Cryptography

Dietrich Burde

Lecture Notes 2007

Contents

Introduction

Cryptography is about secure communication in the presence of an adversary. Party A wants to send secret messages to party B over a communication line which may be tapped by an adversary C. How can we ensure that C is not able to obtain the secret information ? The traditional solution to this problem is the so called *private key encryption*: before starting the remote transmissions, A and B agree on a pair of encryption and decryption algorithms, and an additional piece of information, a *secret key* S, which is used to encrypt, or to decrypt the information. The adversary may know the encryption and decryption algorithm which are being used, but does not know S. The idea is that the encryption is done by a so called *one-way function*, which is relatively easy to compute, but very hard to invert (without the secret key). Indeed, modern cryptography is based on the gap between efficient algorithms for encryption for the legitimate users versus the computational infeasibility of decryption for the adversary.

Let us start with an example, the so called *substitution cipher*. Here A and B agree on some secret permutation $f\colon \Sigma \to \Sigma$, where Σ is the alphabet of the message to be send. To encrypt the message $m = m_1 \cdots m_n$, where $m_i \in \Sigma$, A computes $f(m_1) \cdots f(m_n)$. To decrypt $r = r_1 \cdots r_n$, where $r_i \in \Sigma$, B computes $f^{-1}(r_1) \cdots f^{-1}(r_n) = m_1 \cdots m_n = m$. In this example the (common) secret key is the permutation f. The following special case goes back to Gaius Julius Caesar ($100 - 44$ a.D.). Take

$$\Sigma = \{A, B, \cdots, Z\} = \{0, 1, \cdots 25\} = \mathbb{Z}/26\mathbb{Z},$$

and let $f(x) = x + 3 \mod 26$. In this way, A is encrypted to D, B to E etc. Let us encrypt the message

HEUTE IST DIENSTAG

(today is tuesday). The result is

KHXWH LVW GLHQVWDJ

Clearly we have $f^{-1}(x) = x - 3 \equiv x + 23 \mod 26$. Note that the substitution cipher is easy to break by an adversary who sees a moderate number of ciphertexts. In our special case it is rather easy to break the code. We have only 26 possible keys, which we just can try out all. If the resulting text makes sense, we are done. We also can use statistics on how often a letter appears in an average german text. The most common letters in german language are (in %):

letter	E	N	I	S	R	A	T
%	17.40	9.78	7.55	7.27	7.00	6.51	6.15

The *affine cipher* is as follows: we have $\Sigma = \mathbb{Z}/m\mathbb{Z}$ and

$$f\colon \Sigma \to \Sigma,\ x \mapsto ax + b \mod m, \quad (a, m) = 1.$$

The inverse is found as follows. Choose an $a' \in \mathbb{Z}/m\mathbb{Z}$ such that $aa' \equiv 1 \mod m$. Then we have

$$f^{-1}\colon \Sigma \to \Sigma,\ y \mapsto a'(y-b) \mod m.$$

Indeed, $a'(ax+b-b) \equiv a'ax \equiv x \mod m$.
Consider for example $(a,b) = (7,3)$ and $m = 26$. We have $(a,m) = (7,26) = 1$ and f is given by

$$x \mapsto 7x + 3.$$

Let us encrypt IDIOT, that is $(8,3,8,14,19)$. We obtain $(7,24,7,23,6)$, that is HYHXG. Indeed $7 \cdot 8 + 3 \mod 26 = 7$ and so on. To decrypt it, we have to find an a' with

$$7a' \equiv 1 \mod 26$$

This can be done by the *extended Euclidean algorithm*, solving the Diophantine equation $26x + 7y = 1$ over $\mathbb{Z}$. Then $a' = y \mod 26$ is the required solution.

$$\begin{aligned} 26 &= 3 \cdot 7 + 5, \quad a_0 = 3 \\ 7 &= 1 \cdot 5, \quad a_1 = 1 \\ 5 &= 2 \cdot 2 + 1, \quad a_2 = 2. \end{aligned}$$

This gives on one hand the gcd of 26 and 7, i.e. $(26,7) = 1$. On the other hand we can compute a solution (x,y) from it. Let $p_0 = 0, q_0 = 1$ and let

$$\begin{aligned} p_{i+1} &= q_i, \quad i \geq 0 \\ q_{i+1} &= p_i - a_{2-i}q_i. \end{aligned}$$

In our case,

$$\begin{aligned} p_1 &= 1,\ q_1 = p_0 - a_2 q_0 = -2 \\ p_2 &= -2,\ q_2 = p_1 - a_1 q_1 = 3 \\ p_3 &= 3,\ q_3 = p_2 - a_0 q_2 = -11. \end{aligned}$$

Then $(x,y) = (p_3, q_3) = (3,-11)$ is a solution to $26x + 7y = 1$ over $\mathbb{Z}$. Indeed, $26 \cdot 3 - 7 \cdot 11 = 78 - 77 = 1$. Together we have

$$a' = -11 \mod 26 = 15,$$

and $x \mapsto 15(x-3) \mod 26$ yields the decryption.
How many possible keys do we have for $x \mapsto ax + b \mod m$? We have $m\varphi(m)$ possible choices for pairs (a,b) with $gcd(a,m) = 1$. Here

$$\varphi(m) = \#\{a \in \mathbb{Z}/m\mathbb{Z}, (a,m) = 1\}$$

is the so called *Euler φ-function*. For $m = 26$ we have $m\varphi(m) = 26 \cdot 12 = 312$. Indeed, $\varphi(26) = 12$, since the numbers in $\{0,1,\ldots 25\}$ coprime to 26 are given by

$$1,3,5,7,9,11,15,17,19,21,23,25.$$

In practice it would be easy to break the affine cipher. The Euclidean algorithm is quite fast. Indeed, to compute the gcd of two integers $k > l$ one needs less than $5\log_{10}(l)$ divisions with remainder. Also it may be easy to guess the pair (a,b). Suppose you know that E goes to R, i.e., $4 \mapsto 17$ and S goes to H, i.e., $18 \mapsto 7$. Hence we know

$$\begin{aligned} 4a + b &\equiv 17 \mod 26, \\ 18a + b &\equiv 7 \mod 26. \end{aligned}$$

Taking the difference just yields $14a \equiv -10 \mod 26$, or $7a \equiv 8 \mod 13$. Then it follows $a \equiv 14a \equiv -10 \equiv 3 \mod 13$, so that $a = 3$. But then $b = 5$ and we have found the function $x \mapsto ax + b \mod 26$.

In the seventies *public key cryptography* was developed. It enables one to drop the requirement that A and B must share a key in order to encrypt. The receiver B can publish authenticated information, called the *public key*, for anyone including the adversary. He keeps secret information (to himself alone), called the *private key* about the public key, which enables him to decrypt the cyphertexts he receives. Such an encryption method is called *public key encryption*. Secure public key encryption is possible given a *trapdoor function*, i.e., a one-way function for which there exists some trapdoor information known to the receiver alone, with which the receiver can invert the function.

How can we find "one-way functions", which are "easy" to compute, but "hard" to invert ? (For public key encryption, it must also have a trapdoor.) By "easy" we mean that the function can be computed by a probabilistic polynomial time algorithm (PPT algorithm), and by "hard" we mean, that any PPT algorithm attempting to invert it will succeed with very "small" probability. There are indeed candidates which seem to posses the above properties of a one-way function:

1. *Factoring* : The function $f : (x, y) \mapsto xy$ is conjectured to be a one-way function. The proven fastest factorizing algorithms (asymptotically) of an integer n to date have running time

$$O\left(e^{\sqrt{\log(n)\cdot\log(\log(n))}}\right),$$

for example, the quadratic sieve algorithm. This seems "hard" enough. However, if the quantum computer is ever build with a sufficient number of qubits, then Peter Shor has discovered an algorithm to factor integers in polynomial time on it.
Until then, consider the *Fermat-numbers* $F_n = 2^{2^n} + 1$, named after Pierre de Fermat, $1601 - 1665$. They should give an idea how difficult factorization is. The complete factorization of F_n into prime powers is only known for very small n, that is for $n \leq 11$.

n	F_n	factorization
0	3	3
1	5	5
2	17	17
3	257	257
4	65537	65537
5	4294967297	$641 \cdot 6700417$
6	18446744073709551617	$274177 \cdot 67280421310721$
7	F_7	$59649589127497217 \cdot 5704689200685129054721$

The first five Fermat numbers are prime. Until today one does not know any other Fermat number to be prime. F_{33}, which has 2.585.827.974 digits, is the first Fermat number, where it is not known, whether it is prime or not.

2. *The discrete log problem* : Let $p \in \mathbb{P}$ be a prime. It is known that the group of units in the

ring $\mathbb{Z}/p\mathbb{Z}$ is cyclic. For a generator g consider the function

$$f\colon (x,p,g) \mapsto (g^x \mod p, p, g).$$

This is conjectured to be a one-way function. Computing $f(x,p,g)$ can be done in polynomial time using repeated squaring. However, the fastest known proved solution for its inverse, called the *discrete log problem* is the index-calculus algorithm, with expected running time $L(p)^{\sqrt{2}}$, where

$$L(p) = e^{\sqrt{\log(p)\log(\log(p))}}.$$

The problem of efficiently finding a generator for a specific $(\mathbb{Z}/p\mathbb{Z})^*$ is an interesting open research problem. It is not known how to find generators in polynomial time. The conjecture of *Artin* of 1927 says that each positive integer g, which are not a square, is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ for infinitely many primes p. For example, $g = 2$ generates $(\mathbb{Z}/p\mathbb{Z})^*$ for

$$p = 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, \ldots, 1000003, \ldots$$

There is a very interesting result of Heath-Brown in 1985 stating that there are at most three squarefree integers $a > 1$ for which the Artin conjecture is false (but says nothing on integers a which are not squarefree).
Here is an example of an discrete log problem. Let $p = 1000003 \in \mathbb{P}$ and $G = (\mathbb{Z}/p\mathbb{Z})^*$. Then indeed $g = 2$ is a generator, i.e., $g^x = 2^x = y$ has a solution $x \in \mathbb{Z}$ for given $y \in G$. Note that $|G| = 2 \cdot 3 \cdot 166667$. Suppose that $y = 3$, i.e. $2^x = 3$ in G. The discrete log problem consists of finding a solution x. A possible answer is $x = 254227$. We have

$$2^{254277} \equiv 3 \mod p.$$

3. *RSA (Rivest, Shamir, Adleman)* : Let $N = pq$ be the product of two primes. It is believed that such an N is hard to factor (one recommends that $1/2 < |\log_2(p) - \log_2(q)| < 30$ for the size of p and q). The function

$$f(x) = x^e \mod N, \quad (e, \varphi(N)) = (e, (p-1)(q-1)) = 1$$

is believed to be a one-way trapdoor function. The trapdoor is the primes p, q, knowledge of which allows one to invert f efficiently (by finding a d such that $de \equiv 1 \mod \varphi(N)$). To date the best attack is to try to factor N, which seems computationally infeasible.

Instead of using the group $G = (\mathbb{Z}/p\mathbb{Z})^*$ for the discrete log problem, one can also use other finite groups, like the groups $E(\mathbb{F}_q)$ of an elliptic curve over a finite field (which are finite abelian groups). This is called *elliptic curve cryptography* (ECC). It was proposed by Victor Miller and Neal Koblitz in 1985. Elliptic curves are algebraic curves given by an equation

$$y^2 = x^3 + ax + b$$

for $(a,b) \in k \times k$ (if the characteristic of k is not 2 or 3) satisfying $4a^3 + 27b^2 \neq 0$. They appear in complex analysis, in algebraic geometry (as simplest examples of projective varieties admitting a group structure), and in number theory (e.g., in the proof of Fermat's last theorem). Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as, for instance, Lenstra's elliptic curve factorization. The use of elliptic curves in cryptography has the advantage that one needs smaller key sizes in comparison to RSA or other public key cryptosystems. This means that implementations of ECC require smaller chip size, less power consumption etc. Finally, elliptic curves are simply way cooler than $\mathbb{Z}/p\mathbb{Z}$.

CHAPTER 1

Mathematical basics

We set up some mathematical basics used in the the study of cryptography. This will include some notions from elementary number theory, algebra and analytic number theory, in particular about prime numbers.

1.1. Complexity

The amount of time required for the execution of an algorithm on a computer is measured in terms of *bit operations*, i.e., addition, substraction, or multiplication of two binary digits; the division of a two-bit integer by a one-bit integer; or the shifting of a binary digit by one position. The number of bit operations necessary to complete the performance of an algorithm is called the *complexity*. This does not take into account such things as memory access or time to execute an instruction, which usually can be neglected in comparison with a large number of bit operations.
The Big O notation of Landau is as follows:

DEFINITION 1.1.1. Let $A \subseteq \mathbb{R}$ and $f\colon A \to \mathbb{R}$, $g\colon A \to \mathbb{R}_+$ be two functions. Then we will write

$$f(x) = O(g(x)),$$

if there exists a constant $c > 0$ such that $|f(x)| \leq c \cdot g(x)$ for all sufficiently large $x \in A$.

Vinogradov introduced the notation $f(x) \ll g(x)$ instead of $f(x) = O(g(x))$. It is possible to extend this definition to complex functions, as long the image of g is contained in $\mathbb{R}_+$. For an algorithm, Big O is the order of magnitude of its complexity, an upper bound on the number of bit operations required for execution of the algorithm in the worst-case scenario.

EXAMPLE 1.1.2. *$f(x) = O(1)$ just means that f is bounded.*

For example, $\sin(x) = O(1)$. Another example is $e^{-x} = O(x^{-n})$ for each $n \in \mathbb{N}$. If f and g are positive real valued functions then $O(fg) = O(f)O(g)$.
Consider the algorithms for adding, substracting, multiplying and dividing two n-bit integers. One can show that addition and substraction take $O(n)$ bit operations, which is also the number of bit operations required to compare them $(<, =, >)$. On the other hand the multiplication of an n-bit integer with an m-bit integer requires $O(mn)$ bit operations.
Let $a = 2^{n-1}b_{n-1} + \cdots + 2^1 b_1 + 2^0 b_0$ be the binary representation of a positive integer a, meaning b_i are bits such that $b_{n-1} = 1$. The binary length of a, denoted by $\lambda(a)$ is n. Note that

$$\lambda(a) = n \Leftrightarrow 2^{n-1} \leq a < 2^n.$$

Hence we have $n = \lfloor \log_2(n) + 1 \rfloor$, or

$$n = O(\log_2(a)) = O\left(\frac{\log(a)}{\log(2)}\right) = O(\log(a)),$$

where $\log(a)$ denotes the natural logarithm with base e. If a number a has no more than n bits, then $a \leq 2^n$. If we wish to describe complexity in terms of a itself rather than of its bit size, then we can rephrase the above as follows:

LEMMA 1.1.3. *Addition, substraction or comparison of two integers less than a takes $O(\log(a))$ bit operations. The multiplication of two such integers takes $O(\log^2(a))$ bit operations, while division of a by b with $b \leq a$ takes $O(\log(a)\log(b))$ bit operations.*

A more difficult result is the following. Denote by (a, b) the gcd of two integers a and b.

PROPOSITION 1.1.4. *If a, b are positive integers with $a > b$, then the number of bit operations required to compute (a, b), using the Euclidean algorithm, is $O(\log^2(a))$.*

REMARK 1.1.5. Also in analytic number theory the big O notation is very common. For example, the harmonic series can be written as

$$\sum_{n \leq x} \frac{1}{n} = \log(x) + \gamma + O\left(\frac{1}{x}\right),$$

where $\gamma \approx 0.577215664$ is Euler's constant. If we only sum over prime numbers p we have, for $x \geq 2$,

$$\sum_{p \leq x} \frac{1}{p} = \log(\log(x)) + c + O\left(\frac{1}{\log(x)}\right),$$

where $c \approx 0.2614972128$. For $x \to \infty$ we see that the series diverges, so that there must be infinitely many primes.

DEFINITION 1.1.6. An algorithm is called *polynomial*, when its complexity is $O(n^c)$ for some positive constant $c \in \mathbb{R}_+$, where n is the bitlength of the input to the algorithm, and c ist independent of n.

In general, these are the desirable algorithms, since they are the fastest. All above algorithms are examples of polynomial time algorithms: addition, substraction, multiplication division, greatest common divisor. It came as a surprise when in 2002 Agrawal, Kayal and Saxena proved that there is a *polynomial* time algorithm to decide whether an integer $n > 1$ is prime or not.

DEFINITION 1.1.7. An algorithm is called *exponential*, when its complexity is $O(c^{f(n)})$ for some real constant c and f is a polynomial on the input $n \in \mathbb{N}$.

Consider the trial division algorithm for testing primality of an integer n. It uses $\sqrt{n}$ divisions to prove that n is prime, if indeed it is. If we take the maximum bitlenght $k = \log_2(n)$ as input, then

$$\sqrt{n} = 2^{\log_2(n)/2} = 2^{k/2},$$

which is exponential. Also, the naive algorithm to compute $n!$ is exponential in the number of bits of n. There is also a complexity in between polynomial and exponential.

DEFINITION 1.1.8. An algorithm is called *subexponential*, when its complexity is

$$O\left(e^{(c+o(1))\log^r(n)(\log(\log(n)))^{1-r}}\right)$$

where $0 < r < 1$ and c is a real constant, and $o(1)$ denotes a function $f(n)$ converging to 0 for $n \to \infty$.

Supexponential algorithms are still considered to be ineffective. As an example consider Dixon's algorithm which is a subexponential factoring algorithm. The expected number of operations to find a non-trivial factor of an integer n by Dixon's algorithm is bounded by

$$e^{(2+o(1))\sqrt{\log(n)\log(\log(n))}}.$$

1.2. Divisibility

We say that $n \mid m$ in $\mathbb{Z}$ if there is an integer $x \in \mathbb{Z}$ such that $m = xn$. For $a, b, c \in \mathbb{Z}$ we have

(1) $a \mid 0$.
(2) $a \mid b$ implies $ca \mid cb$.
(3) $a \mid b$ and $b \mid c$ imply $a \mid c$.
(4) $a \mid b$ and $b \mid a$ imply $b = \pm a$.

In particular, $d \mid 1$ implies $d = \pm 1$, so that the group of units in $\mathbb{Z}$ is $E(\mathbb{Z}) = \{\pm 1\}$.

PROPOSITION 1.2.1. *If $a \in \mathbb{Z}$ and $b \in \mathbb{N}$, then there exists unique integers $q, r \in \mathbb{Z}$ with $0 \leq r < b$ and $a = bq + r$. In fact, $q = \lfloor \frac{a}{b} \rfloor$ and $r = a - bq$.*

PROOF. For $\alpha \in \mathbb{R}$ let $\lfloor \alpha \rfloor = \max\{b \in \mathbb{Z} \mid b \leq \alpha\}$ be the floor of α. Fixing $a \in \mathbb{Z}, b \in \mathbb{N}$ we define $M = \{a - bq \mid q \in \mathbb{Z}\}$. This set must contain a least positive integer, say $r = a - bq$ for some $q \in \mathbb{Z}$. Hence the "next one" in M, which is $a - b(q+1)$, must be negative. Hence

$$r - b = a - bq - b < 0,$$

i.e., $r < b$. Then we have

$$0 \leq \frac{r}{b} = \frac{a}{b} - q < 1,$$

so that $a/b - 1 < q \leq a/b$, or $q = \lfloor a/b \rfloor$. □

Let $a, b \in \mathbb{Z}$, both different from zero. A *common divisor* of a and b is an integer d satisfying $d \mid a$ and $d \mid b$. Since there are only finitely many such d's, in fact $|d| \leq \min(|a|, |b|)$, there exists a *greatest common divisor*.

DEFINITION 1.2.2. For two integers a and b, different from zero there exists a greatest common divisor (gcd), denoted by (a, b), and there exists a least common multiple (lcd), denoted by $[a, b]$. Both (a, b) and $[a, b]$ are unique. Furthermore a and b are called *coprime* (or relatively prime) if $(a, b) = 1$.

PROPOSITION 1.2.3. *For $a, b \in \mathbb{Z}$ we have $a\mathbb{Z} + b\mathbb{Z} = (a, b)\mathbb{Z}$. In other words, the gcd of a and b, $d = (a, b)$ is the smallest positive integer which can be written as $d = xa + yb$ with integer coefficients.*

PROOF. Let $I = a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\}$. Denote by m the smallest positive integer in this set. Since d divides every integer in I we have $I \subseteq d\mathbb{Z}$, in particular $d \mid m$. We have $a - qm \in I$, since $a, qm \in I$, for all $q \in \mathbb{Z}$. Let $r = a - qm$ be the remainder resulting from the division of a by m. Then $r < m$. Then either $r = 0$, or r is smaller than m in $I \cap \mathbb{N}$, which is impossible. Hence $r = 0$ and $m \mid a$. In the same way, $m \mid b$, so that $m \leq d$. From above we have $d \mid m$, so that $d = m$. This yields $d\mathbb{Z} \subseteq I$, hence $I = d\mathbb{Z}$. □

COROLLARY 1.2.4. *Let $a, b, n \in \mathbb{Z}$. The Diophantine equation $ax + by = n$ has an integer solution if and only if $d = (a, b)$ is a divisor of n.*

PROOF. If $ax + by = n$ is solvable then $n \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, hence $n = m \cdot (a, b)$ for some $m \in \mathbb{Z}$. Conversely, if $n = md$ then $n \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. □

COROLLARY 1.2.5. *Let $d = (a, b)$. There exist $x, y \in \mathbb{Z}$ with $ax + by = d$. If $d = 1$ then $ax + by = 1$ always has an integer solution.*

PROOF. Since $d \in a\mathbb{Z} + b\mathbb{Z}$ there exist $x, y \in \mathbb{Z}$ with $d = ax + by$. The last claim follows from corollary 1.2.4 with $d = 1$. □

REMARK 1.2.6. For $a, b \in \mathbb{Z}$ and $d > 0$ the following two conditions are equivalent:

(1) $d = (a, b)$.

(2) We have $d \mid a$, $d \mid b$, and for all c with $c \mid a$, $c \mid b$ follows $c \mid d$.

LEMMA 1.2.7. *Let $a, b \in \mathbb{Z}$, not both zero, and $\ell \in \mathbb{N}$. Then we have*

$$(\ell a, \ell b) = \ell \cdot (a, b)$$
$$[a, b](a, b) = |ab|$$
$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1.$$

LEMMA 1.2.8. *If $(a, b) = 1$ and $a \mid bc$ then $a \mid c$.*

PROOF. Because of $(a, b) = 1$ there exist $x, y \in \mathbb{Z}$ such that $ax+by = 1$. Then $cax+cby = c$. But $a \mid cby$ and $a \mid cax$. Hence also $a \mid c$. □

COROLLARY 1.2.9. *If p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.*

PROOF. If $p \nmid a$ then $(p, a) = 1$, hence $p \mid b$ by the lemma. □

For $(a, b) > 1$ the statement of the lemma need not be true: $6 \mid 24 = 3 \cdot 8$, but $6 \nmid 3$ and $6 \nmid 8$.

Let us shortly describe the *extended Euclidean algorithm* (EEA).

Input: integers $a > b \geq 0$

Output: integers x, y with $(a, b) = ax + by$

while $b \neq 0$ do
$q := \lfloor a/b \rfloor$
$\begin{pmatrix} x & u \\ y & v \end{pmatrix} := \begin{pmatrix} x & u \\ y & v \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}$
od;
return (x, y), the so called Bezout coefficients.

Indeed, each iteration of the usual EA substitutes (a, b) by $(b, a \mod b)$; we have $(a, b) = (b, a \mod b)$ if $b \neq 0$. This can be formulated in terms of matrix multiplication:

$$(b, a \mod b) = (a, b) \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix},$$

where $q := \lfloor a/b \rfloor$. If the EA terminates after k iterations we obtain

$$\begin{aligned}(gcd(a, b), 0) &= (a, b) \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \\ &= (a, b) \begin{pmatrix} x & u \\ y & v \end{pmatrix} = \begin{pmatrix} ax + by & au + bv \end{pmatrix},\end{aligned}$$

so that $gcd(a, b) = ax + by$ and $au + bv = 0$.

EXAMPLE 1.2.10. *Let* $a = 19$ *and* $b = 17$. *Then* $d = (a, b) = 1$ *and* $1 = -8 \cdot 19 + 9 \cdot 17$.

Indeed, we have $(q_1, q_2, q_3) = (1, 8, 2)$ since

$$\begin{aligned} 19 &= 1 \cdot 17 + 2 \\ 17 &= 8 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Then we have

$$\begin{aligned} (gcd(19, 17), 0) &= (19, 17) \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -8 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \\ (1, 0) &= (19, 17) \begin{pmatrix} -8 & 17 \\ 9 & -19 \end{pmatrix}. \end{aligned}$$

1.3. Congruences

The concept of congruences goes back to C. F. Gauß.

DEFINITION 1.3.1. Let R be a commutative ring, I an ideal in R and $a, b \in R$. Then we say that a is *congruent* to b modulo I, if $b - a \in I$, denoted by

$$a \equiv b \mod I.$$

We will take $R = \mathbb{Z}$. Then I is of the form $m\mathbb{Z}$, so that $b - a \in m\mathbb{Z}$ means $m \mid b - a$. We also write then $a \equiv b \mod m$. Congruence defines an equivalence relation, i.e.,

$$\begin{aligned} &a \equiv a \mod m, \\ &a \equiv b \mod m \text{ implies } b \equiv a \mod m, \\ &a \equiv b \mod m \text{ and } b \equiv c \mod m \text{ implies } a \equiv c \mod m. \end{aligned}$$

Denote the equivalence class (or congruence class, or residue class) of $n \mod m$ by $\overline{n}$. There are exactly m different congruence classes $\mod m$. We denote these congruence classes by $\mathbb{Z}/m\mathbb{Z}$.

PROPOSITION 1.3.2. *The set $(\mathbb{Z}/m\mathbb{Z}, \cdot, +)$ together with the operations $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{ab}$ is a commutative ring.*

If m is not prime then $\mathbb{Z}/m\mathbb{Z}$ has zero divisors. If $m = p$ is prime, then $\mathbb{Z}/p\mathbb{Z}$ is a finite field. We can apply congruences as follows:

EXAMPLE 1.3.3. *The polynomial $f(x) = x^2 - 117x + 31$ in $\mathbb{Z}[x]$ has no integer zeros.*

In fact, if $n \equiv 0 \mod 2$ then $f(n) \equiv 1 \mod 2$, and if $n \equiv 1 \mod 2$ then also $f(n) \equiv 1 \mod 2$.

LEMMA 1.3.4. *If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $ac \equiv bd \mod m$, in particular $a^n \equiv b^n \mod m$ for all $n \in \mathbb{N}$. Let $m' = \frac{m}{(c,m)}$. Then $ac \equiv bc \mod m$ if and only if $a \equiv b \mod m'$.*

PROOF. If we write $a = b + mx$ and $c = d + my$ for some $x, y \in \mathbb{Z}$, then $ac = bd + bmy + dmx + m^2xy$. This is congruent bd modulo m. For the second claim, assume $m \mid (ac - bc)$. Let $c' = \frac{c}{(c,m)}$. Then $m' \mid (a - b)c'$, and hence $m' \mid (a - b)$, since c' and m' are relatively prime by lemma 1.2.7. This shows $a \equiv b \mod m'$. Conversely, $m \mid (c, m)(a-b)$ implies $m \mid (c(a-b))$. □

EXAMPLE 1.3.5. *Prove using congruences that $F_5 = 2^{2^5} + 1 \equiv 0 \mod 641$.*

DEFINITION 1.3.6. A congruence of the form $ax \equiv b \mod m$ for $a, b, m \in \mathbb{Z}$, $m \neq 0$ is called a *linear congruence*.

PROPOSITION 1.3.7. *Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$, $d = (a, m)$. The linear congruence $ax \equiv b \mod m$ is solvable in $\mathbb{Z}$ if and only if $d \mid b$. In that case there are exactly d incongruent solutions: if x_0 is a solution, then they are given by*

$$x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \ldots, x_0 + \frac{(d-1)m}{d}.$$

PROOF. If x_0 is a solution of $ax \equiv b \mod m$, then $ax_0 - b = my_0$ for some $y_0 \in \mathbb{Z}$, i.e., $b = ax_0 - my_0$. The RHS is divisible by d, hence $d \mid b$. Conversely assume that $d \mid b$. We

have $a\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$, since $(a, m) = d$. Hence there are $x_0', y_0' \in \mathbb{Z}$ such that $d = ax_0' - my_0'$. Multiplying by b/d yields

$$b = \frac{ab}{d}x_0' - \frac{mb}{d}y_0' = a\left(\frac{b}{d}x_0'\right) - m\left(\frac{b}{d}x_0'\right).$$

This shows that $x = bx_0'/d$ is an integer solution for $ax \equiv b \mod m$.
Now suppose that x_0 and x_1 are two integer solutions. This implies $a(x_1 - x_0) \equiv 0 \mod m$, i.e., $m \mid (a(x_1 - x_0)$ and

$$\frac{m}{d} \mid \frac{a}{d}(x_1 - x_0).$$

Because of $(\frac{m}{d}, \frac{a}{d}) = 1$ it follows $\frac{m}{d} \mid (x_1 - x_0)$, i.e., $x_1 = x_0 + k \cdot \frac{m}{d}$ for some $k \in \mathbb{Z}$. For $k = 1, \ldots, d-1$ we obtain d solutions, which are pairwise incongruent. □

The case $d = 1$ yields the following result.

Corollary 1.3.8. *For $(a, m) = 1$ the congruence $ax \equiv b \mod m$ has a unique solution.*

Example 1.3.9. *The linear congruence $6x \equiv 3 \mod 15$ has 3 solutions: $x = 3, 8, 13$. The congruence $6x \equiv 4 \mod 15$ has no solution.*

Let us now study the group of units of the ring $\mathbb{Z}/m\mathbb{Z}$, denoted by $E(\mathbb{Z}/m\mathbb{Z})$, or $(\mathbb{Z}/m\mathbb{Z})^*$. Its cardinality is given by $\varphi(m)$. Here φ is called Euler's φ-funktion. It is defined by

$$\varphi(n) = \sum_{\substack{1 \le k \le n \\ (k,n)=1}} 1.$$

By the Chinese remainder theorem we have, for $(m, n) = 1$,

$$E(\mathbb{Z}/n\mathbb{Z}) \times E(\mathbb{Z}/m\mathbb{Z}) \cong E(\mathbb{Z}/nm\mathbb{Z}).$$

It follows that $\varphi(mn) = \varphi(n)\varphi(m)$, i.e., φ is multiplicative.

Proposition 1.3.10. *We have*

$$\sum_{d \mid n} \varphi(d) = n.$$

Proof. Let $S = \{1, 2, \ldots, n\}$. We partition the numbers of S in disjoint sets as follows. For $d \mid n$ let

$$A(d) = \{k \in \mathbb{N} \mid 1 \le k \le n,\ (k, n) = d\}.$$

This set contains all $k \in S$ such that $(k, n) = d$. Define $f(d) = |A(d)|$. Then we have

$$\bigcup_{d \mid n} A(d) = S, \text{ also } \sum_{d \mid n} f(d) = n.$$

Now $(k, n) = d$ is equivalent to $(\frac{k}{d}, \frac{n}{d}) = 1$, where $0 < k \le n$ holds if and only if $0 < \frac{k}{d} \le \frac{n}{d}$. By setting $q = \frac{k}{d}$ we have a bijective correspondence between the elements of $A(d)$ and the elements of $\{q \in \mathbb{N} \mid 0 < q \le \frac{n}{d}, (q, \frac{n}{d}) = 1\}$. The number of such q's is just $\varphi(\frac{n}{d})$. Hence we have $f(d) = \varphi(\frac{n}{d})$, so that

$$\sum_{d \mid n} \varphi\Big(\frac{n}{d}\Big) = n.$$

This statement is equivalent to the claim of the proposition, since with d also $\frac{n}{d}$ runs through all positive divisors of n. □

PROPOSITION 1.3.11. *For a prime p and an integer $\alpha \geq 1$ we have $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ For $n \geq 2$ we have*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

PROOF. For $n \leq p^\alpha$ we have $(n, p^\alpha) = 1$ for all $n = 1, \ldots, p^\alpha$, except for $n = p, 2p, \ldots p^{\alpha-1}p = p^\alpha$. Hence the number is given by $p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right)$. Now let $n = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$. Since φ is multiplicative,

$$\begin{aligned}
\varphi(n) &= \prod_{p_i|n} \varphi(p_i^{\alpha_i}) \\
&= \prod_{p_i|n} p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) \\
&= n \prod_{p|n} \left(1 - \frac{1}{p}\right).
\end{aligned}$$

□

COROLLARY 1.3.12. *There are infinitely many primes.*

PROOF. Suppose there are only finitely many primes $p_1, \ldots, p_r$. Let $n = p_1 p_2 \cdots p_r$. The only integer in $\{1, 2, \ldots, n\}$ relatively prime to n is 1, since all other integers have a prime divisor, which can only be one of the p_i. Hence $\varphi(n) = 1$. But this is impossible, since $\varphi(n) = \varphi(2)\varphi(3)\cdots\varphi(p_r) > 1$. □

REMARK 1.3.13. For $x \to \infty$ we have the following result:

$$\sum_{n \leq x} \varphi(n) = \frac{3}{\pi^2} x^2 + O(x \log(x)).$$

The first 20 values of $\varphi(n)$ are given by

$$1, 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4, 12, 6, 8, 8, 16, 6, 18, 8.$$

Next we want to consider simultaneous linear congruences. Suppose that n coconuts are placed in a pile. If you divide the pile into three, then there are two coconuts left over. If you divide it into five, then three are left over. If you divide it into seven, then two are left over. How many coconuts are there at least ? The answer is given by solving simultaneous congruences:

EXAMPLE 1.3.14. *The system of linear congruences*

$$x \equiv 2 \mod 3, \quad x \equiv 3 \mod 5, \quad x \equiv 2 \mod 7$$

has a unique solution modulo $3 \cdot 5 \cdot 7 = 105$. It is $x = 23$.

What is behind this is the Chinese remainder theorem.

PROPOSITION 1.3.15. *Let $m_1, \ldots, m_k$ be pairwise coprime integers and $m = \prod_{i=1}^k m_i$. Let $b_1, \ldots, b_k \in \mathbb{Z}$. Then the system*

$$x \equiv b_1 \mod m_1, \ldots, x \equiv b_k \mod m_k$$

has a unique solution modulo m.

PROOF. Let $n_i := \frac{m}{m_i}$. Because of $(m_i, m_j) = 1$ for all $i \neq j$ we have $(m_i, n_i) = 1$. Hence there exist $r_i, s_i \in \mathbb{Z}$ such that $r_i m_i + s_i n_i = 1$. Define

$$x := \sum_{i=1}^{k} b_i s_i n_i.$$

Because of $s_i n_i \equiv 1 \mod m_i$ and $s_i n_i \equiv 0 \mod m_j$ for $i \neq j$ we obtain $x \equiv b_i(s_i n_i) \mod m_i$ and $x \equiv b_i \mod m_i$. In other words, x is a solution for our system of congruences. If y is another solution, then $x \equiv y \mod m_i$ for all i, hence also $x \equiv y \mod m$, since all m_i are pairwise relatively prime. □

In the above example we have $(m_1, m_2, m_3) = (3, 5, 7)$, $(b_1, b_2, b_3) = (2, 3, 2)$, $(n_1, n_2, n_3) = (35, 21, 15)$ and $m = 105$. Then there are r_i, s_i for $i = 1, 2, 3$ such that

$$\begin{aligned} 3r_1 + 35s_1 &= 1 \\ 5r_2 + 21s_2 &= 1 \\ 7r_3 + 15s_3 &= 1. \end{aligned}$$

For example, we can take $(r_1, r_2, r_3) = (12, -4, -2)$ and $(s_1, s_2, s_3) = (-1, 1, 1)$. Then

$$\begin{aligned} x &= b_1 s_1 n_1 + b_2 s_2 n_2 + b_3 s_3 n_3 \\ &= -2 \cdot 35 + 3 \cdot 21 + 2 \cdot 15 \\ &= 23. \end{aligned}$$

The following algorithm, the *repeated squaring method* will be valuable lateron.
Given $d, n \in \mathbb{N}$, $d > 1$, $x \in \mathbb{Z}$ and

$$d = \sum_{j=0}^{k} d_j 2^j, \quad d_j = 0, 1.$$

The goal is to find $x^d \mod n$. First, we initialize by setting $c_0 = x$ if $d_0 = 1$, and $c_0 = 1$ if $d_0 = 0$. Also, set $x_0 = x$, $j = 1$, and execute the following steps, starting with $j = 1$:

(1) Compute $x_j \equiv x_{j-1}^2 \mod n$.

(2) If $d_j = 1$, set $c_j = x_j c_{j-1} \mod n$.

(3) If $d_j = 0$, set $c_j \equiv c_{j-1} \mod n$.

(4) Reset j to $j + 1$. If $j = k + 1$, output $c_k \equiv x^d \mod n$, and terminate the algorithm. Otherwise, go to step (1).

1.4. Euler, Fermat and Wilson

The following elementary result is about nonlinear congruences.

PROPOSITION 1.4.1 (Euler). *Let $a, m \in \mathbb{Z}$ such that $(a, m) = 1$. Then*

$$a^{\varphi(m)} \equiv 1 \mod m.$$

PROOF. The order of the group $G = (\mathbb{Z}/m\mathbb{Z})^*$ is $\varphi(m)$. Let U be the cyclic subgroup of G generated by a. Let $\#U = k$. By Lagrange $k \mid \varphi(m)$, say $\varphi(m) = \ell k$ for some integer ℓ. Then

$$a^{\varphi(m)} = (a^k)^\ell = 1$$

in G. □

COROLLARY 1.4.2 (Fermat). *Let p be a prime and $a \in \mathbb{Z}$ such that $p \nmid a$. Then*

$$a^{p-1} \equiv 1 \mod p.$$

PROOF. Apply Euler's result with $m = p$ and $\varphi(p) = p - 1$. The assumtion $p \nmid a$ ensures that $(a, m) = (a, p) = 1$. □

We can also prove Fermat's result by induction on $a \in \mathbb{N}$. For $a = 1$ we have $a^1 = 1$ in $G = (\mathbb{Z}/p\mathbb{Z})^*$. Then assume $a^p = a$. Then we have

$$(a + 1)^p = a^p + 1 = a + 1.$$

Here we used that $(a + b)^p \equiv a^p + b^p \mod p$, since p divides all binomial coefficients $\binom{p}{j}$ for $j = 1, \ldots, p - 1$.

EXAMPLE 1.4.3. *Use Euler's theorem to show that the last 3 digits of 9^{9^9} are given by 289, i.e., that $9^{9^9} \equiv 289 \mod 1000$.*

Indeed, $9^{\varphi(1000)} \equiv 1 \mod 1000$. Since $\varphi(1000) = \varphi(2^3 \cdot 5^3) = \varphi(2^3)\varphi(5^3) = 400$ we know that

$$9^{400} \equiv 1 \mod 1000.$$

Furthermore it is easy to see that $9^9 \equiv 81 \mod 400$. It follows

$$\begin{aligned} 9^{9^9} &= 9^{81+400k} \\ &= 9^{81} \cdot 1 \\ &= (10 - 1)^{89} \equiv -\binom{89}{2} \cdot 10^2 + 89 \cdot 10 - 1 \\ &\equiv 400 - 110 - 1 = 289 \mod 1000. \end{aligned}$$

Note that $10^2 \cdot \binom{89}{2} = 391600 \equiv -400 \mod 1000$.

PROPOSITION 1.4.4 (Wilson). *If p is a prime, then*

$$(p - 1)! \equiv -1 \mod p.$$

PROOF. Consider the following polynomial in $\mathbb{F}_p[x]$:

$$f(x) = x^{p-1} - 1 - (x - 1)(x - 2) \cdots (x - p + 1)$$

By Fermat's theroem f has $(p-1)$ different zeros in $\mathbb{F}_p$. But $\deg(f) < p-1$, since the monomial x^{p-1} cancels out. Hence f is the zero polynomial. For $x = 0$ we obtain, using $(-1)^{p-1} = 1$,

$$0 \equiv f(0) \equiv -1 - 1 \cdot 2 \cdots (p - 1).$$

□

Also the converse of Wilson's theorem holds.

PROPOSITION 1.4.5. *If $n \in \mathbb{N}$ satisfies $(n-1)! \equiv -1 \mod n$, then n is a prime.*

PROOF. Suppose there is a prime $p < n$ such that $p \mid n$. Then $p \mid (n-1)!$, so that

$$0 \equiv (n-1)! \equiv -1 \mod p,$$

a contradiction. □

1.5. Prime numbers

A positive integer p is called a *prime number*, if $p > 1$ and the only positive divisors of p are 1 and p. Let us denote the set of primes by $\mathbb{P}$.

DEFINITION 1.5.1. Let R be a commutative ring with 1. An element $p \in R$ is called *prime*, if it is not a unit and $p \mid ab$ implies $p \mid a$ or $p \mid b$. It is called *irreducible*, if it is not a unit and there is no factorization $p = ab$ with $a, b \in R \setminus E(R)$.

Since $R = \mathbb{Z}$ is a principal ideal ring, the concepts of prime and irreducible are equivalent. Thus we recover the usual definition for p to be prime. Integers which are not prime are called *composed*. It holds the important *fundamental theorem of arithmetic* (FTA):

THEOREM 1.5.2 (FTA). *For each positive integer n there exist unique numbers $e(p) \in \mathbb{N}_0$, so that*

$$n = \prod_{p \in \mathbb{P}} p^{e(p)}$$

In particular only finitely many of the numbers $e(p)$ are non-zero.

Here we interpret $n = 1$ as the empty product. The existence of such a representation is proved by induction over n; the uniqueness uses the fact that $p \mid q_1 \cdots q_r \Rightarrow p \mid q_i$ for some i.

REMARK 1.5.3. The first rigorous proof of the FTA was given by Gauß only in 1801, in his *Disquisitiones arithmeticae*. The result says that $\mathbb{Z}$ is a factorial ring. It is well known that many rings which are considered in number theory are not factorial. The classical example is to consider the ring of integers $\mathcal{O}_d$ in a quadratic number field $\mathbb{Q}[\sqrt{d}]$ for squarefree $d \in \mathbb{Z}$. We have $\mathcal{O}_d = \mathbb{Z}[\alpha]$, with $\alpha = \sqrt{d}$ for $d \equiv 2, 3 \mod 4$ and $\alpha = \frac{1+\sqrt{d}}{2}$ for $d \equiv 1 \mod 4$. These rings are factorial if and only if they are principal ideal rings, i.e., have class number 1. There are examples of such rings without a unique decomposition into prime elements. Consider for example $R = \mathbb{Z}[\sqrt{-5}]$. Then the elements $2, 3, 1 \pm \sqrt{-5}$ are prime, but

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$

represents two different factorizations into primes of $n = 6$ in R. Indeed, this ring has class number 2, and not 1.

How many primes are there in $\mathbb{N}$? It is useful to introduce the prime counting function.

DEFINITION 1.5.4. Let x be a real number. Denote by $\pi(x)$ the number of primes p with $p \leq x$, i.e.,

$$\pi(x) = \sum_{p \leq x} 1.$$

PROPOSITION 1.5.5 (Euklid). *There are infinitely many primes in $\mathbb{Z}$, that is, $\pi(x) \to \infty$ für $x \to \infty$.*

PROOF. Assume there are only finitely many primes, say $p_1, p_2, \ldots, p_r$. Define

$$N := \prod_{i=1}^{r} p_i + 1.$$

Because of theorem 1.5.2 N has a unique factorization, hence there is a prime p_k of our list with $p_k \mid N$. But p_k also divides the product $p_1 \cdots p_r$, and hence the difference: $p_k \mid 1$. This is absurd. □

REMARK 1.5.6. Euclid's proof is wonderful, simple and short. There is an even shorter version using only four symbols:

$$N = n! + 1$$

In fact, N is not divisible by some d with $2 \leq d \leq n$. Hence N has only prime factors $p > n$, and one can always find a prime which is bigger than all primes in a given finite set of primes. There is also an elementary proof showing that the sum

$$\sum_{p \in \mathbb{P}} \frac{1}{p}$$

is divergent, which implies Euclid's result, of course.

Proof of Goldbach, 1730*:* let $F_n = 2^{2^n} + 1$ be the n-th Fermat number. Each two Fermat numbers are relatively prime: $(F_m, F_n) = 1$ for all $n \neq m$. This follows form the recursion

$$F_0 F_1 \cdots F_{n-1} = F_n - 2,$$

which is easily proved by induction. Suppose that $k \in \mathbb{N}$ with $k \mid F_n$ and $k \mid F_m$. Then the formula implies that $k \mid 2$, hence $k = 1$ or $k = 2$. Since all F_n are odd, we must have $k = 1$. It follows that the prime divisors of Fermat numbers are pairwise distinct. Hence one obtains always new primes as divisors of the infinitely many numbers F_n.

This proof also shows that $p_n \leq 2^{2^{n-1}}$ for the n-th prime. The idea can be varied. It suffices, to find any sequence (n_i) of pairwise coprime numbers with $2 \leq n_1 < n_2 < \ldots$.

A group theoretical proof: Suppose that there are only finitely many primes, p being the largest one. Then form the Mersenne number

$$N = 2^p - 1.$$

Let $q \mid N$ be a prime divisor, i.e., $2^p - 1 \equiv 0 \mod q$, or $2^p = 1$ in $\mathbb{F}_q$. The multiplicative group of $\mathbb{F}_q$ has $q - 1$ elements, and its subgroup $U = \langle 2 \rangle$ has p elements, since $2^p = 1$ and p prime. The theorem of Lagrange implies $p \mid (q - 1)$, which means $q > p$, in contradiction to our assumption that p is the largest prime.

DEFINITION 1.5.7. The numbers $M_n = 2^n - 1$ are called *Mersenne numbers.*

In the binary system we have $2^n - 1 = 1 \cdots 1$ with n digits. This is the largest number which can be represented with n digits. It is easy to see that M_n can only be prime if n is prime.

CONJECTURE 1.5.8. *There are infinitely many Mersenne primes M_p.*

The largest known primes are very often Mersenne primes. At the date of writing the largest known prime is

$$2^{32582657} - 1,$$

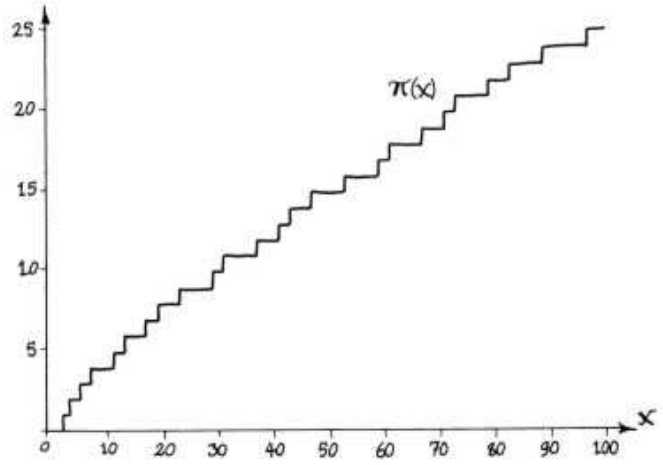
which has 9808358 digits. It was found in 2006 by Boone and Cooper.

It is very interesting to study the question how the primes are distributed. Locally the primes are distributed quite irregular. There is no obvious reason why some number is prime and

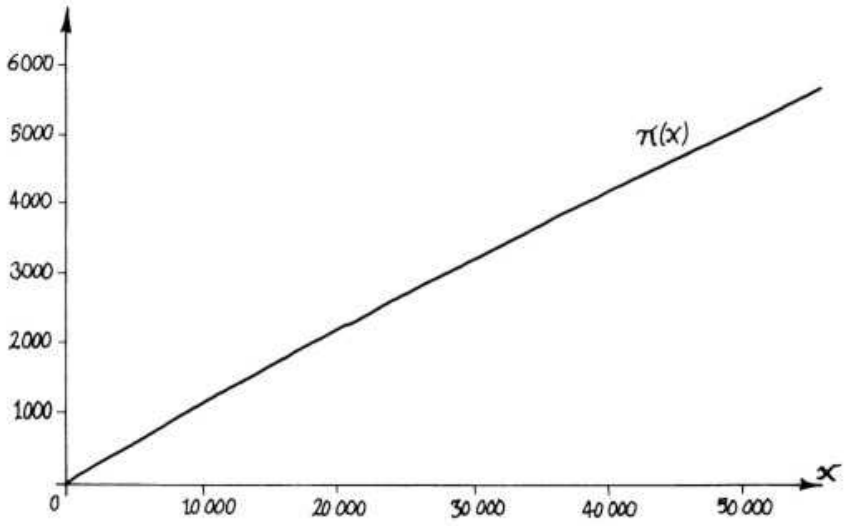
another one isn't. Why are the only prime numbers in the interval $[10000000, 10000100]$ exactly the two numbers

$$10000019,\ 10000079$$

The following graph demonstrates how irregular the values of the function $\pi(x)$ are in the interval $[1, 100]$:



Globally viewed however we obtain a quite different picture:



Don Zagier writes in his paper on the first 50 million prime numbers: "For me, the smoothness with which this curve climbs is one of the most astonishing facts in mathematics." Gauß studied as a 15-year old boy many tables of prime numbers. He already conjectured in 1792 that

$$\pi(x) \sim \int_2^x \frac{dt}{\log(t)}.$$

The integral there is called $\mathrm{li}(x)$, and we have

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log(t)} = \frac{x}{\log(x)} + O\left(\frac{x}{\log^2(x)}\right).$$

Legendre published the conjecture $\pi(x) \sim x/\log(x)$ in 1798. A proof was given only much later, in 1896 by Hadamard, and independently by de la Vallée Poussin:

THEOREM 1.5.9 (PNT). *For $x \to \infty$ we have*

$$\pi(x) \sim \frac{x}{\log(x)} \sim \mathrm{li}(x).$$

Note that $\mathrm{li}(x)$ is the much better approximation of $\pi(x)$. It is not difficult to show that *if* the limit

$$\lim_{x\to\infty} \pi(x)\frac{\log(x)}{x}$$

exists, then it has to be equal to 1. The difficulty is to prove that the limit exists at all. There is no easy proof for this to date. The shortest proofs all rely on the analytical properties of the Riemann Zeta-function

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

using complex analysis. The idea came from Riemann in 1859. For a reasonable short proof of the PNT see [**10**]. There are also so called *elementary* proofs (Erdös, Selberg), avoiding complex analysis. However, they do not seem to be simpler. The following table gives an impression about the number of primes. The numbers for $\mathrm{li}(x)$ are in fact the numbers for $[\mathrm{li}(x)]$. As an example, for $x = 10^{10}$ we have $\pi(x) = 455052511$ and

$$[\mathrm{li}(x)] = 455055614, \quad \left[\frac{x}{\log(x)}\right] = 434294482.$$

x	$\pi(x)$	$\mathrm{li}(x)$
10^1	4	5
10^2	25	29
10^3	168	177
10^4	1229	1245
10^5	9592	9629
10^6	78498	78627
10^7	664579	664917
10^8	5761455	5762208
10^9	50847534	50849234
10^{10}	455052511	455055614
10^{11}	4118054813	4118066400
10^{12}	37607912018	37607950280

The table gives reason to conjecture that $\mathrm{li}(x) - \pi(x) > 0$. It is perhaps a surprise that this is quite wrong.

THEOREM 1.5.10 (Littlewood, 1914). *There are infinitely many values for x such that $\pi(x) > \mathrm{li}(x)$.*

What is the smallest value x_1 such that $\pi(x_1) > \mathrm{li}(x_1)$? Here only some huge estimates are known. The one of Bays and Hudson (1999) says

$$x_1 < 1.3982 \cdot 10^{316}.$$

And indeed, Bays and Hudson make it plausible, that the order of magnitude for x_1 should be like this.
Riemann even found an exact formula for $\pi(x)$ (but depending on the knowledge of the zeros of $\zeta(s)$). He considered

$$R(x) = 1 + \sum_{n=1}^{\infty} \frac{1}{n\zeta(n+1)} \frac{\log^n(x)}{n!}.$$

The series converges quite rapidly and Riemann found the formula

$$\pi(x) = R(x) - \sum_{\rho \in \mathcal{N}} R(x^\rho),$$

where the sum runs over the zeros of $\zeta(s)$. Since the sum over the zeros does not converge absolutely, one has to sum up in the right order, that is, according to the increasing absolute value of $\mathrm{Im}(\rho)$. This formula was proven by Mangoldt in 1895. $\zeta(s)$ has so called trivial zeros at $\rho = -2, -4, -6, \ldots$. The other ones are a mystery up to date. Perhaps the most important conjecture in number theory is the Riemann Hypothesis (RH):

CONJECTURE 1.5.11 (Riemann). *All zeros of the zeta-function $\zeta(s)$ in the strip $0 < \mathrm{Re}(s) < 1$ lie on the critical line $\mathrm{Re}(s) = \frac{1}{2}$.*

The first zeros are

$$\begin{aligned}
\rho_1 &= \frac{1}{2} + 14.134725i \\
\rho_2 &= \frac{1}{2} + 21.022040i \\
\rho_3 &= \frac{1}{2} + 25.010856i \\
\rho_4 &= \frac{1}{2} + 30.424878i \\
\rho_5 &= \frac{1}{2} + 32.9345057i.
\end{aligned}$$

With ρ also $\overline{\rho}$ appears. RH is equivalent to the statement that for each $\varepsilon > 0$ there is a constant $C_\varepsilon > 0$ such that

$$|\pi(x) - \mathrm{li}(x)| \leq C_\varepsilon x^{\frac{1}{2}+\varepsilon}.$$

Lagarias showed in 2001 that the RH is equivalent to the following "elementary" statement:

CONJECTURE 1.5.12. *Let* $h_n = \sum_{j=1}^{n} \frac{1}{j}$. *Then for each* $n \geq 1$,

$$\sum_{d|n} d \leq h_n + \exp(h_n)\log(h_n),$$

with equality only for $n = 1$.

This relies on Robin's criterion saying that RH is true if and only if

$$\sigma(n) < e^{\gamma} \cdot n \log(\log(n)), \quad \forall\, n \geq 5041,$$

where $\sigma(n)$ is the sum of the positive divisors of n.

Many mathematicians, and many other people have tried to find formulas which produce primes. It would be nice, if there were a polynomial $f \in \mathbb{Z}[x]$ producing all prime numbers among its values. However, already Goldbach pointed out that this is impossible. We will show the following easier statement.

PROPOSITION 1.5.13. *Let* a *be a positive integer. Suppose* $f \in \mathbb{Z}[x]$ *is a polynomial such that* $f(n) \in \mathbb{P}$ *for all* $n \geq a$. *Then* f *is constant.*

PROOF. Let $f(a) = p \in \mathbb{P}$. Then, for all integers $k \geq 0$ we have

$$f(a + kp) \equiv 0 \mod p$$

To see this, one can use the Taylor formula

$$f(x + y) = \sum_{k \geq 0} \frac{1}{k!} f^{(k)}(x) y^k$$

with $x = a$ and $y = kp$. Then the claim is obvious since $1/k! f^{(k)} \in \mathbb{Z}[x]$. Hence the prime p divides all other primes $f(a + kp)$, that is $f(a + kp) = p$ for all $k \geq 0$. Since $\deg(f) + 1$ values determine a polynomial f, the claim follows. □

Euler found a polynomial which produces primes for the first 40 successive numbers $n = 0, \ldots, 39$:

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

Indeed, $(f(0), \ldots, f(39)) = (41, 43, 47, 53, 61, \ldots, 1601)$ are all prime. There is a remarkable result of Rabinovitsch, Baker and Stark behind it.

THEOREM 1.5.14. *For a prime* p *are equivalent:*

(1) $x^2 + x + p$ *has only prime number values at* $x = 0, 1, 2, \ldots, p-2$, *which are all different.*
(2) $4p - 1$ *is squarefree and the ring of integers in* $\mathbb{Q}(\sqrt{1 - 4p})$ *is factorial.*
(3) $p = 2, 3, 5, 11, 17, 41$.

If we consider cubic polynomials we find less successive prime values. A good choice is

$$f(x) = x^3 - 16x^2 + 151x - 23$$

which has different prime values $f(1), \ldots, f(20)$. Balog proved that there exist infinitely many polynomials of degree n having prime values at $2n + 1$ consecutive integers.
There are polynomials in several variables whose positive values as the variables range over all positive integers are exactly the primes. The first such polynomial was discovered in 1976, see [**4**]:

PROPOSITION 1.5.15. *The set of all prime numbers is equal to the set of all positive values of the following polynomial in 26 variables $a, b, c, \ldots, z$ of degree 25:*

$$\begin{aligned}(k+2)(1 &- [wz+h+j-q]^2 \\ &- [(gk+2g+k+1)(h+j)+h-z]^2 \\ &- [2n+p+q+z-e]^2 \\ &- [16(k+1)^3(k+2)(n+1)^2+1-f^2]^2] \\ &- [e^3(e+2)(a+1)^2+1-o^2]^2 \\ &- [(a^2-1)y^2+1-x^2]^2 \\ &- [16r^2y^4(a^2-1)+1-u^2]^2 \\ &- [([a+u^2(u^2-a)]^2-1)(n+4dy)^2+1-(x+cu)^2]^2 \\ &- [n+l+v-y]^2-[(a^2-1)l^2+1-m^2]^2 \\ &- [ai+k+1-l-i]^2 \\ &- [p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2 \\ &- [q+y(a-p-1)+s(2ap+2a+p^2-2p-2)-x]^2 \\ &- [z+pl(a-p)+t(2ap-p^2-1)-pm]^2).\end{aligned}$$

Note that if $k+2$ is not a prime, then the second factor is 0 or negative, and if $k+2$ is prime, then the second factor is equal to 1. It is known that there is such a polynomial in only 10 variables (but with a very high degree).

REMARK 1.5.16. There are many fascinating open questions on primes. A few more examples are: the twin prime conjecture, the Goldbach conjecture, is there always a prime between two squares, are there infinitely many primes of the form n^2+1, or infinitely many Sophie Germain primes, i.e., where p and $2p+1$ are prime ?

1.6. Primitive roots

In order to study alogithms related to cryptography we need to acquaint ourselves with primitive roots.

DEFINITION 1.6.1. Let G be a group and $g \in G$. The *order* of g in G is the smallest positive integer e such that $g^e = 1$. If it exists, we denote it by $\mathrm{ord}(g)$.

We set $\mathrm{ord}(g) = \infty$ if there is no smallest e such that $g^e = 1$. For example, consider $g = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ in $G = SL_2(\mathbb{Z})$. If $G = E(\mathbb{Z}/n\mathbb{Z})$ and $\overline{a} \in G$, i.e., $(a, n) = 1$, then we write $\mathrm{ord}_n(a)$ for $\mathrm{ord}(\overline{a})$. This is the smallest positive integer e such that $a^e \equiv 1 \mod n$. It is sometimes called the *modular order* of an integer.

DEFINITION 1.6.2. Let $n \in \mathbb{N}$. An integer $a \in \mathbb{Z}$ is called *primite root* modulo n, if $\mathrm{ord}_n(a) = \varphi(n)$.

LEMMA 1.6.3. *There exists a primitive root modulo n if and only if the group $E(\mathbb{Z}/n\mathbb{Z})$ is cyclic.*

PROOF. If the group $E(\mathbb{Z}/n\mathbb{Z})$ is cyclic with generator $\overline{a}$, then $\mathrm{ord}_n(a) = \varphi(n) = |E(\mathbb{Z}/n\mathbb{Z})|$. Hence a is a primite root modulo n. Conversely, if a is a a primite root modulo n, then $a, a^2, \ldots, a^{\varphi(n)}$ are pairwise incongruent, and all coprime to n, so that $E(\mathbb{Z}/n\mathbb{Z}) = \{a, a^2, \ldots, a^{\varphi(n)} = 1\}$ is cyclic with generator a. □

EXAMPLE 1.6.4. *There is no primitive root modulo* 15.

Indeed, we have $E(\mathbb{Z}/n\mathbb{Z}) = \{\pm 1, \pm 2, \pm 4, \pm 7\}$. Here $g = 1$ has order 1, $-1, \pm 4$ have order 2, and $\pm 2, \pm 7$ have order 4. Hence there is no element of order $\varphi(15) = 8$.

We recall the following lemmas.

LEMMA 1.6.5. *Let G be a group, $g \in G$ and $e \in \mathbb{N}$. Then $g^e = 1$ if and only if* $\mathrm{ord}(g) \mid e$.

PROOF. Let $\mathrm{ord}(g) = n$ and $e = kn$. Then $g^e = (g^n)^k = 1$. Conversely, let $g^e = 1$. Then $e = qn + r$ with $0 \leq r < n$, hence

$$g^r = g^{e-qn} = g^e (g^n)^{-q} = 1.$$

Since $n = \mathrm{ord}(g)$ is the smallest such integer we must have $r = 0$. This means $e = qn$ and $n \mid e$. □

LEMMA 1.6.6. *Let $a \in \mathbb{Z}$, $n \in \mathbb{N}$ with $(a, n) = 1$ and $k = \mathrm{ord}_n(a)$. Then*

$$\mathrm{ord}(a^\ell) = \frac{k}{(k, \ell)}, \quad \ell = 1, 2, 3, \ldots.$$

In particular, $\mathrm{ord}_n(a^\ell) = k$ *if and only if* $(k, \ell) = 1$.

PROOF. Let $k_\ell = \mathrm{ord}_n(a^\ell)$, i.e., $a^{\ell k_\ell} \equiv 1 \mod n$. Because of lemma 1.6.5 this implies $k = \mathrm{ord}_n(a) \mid \ell k_\ell$, hence $\frac{k}{(k,\ell)} \mid k_\ell$. On the other hand we have $a^k \equiv 1 \mod n$, that is

$$(a^\ell)^{\frac{k}{(k,\ell)}} \equiv 1 \mod n.$$

Again by lemma 1.6.5 we have

$$k_\ell = \mathrm{ord}(a^\ell) \mid \frac{k}{(k, \ell)}.$$

Together this implies $k_\ell = \frac{k}{(k,\ell)}$. □

COROLLARY 1.6.7. *If $n \in \mathbb{N}$ has a primitive root, there are $\varphi(\varphi(n))$ incongruent primitive roots modulo n.*

PROOF. Let a be a primitive root modulo n, hence $\mathrm{ord}_n(a) = \varphi(n)$. By the above lemma exactly those a^ℓ are primite roots again (e.g., $k = \varphi(n)$), for which we have $(\ell, \varphi(n)) = 1$. There are exactly $\varphi(k) = \varphi(\varphi(n))$ such ℓ in $\{1, \ldots, n\}$. □

PROPOSITION 1.6.8. *Let p be a prime. The group $E(\mathbb{Z}/p\mathbb{Z})$ is cyclic. Hence there are always exactly $\varphi(\varphi(p)) = \varphi(p-1) \geq 1$ incongruent primitive roots modulo p.*

PROOF. The group $E(\mathbb{Z}/p\mathbb{Z})$ is the multiplicative group of the finite field $\mathbb{Z}/p\mathbb{Z}$. For this reason it is cyclic. By the above corollary there exist $\varphi(\varphi(p))$ incongruent primitive roots modulo p. □

REMARK 1.6.9. Every finite subgroup of the multiplicative group of any field is cyclic.

The following table shows the primitive roots modulo p for $p = 2, \ldots, 43$:

p	$\varphi(p-1)$	primitive roots modulo p
2	1	1
3	1	2
5	2	2, 3
7	2	3, 5
11	4	2, 6, 7, 8
13	4	2, 6, 7, 11
17	8	3, 5, 6, 7, 10, 11, 12, 14
19	6	2, 3, 10, 13, 14, 15
23	10	5, 7, 10, 11, 14, 15, 17, 19, 20, 21
29	12	2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27
31	8	3, 11, 12, 13, 17, 21, 22, 24
37	12	2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35
41	16	6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35
43	12	3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34

The table shows in particular, that $a = 2$ is a primitive root modulo
$3, 5, 11, 13, 19, 29, 37$. This may suggest the following question. Is $a = 2$ a primitive root for infinitely many primes ? This is unknown, but a positive answer is conjectured. In fact, there is a more general famous conjecture as follows.

CONJECTURE 1.6.10 (Artin). *Every nonsquare integer $a \neq -1$ is a primitive root modulo p for infinitely many primes p.*

More precisely, denote by $N(x, a)$ the number of primes $p \leq x$, such that a is a primitive root modulo p. Artin's conjecture says that $\lim_{x\to\infty} N(x, a) = \infty$ for nonsquare $a \neq -1$. It is conjectured, that

$$N(x, a) \sim C_a \cdot \pi(x), \quad x \to \infty,$$

where $C_a > 0$ is a constant depending on a. For $a = 2$ it is conjectured that $N(x, 2) \sim C_2 \cdot \pi(x)$, where

$$C_2 = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p(p-1)}\right) \sim 0.3739558136192\cdots$$

is the so called *Artin constant*. Hooley proved that the GRH (generalized Riemann Hypothesis) implies Artin's conjecture. Heath-Brown proved in 1985 that there exist at most three squarefree integers $a > 1$, for which the Artin conjecture is not true. This does not say anything on integers a which are not squarefree.

REMARK 1.6.11. Denote by $g(p)$ the smallest positive primitive root modulo p. For example, $g(3) = 2$, $g(7) = 3$, $g(23) = 5, \ldots, g(107227) = 20$. How fast is the function g growing ? Burgess proved, that

$$g(p) = O\left(p^{\frac{1}{4}+\varepsilon}\right).$$

It is conjectured that g grows more slowly than $p^{\frac{1}{4}}$.

Finally we mention that it is known which groups $E(\mathbb{Z}/n\mathbb{Z})$ are cyclic.

THEOREM 1.6.12 (Gauß). *There exist primitive roots modulo n if and only if $n = 2, 4, p^\ell, 2p^\ell$, where $p \geq 3$ is a prime and $\ell \in \mathbb{N}$.*

1.7. Legendre, Jacobi and quadratic reciprocity

We start with the definition of a quadratic (non)residue.

DEFINITION 1.7.1. Let $p \in \mathbb{P}$ and $n \in \mathbb{N}$ such that $(p, n) = 1$. If the quadratic congruence $x^2 \equiv n \mod p$ has a solution then n is called a *quadratic residue modulo* p. Otherwise n is called a quadratic nonresidue modulo p.

EXAMPLE 1.7.2. *For $p = 11$ the quadratic residues are $\{1, 3, 4, 5, 9\}$, and the quadratic non-residues are $\{2, 6, 7, 8, 10\}$.*

Indeed, if $\{0, 1, \ldots, 10\}$ is a reduced residue system modulo 11, then we can compute the squares modulo 11. For example, $1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 5$ etc. Because of $(n, 11) = 1$, we must omit $n = 0$. It is no coincidence that there are as many quadratic residues as nonresidues.

PROPOSITION 1.7.3. *Let $p > 2$ be a prime. Then any reduced residue system modulo p contains exactly $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues.*

PROOF. Let $S = \{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\}$. These integers are pairwise incongruent modulo p: if $x^2 \equiv y^2 \pmod p$ with $1 \leq x, y \leq (p-1)/2$, then $(x-y)(x+y) \equiv 0 \pmod p$. Since $1 < x + y < p$, it follows $x - y \equiv 0 \pmod p$, so that $x = y$. Any quadratic residue modulo p is congruent to exactly one integer in S because of $(p-k)^2 \equiv k^2 \pmod p$. The set S has $\frac{p-1}{2}$ elements. □

DEFINITION 1.7.4. Let $p > 2$ be prime and $n \in \mathbb{Z}$. The *Legendre symbol* is defined as

$$\left(\frac{n}{p}\right) = \begin{cases} +1 & \text{if } n \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } n \text{ is a quadratic nonresidue modulo } p, \\ 0 & \text{if } n \equiv 0 \bmod p. \end{cases}$$

THEOREM 1.7.5 (Euler). *Let $p > 2$ be a prime. Then we have for all $n \in \mathbb{N}$*

$$\left(\frac{n}{p}\right) \equiv n^{(p-1)/2} \pmod p.$$

COROLLARY 1.7.6. *The Legendre symbol $\chi(n) = (n \mid p)$ is a strongly multiplicative function.*

PROOF. For $p \mid m$ or $p \mid n$ we have $p \mid nm$, so that both sides are equal to zero. For $p \nmid n, p \nmid m$ we have

$$\left(\frac{nm}{p}\right) \equiv (nm)^{(p-1)/2} = n^{(p-1)/2} m^{(p-1)/2} \equiv \left(\frac{n}{p}\right)\left(\frac{m}{p}\right) \pmod p.$$

The values of the LHS and the RHS can only be 1 or -1. Hence the difference

$$\left(\frac{nm}{p}\right) - \left(\frac{n}{p}\right)\left(\frac{m}{p}\right)$$

equals 0,2 or -2. Since it is divisible by $p > 2$, it is equal to zero. □

Gauß has proved in 1796 the following famous quadratic reciprocity law.

THEOREM 1.7.7. *If $p \neq q$ are odd primes, then*

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2},$$

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8},$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

It follows that $(-1 \mid p) = 1$, if $p \equiv 1(4)$, and $(2 \mid p) = 1$, if $p \equiv \pm 1(8)$. The third part says that we have $(p \mid q) = (q \mid p)$, except if $p \equiv q \equiv 3(4)$, in which case we have $(p \mid q) = -(q \mid p)$. This enables one to determine recursively whether or not p is a quadratic residue modulo q.

EXAMPLE 1.7.8. *$p = 1997$ is a quadratic nonresidue modulo $q = 1999$.*

Note that 1997 and 1999 are twin primes. Hence they cannot be simultaneously congruent 3 modulo 4. It follows that $(1997 \mid 1999) = (1999 \mid 1997) = (2 \mid 1997)$. In fact, if $p, p+2$ are twin primes, then always

$$\left(\frac{p}{p+2}\right) = \left(\frac{p+2}{p}\right) = \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

In our case $(2 \mid 1997) = -1$, since $1997 \equiv -3 \pmod 8$.

DEFINITION 1.7.9. Let $n \geq 3$ be an odd integer with $n = p_1^{e_1} \cdots p_\ell^{e_\ell}$ and $a \in \mathbb{Z}$. The *Jacobi symbol* of a w.r.t. n is given by

$$\left(\frac{a}{n}\right) = \prod_{j=1}^{\ell} \left(\frac{a}{p_j}\right)^{e_j},$$

where the symbols on the RHS are Legendre symbols.

The Jacobi symbol generalizes the Legendre symbol. But it is no longer true that $(a \mid n) = 1$ if and only if a is a quadratic residue modulo n, i.e., $x^2 \equiv a \mod n$ is solvable. We have only one direction. If a is a quadratic residue modulo n with $n \nmid a$ then $(a \mid n) = 1$.

EXAMPLE 1.7.10. *For $n = 15$ we have*

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1,$$

but 2 is not a quadratic residue modulo 15.

This follows from the following properties.

PROPOSITION 1.7.11. *Let $m, n \in \mathbb{Z}$, with n odd, and $a, b \in \mathbb{Z}$. Then*

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right),$$

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right), \quad \textit{if } a \equiv b \mod n$$

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{m}\right), \quad \textit{if } m \equiv 1 \mod 2.$$

Also, the quadratic reciprocity law is true, i.e., if a, n are odd and $(a, n) = 1$, then

$$\left(\frac{a}{n}\right)\left(\frac{n}{a}\right) = (-1)^{\frac{a-1}{2}\frac{n-1}{2}}.$$

CHAPTER 2

Public key cryptography

The security of cryptosystems is based on one-way functions, such as factoring (for RSA) and the discrete logarithm problem (for ElGamal). Let us explain in more detail, what the discrete log problem is.

Consider the following equation in a finite group G, for $a, g \in G$ and $x \in \mathbb{Z}$:

$$g^x = a.$$

Such an equation may have no solution, as the example

$$2^x = 3$$

in $(\mathbb{Z}/7\mathbb{Z})^*$ shows. However, if G is cyclic, and g is a generator, then there must be a solution.

DEFINITION 2.0.12. Let G be a finite cyclic group of order n. Let g be a generator of G. Then for each $a \in G$ there is an integer exponent $0 \leq x \leq n-1$ such that $g^x = a$. This exponent is called the *discrete logarithm* of a with basis g.

Note that x is only unique modulo n. The *discrete log problem* (DLP) consists in computing x, given G, g, a. For suitable groups G, like $(\mathbb{Z}/n\mathbb{Z})^*$ this is considered to be a hard problem.

EXAMPLE 2.0.13. *Let $G = (\mathbb{Z}/p\mathbb{Z}, +)$ be the additive group of $\mathbb{Z}/p\mathbb{Z}$ with the prime $p = 1000003$. Solve $2^x = 3$ in G, i.e., $2x \equiv 3 \mod p$.*

Since $(2, p) = 1$ there exist $r, s \in \mathbb{Z}$ such that $2r + ps = 1$. We can find r, s quickly by the EA. Indeed $r = -500001$ and $s = 1$. Then $x = 3r, y = 3s$ gives $2x + py = 3$, i.e., $2x \equiv 3 \mod p$ with $x = -3 \cdot 500001 \equiv 500003$.

REMARK 2.0.14. We see that for the additive group of $\mathbb{Z}/n\mathbb{Z}$ the discrete log problem is easy to solve. A much better choice are the multiplicative groups $(\mathbb{Z}/n\mathbb{Z})^*$, which are cyclic if and only if $n = 2, 4, p^\ell$ or $2p^\ell$, where $p > 2$ is a prime and $\ell \geq 1$.

2.1. RSA

RSA stands for the names Ron Rivest, Idi Shamir and Len Adleman. They published their work in 1978, see [**6**].
Suppose A wants to send a secret message to B. Then the RSA key generation goes as follows:

1. B generates two large, random primes $p \neq q$ of roughly the same size and computes both $n = pq$ and $\varphi(n) = (p-1)(q-1)$. The integer n is called his RSA modulus.

2. B selects a random integer e such that $1 < e < \varphi(n)$ and $(e, \varphi(n)) = 1$. Then using the extended Euclidean algorithm B computes the unique integer d with $1 < d < \varphi(n)$ such that

$$de + k\varphi(n) = 1, \quad \text{i.e. , } ed \equiv 1 \mod \varphi(n).$$

3. B publishes the *public key* (n, e) in some public database and keeps d and $p, q, \varphi(n)$ private. The *private* key is d.

Now we assume that the plaintext message is numerical of the form $m < n$. The enciphering goes as follows:

1. A obtains B's public key (n, e) from the database.

A enciphers $m < n$ by applying

$$E_e \colon m \mapsto m^e \mod n.$$

A uses the repeated squaring method for this computation.

The deciphering goes as follows:

1. Once B receives $c = E_e(m)$, he uses d to compute m via

$$D_d \colon c \mapsto c^d \mod n.$$

To see that B really recovers m we observe the following.

LEMMA 2.1.1. *We have* $D_d(E_e(m)) = m$.

PROOF. Since $de = 1 + \ell\varphi(n)$ for some $\ell \in \mathbb{Z}$ and $m^{\varphi(n)} \equiv 1 \mod n$ for $(m, n) = 1$ by Euler's theorem we have

$$\begin{aligned}(m^e)^d = m^{de} &= m^{1+\ell\varphi(n)} \\ &= m(m^{\varphi(n)})^\ell \\ &\equiv m \cdot 1^\ell = m \mod n.\end{aligned}$$

For $(m, n) > 1$ and $n = pq$ we may assume that $p \mid m$, hence $p \mid m^e$. It follows $(m^e)^d \equiv 0 \equiv m \mod p$ and hence $(m^e)^d \equiv m \mod n$. □

Here is an unrealistic, but very easy example.

EXAMPLE 2.1.2. *We want to encrypt and decrypt the message* HI*, which is* 78 *if we identify* $A, B, \ldots, Z$ *with* $0, 1, \ldots, 25$.

1. B chooses $(p, q) = (47, 79)$ and computes $n = 3713$ and $\varphi(n) = 46 \cdot 78 = 3588$.

2. B selects randomly $e = 37$ satisfying $(e, \varphi(n)) = (37, 3588) = 1$. Then B finds d and k such that $37d + 3588k = 1$ using the EEA:

$$\begin{aligned}3588 &= 96 \cdot 37 + 36, \quad q_1 = 96 \\ 37 &= 1 \cdot 36 + 1, \quad q_2 = 1 \\ 36 &= 36 \cdot 1 + 0, \quad q_3 = 36.\end{aligned}$$

B computes

$$\begin{pmatrix}0 & 1 \\ 1 & -96\end{pmatrix}\begin{pmatrix}0 & 1 \\ 1 & -1\end{pmatrix}\begin{pmatrix}0 & 1 \\ 1 & -36\end{pmatrix} = \begin{pmatrix}-1 & 37 \\ 97 & -3588\end{pmatrix}$$

This yields $d = 97$ and $k = -1$.

3. The public key is $(n, e) = (3713, 37)$. The private key is $d = 97$. Now A enciphers the message $m = 78$ with B's public key to

$$c = m^{37} = 78^{37} \mod 3713.$$

Repeated squaring modulo 3713 yields

$$\begin{aligned} 78^2 &\equiv 2371 \\ 78^4 &\equiv 2371^2 \equiv 159 \\ 78^8 &\equiv 159^2 \equiv 3003 \\ 78^{16} &\equiv 3003^2 \equiv 2845 \\ 78^{32} &\equiv 2845^2 \equiv 3398 \end{aligned}$$

so that $c \equiv 3398 \cdot 1263 \equiv 3159 \mod 3713$. So the encrypted message is 3159 or $DBFJ$. Now A sends this to B who uses his private key to compute

$$3159^{97} \equiv 78 \mod 3713.$$

REMARK 2.1.3. If the value of the message m satisfies $m \geq n$ we cannot properly encipher the plaintext. In this case we must subdivide the (numerical) plaintext into blocks of equal size, which are small enough. This process is called message blocking.

It is worthy to discuss the possible choices for the parameters in the RSA algorithm, because some of the choices are bad. First of all, choosing $1 < e < \varphi(n)$, one should avoid $e = \frac{1}{2}\varphi(n)+1$, since

$$\begin{aligned} m^{\frac{1}{2}\varphi(n)+1} &= (m^{\varphi(p)})^{\frac{1}{2}\varphi(q)} m \equiv m \mod p \\ &\equiv m \mod q \end{aligned}$$

so that $m^e \equiv m \mod n$, clearly not a desirable outcome.
Secondly, the primes p and q should not be chosen too close together. Suppose that $p > q$ and p is "close" to q in the sense, that $(p + q)/2$ is only slightly bigger than $\sqrt{n} = \sqrt{pq}$. In that case we only need to test a "few" integers $x > \sqrt{n}$ until $x^2 - n$ is a square, say y, and we have a factorization

$$n = x^2 - y^2 = (x - y)(x + y).$$

This will happen "quite soon" under our assumption, that is, already for $x = (p + q)/2$, in which case $y = (p - q)/2$ and $n = pq = (x - y)(x + y)$.

REMARK 2.1.4. There are more restrictions known choosing parameters. In 1989 Martin Wiener showed that using a small decryption exponent d was not wise, because it was possible to reveal it using continued fractions. Because of the "Wiener attack" one should choose d to have approximately the size $\sqrt{n}$. Also the knowledge of good factoring algorithms will give information on how not to choose parameters. Recall that if one is able to factor n, RSA is broken. For example, to prevent factoring of n with specialized algorithms like *Pollard's* $p - 1$, one can use *strong* primes p and q. Here a prime number p is called strong, if $p - 1$ and $p + 1$ have a large prime factor.

About the security of the RSA there is the following conjecture

CONJECTURE 2.1.5. *Cryptanalyzing RSA is as difficult as factoring.*

Although there is no proof of this conjecture there is strong evidence that the conjecture is valid. A good reason for believing this is that the only known method for finding d given e is the EEA applied to e and $\varphi(n)$. Yet, to compute $\varphi(n)$, we need to know p and q, namely, we need to know how to factor n. It can be shown that computing the deciphering exponent d in RSA has the same complexity as factoring the modulus n. In other words, knowing how to factor n allows us to compute d, and knowing how to compute d can be converted into an algorithm for factoring n.

REMARK 2.1.6. The RSA cryptosystem works on the finite abelian group $G = (\mathbb{Z}/n\mathbb{Z})^*$. It is possible to create RSA-like schemes using various other finite groups, for example the abelian groups $G = E(\mathbb{F}_q)$ of an elliptic curve over $\mathbb{F}_q$. The latter has been done, and the scheme is called KMOV. However, in practice it did not show any great advantage over the original scheme. On the other hand, there are many other groups which have not been tried, like certain matrix groups over $\mathbb{Z}/n\mathbb{Z}$, i.e., $G = GL_m(\mathbb{Z}/n\mathbb{Z})$.

2.2. ElGamal

The ElGamal cryptographic scheme bases its security upon the DLP. It is named after Taher ElGamal who published it in 1985 see [**3**]. Suppose A wants to send a secret (numerical) message m to B. The ElGamal key generation goes as follows:

1. B chooses a large random prime p and a primitive root α modulo p.
2. B then chooses a random integer a with $2 \leq a < p-1$ and computes $\alpha^a \mod p$.
3. B's public key is (p, α, α^a) and his private key is a.

The Enciphering goes as follows:

1. A obtains B's public key (p, α, α^a).
2. A chooses a random natural number $b < p-1$.
3. A computes $\alpha^b \mod p$ and $m\alpha^{ab} \mod p$.
4. A then sends the ciphertext $c = (\alpha^b, m\alpha^{ab})$ to B.

The Deciphering goes as follows:

1. B uses his private key to compute $(\alpha^b)^{-a} \equiv (\alpha^b)^{p-1-a} \mod p$.
2. B then deciphers m by computing $(\alpha^b)^{-a} m\alpha^{ab} \mod p$.

To see that B really recovers m we observe that

$$(\alpha^b)^{-a} m\alpha^{ab} \equiv m\alpha^{ab-ba} \equiv m \mod p.$$

EXAMPLE 2.2.1. *Suppose A wants to send the message $m = 2132$ to B using ElGamal.*

1. B chooses $p = 3359$, the primitive root $\alpha = 11$ and $a = 5$ his private key. He computes $\alpha^a \equiv 11^5 \equiv 3178 \mod 9$. Hence B's public key is

$$(p, \alpha, \alpha^a) = (3359, 11, 3178)$$

2. A downloads this from some public database and chooses $b = 69$ and computes

$$\alpha^b \equiv 11^{69} \equiv 193 \mod p$$
$$m\alpha^{ab} \equiv 2132 \cdot 3178^{69} \equiv 2719 \mod p.$$

The ciphertext is $c = (193, 2719)$, which A sends to B.

3. B uses his private key to compute

$$(\alpha^b)^{p-1-a} \equiv 193^{3353} \equiv 2243 \mod p$$
$$(\alpha^b)^{-a} m\alpha^{ab} \equiv 2243 \cdot 2719 \equiv 2132 \mod p,$$

thereby recovering $m = 2132$.

REMARK 2.2.2. The ciphertext has almost double length than the plain message text. Note that a b should never be used twice. Suppose that A uses b for two different messages m_1 and m_2, and an adversary C already knows m_1. Then C can obtain also m_2: if the two ciphertexts are $c_1 = (\alpha^b, m_1\alpha^{ab})$ and $c_2 = (\alpha^b, m_2\alpha^{ab})$, then C calculates

$$(m_2\alpha^{ab}m_1)(m_1\alpha^{ab})^{-1} = m_2.$$

Finally one can show that the security of the ElGamal cipher is based on the DLP.

CHAPTER 3

Algorithms related to cryptography

The security of cryptosystems relies on certain one-way functions, which are hard to invert. Here mathematical problems like factoring or computing discrete logarithms are involved. It is then quite important to known about possible algorithms or ideas to attack these problems, and what the complexity of these algorithms is.

3.1. Primality testing

The two most natural arithmetic problems of computational interest are the following. Firstly, to decide if a given integer is a prime. Secondly, to factorize an integer known to be composite. Both problems are also important for cryptography.

DEFINITION 3.1.1. A *true primality test* is a deterministic algorithm that, given an input n, verifies the hypothesis of a theorem whose conclusion is that n is prime. In this case n is called a *provable prime*.

The classical example of a true primality test is the so called *Lucas-Lehmer test*, for Mersenne numbers $M_n = 2^n - 1$ with $n \geq 3$. The algorithm consists of the following steps:

(1) Set $s_1 = 4$ and compute $s_j \equiv s_{j-1}^2 - 2 \mod M_n$ for $2 \leq j \leq n-1$.

(2) If $s_{n-1} \equiv 0 \mod M_n$, then conclude that M_n is prime. Otherwise, conclude that M_n is composite.

Note that M_n can only be prime if n is prime: if $n = \ell m$ for $\ell, m \geq 2$, set $x = 2^\ell, y = 1$. Then we have

$$x - y = M_\ell,$$
$$x^m - y^m = 2^{\ell m} - 1 = M_n.$$

But then $M_\ell \mid M_n$, since $(x-y) \mid x^m - y^m$. Here M_ℓ is a proper divisor since $\ell \neq 1, n$. Indeed, the theorem is the following.

THEOREM 3.1.2. *Define a sequence s_j by $s_1 = 4$ and $s_j = s_{j-1}^2 - 2$. Let $p > 2$ be a prime. Then $M_p = 2^p - 1$ is prime if and only if $s_{p-1} \equiv 0 \mod M_p$.*

For a proof, see for example [**7**]. A related result which is easier to prove is

THEOREM 3.1.3 (Pepin). *Let $n \in \mathbb{N}$. The Fermat number $F_n = 2^{2^n} + 1$ is prime if and only if*

$$3^{\frac{F_n - 1}{2}} \equiv -1 \mod F_n.$$

PROOF. Suppose that F_n is prime. Then, since $E(\mathbb{Z}/F_n\mathbb{Z})$ is cyclic, the above congruence holds if and only if 3 is a quadratic nonresidue modulo F_n (this is Euler's criterion). But the

latter can be proved using quadratic reciprocity. Since $F_n \equiv 1 \mod 4$, we have

$$\begin{aligned}\left(\frac{3}{F_n}\right) &= \left(\frac{F_n}{3}\right) \\ &= \left(\frac{(-1)^{2^n}+1}{3}\right) \\ &= \left(\frac{2}{3}\right) = -1.\end{aligned}$$

Conversely, suppose that F_n is not prime, and let $p < F_n$ be a prime divisor. The assumed congruence modulo F_n implies also that $3^{(F_n-1)/2} \equiv -1 \mod p$, so that $3^{F_n-1} \equiv 1 \mod p$. It follows, that the order of 3 in $E(\mathbb{Z}/p\mathbb{Z})$ is exactly $F_n - 1$. But ord(3) divides the order of the group $E(\mathbb{Z}/p\mathbb{Z})$, which is $p-1$. Hence $F_n - 1 \mid p-1$, which is not possible for $p < F_n$. Hence F_n is prime. □

The above true primality tests only work well with special numbers. We would like to have a test which applies to all numbers. Let us consider Fermat's little theorem. If the converse of it would be true, then we would have a simple and fast method for obtaining provable primes in general. If $a^{n-1} \not\equiv 1 \mod n$, then we know that n cannot be prime. Unfortunately the converse of Fermat's result fails in the worst possible way. There exist infinitely many composite $n \in \mathbb{N}$ such that

$$a^{n-1} \equiv 1 \mod n \quad \text{for any integers } a \text{ relatively prime to } n.$$

Such integers are called *Carmichael numbers*, or C-numbers. It is not difficult to show that C-numbers are squarefree and have at least 3 different prime divisors. The first C-numbers are as follows

$$\begin{aligned}561 &= 3 \cdot 11 \cdot 17 \\ 1105 &= 5 \cdot 13 \cdot 17 \\ 1729 &= 7 \cdot 13 \cdot 19 \\ 2465 &= 5 \cdot 17 \cdot 29 \\ 2821 &= 7 \cdot 13 \cdot 31 \\ 6601 &= 7 \cdot 23 \cdot 41 \\ 8911 &= 7 \cdot 19 \cdot 67\end{aligned}$$

Of course, some C-numbers really have more than 3 different prime divisors, like $41041 = 7 \cdot 11 \cdot 13 \cdot 41$.

PROPOSITION 3.1.4 (Korselt). *An integer $n \geq 1$ is a C-number if and only if n is squarefree and satisfies $p-1 \mid n-1$ for each prime divisor $p \mid n$.*

PROPOSITION 3.1.5 (Chernick). *Assume that there is an integer $m \geq 1$ such that $p = 6m+1$, $q = 12m+1$ and $r = 18m+1$ are all prime. Then $n = pqr$ is a C-number.*

Erdös has conjectured that there are infinitely many C-numbers. In 1994, Alford, Granville and Pommerance proved the following result, which in particular says that there are more C-numbers than squares.

THEOREM 3.1.6. *The number $C(x)$ of C-numbers not exceeding x satisfies*

$$C(x) > x^{2/7}$$

for all $x \geq x_0$.

Erdös has conjectured that $C(x) \geq x^{1-\varepsilon}$ for all $\varepsilon > 0$ and all sufficiently big $x \geq x(\varepsilon)$.

About the "Fermat test" we have the following result.

PROPOSITION 3.1.7. *If n is composed, but not a C-number, then the Fermat test gives as output "n is composed" with probability $\geq 1/2$. The algorithm uses $O(\log(n)M(\log(n)))$ bit operations.*

Here $M(m)$ is the number of bit operations, to multiply two numbers of length m. By the classical algorithm we know that $M(m) = O(m^2)$, but the fast multiplication introduced by Schönhage yields

$$M(m) = O(m \log(m) \log(\log(m))).$$

We can modify Fermat's test in such a way, that we obtain a true primality test.

THEOREM 3.1.8. *If $n \in \mathbb{N}$ with $n \geq 3$, then n is prime if and only if there is an $m \in \mathbb{N}$ such that*

$$m^{n-1} \equiv 1 \mod n,$$
$$m^{\frac{n-1}{q}} \not\equiv 1 \mod n \quad \text{for any prime } q \mid (n-1).$$

Of course, the major pitfall with this theorem is that it requires a knowledge of the factorization of $n-1$. So the problem is the speed.

If we would like to maintain speed and generality, then very often *correctness*, obtaining provable primes, is sacrified, and one deals with *probabilistic primality tests*. We will see this later. Denote by $\mathcal{P}$ the class of problems, for which one can answer with yes or no, and for which each example of the problem can be solved by a deterministic polynomial-time algorithm. Here an algorithm is called deterministic if its behaviour is completely determined by the input. Denote by $\mathcal{NP}$ the class of problems which can be solved in polynomial time with a non-deterministic algorithm. This means, for such a problem the solution can be *verified (not found)* in polynomial time.

EXAMPLE 3.1.9. The subset sum problem*: Let $M = \{a_1, \ldots, a_n\}$ be a set of positive integers and $k \in \mathbb{N}$. Determine whether or not there exists a subset $S \subset M$ such that $\sum_{i \in S} a_i = k$.*

This problem is in $\mathcal{NP}$. If one has found such a subset S, then the solution can be verified in polynomial time. It is not known if the problem is in $\mathcal{P}$. Obviously $\mathcal{P} \subseteq \mathcal{NP}$. The converse is a famous conjecture, a *millenium problem*.

CONJECTURE 3.1.10 (Cook, Levin). *We have $\mathcal{P} = \mathcal{NP}$.*

The following is an unconditional deterministic polynomial-time algorithm for primality testing, presented by M. Agrawal, N. Kayal, and N. Saxena [**1**] in 2004. Here Primes denotes the problem to decide whether or not a given n is prime.

THEOREM 3.1.11 (AKS). *Primes are in $\mathcal{P}$.*

Let $R = (\mathbb{Z}/n\mathbb{Z})[x]$ and $h \in R$. Consider the ideal $(n, h(x))$ in R. We write $f(x) \equiv g(x) \mod (n, h(x))$ for $f, g, h \in \mathbb{Z}[x]$, if there exist $u, v \in \mathbb{Z}[x]$, such that

$$f(x) - g(x) = n \cdot u(x) + h(x)v(x).$$

In other words, $f(x) = g(x)$ in the quotient ring $R/(h(x))$. The algorithm for the AKS-test is as follows. Input an integer $n > 1$ and execute the following steps:

1. If $n = a^k$ for some integer $k \geq 2$ then return "n is composite".
2. Find the smallest $r \in \mathbb{N}$ such that $\mathrm{ord}_r(n) > 4(\log_2(n))^2$.
3. If $1 < (a, n) < n$ for some $a \leq r$ then output "n is composite".
4. If $n \leq r$, then output "n is prime".
5. For $a = 1$ to $\lfloor 2\sqrt{\varphi(r)}\log_2(n) \rfloor$ do
   if $(x + a)^n \not\equiv x^n + a \mod (n, x^r - 1)$ then output "n is composite".
6. Output "n is prime".

The algorithm uses the following polynomial primality criterion.

LEMMA 3.1.12. *Let $a \in \mathbb{Z}$, $n \geq 2$ such that $(a, n) = 1$. Then n is prime if and only if, in $\mathbb{Z}[x]$,*

$$(x + a)^n \equiv x^n + a \mod n.$$

PROOF. If $n = p$ is prime, then we have $(x + a)^p = x^p + a^p = x^p + a$ in $\mathbb{F}_p[x]$. Conversely let n be composed. Choose a prime divisor $p \mid n$. By assumption $1 < p < n$. The coefficient of x^p in $(x + a)^n - x^n - a$ is given by

$$\binom{n}{p} a^{n-p} = \frac{n}{p} \cdot \frac{(n-1)\cdots(n-p+1)}{(p-1)(p-2)\cdots 1} a^{n-p}.$$

This number contains the factor p one time less than n itself, and hence is not divisible by n. Hence the polynomial $(x+a)^n - x^n - a$ is not the zero polynomial in $\mathbb{F}_n[x]$. Thus $(x+a)^n \not\equiv x^n + a \mod n$ in $\mathbb{Z}[x]$. □

The satisfaction of this polynomial congruence is a simple test, but too much time consuming. It is exponential, in fact, and worse than just using the sieve of Eratosthenes, because of computing $(x - a)^n$. But if one does the computation modulo f, with the degree of f much smaller than our big n, than we can save time. A good choice is $f(x) = x^r - 1$ for a suitable r. So we test the congruence

$$(x + a)^n \equiv x^n + a \mod (x^r - 1, n).$$

The above lemma says that the congruence is satisfied for all a, r, if $n = p$ is prime. Unfortunately this is also true for some composed n. But one can show that in this case n is already a prime power. So the first step of the algorithm would output n is composed.
The authors were able to establish the following facts about their algorithm.

PROPOSITION 3.1.13. *The algorithm outputs "n is prime" if and only if n is prime. Furthermore there exists an $r \leq \lceil 16(\log_2(n))^5 \rceil$ such that $\mathrm{ord}_r(n) > 4(\log_2(n))^2$. The asymptotic time complexity is $O((\log(n))^{10.5+\varepsilon})$ for any $\varepsilon > 0$.*

If the so called *Sophie Germain conjecture* holds, the complexity of the algorithm can be improved. Here is the statement of the Sophie Germain prime density conjecture:

CONJECTURE 3.1.14 (Hardy). *The number of primes $p \leq x$ such that $2p+1$ is also prime is asymptotically $\frac{2 \cdot C_2 x}{\log^2(x)}$, where C_2 is the twin prime constant, i.e.,*

$$\sum_{\substack{p \leq x \\ p, 2p+1 \in \mathbb{P}}} 1 \sim \frac{2C_2 x}{\log^2(x)}, \quad x \to \infty,$$

$$C_2 = \prod_{p \geq 3} \frac{p(p-2)}{(p-1)^2} \simeq 0.6601611816.$$

Suppose that this conjecture holds, then $r = O(\log^{2+\varepsilon}(n))$ for any $\varepsilon > 0$ such that $\mathrm{ord}_r(n) \geq 4\log^2(n)$. Hence, the algorithm, with this r-value, yields the complexity of

$$O(\log^{6+\varepsilon}(n))$$

for any $\varepsilon > 0$. Now Lenstra and Pommerance were able to modify the AKS-test in such a way, that its complexity is just this, without assuming the Sophie Germain conjecture.

Next we will come to probabilistic primality tests. They are based on randomized algorithms, namely those that make random decisions at certain points in the execution, so that the execution paths may differ each time the algorithm is invoked with the same input. We start with the MSR primality test (Miller-Selfridge-Rabin), which will improve the Fermat test substantially. All modular exponentiations are done using the repeated squaring method. Let $n - 1 = 2^k m$ with $m \in \mathbb{N}$ odd, and $k \in \mathbb{N}$. The input is n. By "return 1" we mean the output "n is probably prime", by "return 0" we mean that "n is definitely composite".

1. Choose a random integer a with $2 \leq a \leq n-2$.
2. Let $g = (a, n)$. If $g > 1$ then return g.
3. Compute $x_0 \equiv a^m \mod n$. If the result is ± 1 then return 1 and terminate the algorithm.
4. for $1 \leq i \leq k$ compute $x_i \equiv x_{i-1}^2 \mod n$.
5. if $x_k \equiv 1 \mod n$, then set $j = \min\{0 \leq i < k \mid x_{i+1} \equiv 1 \mod n\}$. Else return 0.
6. Let $g = (x_j + 1, n)$. If $g = 1$ or $g = n$ then return 1. Else return g.

This algorithm does not fail systematically on a certain input, like the Fermat test. If n is a C-number, then the algorithm will probably detect that n is composite, and return a factor of n.

PROPOSITION 3.1.15. *If n is prime, the MSR-test outputs that n is probably prime. If n is composed, and not a C-number, then the algorithms outputs "n is composed" with probability $\geq \frac{3}{4}$. If n is a C-number, then the algorithms finds a factor with probability $\geq \frac{3}{4}$. The algorithms uses $O(\log(n)M(\log(n))$ bit operations.*

Note that $x_i \equiv a^{2^i m} \mod n$ for $0 \leq i \leq k$, so that $x_k \equiv a^{n-1} \mod n$. If we have done the test 1000 times with the output "n is probably prime", we can conclude that the probability for n not to be prime is less than $(\frac{1}{4})^{1000}$. At this point any reasonable person would consider n to be prime.

EXAMPLE 3.1.16. *Try the MSR-test on the C-number $n = 561$, with $n - 1 = 2^4 \cdot 35$, i.e., with $k = 4$ and $m = 35$.*

1. Choose $a = 2$.
2. Then $g = (2, 561) = 1$.
3. $x_0 \equiv 2^{35} \mod 561 = 263$.
4. Then $(x_1, x_2, x_3, x_4) = (166, 67, 1, 1) \mod 561$.
5. $x_3 \equiv 1 \mod n$, hence $j = 2$ and $x_j + 1 = 68$.
6. Return $g = (68, 561) = 17$.

So indeed the MSR-test yields a factor of $n = 561$.

Another related algorithm is the Solovay-Strassen test, where Jacobi symbols are computed. But the MSR-test is computationally less expensive, easier to implement, and at least as correct. For this reason we will not discuss it here.

3.2. Factoring

Given the importance of factoring in the security of RSA and other cryptosystems, its worth having a closer look at some well known algorithms for factoring.

The integer factoring problem (IFP) consists of finding the prime decomposition of n. Before doing this, there are very fast tests which will tell us whether n is composed, or whether n is probably prime. If n is composed we start finding the factors. A simpler problem than IFP is the notion of *splitting*, which means the finding of one proper factor r of n, so that $n = rs$, where $s = n/r$. Typically, first one would try to find a "small" factor of n. The oldest method of splitting n is *trial division*, by which we mean dividing n by all primes up to $\sqrt{n}$. It works reasonably well if n is small, or if n has small divisors. Here "small" could mean $n < 10^8$ by the current standards of computers. This will not be successful for the following example.

EXAMPLE 3.2.1. *Find a factor of* $2^{227} - 1$.

Indeed, $n = pq$, where p and q are primes with $p < q$, namely

$$p = 26986333437777017$$
$$q = 79921777382059796264915069508677209535456601216886 31$$

This is a good example to test various factoring algorithms. If we have a random n, then how many "small" divisors can we expect ? Consider the following list of numbers and their factoring in the interval $[10^7, 10^7 + 10]$.

$$\begin{aligned}
10^7 &= 2^7 \cdot 5^7 \\
10^7 + 1 &= 11 \cdot 909091 \\
10^7 + 2 &= 2 \cdot 3 \cdot 47 \cdot 35461 \\
10^7 + 3 &= 13 \cdot 769231 \\
10^7 + 4 &= 2^2 \cdot 7 \cdot 19 \cdot 18797 \\
10^7 + 5 &= 3 \cdot 5 \cdot 666667 \\
10^7 + 6 &= 2 \cdot 83 \cdot 107 \cdot 563 \\
10^7 + 7 &= 941 \cdot 10627 \\
10^7 + 8 &= 2 \cdot 3 \cdot 138889 \\
10^7 + 9 &= 23 \cdot 434783 \\
10^7 + 10 &= 2 \cdot 5 \cdot 101 \cdot 9901
\end{aligned}$$

Indeed, there are a lot of "small" divisors. We can make this more precise. If we fix the first r primes $p_1, \ldots, p_r$, and declare these to be small in comparison to $n = p_1 \cdots p_r$, then we can count how many numbers in $\{1, \ldots, n\}$ have a small factor, i.e., a number divisible by some some p_i, for $i \leq r$. For example, if $r = 3$, then $(p_1, p_2, p_3) = (2, 3, 5)$ and $n = 30$. Among the numbers $\{1, \ldots, 30\}$ we have 22 numbers having a small prime divisor (that is, divisible by 2, 3 or 5). The ratio is $\frac{22}{30}$.

LEMMA 3.2.2. *Let* $p_1, \ldots, p_r$ *be the first* r *primes, and* $n = p_1 \cdots p_r$. *Then the* n *numbers* $k + 1, \ldots, k + n$ *for* $k \geq 0$ *contain exactly* $n - \varphi(n)$ *numbers divisible by some of the first* r

primes. For $k = 0$ this means, that the ratio of all numbers from 1 to n divided by those which are divisible by some p_i, $i \leq r$, is given by

$$1 - \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

PROOF. The set $\{k+1, \ldots, k+n\}$ is a full residue system modulo n. Hence $\varphi(n)$ of these numbers is coprime to n, so that the gcd with the other $n - \varphi(n)$ numbers is greater than 1, and hence the gcd is a divisor of n. So these other numbers have a divisor p_i. Because of

$$n - \varphi(n) = n \cdot \left(1 - \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)\right)$$

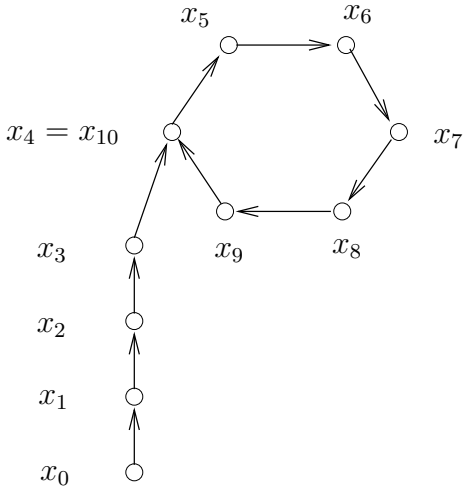
the claim follows. □

EXAMPLE 3.2.3. *Let $r = 10$ and $n = 6469693230$. The ratio of numbers in $[1, n]$ having a small prime divisor in the first 10 primes $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29\}$ is given by*

$$1 - \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{2}\right) \cdots \left(1 - \frac{1}{29}\right) = \frac{2358365}{2800733} \simeq 0.84205277.$$

Indeed, $n = 2 \cdot 3 \cdots 29$. So more than 84% of the numbers in $[1, n]$ have a small prime divisor $p \leq 29$.

Next we come to a probabilistic method of finding a factor of n invented by *Pollard* in 1975. The basic idea is as follows. Choose a polynomial $f \in \mathbb{Z}[x]$ and an integer x_0 with $0 \leq x_0 \leq n-1$. Then consider the sequence $(x_i)_{i \geq 0}$ recursively defined by $x_i := f(x_{i-1}) \mod n$. Since there are only finitely many values for this infinite sequence we must run into a period. This is demonstrated by the following diagram:



The shape of the symbol is reminiscent of the greek symbol ρ. For this reason, this factoring algorithm has the name *Pollard's Rho method*. It works now as follows. Having computed the sequence we compute the gcd's $(n, x_k - x_\ell)$. If, really, n is composed, there would be a prime divisor $p \mid n$, so that the sequence $x_i \mod p$ would be periodic in much shorter time, in general, with a shorter period, say k. But then, with high probability, the gcd $(n, x_n - x_{n+k})$ will be a divisor. It will be a divisor > 1, since $p \mid (n, x_n - x_{n+k})$, if $x_n \equiv x_{n+k} \mod p$.
For practical reasons we first need a good method to find for our sequence $(x_i)_{i \geq 0}$ two indices $i \neq j$ such that $x_i = x_j$.

EXAMPLE 3.2.4. *Let $f(x) = x^2+2$, $x_0 = 2$ and $n = 61$. Then the sequence $(x_i)_{i\geq 0}$ in $\mathbb{Z}/61\mathbb{Z}$ is given by*

$$(2, 6, 38, 43, 21, 16, 14,\ 15, 44, 47,\ \ 15, 44, 47,\ \ 15, 44, 47, \cdots$$

Here $t = 7$ is the length of the preperiod, and $\ell = 3$ the cycle length. We have $x_i = x_{i+\ell}$ for all $i \geq t$. The first two indices $i \neq j$ with $x_i = x_j$ are $(i, j) = (7, 10)$ in this example. In general, to find these indices, it is not a good idea to compute the whole sequence. This will use too much memory. The following algorithm, called *Floyd's cycle detection trick*, uses along with (x_i) a second sequence (y_i), which iterates f with double speed, so that $y_i = x_{2i}$. The input is an integer x_0 with $0 \leq x_0 \leq p-1$ and a polynomial $f \in (\mathbb{Z}/p\mathbb{Z})[x]$. The output is an $i > 0$ with $x_i = x_{2i}$.

1. $y_0 \leftarrow x_0$, $i \leftarrow 0$.

2. repeat $i \leftarrow i+1$, $x_i \leftarrow f(x_{i-1})$, $y_i \leftarrow f(f(y_{i-1}))$, until $x_i = y_i$.

3. return i.

When the faster sequence overtakes the slower one, for some i, then we have $x_{2i} = y_i = x_i$. Denote by p the smallest prime factor of n, which we don't know yet. Then we consider the sequence (x_i) with, say $x_{i+1} \equiv x_i^2 + 1 \mod p$. After $O(\sqrt{p})$ steps, in general, we can expect a collision, i.e., an i such that $x_i = x_{2i}$. How many terms of the sequence should we consider so that there are two equal ones with high probability ? The answer is given as follows.

PROPOSITION 3.2.5. *If M is a set with p elements and $(x_1, \ldots, x_k)$ a k-tuple of a random sequence (x_i) in M such that $k \geq \frac{31}{10}\sqrt{p}$, then the probability that two terms of the sequence in $(x_1, \ldots, x_k)$ coincide is more than 99%.*

If we generate our sequence using a polynomial f, it is not clear whether or not it is a random sequence. Surely, f should not be linear. In practice, one takes $f(x) = x^2 + a$ with $a \neq 0, -2$.
Finally, we come to Pollard's algorithm. Suppose we want to factorize n. Fix the smallest prime $p \mid n$, which we don't know explicitly, of course. Suppose that $x_1, \ldots, x_k$ is a random sequence modulo n, say, in $\{0, 1, \ldots, n-1\}$. By reduction modulo p we have a sequence in $\{0, 1, \ldots, p-1\}$. For $k \geq \frac{31}{10}\sqrt{p}$ we will have indices $i \neq j$ with $x_i \equiv x_j \mod p$ with probability ≥ 0.99. Then we have $p \mid (n, x_i - x_j)$, so that $(n, x_i - x_j) > 1$.
The input to Pollards ρ-method is $n \geq 3$, n not prime. The output is a proper divisor of n, or "failure".

1. Pick $0 \leq x_0 \leq n-1$ at random and set $y_0 \leftarrow x_0$, $i \leftarrow 0$.

2. repeat $i \leftarrow i+1$, $x_i \leftarrow x_{i-1}^2 + 1 \mod n$ and $y_i \leftarrow (y_{i-1}^2 + 1)^2 + 1 \mod n$.

3. $g \leftarrow (n, x_i - x_j)$. If $1 < g < n$ then return g,
   else if $g = n$ then return "failure".

Here is an example.

EXAMPLE 3.2.6. *Factorize $n = 82123$ by Pollard's ρ-method.*

Choose $x_0 = 631$. Then the following table yields the non-trivial divisor 41, so that

$$82123 = 41 \cdot 2003.$$

i	$x_i \mod n$	$y_i \mod n$	$(n, x_i - y_i)$
0	631	631	1
1	69670	28986	1
2	28986	13166	1
3	69907	40816	1
4	13166	20459	1
5	64027	6685	1
6	40816	75835	1
7	80802	17539	41

What is not immediately visible is the fact, that for the smallest prime divisor of n, namely $p = 41$, the collision of (x_i) and (y_i) modulo p occurs exactly at $i = 7$:

$$(x_i)_{i\geq 0} = (16, 11, 40, 2, 5, 26, 21, 32, \ldots)$$
$$(y_i)_{i\geq 0} = (16, 40, 5, 21, 0, 2, 26, 32, \ldots)$$

PROPOSITION 3.2.7. *Let $n \in \mathbb{N}$ be composed and $p \mid n$ be the smallest prime divisor. Let $f(x) = x^2 + 1$. Suppose that the sequence (x_i) modulo p is random. Then the running time of the Pollard's ρ-algorithm is*

$$O(\sqrt{p}M(\log(n))\log(\log(n)))).$$

This algorithm will not be useful if n has only large prime factors. There is another factoring algorithm by Pollard, published in 1974, that utilizes Euler's theorem.

DEFINITION 3.2.8. An integer $n \geq 1$ is called a *B-powersmooth number* if all prime powers $p_i^{e_i}$ dividing n satisfy $p_i^{e_i} \leq B$.

If $p_1, \ldots, p_r$ are the primes $p \leq B$, and the e_i the largest natural numbers with $p_i^{e_i} \leq B$, then $V_B = lcm(1, 2, \ldots, B) = \prod_{i=1}^{r} p_i^{e_i}$. Hence n is B-powersmooth if and only if $n \mid V_B$. Note that V_B is much smaller than $B!$.

LEMMA 3.2.9. *Let $n \in \mathbb{N}$, $p \in \mathbb{P}$, $a \in \mathbb{Z}$ such that $(a, n) = 1$ and $p \mid n$. Assume that $p - 1$ is B-powersmooth. Then*

$$p \mid (a^{V_B} - 1, n),$$

hence the gcd is a divisior > 1 of n.

PROOF. Let $p - 1 = q_1^{e_1} \cdots q_r^{e_r}$ be the prime decomposition of $p - 1$. Because of $q_i^{e_i} \leq B$ we have $q_i^{e_i} \mid V_B$, hence $p - 1 \mid V_B$. Since $a^{p-1} \equiv 1 \mod p$ we have $a^{V_B} \equiv 1 \mod p$, i.e., $p \mid (a^{V_B} - 1)$. Now $p \mid n$ implies $p \mid (a^{V_B} - 1, n)$. □

Pollard's $p - 1$ method works as follows. The input is an $n \geq 3$ and a $B \geq 2$. The output is a proper divisor of n, or "failure".

1. $v \leftarrow lcm(1, 2, \ldots, B)$.

2. Choose some a with $2 \leq a \leq n - 2$ and $(a, n) = 1$.

3. $b \leftarrow a^v \mod n$, $d \leftarrow (b - 1, n)$.

4. if $1 < d < n$ then return d

else return "failure".

If the algorithm outputs "failure", one can try again with a larger B.

EXAMPLE 3.2.10. *Factorise $n = 1007$ with $B = 5$ and $B = 10$.*

If $B = 5$, then $v = 60$. Choose $a = 2$. Then $b = 2^{60} \equiv 786 \mod 1007$, $d = (785, 1007) = 1$. The output is "failure".

If $B = 10$, then $v = 2520$. Choose $a = 2$. Then $b = 2^{2520} \equiv 172 \mod 1007$, and $d = (171, 1007) = 19$. Indeed, 19 is a divisor, and we have $1007 = 19 \cdot 53$. Here $19 - 1 = 2 \cdot 3^2$ is not 5-powersmooth and $53 - 1 = 2^2 \cdot 13$ is not 10-powersmooth.

REMARK 3.2.11. If the result is $(a^{V_B} - 1, n) = 1$ for some B, and $p \mid n$ is any prime divisor, then $a^{V_B} \not\equiv 1 \mod p$, since $p \nmid 1$ and $a^{p-1} \equiv 1 \mod p$. It follows $(p-1) \nmid V_B$, so that $p - 1$ is *not* B-powersmooth. In other words, if the algorithm outputs "failure", no prime divisor $p \mid n$ will yield a B-powersmooth $p - 1$. Hence we must choose a bigger B. This shows how much the success of the algorithm depends on the prime decomposition of $p-1$ for the prime divisors of n. If B has to be chosen too big, the algorithm will be very slow.

EXAMPLE 3.2.12. *Factorize $n = 10^{30} + 25$.*

Factorizing with Pollard's ρ-method takes some time, but factorizing with Pollard's $p - 1$ method is very quick, i.e. 0.1 seconds, with $B = 10^5$.

$$10^{30} + 25 = 5^2 \cdot 13 \cdot 15 \cdot 15384616923077 \cdot 199999980000001$$

Here we have, with $5^7 = 78125$,

$$\begin{aligned} 199999980000000 &= 2^8 \cdot 3^2 \cdot 5^7 \cdot 239 \cdot 4649 \\ 15384616923076 &= 2^2 \cdot 769231 \cdot 4999999, \end{aligned}$$

so that the first number is 10^5-powersmooth.

EXAMPLE 3.2.13. *Factorize $n = 10^{30} + 35$.*

Here Pollard's $p - 1$ method fails. The factorization is

$$10^{30} + 35 = 3^2 \cdot 5 \cdot 32552664510871 \cdot 682654478707913.$$

For the big prime divisors p and q we have

$$\begin{aligned} p - 1 &= 32552664510870 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 47 \cdot 1099380767, \\ q - 1 &= 682654478707912 = 2^3 \cdot 67 \cdot 1031 \cdot 1235314357. \end{aligned}$$

Hence $p - 1$ and $q - 1$ are not 10^9-pwoersmooth, and the algorithm is not effective.

Note that, for given B, only finitely many primes exist such that $p - 1$ is B-powersmooth. If $p - 1 = q_1^{e_1} \cdots = q_r^{e_r}$ is B-powersmooth, then $p - 1 \leq B^r$, so that $p \leq B^r + 1$. This also means that there are only "few" primes p such that $p - 1$ is B-powersmooth. For example, in the interval $[10^{15}, 10^{15} + 10000]$ there are just 15% of all primes $B = 10^6$-powersmooth. Hence Pollard's $p - 1$ method is useless for 85% of all primes of that size.

REMARK 3.2.14. If $n = pq$, and neither $p-1$ nor $q-1$ is B-powersmooth for some fixed, realistic B, then Pollard's classical $p-1$ method will not be succesful. But we can use a version for elliptic curves of Pollard's algorithm. In the classical case we make computations more or less in the group $E(\mathbb{Z}/p\mathbb{Z})$ of order $p-1$, where $p \mid n$. Hence we are fixed on $p-1$. In the elliptic curve case over $\mathbb{F}_p$ we have many groups $E_{a,b}(\mathbb{F}_p)$ of arbitrary order in the interval

$$(p+1-2\sqrt{p}, p+1+2\sqrt{p}),$$

depending on the parameters a, b of the elliptic curve $y^2 = x^3 + ax + b$ with $\Delta = -16(4a^3 + 27b^2) \neq 0$. We can vary a, b then until, perhaps, the order of $E_{a,b}(\mathbb{F}_p)$ is B-powersmooth. Sometimes this is possible.

As an example, let $n = pq = 59 \cdot 101 = 5959$ and $B = 20$. Then $p-1 = 2 \cdot 29$ and $q-1 = 2^2 \cdot 5^2$ are not 20-powersmooth. But $p-2 = 57 = 3 \cdot 19$ would be 20-powersmooth. Indeed, with $(a, b) = (1, 54)$ the cyclic group $E_{a,b}(\mathbb{F}_p)$ has order $57 = p-2$, which is 20-powersmooth. Here $E\colon y^2 = x^3 + x + 54$.

3.3. Discrete Logarithms

Let $p > 2$ be a prime. We want to solve the equation $g^x = a$ over $\mathbb{F}_p^*$. We assume that g is a primitive root modulo p, so that there exists a solution, which is unique modulo $p-1$. We write $x = \mathrm{ind}_g(a)$, the index. The most direct method to find a solution is to compute all powers $g^n \mod p$ until we arrive at $g^x \equiv a \mod p$. We will need $O(p\log^2(p))$ bit operations to do this. The *Silver-Pohlig-Hellman algorithm* works as follows:

1. Suppose we know a factor t of $p-1$. Then our equation yields

$$g^{\frac{p-1}{t}x} = (g^x)^{\frac{p-1}{t}} = a^{\frac{p-1}{t}}.$$

Since $g^{\frac{p-1}{t}}$ has order t, there exists a y with $0 < y < t$ such that

$$g^{\frac{p-1}{t}y} = a^{\frac{p-1}{t}}.$$

We can find such an y by trying all possible values. If we have found it, then $x = y \mod t$ solves the above equation: we have

$$g^{\frac{p-1}{t}x} = g^{\frac{p-1}{t}y} = a^{\frac{p-1}{t}}.$$

2. Suppose we know the prime decomposition of $p-1$, i.e.

$$p - 1 = q_1^{e_1} \cdots q_r^{e_r} = t_1 \cdots t_r.$$

By 1. we can find for each $i = 1, \ldots, r$ an y_i such that, in $\mathbb{F}_p^*$,

$$g^{\frac{p-1}{t_i}y_i} = a^{\frac{p-1}{t_i}}.$$

3. By the Chinese remainder theorem we can find a solution x' such that $x' \equiv y_i \mod t_i$, for $i = 1, \ldots, r$. We claim that x' solves the DL-problem, i.e., $g^{x'} = a$. We have

$$g^{\frac{p-1}{t_i}x'} = g^{\frac{p-1}{t_i}y_i} = a^{\frac{p-1}{t_i}},$$

so that

$$\mathrm{ord}(g^{x'}a^{-1}) \mid \left(\frac{p-1}{t_1}, \ldots, \frac{p-1}{t_r}\right) = 1.$$

It follows $\mathrm{ord}_p(g^{x'}a^{-1}) = 1$, and $g^{x'}a^{-1} = 1$, or $g^{x'} = a$.

Example 3.3.1. *Let $p = 10^{10} + 19$. Then $g = 2$ is a primite root modulo p. Solve the DL-problem $2^x = 3$ over $\mathbb{F}_p^*$.*

The prime decomposition of $p-1$ is given by

$$p - 1 = 2 \cdot 131 \cdot 521 \cdot 73259 = t_1 t_2 t_3 t_4.$$

Then we have to find $y_i \mod t_i$ for $i = 1, 2, 3, 4$ such that

$$2^{\frac{p-1}{2}y_1} = 3^{\frac{p-1}{2}}$$
$$2^{\frac{p-1}{131}y_2} = 3^{\frac{p-1}{131}}$$
$$2^{\frac{p-1}{521}y_1} = 3^{\frac{p-1}{521}}$$
$$2^{\frac{p-1}{73259}y_1} = 3^{\frac{p-1}{73259}}$$

over $\mathbb{F}_p^*$. Because of $3^{\frac{p-1}{2}} \equiv 1 \mod p$ we can choose $y_1 = 0$, i.e., $y_1 \equiv 0 \mod 2$. Secondly,

$$3^{\frac{p-1}{131}} \equiv 1\,552\,837\,932 \mod p.$$

Just try all $y_2 = 1, \ldots, 131$ and find $2^{\frac{p-1}{131}92} \equiv 3^{\frac{p-1}{131}} \mod p$, i.e., $y_2 \equiv 92 \mod 131$. In the same way we find $y_3 \equiv 223 \mod 521$ and $y_4 \equiv 55292 \equiv 73259$.

The Chinese remainder theorem yields

$$x = 5\,181\,957\,398.$$

This solves $2^x = 3$ over $\mathbb{F}_p^*$.

REMARK 3.3.2. We solve the equations of the type $g^{\frac{p-1}{t_i}y_i} = b$ by trying all $y_i = 0, 1, \ldots, t_i - 1$. This takes $O(t_i)$ steps. There are better ways, which only use $O(\sqrt{q_i}\log(q_i))$ steps, where $t_i = q_i^{e_i}$. For example, the *baby-step-giant-step* method, invented by Shanks in 1971.

Again, let $p \in \mathbb{P}$ and $g, a \in \mathbb{N}$ with $1 \le a, g \le p-1$. We want to solve $g^x \equiv a \mod p$. The baby-step-giant-step method works as follows:

1. Let $m = \lceil\sqrt{p}\rceil$. Then we can represent x, with $0 \le x \le p-2$, as $x = mj - i$ for some $1 \le i, j \le m$. Indeed, if $x = qm + r$ with $0 \le r, q \le m-1$ after division, then $x = (q+1)m - (m-r)$. So we can take $j = q+1$ and $i = m - r$.

2. Instead of $g^x \equiv a \mod p$ we write $g^{mj-i} \equiv a \mod p$. This is equivalent to

$$ag^i \equiv (g^m)^j \mod p, \quad 1 \le i, j \le m.$$

3. Now we compute the LHS and the RHS separately, organizing two different lists:

$$[ag^i \mod p \mid i = 1, \ldots, m], \text{ the baby-steps,}$$
$$[(g^m)^j \mod p \mid j = 1, \ldots, m], \text{ the giant-steps}$$

Then we compare the two lists. Is there a pair (i, j) such that $ag^i \equiv (g^m)^j \mod p$? If yes, then $x = mj - i$ is a solution to $g^x \equiv a \mod p$.

Comparing the two lists should be done quicker than just testing all g^x for $x = 1, \ldots, p-1$.

EXAMPLE 3.3.3. *Let* $p = 101$ *and solve* $2^x \equiv 3 \mod p$.

We can just compute all $2^n \mod p$, i.e., $2^0 \equiv 1, \ldots, 2^{99} \equiv 51$, and finally $2^{69} \equiv 3$. This takes 70 steps. The baby-step-giant-step method yields the result after $m = \lceil\sqrt{p}\rceil = 11$ steps. We have $g = 2$, $a = 3$. Here are the two lists:

i, j	1	2	3	4	5	6	7	8	9	10	11
$ag^i \mod p$	6	12	24	48	96	91	81	**61**	21	42	84
$g^{mj} \mod p$	28	77	35	71	69	13	**61**	92	51	14	89

For $(i, j) = (8, 7)$ tow entries coincide. Hence $x = mj - i = 11 \cdot 7 - 8 = 69$ is a solution.

REMARK 3.3.4. The method requires $O(\sqrt{p})$ steps and $O(\sqrt{p})$ storage, mainly for computing and sorting the two lists. In other words, the method requires a lot of storage for bigger p. Here Pollard's ρ method is much better. It can be adapted to solve the DL problem, and it requires very little storage.

Finally we want to discuss the *index calculus method* for solving the DL-problem. Let $p > 2$ be a prime and g be a primitive root modulo p. We want to find a solution to $g^x \equiv a \mod p$ by generating (and solving) a system of linear equations. The first step goes as follows:

1. Choose an integer $n \in \mathbb{N}$. Denote by $p_1, \ldots, p_n$ the first n primes. For an $m \geq n$ we want to find m relations

$$\prod_{j=1}^{n} p_j^{a_{ij}} \equiv g^{b_i} \mod p, \quad i = 1, \ldots, m, \tag{3.1}$$

with $a_{ij}, b_i \in \mathbb{Z}$. This works as follows:

(a) Choose a random $b \in \mathbb{Z}$ with $0 \leq b \leq p-2$.

(b) Compute $x \equiv g^b \mod p$, with $1 \leq x \leq p-1$.

(c) Write $x = p_1^{a_1} \cdots p_n^{a_n} y$ with $(y, p_1 \cdots p_n) = 1$.

(d) If $y = 1$ then $x \equiv g^b \mod p$ is a required relation of type (3.1). If $y > 1$, restart at (a) and try again with a new b.

Example 3.3.5. *Let $p = 10009$, $g = 11$, $n = 3$ and $m = 4$. Then $(p_1, p_2, p_3) = (2, 3, 5)$. We want to find 4 relations of the form*

$$2^{a_{i1}} \cdot 3^{a_{i2}} \cdot 5^{a_{i3}} \equiv 11^{b_i}, \quad 1 \leq i \leq 4.$$

We execute (a) – (d) again and again, until we have found all relations. The result is

$$\begin{aligned} 2^{11} \cdot 3^1 \cdot 5^0 &\equiv 11^{5140} \mod p, \text{ i.e., } i = 1, b_1 = 5140. \\ 2^2 \cdot 3^1 \cdot 5^1 &\equiv 11^{3438} \mod p, \text{ i.e., } i = 2, b_2 = 3438. \\ 2^4 \cdot 3^2 \cdot 5^2 &\equiv 11^{6876} \mod p, \text{ i.e., } i = 3, b_3 = 6876. \\ 2^2 \cdot 3^2 \cdot 5^0 &\equiv 11^{4374} \mod p, \text{ i.e., } i = 4, b_4 = 4374. \end{aligned}$$

The second step in the algorithm goes as follows

2. With $\ell_j = \log_g(p_j)$ we have $p_j \equiv g^{\ell_j} \mod p$, so that

$$\prod_{j=1}^{n} p_j^{a_{ij}} \equiv g^{a_{i1}\ell_1} \cdots g^{a_{in}\ell_n} \equiv g^{\sum_{j=1}^{n} a_{ij}\ell_j} \equiv g^{b_i} \mod p.$$

By Fermat's little theorem we obtain linear equations modulo $p-1$, in the unknowns $\ell_1, \ldots, \ell_n$:

$$\sum_{j=1}^{n} a_{ij}\ell_j \equiv b_i \mod p-1, \quad 1 \leq i \leq m. \tag{3.2}$$

The extended matrix is given by

$$\left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & \cdots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right)$$

Despite of the fact that $m \geq n$ we know that the system must have a solution, since g is a primitve root modulo p, so that such ℓ_i will exist. Using the Gauß algorithm for the principal ideal ring $\mathbb{Z}$ we reduce A to

$$\left(\begin{array}{ccc|c} d_1 & & & * \\ & d_2 & & \vdots \\ 0 & \cdots & d_n & * \\ 0 & \cdots & 0 & 0 \end{array}\right)$$

where $d_1 \mid d_2 \mid \cdots \mid d_n$ in $\mathbb{Z}$. If all d_i are invertible modulo $p-1$, then we can compute the ℓ_i recursively, modulo $p-1$. If $(d_i, p-1) > 1$ for some i, then this fails and we have to restart with more relations, i.e., with a bigger $m \geq n$.

EXAMPLE 3.3.6. *We perform the second step with the data form the previous example, i.e., with $p = 10009$, $g = 11$, $n = 3$.*

The extended matrix and its normal form is given by

$$\left(\begin{array}{ccc|c} 11 & 1 & 0 & 5140 \\ 2 & 1 & 1 & 3438 \\ 4 & 2 & 2 & 6876 \\ 2 & 2 & 0 & 4374 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|c} 1 & -4 & -5 & -12050 \\ 0 & 1 & 15 & 23794 \\ 0 & 0 & 31 & 46652 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

The third line yields $31\ell_3 = 46652$ modulo $p-1$. Since 31 is invertible modulo 10008, we obtain $\ell_3 = 31^{-1} \cdot 46652 \equiv 7316 \mod p-1$. Recursively, $\ell_2 \equiv 4126 \mod p-1$ and $\ell_1 \equiv 1002 \mod p-1$.
Finally, the third step of the algorithm goes as follows:

3. By step 1. we find a $b \in \mathbb{Z}$ such that

$$ag^b \equiv \prod_{j=1}^{n} p_j^{e_j} \mod p$$

for $e_j \in \mathbb{Z}$. By step 2. we find ℓ_i such that $p_j \equiv g^{\ell_j} \mod p$, i.e.,

$$ag^b \equiv \prod_{j=1}^{n} g^{e_j \ell_j} \equiv g^{\sum_{j=1}^{n} e_j \ell_j} \mod p.$$

This yields the solution

$$x = \log_g(a) = -b + \sum_{j=1}^{n} \log_g(p_j) e_j \mod p-1.$$

EXAMPLE 3.3.7. *Continuing the example, we will solve $g^x \equiv a \mod p$, i.e., $11^x \equiv a \mod 10009$ for $a \in \mathbb{Z}$.*

If $a = 101$, then $b = 6373$ and $(e_1, e_2, e_3) = (0, 1, 1)$. Hence $g^x \equiv a \mod p$ is solved by

$$\begin{aligned} x &= -6373 + \log_g(3) + \log_g(5) \\ &= -6373 + 4126 + 7316 \equiv 5069 \mod 10008. \end{aligned}$$

REMARK 3.3.8. The first step is critical. If n is chosen too small, then we will not find enough relations. If n is chosen too big, then there are too many relations, so that the linear system of equations becomes too complicated. The expected running time of the index calculus is $O(\exp(\sqrt{2\log(p)\log(\log(p))}))$, which means that it is a subexponential algorithm.

CHAPTER 4

Elliptic curves and cryptography

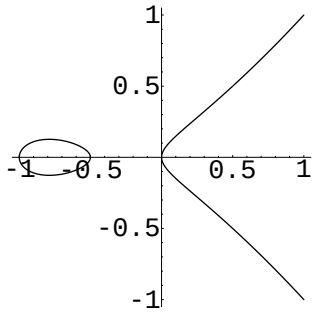
We start with two illustrative examples of elliptic curves. The first example arises from piling up cannonballs, or oranges perhaps, and the second by congruent numbers.
Suppose a collection of cannonballs is piled in a square pyramid with one ball on the top layer, four on the second layer, nine on the third layer, and so on. Can we rearrange the balls into a square array ? If the pyramid has height x, then there are

$$1^2 + 2^2 + \cdots + x^2 = \frac{x(x+1)(2x+1)}{6}$$

balls. We want this to be a perfect square, which means that we want to find an integer solution (x, y) to the equation $y^2 = x(x+1)(2x+1)/6$, or

$$y^2 = \frac{1}{3}x^3 + \frac{1}{2}x^2 + \frac{1}{6}x.$$

An equation of this type represents an *elliptic curve*. The graph of the real points of our curve looks as follows:



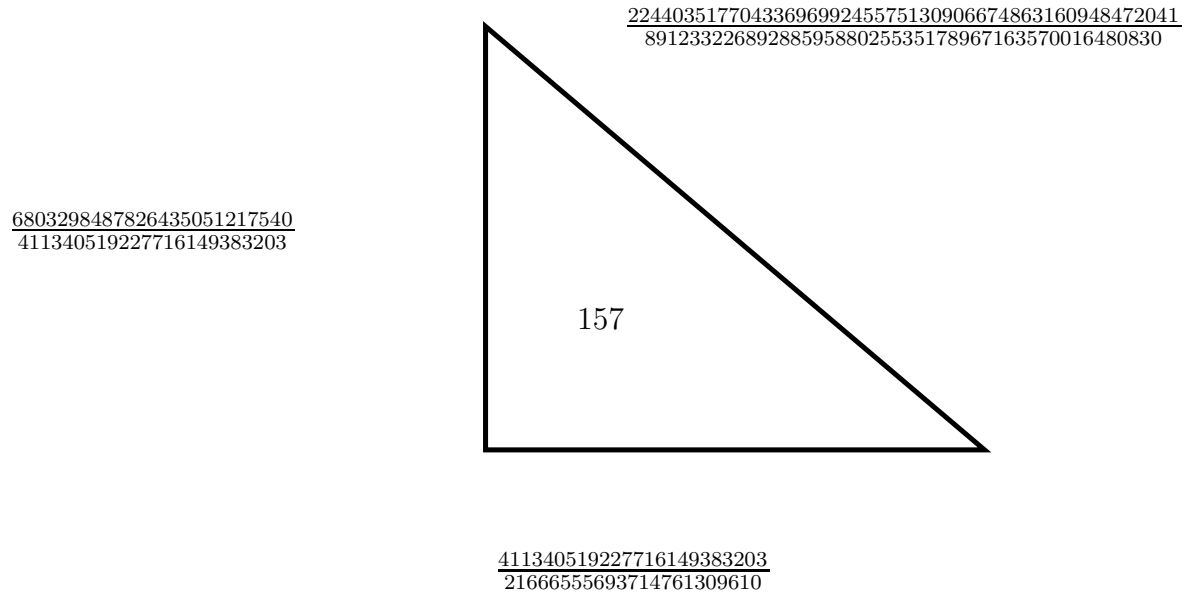
What are the integer points on this curve ? For trivial reasons, $P = (0, 0)$ and $Q = (1, 1)$ are on the curve. As we will see, we can add points, but the result will be a point with rational coordinates, in general. Indeed, $P + Q = (\frac{1}{2}, -\frac{1}{2})$. But $P + Q + Q = (24, -70)$ is an integer point, and because of the symmetry, also $(24, 70)$ lies on the curve. This means that

$$1^2 + 2^2 + \cdots + 24^2 = 70^2.$$

If we have 4900 cannonballs, in a pyramid of height 24, then we can rearrange them in a 70-by-70 square! It can be shown that this is the only non-trivial solution to our problem in positive integers. However, this requires more sophisticated techniques. By a famous result of *C.L. Siegel* we know that the set of integral points on an elliptic curve is always finite.

The second example comes from computing the area of right triangles with rational sides. A positive integer n is called *congruent*, if it is the area of a right triangle with rational sides. For example, if the sides (x, y, z) are $(3, 4, 5)$, then the area of the right triangle is 6. Hence 6 is a

congruent number. A less obvious example is $n = 157$. The simplest right triangle, in terms of number of digits, with area 157, looks as follows:



This example is due to Don Zagier. On the other hand, one can show that 1 is not a congruent number, because $x^4 + y^4 = z^4$ does not have a non-trivial integer solution. By definition, n is congruent, if there are rational numbers x, y, z such that

$$x^2 + y^2 - z^2 = 0 \tag{4.1}$$

$$xy - 2n = 0. \tag{4.2}$$

The first few congruent numbers less than 214 are as follows:

$$\begin{gathered}5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, 47,\\ 52, 53, 54, 55, 56, 60, 61, 62, 63, 65, 69, 70, 71, 77, 78, 79, 80, 84, 85, 86, 87, 88,\\ 92, 93, 94, 95, 96, 101, 102, 103, 109, 110, 111, 112, 116, 117, 118, 119, 120, 124,\\ 125, 126, 127, 133, 134, 135, 136, 137, 138, 141, 142, 143, 145, 148, 149, 150, 151,\\ 152, 154, 156, 157, 158, 159, 161, 164, 165, 166, 167, 173, 174, 175, 180, 181, 182,\\ 183, 184, 188, 189, 190, 191, 194, 197, 198, 199, 205, 206, 207, 208, 210, 212, 213.\end{gathered}$$

Of course, if n is congruent with (x, y, z), than d^2n is congruent with (dx, dy, dz). So we may assume that n is squarefree. Denote by E_n the elliptic curve defined by $y^2 = x^3 - n^2x$. There is the following surprising connection.

PROPOSITION 4.0.9. *A squarefree $n \in \mathbb{N}$ is congruent if and only if there is a rational point (x, y) on the elliptic curve E_n with $x = \pm r^2$ for some $r \in \mathbb{Q}^*$, and $\nu(x)$ even.*

Here $\nu(x)$ is the denominator of x. If $x = \frac{a}{b}$ with $(a, b) = 1$, then $\nu(x) = b$.

PROOF. The equations (4.1), (4.2) imply, forming the sum and the difference,

$$x^2 + 2xy + y^2 = z^2 + 4n$$
$$x^2 - 2xy + y^2 = z^2 - 4n.$$

This means that

$$\left(\frac{x+y}{2}\right)^2 = \left(\frac{z}{2}\right)^2 + n$$
$$\left(\frac{x-y}{2}\right)^2 = \left(\frac{z}{2}\right)^2 - n.$$

Multiplying these equations yields

$$\left(\frac{x^2-y^2}{4}\right)^2 = \left(\frac{z}{2}\right)^4 - n^2. \tag{4.3}$$

Substituting $u = \left(\frac{z}{2}\right)^2$ and $v = \frac{x^2-y^2}{4}\frac{z}{2}$ we obtain $v^2/u = u^2 - n^2$, i.e.,

$$v^2 = u^3 - un^2,$$

where $u, v \in \mathbb{Q}$. Note that $(u, v) \neq (0, 0)$, otherwise $u = 0$ and $z = 0$, hence $x^2 = y^2$ and $n = 0$ by (4.3), which is absurd. In fact, the elliptic curve

$$E_n \colon y^2 = x^3 - n^2x$$

has two other obvious rational points besides $(0, 0)$: namely $(\pm n, 0)$. It is clear that also $(u, v) \neq (\pm n, 0)$. □

EXAMPLE 4.0.10. *The elliptic curve* $E_5 \colon y^2 = x^3 - 25x$ *has a non-trivial solution* $(x, y) = (-4, 6)$*, hence* 5 *is congruent.*

Indeed, the right triangle given by $(x, y, z) = (\frac{20}{3}, \frac{3}{2}, \frac{41}{6})$ has area 5.

We will see that the rational points on an elliptic curve form an abelian group $E(\mathbb{Q})$ under addition of points, which is finitely generated, by a result of Mordell. We have $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$, where T is a finite torsion group and $r = \operatorname{rank} E(\mathbb{Q}) \geq 0$ is the *rank* of the elliptic curve. It is conjectured, that r can be arbitrarily large. By the time of writing the world record for r is $r = 28$. Elkies has found an elliptic curve of rank $r \geq 28$ in 2006:

$$\begin{aligned} y^2 + xy + y = x^3 - x^2 & \\ - 2006776241557552658503320820933854275093023031217895650 2x & \\ + 3448161179503055646703298569039072037485594435931918036 & \\ 126600829629193944873224342 9 & \end{aligned}$$

There are 28 independent rational points of infinite order on this curve. The "last one" given by

$$P_{28} = (2230868289773576023778678737,$$
$$2855876003059748566338702060076864002 8531).$$

Unfortunately, it is very difficult to compute the rank in general. There is no known algorithm guaranteed to determine the rank. It is not exactly known which positive integers can occur as the rank of an elliptic curve. There is the following result.

PROPOSITION 4.0.11. *A positive integer n is congruent if and only if the elliptic curve E_n over $\mathbb{Q}$ has positive rank.*

EXAMPLE 4.0.12. *The elliptic curve $E_1\colon y^2 = x^3 - x$ has rank 0. Hence $n = 1$ is not a congruent number.*

In fact, $E(\mathbb{Q}) = \{(0,0),(1,0),(-1,0),\infty\} = E(\mathbb{Q})_{\text{tors}}$. Fortunately there is a famous conjecture of Birch and Swinnerton-Dyer, offering considerable help concerning the rank.

CONJECTURE 4.0.13 (BSD). *For every elliptic curve over $\mathbb{Q}$ we have*

$$\operatorname{rank}(E) = \operatorname*{ord}_{s=1} L(E,s).$$

Here $L(E,s)$ is the Hasse-Weil L-function of E, a function of a complex variable s. Furthermore, $\operatorname{ord}_{s=1} L(E,s)$ is the order of vanishing of $L(E,s)$ at $s = 1$, the so called *analytic rank* of E.

EXAMPLE 4.0.14. *For the above curve $E_1\colon y^2 = x^3 - x$ we have*

$$L(E,1) = 0.65551438857302995... \neq 0.$$

Hence $\operatorname{rank}(E) = 0$.

The BSD-conjecture together with a result of Tunnell implies the following conjecture:

CONJECTURE 4.0.15. *Let n be an odd, squarefree, positive integer. Then $y^2 = x^3 - n^2x$ has more than 3 rational solutions, i.e., n is congruent, if and only if*

$$\#\{(a,b,c) \in \mathbb{Z}^3 \mid 2a^2 + b^2 + 8c^2 = n\}$$

equals

$$2\#\{(a,b,c) \in \mathbb{Z}^3 \mid 2a^2 + b^2 + 32c^2 = n\}.$$

In other words, n is congruent if and only if the number of integer solutions to $2a^2+b^2+8c^2 = n$ with c even equals the number of solutions with c odd. If $n = 2m$ with m odd, squarefree and positive, we have a similar criterion. Then n is congruent if and only if the number of integer solutions to $4a^2 + b^2 + 8c^2 = m$ with c even equals the number of integer solutions with c odd.

REMARK 4.0.16. Tunnell proved that **if** n is congruent, then the number of odd solutions equals the number of even solutions. However, for the converse one needs the BSD-conjecture, which is not yet proved.

EXAMPLE 4.0.17. *Let $n = 5$, or $n = 37$. Then there are no integer solutions, i.e., we have $0 = 0$ and the conjecture predicts that both numbers should be congruent.*

In this case the BSD-conjecture predicts interesting rational solutions of $y^2 = x^3 - 37^2x$. Indeed, we find

$$(x,y) = \left(\frac{28783225}{1764}, -\frac{154421605115}{74088}\right).$$

This can be used to construct a right triangle with rational sides (a,b,c) and area $n = 37$, i.e.,

$$a = \frac{777923}{6090}$$

$$b = \frac{450660}{777923}$$

$$c = \frac{605170417321}{4737551070}.$$

EXAMPLE 4.0.18. *If $n = 8k + 5$ then n should be congruent.*

Indeed, then again $0 = 0$ in the above conjecture. For example, $n = 157 = 19 \cdot 8 + 5$ should be congruent (and it is). But it is hard to find a right triangle with area 157, as we have seen.

EXAMPLE 4.0.19. *Show that $n = 34$ is a congruent number by finding a rational right triangle of area 34.*

In fact, with a little bit of trying we will find out that $P = (-2, 48)$ is a non-trivial integer point on the elliptic curve $E_n \colon y^2 = x^3 - n^2x$ for $n = 34$. Then the function

$$g(x, y) = \left(\frac{n^2 - x^2}{y}, -\frac{2xn}{y}, \frac{n^2 + x^2}{y} \right)$$

produces such a right triangle: $g(-2, 48) = (24, 17/6, 145/6)$.

PROPOSITION 4.0.20. *If E_n has a nontrivial rational point (i.e., with $y \neq 0$), then it has infinitely many rational points.*

COROLLARY 4.0.21. *A squarefree n is congruent if and only if E_n has infinitely many rational points.*

To give an example, consider $n = 6$. We list some rational right triangles $(a, b, c) = (a, 12/a, \sqrt{a^2 + b^2})$ with area $n = 6$, where a denotes the shortest side.

$$\begin{aligned}
(a, b, c) &= (3, 4, 5) \\
&= (\frac{7}{10}, \frac{120}{7}, \frac{1201}{70}) \\
&= (\frac{3404}{1551}, \frac{4653}{851120}, \frac{7776485}{1319901}) \\
&= (\frac{2017680}{1437599}, \frac{1437599}{168140}, \frac{2094350404801}{241717895860}) \\
&= (\frac{3122541453}{2129555051}, \frac{8518220204}{1040847151}, \frac{18428872963986767525}{2216541307731009701}) \\
&= (\frac{43690772126393}{20528380655970}, \frac{46340567871640}{43690772126393}, \frac{5405257799550679424342410801}{8969008013638393250900162 10}).
\end{aligned}$$

4.1. Plane curves

Elliptic curves are a special case of plane algebraic curves. An affine plane algebraic curve C over a field K is given by a polynomial equation $C\colon f(x,y)=0$ with some $0\neq f\in K[x,y]$. Denote by $\mathbb{A}^2_K$ the affine plane over K. For each extension field $L\supseteq K$ the the set of L-rational points of C is given by

$$\begin{aligned} C(L) &= \{P\in\mathbb{A}^2_K(L)\mid f_L(P)=0\}\\ &= \{(\alpha,\beta)\in L\times L\mid f(\alpha,\beta)=0\}. \end{aligned}$$

A *regular function on* $\mathbb{A}^2_K$ is given by a polynomial $f\in K[x,y]$. The ring of regular functions $K[x,y]$ on $\mathbb{A}^2_K$ is called the *affine coordinate ring* of $\mathbb{A}^2_K$. A *rational function* on $\mathbb{A}^2_K$ is given by some

$$f=\frac{g}{h}\in K(x,y),$$

where $K(x,y)$ is the quotient field of $K[x,y]$, called the *functional field* of $\mathbb{A}^2_K$. Such an f is called *regular in* $P=(\alpha,\beta)\in\mathbb{A}^2_K(L)$, if $h(\alpha,\beta)\neq 0$.

Example 4.1.1. *The unit circle over K is the plane curve defined by*

$$C\colon x^2+y^2-1=0.$$

For each $L\supseteq K$ the points $(0,\pm1)$ and $(\pm1,0)$ are L-rational points.

In fact, all L-rational points are given by

$$C(L)=\left\{\left(\frac{2t}{1+t^2},\frac{1-t^2}{1+t^2}\right)\mid t\in L, t^2\neq -1\right\}\cup\{(0,-1)\}.$$

Denote by $\mathbb{P}^2_K$ the projective plane over K. It has the property that all L-rational points of $\mathbb{P}^2_K$ are given by

$$\mathbb{P}^2_K(L)=\{(\alpha,\beta,\gamma)\in L^3\mid(\alpha,\beta,\gamma)\neq(0,0,0)\}/\sim_L$$

where the equivalence relation $\sim_L$ is given by

$$(\alpha,\beta,\gamma)\sim_L(\alpha',\beta',\gamma')$$

iff there is a $\lambda\in L^\times$ such that $(\alpha',\beta',\gamma')=(\lambda\alpha,\lambda\beta,\lambda\gamma)$. The point represented by (α,β,γ) is written as $(\alpha:\beta:\gamma)$. Obviously points in $\mathbb{P}^2_K$ correspond to lines through the origin in $\mathbb{A}^3_K$. An embedding $\mathbb{A}^2_K(L)\hookrightarrow\mathbb{P}^2_K(L)$ is given by $(\alpha,\beta)\mapsto(\alpha:\beta:1)$. Conversely, for $\gamma\neq0$ we have the map $(\alpha:\beta:\gamma)\mapsto(\alpha/\gamma,\beta/\gamma)\in\mathbb{A}^2_K(L)$. Hence $\mathbb{P}^2_K(L)$ consists of the points of $\mathbb{A}^2_K(L)$ and of the L-rational points at infinity on the line $z=0$.

Definition 4.1.2. A *projective plane curve* of degree d is given by an equation

$$C\colon f(x,y,z)=0$$

for some homogeneous polynomial $0\neq f\in K[x,y,z]$ of degree d.

The condition on f means that we can write $f=\sum_{r+s+t=d}a_{rst}x^ry^sz^t$. Let $C\colon f(x,y)=0$ be an affine curve and d be the total degree of f. Then

$$F(x,y,z)=z^df(\frac{x}{z},\frac{y}{z})$$

is a homogeneous polynomial of degree d. The associated projective curve $\overline{C}\colon F(x,y,z)=0$ is called the *projective closure* of C. The newly added points in $\overline{C}(L)\setminus C(L)$ are called *points at infinity*. Conversely, if $C\colon F(x,y,z)=0$ is a projective curve of degree d, then $f(x,y)=$

$F(x, y, 1)$ is a polynomial of degree $\leq d$, and the affine curve $C'\colon f(x, y) = 0$ is called the *affine part* of C.

EXAMPLE 4.1.3. *The projective closure of an affine line* $C\colon f(x, y) = ax + by - c = 0$ *is the projective line* $\overline{C}\colon F(x, y, z) = ax + by - cz = 0$.

It has exactly one point at infinity, i.e., $(-b : a : 0)$.

EXAMPLE 4.1.4. *The projective closure of the affine unit circle* $C\colon f(x, y) = x^2 + y^2 - 1 = 0$ *is* $F(x, y, z) = x^2 + y^2 - z^2 = 0$.

If -1 is a square in L, and $\mathrm{char}(L) \neq 2$, then there are two L-rational points at infinity: $(1 : i : 0)$ and $(1 : -i : 0)$. If $\mathrm{char}(L) = 2$, then there is only one point, namely $(1 : 1 : 0)$.

DEFINITION 4.1.5. Define an affine curve E by the *long Weierstraß equation*

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The projective closure is given by

$$\overline{E}\colon y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

The names of the constants $(a_1, a_2, a_3, a_4, a_6)$ have historial reasons. For $(a_1, a_2, a_3, a_4, a_6) = (0, 0, 0, a, b)$ we obtain the *short Weierstraß equation*

$$E\colon y^2 = x^3 + ax + b,$$

and its projective closure

$$\overline{E}\colon y^2z = x^3 + axz^2 + bz^3.$$

We mention the following theorem:

PROPOSITION 4.1.6 (Bézout). *Two projective curves* C_1, C_2 *of degree* d_1, *resp.* d_2 *intersect in* d_1d_2 *points, counted with multiplicities.*

DEFINITION 4.1.7. An affine curve $C\colon f(x, y) = 0$ is called *smooth* in the point $P = (\alpha, \beta) \in C(L)$, if $\left(\frac{\partial f}{\partial x}(\alpha, \beta), \frac{\partial f}{\partial y}(\alpha, \beta)\right) \neq (0, 0)$.

The curve C is called *smooth*, if it is smooth in all points $P \in C(\overline{K})$.

DEFINITION 4.1.8. A projective curve $C\colon F(x, y, z) = 0$ is called *smooth* in the point $P = (\alpha : \beta : \gamma) \in C(L)$, if

$$\left(\frac{\partial F}{\partial x}(\alpha, \beta, \gamma), \frac{\partial F}{\partial y}(\alpha, \beta, \gamma), \frac{\partial F}{\partial z}(\alpha, \beta, \gamma)\right) \neq (0, 0, 0).$$

EXAMPLE 4.1.9. *The affine curve* $C\colon y^2 = x^3 - x^2$ *is not smooth in the point* $P = (0, 0)$, *since* $\frac{\partial f}{\partial x} = 3x^2 - 2x$ *and* $\frac{\partial f}{\partial y} = 2y$ *vanish at* P.

Indeed, C has a double point at P.

EXAMPLE 4.1.10. *The projective curve* $C\colon y^2z - x^3 - z^3 = 0$ *is smooth, if* $\mathrm{char}(K) \neq 2, 3$.

Assume there would be a point $P = (\alpha : \beta : \gamma)$ where all three partial derivatives vanish. This would mean

$$-3\alpha^2 = 2\beta\gamma = \beta^2 - 3\gamma^2 = 0 \quad \Rightarrow \alpha = \beta = \gamma = 0,$$

in contradiction to the fact that it is impossible that all projective coordinates vanish. Note that the affine part is given by $C\colon y^2 = x^3 + 1$.

4.2. The basic theory of elliptic curves

DEFINITION 4.2.1. An *elliptic curve* over K is a smooth (projective) curve E of degree 3, given by the long Weierstraß equation, i.e.,

$$E\colon y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{4.4}$$

The affine part is given by the equation

$$E'\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4.5}$$

LEMMA 4.2.2. *E has exactly one point at infinity, namely $O = (0 : 1 : 0)$. This point is K-rational, and E is smooth in O.*

PROOF. For $z = 0$ the equation (4.4) reduces to $x^3 = 0$. Hence $O = (0 : 1 : 0)$ is the only possible point. Since the coordinates of O lie in K we have $O \in E(K)$. Furthermore E is smooth in O, since the partial derivative $\frac{\partial}{\partial z}$ is $y^2 + \cdots$ plus terms containing x or z, so that it does not vanish in O. □

REMARK 4.2.3. The tangent on E in O is the line $z = 0$ of points at infinity. It intersects E in O with multiplicity 3, i.e., O is an inflection point of E.

If the affine curve (4.5) is smooth, then it represents a curve, which we again call an *elliptic curve*. The short Weierstraß equation is then

$$E\colon y^2 = x^3 + ax + b. \tag{4.6}$$

LEMMA 4.2.4. *The affine curve* (4.5) *is smooth if and only if $\Delta \neq 0$, where*

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{aligned}$$

If E is given as in (4.6)*, then $\Delta = -16(4a^3 + 27b^2)$.*

Two elliptic curves are called *isomorphic*, if there are rational morphisms $\varphi\colon C \to D$ and $\psi\colon D \to C$ such that $\varphi \circ \psi = \mathrm{id}_{|D}$ and $\psi \circ \varphi = \mathrm{id}_{|C}$.

LEMMA 4.2.5. *Let E be an elliptic curve over K, given by* (4.5)*. If* $\mathrm{char}(K) \neq 2$*, then E is isomorphic to an elliptic curve of the form*

$$E'\colon y^2 = x^3 + c_2x^2 + c_4x + c_6.$$

If furthermore $\mathrm{char}(K) \neq 3$*, then E is isomorphic to an elliptic curve of the form* (4.6)*.*

PROOF. Indeed, we have an isomorphism $\Phi\colon E \to E'$ given by

$$\Phi((x : y : z)) = (2x : 2y + a_1x + a_3z : 2z)).$$

For the new coefficients we have

$$c_2 = a_2 + \frac{1}{4}a_1^2$$
$$c_4 = a_4 + \frac{1}{2}a_1a_3$$
$$c_6 = a_6 + \frac{1}{4}a_3^2.$$

For $3 \neq 0$ we can choose a suitable transformation of the form $(x, y) \mapsto (x + c_2/3, y)$ to obtain $c_2 = 0$ for the new equation. □

DEFINITION 4.2.6. Let E be an elliptic curve over K. Then $j = j(E) = c_4^3/\Delta$ is an invariant of E, called the *j-invariant*. If E is given by (4.6), then

$$j(E) = \frac{2^8 3^3 a^3}{4a^3 + 27b^2}.$$

Indeed, if E and E' are isomorphic, then $j(E) = j(E')$. If K is algebraically closed, then also the converse is true:

PROPOSITION 4.2.7. *Let E and E' be two elliptic curves over K. If $j(E) = j(E')$, then E and E' are isomorphic over $\overline{K}$. Moreover, for each $j \in K$ there exists an elliptic curve E over K with $j(E) = j$.*

PROOF. Suppose that $j(E) = j(E') = j$. If $j = 0$ then $c_4(E) = c_4(E') = 0$. Otherwise $j \neq 0$ and

$$\frac{c_6(E)^2}{c_4(E)^3} = \frac{c_6(E')^2}{c_4(E')^3}.$$

In both cases there exists a $u \in (\overline{K})^*$ with $c_4(E')u^4 = c_4(E)$ and $c_6(E')u^6 = c_6(E)$. Transforming E and E' into the short Weierstraß form, we may assume that

$$E\colon y^2 = x^3 - 27c_4(E)x - 54c_6(E)$$
$$E'\colon y^2 = x^3 - 27c_4(E')x - 54c_6(E'),$$

since after rescaling, the equation (4.6) may also be written

$$y^2 = x^3 - 27c_4x - 54c_6.$$

If the characteristic of K equals 2 or 3 this step is more complicated, but can be done similarly. Now $(x, y) \mapsto (u^2x, u^3y)$ is an isomorphismus of elliptice curves.
Finally, if $j \neq 0, 1728 = 12^3$ we can consider the elliptic curve

$$E\colon y^2 = x^3 - \frac{27}{4}\frac{j}{j - 1728}x - \frac{27}{4}\frac{j}{j - 1728}.$$

It has j-invariant equal to j. For $j = 0$ we consider the elliptic curve $y^2 = x^3 + 1$, which has j-invariant zero; and for $j = 12^3$, we may consider $y^2 = x^3 + x$. □

REMARK 4.2.8. If K is not algebraically closed, then we may have non-isomorphic elliptic curves with the same j-invariant. As an example, consider the family $E_d\colon y^2 = x^3 + d^2x + d^3$

of elliptic curves over $K = \mathbb{Q}$. Here two curves E_d and $E_{d'}$ are isomorphic if and only if d/d' is a square in $\mathbb{Q}$. However, all curves E_d have the same j-invariant:

$$j(E_d) = \frac{2^8 3^3 d^6}{4d^6 + 27d^6} = \frac{2^8 3^3}{31}.$$

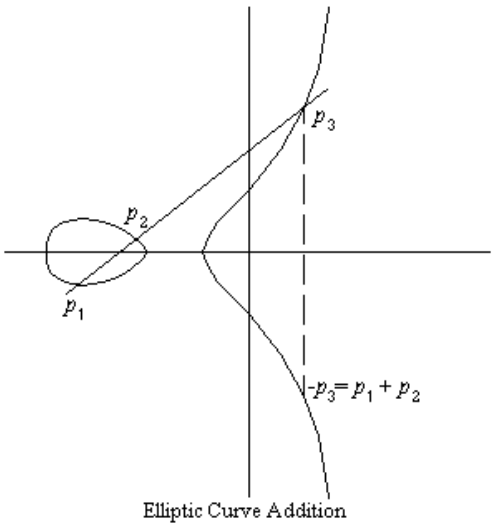
Let E be an elliptic curve over K and L be a field with $L \supseteq K$. Denote by $E(L)$ the L-rational points on E, including the point O. In the affine plane we may regard this point as (∞, ∞). Now we will define the structure of an abelian group on $E(L)$. This goes as follows. Consider the elliptic curve

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

PROPOSITION 4.2.9. *A structure of an abelian group on $E(L)$ is given as follows:*

(1) *The point $O \in E(L)$ is the zero element.*
(2) *Suposse that G is a line intersecting E in the points P, Q, R, allowing multiplicities. Then $P + Q + R = O$.*
(3) *In particular, the inverse of $P = (\alpha, \beta)$ is given by $-P := (\alpha, -\beta - a_1\alpha - a_3)$.*

PROOF. We will first show that (3) follows from (1) and (2). If E is given by (4.6), then we have just $-P = (\alpha, -\beta)$. In this case the following picture shows how this geometric addition looks like:



Elliptic Curve Addition

If $P = Q$, then we call this doubling.
Let $P = (\alpha, \beta)$ and $Q = (\alpha', \beta')$, and E in general form. The line G through P and O is given by $x = \alpha$, parallel to the y-axis. By definition the third point of intersection is given by $Q = -P$. We want to find the coordinates of this point. Intersecting E and G we obtain the equation, over $\overline{K}$

$$\begin{aligned} 0 &= y^2 + (a_1\alpha + a_3)y - (\alpha^3 + a_2\alpha^2 + a_4\alpha + a_6) \\ &= (y - \beta)(y - \beta'), \end{aligned}$$

for some β', since the quadratic equation in y over $\overline{K}$ must have two zeros, and we already now one intersection point on $E(K) \cap G$, i.e., $P = (\alpha, \beta)$. The second one, $Q = -P = (\alpha', \beta')$ we will compute now. Comparing coefficients above yields $\beta' = -\beta - a_1\alpha - a_3$ and $\alpha' = x = \alpha$.

Now we will derive algebraic formulas for the geometric addition, in terms of the coordinates $\alpha, \beta, \alpha', \beta'$: We may assume that $P + Q \neq O$. Then we claim that $P + Q = (\alpha'', \beta'')$, where

$$\alpha'' = \lambda^2 + a_1\lambda - a_2 - \alpha - \alpha' \tag{4.7}$$

$$\beta'' = -(\lambda + a_1)\alpha'' - \mu - a_3. \tag{4.8}$$

Here λ, μ are defined as follows: if $\alpha \neq \alpha'$, then

$$\lambda = \frac{\beta' - \beta}{\alpha' - \alpha}$$

$$\mu = \frac{\beta\alpha' - \beta'\alpha}{\alpha' - \alpha}.$$

If $\alpha = \alpha'$ then we have

$$\lambda = \frac{3\alpha^2 + 2a_2\alpha + a_4 - a_1\beta}{2\beta + a_1\alpha + a_3}$$

$$\begin{aligned}\mu &= \beta - \lambda\alpha \\ &= \frac{-\alpha^3 + a_4\alpha + 2a_6 - a_3\beta}{2\beta + a_1\alpha + a_3}.\end{aligned}$$

The proof goes as follows: let $\alpha \neq \alpha'$. The line G through P and Q is given by

$$y = \lambda x + \mu.$$

Since P and Q lie on G we have

$$\begin{aligned}\beta &= \lambda\alpha + \mu, \\ \beta' &= \lambda\alpha' + \mu,\end{aligned}$$

so that $\lambda(\alpha' - \alpha) = \beta' - \beta$, and hence

$$\mu = \beta - \lambda\alpha = \frac{\beta\alpha' - \beta'\alpha}{\alpha' - \alpha}.$$

For $\alpha = \alpha'$ and $Q \neq -P$ we have $P = Q$. Then also $\beta' = \beta$. In this case G is tangent on E at P. We will compute λ by an limiting argument. Suppose P and Q are very close together, but different. Since they both lie on E we have

$$\begin{aligned}\beta^2 + a_1\alpha\beta + a_3\beta &= \alpha^3 + a_2\alpha^2 + a_4\alpha + a_6, \\ (\beta')^2 + a_1\alpha'\beta' + a_3\beta' &= (\alpha')^3 + a_2(\alpha')^2 + a_4\alpha' + a_6,\end{aligned}$$

so that, multiplying crosswise,

$$\frac{\beta' - \beta}{\alpha' - \alpha} = \frac{(\alpha')^2 + \alpha'\alpha + \alpha^2 + a_2(\alpha + \alpha') + a_4 - a_1\beta'}{\beta + \beta' + a_1\alpha + a_3}.$$

Taking the limit $\beta' \to \beta$ and $\alpha' \to \alpha$ we obtain the above formulas for λ and μ.

Now substitute the equation for G into the one for E, to eliminate y:

$$\begin{aligned}0 &= x^3 - (\lambda^2 + a_1\lambda - a_2)x^2 - (2\lambda\mu + a_1\mu + a_3\lambda - a_4)x - (\mu^2 + a_3\mu - a_6) \\ &= (x - \alpha)(x - \alpha')(x - \alpha'')\end{aligned}$$

over $\overline{K}$. Then, by Vieta,

$$\alpha + \alpha' + \alpha'' = \lambda^2 + a_1\lambda - a_2,$$

which means $\alpha'' = \lambda^2 + a_1\lambda - a_2 - \alpha - \alpha'$ as claimed in (4.7). Computing β'' as the image of α'' we obtain (4.8).

It remains to show that geometric addition satisfies the group laws. The commutativity is obvious, either from the formulas or from the fact that the line through P and Q is the same as the line through Q and P. Indeed, everything is obvious except for the associativity. This property is non-obvious. In fact, it is rather surprising that such a law of composition that we have defined is associative. We may verify this by calculations with the formulas. There are several cases, depending on whether or not $P = Q$, and whether or not $R = (P + Q)$ etc., to show that $(P + Q) + R = P + (Q + R)$. This makes the proof rather messy. If we assume the short Weierstraß form, it will be slightly better. Nevertheless there are other proofs which are more elegant, see [**8**]. □

COROLLARY 4.2.10. *If E is given by (4.6), then the formulas simplify as follows: let $P = (\alpha, \beta)$ and $Q = (\alpha', \beta')$. Then*

$$P + Q = (\lambda^2 - \alpha - \alpha', -\lambda(\lambda^2 - \alpha - \alpha') - \mu),$$

where

$$\begin{aligned}\lambda &= \frac{3\alpha^2 + a}{2\beta}, \text{ if } \alpha = \alpha', \beta \neq -\beta',\\ &= \frac{\beta' - \beta}{\alpha' - \alpha}, \text{ if } \alpha \neq \alpha',\\ \mu &= \beta - \lambda\alpha.\end{aligned}$$

If $\beta' + \beta = 0$ and $\alpha = \alpha'$ then $P + (-P) = (\alpha, \beta) + (\alpha, -\beta) = O$.

EXAMPLE 4.2.11. *Let $E\colon y^2 = x^3 - 43x + 166$. Then $P = (3, 8) \in E(\mathbb{Q})$ is a rational point and $E(\mathbb{Q}) \cong \mathbb{Z}/7\mathbb{Z}$.*

Indeed, $2 \cdot P = P + P = (-5, -16)$ by the formulas, with $\alpha = \alpha' = 3$, $\beta = \beta' = 8$, $\lambda = -1$, $\mu = 8+1\cdot 3 = 11$. Furthermore $3\cdot P = (11, -32)$, $4\cdot P = (11, 32)$, $5\cdot P = (-5, 16)$, $6\cdot P = (3, -8)$ and $7 \cdot P = O$. Note that P generates $E(\mathbb{Q})$.

EXAMPLE 4.2.12. *Let $E\colon y^2 = x^3 + x + 1$. Then $E(\mathbb{Q}) \cong \mathbb{Z}$ with generator $P = (0, 1)$.*

We compute

$$\begin{aligned}P &= (0, 1)\\ 2P &= (\frac{1}{4}, -\frac{9}{8})\\ 3P &= (72, 611)\\ 4P &= (-\frac{287}{1296}, \frac{40879}{46656})\\ 5P &= \left(\frac{43992}{82369}, -\frac{30699397}{23639903}\right)\end{aligned}$$

Without the group law it would not be so easy to find such rational points on E. The discriminant of E is $-2^4 \cdot 31$. For $p \neq 2, 31$ we obtain an elliptic curve over $\mathbb{F}_p$. For small primes p the group $E(\mathbb{F}_p)$ is often cyclic, but not always. In general, for each $k \in \mathbb{N}$ there exist

infinitely many primes p such that $E(\mathbb{F}_p)$ contains a subgroup of the form $\mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$. Here is a small list:

$$
\begin{aligned}
E(\mathbb{F}_3) &= \langle (0,1) \rangle = \mathbb{Z}/4\mathbb{Z} \\
E(\mathbb{F}_5) &= \langle (0,1) \rangle = \mathbb{Z}/9\mathbb{Z} \\
E(\mathbb{F}_7) &= \langle (0,1) \rangle = \mathbb{Z}/5\mathbb{Z} \\
E(\mathbb{F}_{11}) &= \langle (1,5) \rangle = \mathbb{Z}/14\mathbb{Z} \\
E(\mathbb{F}_{13}) &= \langle (1,4) \rangle = \mathbb{Z}/18\mathbb{Z} \\
E(\mathbb{F}_{17}) &= \langle (0,1) \rangle = \mathbb{Z}/18\mathbb{Z} \\
E(\mathbb{F}_{19}) &= \langle (0,1) \rangle = \mathbb{Z}/21\mathbb{Z} \\
E(\mathbb{F}_{23}) &= \langle (0,1) \rangle = \mathbb{Z}/28\mathbb{Z} \\
E(\mathbb{F}_{29}) &= \langle (8,12) \rangle = \mathbb{Z}/36\mathbb{Z} \\
E(\mathbb{F}_{37}) &= \langle (6,1) \rangle = \mathbb{Z}/48\mathbb{Z} \\
E(\mathbb{F}_{47}) &= \langle (0,1) \rangle = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}
\end{aligned}
$$

It is known that the group $E(\mathbb{F}_q)$ is always either cyclic or isomorphic to $\mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\ell\mathbb{Z}$ for some $k, \ell \in \mathbb{N}$.

4.3. Elliptic curves over finite fields

Let $\mathbb{F}_q$ denote the finite field with $q = p^n$ elements. Then the group $E(\mathbb{F}_q)$ is finite. Various properties of this group, for example, its order, turn out to be important. Two main restrictions on the group $E(\mathbb{F}_q)$ are given in the next two theorems:

THEOREM 4.3.1. *Let E be an elliptic curve over $\mathbb{F}_q$. Then*

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z} \quad \text{or} \quad E(\mathbb{F}_q) \cong \mathbb{Z}/r\mathbb{Z} \oplus \mathbb{Z}/s\mathbb{Z}$$

for some integer $n \geq 1$, or for some integers $r, s \geq 1$ with $r \mid s$.

THEOREM 4.3.2 (Hasse, 1922). *Let E be an elliptic curve over $\mathbb{F}_q$ and let $N = \#E(\mathbb{F}_q)$. Then*

$$|q + 1 - N| \leq 2\sqrt{q}.$$

For a proof, see for example chapter 4 in [**9**]. It uses a result on torsion points, namely those whose orders are finite. We set

$$E[n] = \{P \in E(\overline{K}) \mid nP = O\}.$$

The result is as follows:

PROPOSITION 4.3.3. *Let E be an elliptic curve over K and $n \in \mathbb{N}$. If* $\mathrm{char}(K) \nmid n$, *or if* $\mathrm{char(K)} = 0$ *then*

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

If $\mathrm{char(K)} = p > 0$ *and $p \mid n$, write $n = p^r m$ with $p \nmid m$. Then*

$$E[n] \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}, \quad \text{or} \quad \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

Concerning the size of N above it is trivial to see that $N \leq 2q + 1$: there are at most $2q$ points $(x, y) \in \mathbb{F}_q$ satisfying $y^2 = f(x)$, and the point O. In fact, we would expect N to be approximately $\frac{1}{2} \cdot 2 \cdot q + 1 = q + 1$, since there is a 50% chance that the value of $f(x) = x^3 + ax + b$ is a square in $\mathbb{F}_q^*$. Indeed, it is easy to see that

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + ax + b}{q} \right),$$

where (x/q) generalizes the Legendre symbol, i.e.,

$$\left(\frac{x}{q}\right) = \begin{cases} +1 & \text{if } t^2 = x \text{ has a solution } t \in \mathbb{F}_q^*, \\ -1 & \text{if } t^2 = x \text{ has no solution } t \in \mathbb{F}_q^*, \\ 0 & \text{if } x = 0. \end{cases}$$

EXAMPLE 4.3.4. *Let $E\colon y^2 = x^3 + x + 1$. Then $\#E(\mathbb{F}_5) = 9$.*

Indeed, the nonzero squares modulo 5 are 1 and 4, so that

$$\begin{aligned} \#E(\mathbb{F}_5) &= 5 + 1 + \sum_{x=0}^{4} \left(\frac{x^3 + x + 1}{5} \right) \\ &= 6 + \left(\frac{1}{5}\right) + \left(\frac{3}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{4}{5}\right) \\ &= 9. \end{aligned}$$

Another natural question then is what groups can actually occur as groups $E(\mathbb{F}_q)$. The following two results give an answer. For references, see [**9**].

PROPOSITION 4.3.5. *Let $q = p^n$ be a prime power and let $N = q+1-a$. There is an elliptic curve E defined over $\mathbb{F}_q$ such that $\#E(\mathbb{F}_q) = N$ if and only if $|a| \leq 2\sqrt{q}$ and $a \in \mathbb{Z}$ resp. p and n satisfy one of the following conditions:*

(1) $(a, p) = 1$.
(2) *n is even and* $a = \pm 2\sqrt{q}$.
(3) *n is even,* $p \not\equiv 1 \mod 3$, *and* $a = \pm\sqrt{q}$.
(4) *n is odd,* $p = 2$ *or* $p = 3$, *and* $a = \pm p^{(n+1)/2}$.
(5) *n is even,* $p \not\equiv 1 \mod 4$, *and* $a = 0$.
(6) *n is odd and* $a = 0$.

PROPOSITION 4.3.6. *Let N be an integer that occurs as some $\#E(\mathbb{F}_q)$, as specified in the above proposition. Write $N = p^e n_1 n_2$ with $p \nmid n_1 n_2$ and $n_1 \mid n_2$, where $n_1, n_2 \geq 1$. There is an elliptic curve E over $\mathbb{F}_q$ such that*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/p^e\mathbb{Z} \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$$

if and only if

(a) *$n_1 \mid (q-1)$ in cases (1), (3), (4), (5), (6) above.*
(b) *$n_1 = n_2$ in case (2) above.*

These are the only groups that occur as groups $E(\mathbb{F}_q)$.

Note that $E(\mathbb{Z}/rs\mathbb{Z}) \simeq E(\mathbb{Z}/r\mathbb{Z}) \oplus E(\mathbb{Z}/s\mathbb{Z})$ for coprime integers r and s, so that the statement does not contradict theorem 4.3.1.

Let E be defined over $\mathbb{F}_q$, and let $(x, y) \in E(\overline{\mathbb{F}_q})$. The *Frobenius map* is the function $\tau_q \colon E(\overline{\mathbb{F}_q}) \to E(\overline{\mathbb{F}_q})$ given by $\tau_q(x, y) = (x^q, y^q)$ and $\tau_q(O) = O$. One has to verify, of course, that $\tau_q(x, y) \in E(\overline{\mathbb{F}_q})$. We have $(x, y) \in E(\mathbb{F}_q)$ if and only if $\tau_q = \mathrm{id}$. By an *endomorphism* of E, we mean a homomorphism $\varphi \colon E(\overline{K}) \to E(\overline{K})$ that is given by rational functions.

LEMMA 4.3.7. *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then τ_q is an endomorphism of E, and $\ker(\tau_q^m - \mathrm{id}) = E(\mathbb{F}_{q^m})$ for each $m \geq 1$.*

Let $a = q + 1 - \#E(\mathbb{F}_q)$.

PROPOSITION 4.3.8. *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then*

$$\tau_q^2 - a\tau_q + q \cdot \mathrm{id} = 0$$

as endomorphisms of E.

In other words, if $(x, y) \in E(\overline{\mathbb{F}_q})$, then

$$(x^{q^2}, y^{q^2}) - a \cdot (x^q, y^q) + q \cdot (x, y) = O.$$

Moreover, a is the unique integer such that this relation holds for all $(x, y) \in E(\overline{\mathbb{F}_q})$. This a, or more precisely a_q, is called the trace of the Frobenius, and the polynomial $t^2 - a_q t + q$ is often called the characteristic polynomial of Frobenius. Hasse's theorem says that $|a_q| \leq 2\sqrt{q}$.

Let us denote the number of points on E over $\mathbb{F}_{q^n}$ by

$$N_n = \#E(\mathbb{F}_{q^n}).$$

What are the relations between the numbers $N_1, N_2, N_3, \ldots$? In this context it is interesting to consider the following object.

DEFINITION 4.3.9. Let E be a smooth projective curve over $\mathbb{F}_q$. The *zeta function of* E is the following power series in t with rational coefficients,

$$Z(E,t) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n}{n} t^n\right).$$

Here E need not be an elliptic curve (but in our context often is one). The presence of the exponential function will turn out to be of advantage.

PROPOSITION 4.3.10. *Let E be an elliptic curve defined over $\mathbb{F}_q$, and let $N_1 = q + 1 - a$. Then*

$$Z(E,t) = \frac{qt^2 - at + 1}{(1-t)(1-qt)}.$$

More generally we have the following result:

PROPOSITION 4.3.11. *Let E be a smooth projective curve over $\mathbb{F}_q$. Then $Z(E,t) \in \mathbb{Q}(t)$ is a rational function, and*

$$Z(E,t) = \frac{p(t)}{(1-t)(1-qt)}$$

with a polynomial $p(t)$, which factorizes over $\mathbb{C}$ as

$$p(t) = \sum_{j=1}^{g} (1 - \alpha_j t)(a - \overline{\alpha_j} t)$$

with $|\alpha_j| = \sqrt{q}$. Here g denotes the genus of E.

If E is an elliptic curve, then $g = 1$. Let $\zeta_E(s) = Z(E, q^{-s})$. It makes sense to name this the zeta function of E, instead of $Z(E,t)$. In fact, $\zeta_E(s)$ can be regarded as an analogue of the classical Riemann zeta function $\zeta(s)$ (it also has an analogous functional equation).

COROLLARY 4.3.12. *Let E be a smooth projective curve defined over $\mathbb{F}_q$. Then $\zeta_E(1-s) = q^{(g-1)(2s-1)}\zeta_E(s)$, and $\zeta_E(s)$ satisfies the analogue of the Riemann Hypothesis: if $\zeta_E(s) = 0$, then $\Re(s) = \frac{1}{2}$.*

REMARK 4.3.13. There is also a zeta function of higher-dimensional projective varieties over finite fields. Weil had predicted analogous results for these zeta functions. Rationality was first proved by Dwork in 1960. The functional equation was proved afterwards by Artin, Grothedieck, and Verdier, and the analogue of the Riemann Hypothesis was proved by Deligne in 1973. He also gave a new proof of rationality using ℓ-adic cohomology for $\ell \neq p$. Much of Grothendieck's algebraic geometry was developed for the purpose of proving these "Weil conjectures".

4.4. Elliptic curve cryptography

There are several cryptosystems which can also be based on elliptic curves, such as, for example, the DLP for elliptic curves. One might wonder why elliptic curves are used in crytography. One reason is, as we said, that elliptic curves provide security equivalent to classical systems while using fewer bits. For example, the key size of 4096 bits for RSA gives the same level of security as 313 bits in an elliptic curve system. This means that implementations of elliptic curves cryptosystems require smaller ship size and less power consumption. We start with the Diffie-Hellman problem, which originally appeared in the context of multiplicative groups $\mathbb{F}_q^*$ of finite fields.

Diffie-Hellman Key Exchange:

1. Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$ such that the DLP is hard in $E(\mathbb{F}_q)$. They also agree on a point $P \in E(\mathbb{F}_q)$ such that the subgroup generated by P has large (prime) order.

2. Alice chooses a secret integer a, computes $P_a = aP$, and sends P_a to Bob.

3. Bob chooses a secret integer b, computes $P_b = bP$, and sends P_b to Alice.

4. Alice computes $aP_b = (ab)P$.

5. Bob computes $bP_a = (ba)P$.

6. Alice and Bob use some publicly agreed method to extract a key from abP.

The only information that the eavesdropper Eve sees is the curve E, the finite field $\mathbb{F}_q$, and the points P, aP, bP. She therefore needs to solve the

Diffie-Hellman Problem: Given P, aP, bP in $E(\mathbb{F}_q)$, compute abP.

If Eve can solve the the DLP in $E(\mathbb{F}_q)$, then she can use P and aP to find a, which enables her to compute $a(bP) = abP$. However, it is not known whether there is some *other* way to compute abP, without first solving a DLP. On the other hand it is believed that the Diffie-Hellman Problem and the DLP are equivalent, in complexity-theoretic sense.

ElGamal Public Key Encryption:

Alice wants to send a message to Bob. First, Bob establishes his public key as follows. he chooses an elliptic curve E over $\mathbb{F}_q$ such that the DLP is hard in $E(\mathbb{F}_q)$. Then he chooses a point P on E (such that $\text{ord}(P)$ is a large prime), and chooses a secret integer s and computes $B = sP$. Bob's public key consists of the quadruple $(E, \mathbb{F}_q, P, B)$. Bob's private key is s. To send a message to Bob, Alice does the following:

1. She downloads Bob's public key.

2. She expresses her message as a point $M \in E(\mathbb{F}_q)$.

3. She chooses a secret random integer k and computes $M_1 = kP$.

4. She computes $M_2 = M + kB$.

5. She sends M_1, M_2 to Bob.

Bob decrypts by calculating $M = M_2 - sM_1$. This really works because we have

$$\begin{aligned} M_2 - sM_1 &= (M + kB) - s(kP) \\ &= M + k(sP) - skP = M. \end{aligned}$$

The eavesdropper Eve Bob's public information and the points M_1, M_2. If she could solve the DLP, she could use P, B to find out s, which she could then use to decrypt the message $M = M_2 - kB$. On the other hand, there does not appear to be any other way to find M for Eve.

There is of course a lot more to say on this topic. We refer to the book [**2**] on elliptic curves in cryptography.

4.5. Factoring and Primality testing using elliptic curves

In the mid 1980s, H. Lenstra developed an efficient factoring algorithm that used elliptic curves. It is called "elliptic curve factorization method", usually referred to as ECM. Recall that the main advantage of elliptic curves here stems from the fact that there are many elliptic curves modulo n (see 2.10 in [**9**] for elliptic curves over rings), so if one elliptic curve does not work, another can be tried. We start with an example.

EXAMPLE 4.5.1. *We want to factor* $n = 4453$ *using the elliptic curve* $y^2 = x^3 + 10x - 2 \mod 4453$ *and* $P = (1, 3)$.

We need to use elliptic curves over rings R which are not necessarily fields. In this case it is also possible to define the structure of an abelian group on

$$E(R) = \{(x : y : z) \in \mathbb{P}^2(R) \mid y^2z = x^3 + axz^2 + bz^3\},$$

where $\mathbb{P}^2(R)$ is the projective space over R, under mild conditions on R. If E is an elliptic curve over $R = \mathbb{Z}/(n_1n_2)\mathbb{Z}$ with $(n_1, n_2) = (2, n_1) = (2, n_2) = 1$, then there is a group homomorphism

$$E(\mathbb{Z}/(n_1n_2)\mathbb{Z}) \cong E(\mathbb{Z}/n_1\mathbb{Z}) \oplus E(\mathbb{Z}/n_2\mathbb{Z}).$$

In our example, let us try to compute $3P$. First, we compute $2P$. Since $(6, 4453) = 1$ we find, using the extended Euclidean algorithm, that $6^{-1} = 3711 \mod 4453$. The slope of the tangent line at P is

$$\frac{3x^2 + 10}{2y} = \frac{13}{6} \equiv 3713 \mod 4453.$$

Then $2P = (x, y)$ with

$$x \equiv 3713^2 - 2 \equiv 4332,$$
$$y \equiv -3713(x - 1) - 3 \equiv 3230.$$

Now, to obtain $3P$ we add P and $2P$. The slope is

$$\frac{3230 - 3}{4332 - 1} = \frac{3227}{4331}.$$

But 4331^{-1} does not exist modulo 4453 since $(4331, 4453) = 61 \not\equiv 1$. We cannot evaluate the slope - however, we have found the factor 61 of 4453, so that

$$4453 = 61 \cdot 73.$$

Here is the elliptic curve factorization method (which is related to the classical $p - 1$ method of Pollard):

1. Choose several (usually around 10 to 20) random elliptic curves $E_i \colon y^2 = x^3 + a_ix + b_i \mod n$ and points P_i.

2. Choose an integer B (perhaps around 10^8) and compute the points $(B!)P_i$ on E_i for each i.

3. If 2. fails because some slope does not exist modulo n, then we have found a factor of n.

4. If 2. is successful, increase B or choose new random elliptic curves E_i and points P_i, and start over.

ECM is very successful in finding a prime factor p of n when $p < 10^{40}$. In cryptographic applications we often have $n = pq$ with both p and q large primes. Why does ECM work ?

Assume, for simplicity, $n = pq$. A random elliptic curve modulo n can be regarded as an elliptic curve mod p and an elliptic curve mod q. By Hasse's theorem,

$$p + 1 - 2\sqrt{p} < \#E(\mathbb{F}_p) < p + 1 + 2\sqrt{p}.$$

In fact, each integer in the interval $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ occurs for some elliptic curve. If B is of reasonable size, then the density of B-smooth integers (we say that m is B-smooth if all of the prime factors of m are less or equal to B) in this interval is high enough, and the distribution of orders $\#E(\mathbb{F}_p)$ of random elliptic curves is sufficiently uniform. Therefore, if we choose several random elliptic curves, at least one will probably have B-smooth order. In particular, if P lies on this curve E, then it is likely that $(B!)P = O \mod p$, and unlikely that $(B!)P = O \mod q$ for the corresponding point P on $E \mod q$. Therefore, when computing $(B!)P = O \mod p$, we expect to obtain a slope whose denominator is divisible by p but not by q. The gcd of this denominator with n then yields the factor p (if the denominator is also divisible by q then the gcd equals n and we have not found a factor).

The following elliptic curve primality test is an elliptic curve version of the classical Pocklington-Lehmer primality test. The latter one is based on the following result.

PROPOSITION 4.5.2. *Let $n > 1$ be an integer, and let $n - 1 = rs$ such that $r \geq \sqrt{n}$. Suppose that, for each prime $\ell \mid r$, there exists an integer a_ℓ with*

$$a_\ell^{n-1} \equiv 1 \mod n$$
$$(n, a_\ell^{\frac{n-1}{\ell}} - 1) = 1.$$

Then n is prime.

PROOF. Let p be a prime factor of n and let ℓ^e be the highest power of ℓ dividing r. Let $b \equiv a_\ell^{\frac{n-1}{\ell^e}} \mod p$. Then

$$b^{\ell^e} \equiv a_\ell^{n-1} \equiv 1 \mod p,$$
$$b^{\ell^{e-1}} \equiv a_\ell^{\frac{n-1}{\ell}} \not\equiv 1 \mod p,$$

by the second assumption. It follows that $\mathrm{ord}_p(b) = \ell^e$. The order of $E(\mathbb{Z}/p\mathbb{Z})$ equals $p - 1$, so that $\ell^e \mid p - 1$. Since this is true for every prime power factor ℓ^e of r, we have $r \mid p - 1$. In particular, $p > r \geq \sqrt{n}$. But then n cannot be composite, otherwise there would be a prime divisor p of n with $p \leq \sqrt{n}$. Hence n is prime. □

EXAMPLE 4.5.3. *Let $n = 153533$. Then $n - 1 = 4 \cdot 131 \cdot 293$. Choose $r = 4 \cdot 131$. The primes $\ell \mid r$ are $\ell = 2$ and $\ell = 131$. Then the hypothesis of the above proposition is satisfied with $a_2 = a_{131} = 2$, so that 153533 is prime.*

Indeed we have

$$2^{n-1} \equiv 1 \mod n, \quad (2^{\frac{n-1}{2}} - 1, 2) = 1,$$
$$2^{n-1} \equiv 1 \mod n, \quad (2^{\frac{n-1}{131}} - 1, 2) = 1.$$

The following version of this test for elliptic curves is due to Goldwasser and Kilian. Recall that a *finite point* in $E(\mathbb{Z}/n\mathbb{Z})$ is a point (x, y) with $x, y \in \mathbb{Z}/n\mathbb{Z}$ (not all points can be expressed using coordinates in $\mathbb{Z}/n\mathbb{Z}$).

PROPOSITION 4.5.4. *Let $n > 1$ and let E be an elliptic curve mod n. Suppose that there exist k distinct primes $\ell_1, \ldots, \ell_k$ and finite points $P_i \in E(\mathbb{Z}/n\mathbb{Z})$ such that*

$$\ell_i P_i = O, \quad 1 \leq i \leq k,$$

$$\prod_{i=1}^{k} \ell_i > (n^{\frac{1}{4}} + 1)^2.$$

The n is prime.

PROOF. Let $p \mid n$ be a prime factor. Write $n = p^e m$ with $p \nmid m$. Then

$$E(\mathbb{Z}/n\mathbb{Z}) = E(\mathbb{Z}/p^e\mathbb{Z}) \oplus E(\mathbb{Z}/m\mathbb{Z}).$$

Since P_i is a finite point in $E(\mathbb{Z}/n\mathbb{Z})$, it follows that $P_i \mod p^e$ is a finite point in $E(\mathbb{Z}/p^e\mathbb{Z})$. Consider the point $P_{i,p} := P_i \mod p$ in $E(\mathbb{F}_p)$, which is also finite. Since $\ell_i P_i = O \mod n$, we have $\ell_i P_i = O \mod t$ for every factor $t \mid n$. In particular, $\ell_i P_{i,p} = O$ in $E(\mathbb{F}_p)$, which means that $P_{i,p}$ has order ℓ_i. Hence

$$\ell_i \mid \#E(\mathbb{F}_p) \; \forall \, i,$$

hence $\prod_i \ell_i \mid \#E(\mathbb{F}_p)$. Therefore

$$\begin{aligned}(n^{\frac{1}{4}} + 1)^2 &< \prod_{i=1}^{k} \ell_i \\ &\leq \#E(\mathbb{F}_p) \\ &< p + 1 + 2\sqrt{p} = (p^{\frac{1}{2}} + 1)^2,\end{aligned}$$

so that $p > \sqrt{n}$. We obtain that all prime factors of n are greater than $\sqrt{n}$, so that n is prime. □

EXAMPLE 4.5.5. *Let $n = 907$ and choose $E\colon y^2 = x^3 + 10x - 2 \mod n$, $\ell = 71$ and $P = (819, 784)$. Then the hypothesis of the test is satisfied, so that 907 is prime.*

Indeed, $\ell = 71 > (907^{\frac{1}{4}} + 1)^2 \simeq 42.1$ and $71P = O$ on E.

For large n, the hardest part of this test is finding an elliptic curve E with a suitable number of points. There is a procedure, due to Atkin and Morain, which uses the theory of complex multiplication to find suitable curves.

Bibliography

[1] M. Agrawal, N. Kayal, N. Saxena: *PRIMES is in P.* Ann. of Math. (2) **160** (2004), no. 2, 781–793.

[2] I. Blake, G. Seroussi, N. Smart: *Elliptic curves in Cryptography.* LMS Lecture Note Series **265** (2000).

[3] T. ElGamal: *A public key cryptosystem and a signature scheme based on discrete logarithms.* Adv. in Cryptology, Springer-Verlag (1985).

[4] J.P. Jones, Hideo Wada, Daihachiro Sato and Douglas Wiens: *Diophantine representation of the set of prime numbers.* Amer. Math. Monthly **83** (1976), 449-464.

[5] R. A. Mollin: *An Introduction to Cryptography.* Chapman and Hall (2007).

[6] R. L. Rivest, A. Shamir, L. Adleman: *A method for obtaining digital signatures and public-key cryptosystems.* Comm. ACM **21** (1978), 120-126.

[7] M. I. Rosen, *A proof of the Lucas-Lehmer test.* Amer. Math. Monthly **95** No. 9, (1988), 855–856.

[8] J. H. Silverman, *The arithmetic of elliptic curves.* Corrected reprint of the 1986 original. Graduate Texts in Mathematics, **106** (1992). Springer-Verlag, New York.

[9] L. Washington: *Elliptic curves: Number theory and cryptography.* Chapman & Hall, 2003.

[10] D. Zagier: *Newman's short proof of the prime number theorem.* Amer. Math. Monthly **104**, No. 8 (1997), 705-708.