Riemann showed that the function ζ(s) is extendable to the whole of the complex plane* and that the distribution of prime numbers is strictly connected to the *distribution of zeros* of the ζ(s) function. This connection has given rise to some of the most profound problems in mathematics.

The PNT was proven independently by Hadamard and de la Vallée Poussin in 1896. This ~~demonstration~~ proof, based on Riemann's method, represents the apex of a strand of research on the function theory of one complex variable, carried out mainly by Hadamard. The crucial point of this proof consisted in showing that ζ(1+*it*) ≠ 0** for any real number *t*, nowadays, it is known that the non-cancelling out of the Riemann zeta function on the straight line Re(s)=1 is in fact equivalent to the PNT.

Mainly ~~Chiefly~~ due to the influence of English mathematicians Hardy and Littlewood – who made substantial contributions to the analytical theory of numbers – for most of the first half of the twentieth century it was believed that it was impossible to obtain a proof of the PNT without making use of complex analysis techniques. Such belief turned out to be incorrect when, towards 1950, Selberg and Erdös gave an *elementary proof* of the PNT using what are essentially arithmetic techniques. It should, however, be stressed that "elementary" does not at all mean "easy": in fact, Selberg and Erdös's proof is conceptually more complex than the corresponding analytical proof.

Once the PNT was known, the next step was understanding "how good" the approximation of $\pi(x)$ was through the $x/\log x$ function or, more precisely, through the integral logarithm function

$$li(x) = \int_2^x \frac{dt}{\log t}$$

*: see below

**: see below

*: minus the point s = 1

**: different from zero ($t \neq 0$)

(where $x/\log x$ is the first asymptotic term). Presently, it is not possible to give a definitive answer to this problem, although the famous *Riemann Hypothesis* plays a fundamental role here:

$$\zeta(s) \neq 0 \text{ for } \mathrm{Re}(s) > \frac{1}{2}$$

It can be proved that the Riemann Hypothesis is equivalent to the approximation

$$\pi(x) = li(x) + 0\left(\sqrt{x}\log x\right)$$

that is, basically, the absolute value of the error incurred in approximating $\pi(x)$ with $li(x)$ is smaller than $\sqrt{x}\log x$. It should also be noted that such approximation, if true, is optimal; that several heuristic arguments supporting the Riemann Hypothesis are known and that large-scale computations support its validity.

At this moment in time, many results have been proven, but many more *remain open problems* for the research on the distribution of primes. Apart from the Riemann Hypothesis, there are also several *classical problems*:

1) (*primes represented by polynomials*) Is there an infinite number of natural numbers n for which n^2+1 is a prime? (or, more generally, "Is $P(n)$ a prime for infinite natural numbers n?", where $P(x)$ is an irreducible polynomial with no fixed divisors).
2) (*distance between two consecutive prime numbers*) Does there always exist a prime between two consecutive perfect squares?
3) (*twin primes*) Do there exist infinite prime numbers p such that $p+2$ is still a prime?
4) (*Goldbach's conjecture*) Can each even natural number greater than 2 be written as a sum of two prime numbers?

We conclude this section with the observation that various difficulties are encountered in solving the problems above: for instance, the main difficulty in problems 3) and 4) lies in the fact that prime numbers are defined through the properties of multiplication, while the problems in question involve the properties of addition.

Cryptography

Cryptography is the study of the methods that allow the secure transmission of information. Two main types of cryptography exist:

a) *secret key*: the classical method, used since ancient Rome. It is useful only when the number of users is small, since its correct working requires each

user to agree on – and exchange ~~secret~~ key with – every other user prior to use;

b) *public key*: the modern method. It allows secure communication even when the number of users is ~~high,~~ since it does not require a prior exchange of ~~secret~~ keys. It was first proposed by Diffie and Hellman in 1976.

At first sight, public key cryptography seems impossible. In order to persuade you of the opposite, we propose the classical example of the *double lock*. Suppose that there are two users *A* and *B* and that *A* wants to send a secret message to *B*;

1) *A* puts the message in a box, locks it with her lock L_A (Only *A* has a key to this lock) and then sends it to *B*.
2) *B* receives the box locked with lock L_A and adds her own lock L_B (only *B* has a key to this lock) and sends everything back to *A;*
3) *A* receives the box with double lock, removes lock L_A and re-sends the box to *B*;
4) At this point, having received the box, *B* can remove the lock L_B and read *A*'s message.

The security of this method lies in the fact that the keys to open the two locks are known only to the respective owners (who have not agreed on and exchanged keys prior to the transaction).

One of the "mathematical versions" of this idea is *R.S.A. public key cryptography*, proposed by Rivest, Shamir and Adleman in 1978. Let us briefly examine how *A* can send a secret message to *B* using the *R.S.A.* method:

B randomly chooses:

- two large primes *p*, *q* (consisting of 200-300 digits in base 10) and ~~*calculates*~~ $N = pq$ and $\varphi(N)=(p-1)(q-1)$
- a natural number that is *coprime* with $\varphi(N)$ such that $e < \varphi(N)$ and ~~*calculates*~~ the natural number $d < \varphi(N)$ such that $de \equiv (\text{mod } \varphi(N))$

B then makes public numbers *N* and *e*.

In order to send a message to *B*, *A* carries out the following operations:

1) encodes the message in the standard way using numbers $\leq N$;
2) sends to *B* each number *M* resulting from such encoding under the form of $M^e \ (\text{mod } N)$.

In order to decode the message, *B* simply ~~calculates~~ $(M^e)^d \ (\text{mod } N)$.

What *B* obtains is exactly *M*, thanks to the Fermat-Euler Theorem stating that, in this situation, $(M^e)^d \equiv M \ (\text{mod } N)$.

The main point is now: where does the security of the system lie? From what we have seen so far, in order to decode the message, it is necessary to know *d*. Knowing *e*, in order to calculate *d*, it is necessary to know $\varphi(N)$; but, knowing N, *calculating $\varphi(N)$ is computationally equivalent to factorising N.*

Therefore, all in all, the security of the *R.S.A.* method depends on the following facts:

- in order to encode the message, it is necessary to build large primes. This operation is computationally fast. It can be shown that the computational

complexity of suitable primality tests – used to establish if a number n is a prime – is of the form:

$$(\log n)^{c \log\log\log n},$$

that is, it is "quasi-polynomial" in log *n* (log *n* is essentially the number of digits of *n*)

- in order to *break* the system, it is necessary to be able to factorise large natural numbers obtained as product of two primes. Such operation is computationally "slow" and its computationally complexity is conjectured to be of the form:

$$e^{c\sqrt{\log n(\log\log n)^2}},$$

that is "sub-exponential" in log *n*.

It is exactly such a ~~marked~~ difference in the speed of execution of operations – to determine large primes on the one hand and to factorise large numbers on the other – that guarantees the security of the method, at least for a sufficiently long period of time.

For instance, at the current state of technology, a natural number of 140 digits in base 10 can be produced through multiplication of two random primes in a few seconds on a typical computer available on the market. Yet, ~~the factorisation operation of~~ such 140-digit natural number would require about a month when employing several supercomputers working in parallel! Increasing the number of digits further increases the security of the system: it is currently recommended that numbers of at least 220 digits in base 10 be utilised.

Bibliography

We recommend the classical works by Ingham [1] and Davenport [2] for a clear explanation of the fundamental results on the distribution of prime numbers. We also signal the excellent introduction to the elementary theory of numbers by Davenport [3] that includes a chapter on cryptography.

For further details on the history of the development of cryptography, we recommend the book by Kahn [4] while the works by Koblitz [5] [6] provide a thorough presentation of a more rigorous mathematical modelling of public key cryptography than the one presented in this chapter. For a good treatment of factorisation algorithms and primality tests, see the books by Koblitz [6], Cohen [7] and Riesel [9].

[1] Ingham A E (1932) *The Distribution of Prime Numbers*, Cambridge University Press, Cambridge

[2] Davenport H (1981) *Multiplicative Number Theory*, Springer-Verlag, Berlin Heidelberg New York

[3] Davenport H (1999) *The Higher Arithmetic: An Introduction to the Theory of Numbers,* Cambridge University Press

[4] Kahn D (1967) *The Codebreakers, the Story of Secret Writing*, Macmillan, London

[5] Koblitz N (1987) *A Course in Number Theory and Cryptography*, Springer-Verlag, Berlin Heidelberg New York

[6] Koblitz N (1998) *Algebraic Aspects of Cryptography*, Springer-Verlag, Berlin Heidelberg New York

[7] Cohen H (1994) *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin Heidelberg New York

[8] Riesel H (1994) *Prime Numbers and Computer Method for Factorization*, Birkhäuser, Basel