Théorie des nombres et applications à la cryptographie

Semestre d'été 2013

Université du Luxembourg

Gabor Wiese
gabor.wiese@uni.lu

Version du 5 juillet 2013

Préface

La théorie des nombres est une des disciplines les plus anciennes en mathématiques. Très récemment, elle a trouvé des applications (inattendues) en cryptographie et elle est utilisée quotidiennement par chacun et chacune (souvent sans le savoir).
Ce cours introduit des concepts de base de la théorie élémentaire des nombres, la plus importante étant la réciprocité quadratique. Il contient aussi un traitement du théorème des nombres premiers. Coté applications, RSA, El Gamal, Diffie-Hellman et des tests de primalité sont étudiés.
Le cours sera enseigné en français, mais les notes seront multilingues car elles sont partiellement basées sur des cours enseignés en anglais.

Ces notes sont basées sur :

- Notes d'un cours de Gebhard Böckle donné à l'Universität Duisburg-Essen.
- Notes d'un de mes cours à l'Universität Duisburg-Essen.
- Notes du cours « Courbes algébriques et applications à la cryptographie » donné par Sara Arias-de-Reyna et moi-même à l'université du Luxembourg au semestre d'été 2012.
- Freitag, Busam. *Funktionentheorie*, Springer-Verlag (pour le traitement du théorème des nombres premiers).

Littérature

Voici quelques références : Quelques'uns des livres devraient être ou devenir disponibles dans la bibliothèque au Kirchberg pendant le semestre en cours.

- William Stein. *Elementary Number Theory : Primes, Congruences, and Secrets*, Springer-Verlag. Ce livre est disponible gratuitement sur
  `http ://modular.math.washington.edu/ent/ent.pdf`
  Il est très bien pour le début du cours.
- Siegfried Bosch : *Algebra* (en allemand), Springer-Verlag. Ce livre sur l'algèbre est très complet et bien lisible.
- Serge Lang : *Algebra* (en anglais), Springer-Verlag. C'est comme une encyclopédie de l'algèbre ; on y trouve beaucoup de sujets rassemblés, écrits de façon concise.
- Perrin. *Cours d'algèbre*, Ellipses
- Guin, Hausberger. *Algèbre I. Groupes, corps et théorie de Galois*, EDP Sciences
- Johannes Buchmann. *Einführung in die Kryptographie*, Springer-Verlag
- Albrecht Beutelspacher. *Moderne Verfahren der Kryptographie : Von RSA zu Zero-Knowledge*, Vieweg+Teubner Verlag
- Albrecht Beutelspacher. *Kryptologie : Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen. Ohne alle Geheimniskrämerei...*, Vieweg+Teubner Verlag
- Christof Paar, Jan Pelzl, Bart Preneel. *Understanding Cryptography : A Textbook for Students and Practitioners*, Springer-Verlag
- Jeffrey Hoffstein, Jill Pipher, J.H. Silverman. *An Introduction to Mathematical Cryptography*, Springer-Verlag
- Neal Koblitz. *A Course in Number Theory and Cryptography*, Springer-Verlag

– Neal Koblitz, A.J. Menezes, Y.-H. Wu, R.J. Zuccherato. *Algebraic Aspects of Cryptography : With an Appendix on Hyperelliptic Curves*, Springer-Verlag

Contents

1 Some aspects of elementary number theory

The purpose of this first section is to survey the most basic concepts from elementary number theory. All students (should) have seen them before, but, it cannot hurt to recall them.
The way we present elementary number theory here is that its most fundamental concept is that of Euclid's algorithm. In fact, almost all that comes works for Euclidean rings, which have probably been treated in one of your algebra courses.

Theorem 1.1 (Euclid, Bézout). *Let $a, b \in \mathbb{Z}$ not both zero. Then* Euclid's algorithm *computes the greatest common divisor d of a, b, notation $d = \gcd(a, b)$, that is:*

- $d \geq 1$,
- $d \mid a$, $d \mid b$,
- *for any $e \geq 1$ such that $e \mid a$ and $e \mid b$, one has $e \mid d$.*

Moreover, the extended Euclid's algorithm *gives $r, s \in \mathbb{Z}$ such that*

$$d = ar + bs.$$

In French this is called identité de Bézout.

The proof is completely algorithmic. The algorithm is practiced in an exercise on Sheet 1.

Definition 1.2. *An integer $p \geq 2$ is called a* prime number *if its only positive divisors are 1 and p.*

Theorem 1.3 (Gauß; fundamental theorem of elementary number theory). *Any $n \in \mathbb{N}$, $n \geq 2$, can be written as a finite product of prime numbers: There is $r \in \mathbb{N}$ and there are prime numbers $p_1, \dots, p_r$ such that*

$$n = p_1 \cdot p_2 \cdots p_r.$$

Up to renumbering, the prime numbers occuring in the product are unique, that is: if $n = q_1 \cdot q_2 \cdots q_s$ is another such product, then $r = s$ and there is σ in the symmetric group on the letters $\{1, \dots, r\}$ such that $q_i = p_{\sigma(i)}$ for all $i \in \{1, \dots, r\}$.

We are going to prove this theorem. The proof is not as trivial as one might guess. It essentially uses the extended Euclid's algorithm. The existence part, however, is completely straight forward:

Proof of existence in Theorem 1.3. Let $n \geq 2$. By induction we prove the following statement:

> There are finitely many prime numbers $p_1, \dots, p_r$ such that $n = p_1 \cdot p_2 \cdots p_r$.

Since $n = 2$ is obviously a prime number, the statement for $n = 2$ is true. Let us now suppose we have proved the statement for all integers up to $n - 1$. We prove it for n. First case: n is a prime number. Then the statement is obviously true. Second case: $n = ab$ with $1 < a < n$. We know that we can write a and b both as finite products of prime numbers, hence, the statement for n follows. □

Definition 1.4. *Let R be a ring. By $R^\times$ we denote the set of units of R, i.e. the elements $x \in R$ such that there is $y \in R$ with $1 = xy$.*
An element $0 \neq p \in R \setminus R^\times$ is called a prime element of R *if, whenever p divides a product ab with $a, b \in R$, then p divides one of the factors, i.e. $p \mid a$ or $p \mid b$.*

Lemma 1.5. *Let R be a ring and $p \in R$ a prime element. If p divides a product $r_1 r_2 \cdots r_s$ with $r_i \in R$, then p divides one of the factors, i.e. there is $i \in \{1, \dots, s\}$ such that $p \mid r_i$.*

Proof. Iterated application of the definition. □

The next lemma shows that prime numbers and prime elements in $\mathbb{Z}$ are essentially the same.

Lemma 1.6. *Let $p \geq 2$ be an integer. Then*

$$p \text{ is a prime number } \Leftrightarrow \ p \text{ is a prime element in } \mathbb{Z}.$$

Proof. '⇒': Let $a, b \in \mathbb{Z}$ and suppose $p \mid ab$. If $p \mid a$, then we are done. So assume $p \nmid a$. Since the only positive divisors of p are 1 and p and p does not divide a, it follows that $1 = \gcd(a, p)$. Hence, there are $x, y \in \mathbb{Z}$ such that $1 = ax + py$. Multiply this equation by b and get: $b = abx + py$. As p divides ab by assumption and obviously p divides py, it follows that p divides b, as was to be shown.
'⇐': Suppose $p = ab$ with positive integers a, b. Then, as p is a prime element in $\mathbb{Z}$, it follows $p \mid a$ or $p \mid b$. Consequently, $a \geq p$ or $b \geq p$, thus $a = p$ or $b = p$, showing that p is a prime number. □

Proof of uniqueness in Theorem 1.3. We again prove this by induction on n. The case $n = 2$ is obvious. Let us suppose that we have proved the statement for all positive integers up to $n - 1$. Now consider n. We have, thus, prime numbers $p_1, \dots, p_r$ and $q_1, \dots, q_s$ such that

$$n = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s.$$

By Lemmas 1.6 and 1.5 it follows that the prime number p_1 is a prime element which divides one of the q_i (for $i \in \{1, \dots, s\}$), since it divides the product $q_1 \cdot q_2 \cdots q_s$. As q_i is a prime number, too, we must have $p_1 = q_i$. Dividing both sides by p_1, we obtain

$$n/p_1 = p_2 \cdot p_3 \cdots p_r = q_1 \cdot q_2 \cdots q_i \cdot q_{i+1} \cdots q_s.$$

As we already know the statement for n/p_1, we are done. □

Also the following famous theorem is based on the extended Euclid's algorithm.

Theorem 1.7 (Chinese Remainder Theorem)**.** *Let $n, m \in \mathbb{N}$ such that $\gcd(n, m) = 1$. Then the map*

$$\Phi : \mathbb{Z}/(nm) \to \mathbb{Z}/(n) \times \mathbb{Z}/(m), \quad a + (nm) \mapsto \big(a + (n), a + (m)\big)$$

is an isomorphism of rings.

Proof. The homomorphism property is easily checked.
Injectivity: Suppose $a \in \mathbb{Z}$ is in (n) and in (m). This means that $n \mid a$ and $m \mid a$. As $\gcd(n, m) = 1$, it follows $nm \mid a$, which means $a \in (nm)$, showing the injectivity.

Surjectivity: As $\gcd(n,m)=1$, there are $x,y\in\mathbb{Z}$ such that $1=nx+my$. We just have to interpret this equation in the right way. It means that $N:=nx=1-my$ satisfies:

$$N\equiv 0 \mod (n) \text{ and } N\equiv 1 \mod (m).$$

In the same way we have that $M:=my=1-nx$ satisfies:

$$M\equiv 0 \mod (m) \text{ and } M\equiv 1 \mod (n).$$

Let $b,c\in\mathbb{Z}$ and consider $\big(b+(n),c+(m)\big)\in\mathbb{Z}/(n)\times\mathbb{Z}/(m)$. Then $a:=bM+cN$ is an element such that

$$a\equiv b \mod (n) \text{ and } a\equiv c \mod (m),$$

i.e. $\Phi(a+(nm))=\big(b+(n),c+(m)\big)$, showing the surjectivity. □

Definition 1.8. *Let $n\geq 1$ be an integer. Let*

$$\varphi(n)=|\big(\mathbb{Z}/(n)\big)^{\times}|,$$

the order of the unit group of the ring $\mathbb{Z}/(n)$, that is, the number of units of $\mathbb{Z}/(n)$. One calls φ Euler's totient function (or: Euler's φ-function).

Lemma 1.9. *Let $n=p_1^{e_1}\cdot p_2^{e_2}\cdots p_r^{e_r}$ be the factorisation of n into prime powers with pairwise distinct prime numbers $p_1,\dots,p_r$.*
Then $\varphi(n)=(p_1-1)p_1^{e_1-1}\cdot(p_2-1)p_2^{e_2-1}\cdot(p_r-1)p_r^{e_r-1}$.

Proof. By the Chinese Remainder Theorem 1.7 it suffices to prove $\varphi(p^e)=(p-1)p^{e-1}$ for any prime number p.
In fact, it turns out to be easier to count non-units in $\mathbb{Z}/(p^e)$ instead of counting units. The non-units in $\mathbb{Z}/(p^e)$ are precisely the classes $a+(p^e)$ such that $p\mid a$, that is, $0,p,2p,\dots,(p^{e-1}-1)p$. So, there are p^{e-1} non-units. Hence, $\varphi(p^e)=p^e-p^{e-1}=p^{e-1}(p-1)$. □

Now we need to recall one elementary statement from group theory.

Theorem 1.10 (Lagrange). *Let G be a finite group and $H\leq G$ a subgroup. Denote by $(G:H)$ the index of H in G and by $|G|$ (and $|H|$) the order of G (and H). Then*

$$|G|=|H|\cdot(G:H).$$

Proof. Let us denote by $\circ$ the group operation. As abbreviation write $r=(G:H)$. Then by definition there are r cosets, say, $g_1\circ H,g_2\circ H,\dots,g_rH\circ$ such that

$$G=g_1\circ H\sqcup g_2\circ H\sqcup\cdots\sqcup g_r\circ H,$$

where the symbol $\sqcup$ means 'disjoint union'. Now note that

$$H\to g_i\circ H,\quad x\mapsto g_i\circ x$$

defines a bijection, so that the number of elements of H and $g_i\circ H$ are equal. Thus, $|G|=r|H|$. □

Corollary 1.11. *Let G be a finite group and $g \in G$ an element. The* order $\operatorname{ord}(g)$ *is the smallest positive $n \in \mathbb{Z}$ such that $e = g^n$ (that is, $\underbrace{g \circ g \circ \cdots \circ g}_{n\text{-times}}$), where e is the neutral element in G. Denote by $\langle g \rangle$ the smallest subgroup of G containing g.*
Then $\operatorname{ord}(g) = |\langle g \rangle|$ divides $|G|$ and $g^{|G|} = e$.

Proof. Let $H = \langle g \rangle$. We obviously have $|H| = \operatorname{ord}(g)$. Hence, Theorem 1.10 gives $\operatorname{ord}(g)$ divides $|G|$, say, $|G| = \operatorname{ord}(g) \cdot m$ for some $m \geq 1$. Then

$$g^{|G|} = g^{\operatorname{ord}(g)\cdot m} = \left(g^{\operatorname{ord}(g)}\right)^m = e^m = e,$$

finishing the proof. □

Corollary 1.12 ('Little Fermat'). *Let p be a prime number. We write $\mathbb{F}_p$ for the finite field $\mathbb{Z}/(p)$. (Never use this piece of notation if p is not a prime power!). Let $m \in \mathbb{Z}$ be an integer such that $m \equiv 1 \mod (p-1)$.*
Then for any $x \in \mathbb{F}_p$ one has: $x^m = x$ (equality in $\mathbb{F}_p$).

Elements in $\mathbb{Z}/(p)$ are residue classes, so $x \in \mathbb{Z}/(p)$ is of the form $a + (p)$ for some $a \in \mathbb{Z}$. One, thus, often formulates the corollary in terms of congruences: For any $a \in \mathbb{Z}$, the congruence

$$a^m \equiv a \mod (p)$$

holds if $m \equiv 1 \mod (p-1)$.

Proof. The group of units of $\mathbb{F}_p$ has order $p-1$ as the only non-unit is (the class of) 0. Let $0 \neq x \in \mathbb{F}_p$. By Corollary 1.11, $x^{p-1} = 1$. We have $m = 1 + (p-1)r$ for some $r \in \mathbb{Z}$. Thus:

$$x^m = x^{1+(p-1)r} = x \cdot x^{(p-1)r} = x \cdot \left(x^{p-1}\right)^r = x \cdot 1^r = x.$$

For $x = 0$ we obviously also have $x^m = 0^m = 0 = x$. □

Corollary 1.13. *Let $p_1, p_2, \ldots, p_r$ be pairwise distinct prime numbers and put $n = p_1 \cdot p_2 \cdots p_r$. Let $m \equiv 1 \mod (\varphi(n))$.*
Then for any $x \in \mathbb{Z}/(n)$ one has: $x^m = x$ (equality in $\mathbb{Z}/(n)$).

Proof. Exercise on Sheet 1. □

2 RSA

In this section, we introduce one of the main cryptographic algorithms that are currently in use: the RSA-algorithm, named after Ron Rivest, Adi Shamir and Leonard Adleman. Each of you probably uses this algorithm several times a day (maybe, without knowing it).
There are three people in the set-up:

- Alice: She wants to send a message to Bob.
- Bob: He wants to get a message from Alice.
- Eve: She wants to know what Alice writes to Bob, but, of course, Alice and Bob want to avoid this.

Bob’s preparation step

- Bob chooses two distinct (random) prime numbers p and q.
- Bob computes (multiplications):
$$n := p \cdot q, \quad \varphi(n) = (p-1) \cdot (q-1).$$
- Bob chooses a random $1 < e < \varphi(n)$ such that $\gcd(e, \varphi(n)) = 1$.
- Bob uses the extended Euclid’s algorithm in order to compute s such that
$$es \equiv 1 \mod (\varphi(n)).$$
For that, Bob computes $s, t \in \mathbb{Z}$ such that $1 = se + t\varphi(n)$.
- Bob publishes n and e (for example, on his webpage, in the phone book).
n is called the *modulus* and e the *public key*.
- Bob keeps s top secret.
s is called the *secret key*.

Alice’s message encryption

We assume here that Alice’s message is an integer m such that $0 \leq m \leq n-1$. In an exercise on Sheet 2, you will show how to transform a text message into a sequence of such numbers. In fact, on Sheet 2, you show how to turn a sentence (or a text) into some positive integer M. However, the integer M might be bigger than n. In that case, what one does is to write M in its n-adic expansion, i.e.
$$M = \sum_{i=0}^{s} m_i n^i \text{ with } 0 \leq m_i \leq n-1.$$
Like this one breaks the message M up into the pieces $m_0, \ldots, m_s$ and one encrypts (and decrypts) each piece separately. But, as already said, for the sake of simplicitiy of the exposition, we suppose that the message only consists of one single piece $0 \leq m \leq n-1$.

- Alice looks up Bob’s (n, e) (e.g. in the phone book).
- Alice computes $M := m^e \mod (n)$; we can take $0 \leq M \leq n-1$. The computation can be done by fast exponentiation, see exercise on Sheet 2.
- Alice sends M to Bob.

Bob's message decryption

Bob receives the message M from Alice.

- Bob computes $N := M^s \mod (n)$ with $0 \leq M \leq n-1$. That computation can again be done by fast exponentiation.

  He finds $N = m$ because:

  $$M^s = \big(m^e\big)^s = m^{es} \equiv m \mod (n)$$

  by Corollary 1.13.

Eve's problem

Eve knows the following:

- Bob's (n, e) (she can look them up in the phone book, too).
- The encrypted message M (because she was eavesdropping – secretly listening; that's why she's called Eve).

If Eve can compute the prime factors p and q of n, then she can decrypt the message very easily:

- Like Bob, she computes $\varphi(n) = (p-1)(q-1)$.
- Like Bob, she uses the extended Euclid's algorithm in order to compute s such that

  $$es \equiv 1 \mod (\varphi(n)).$$

  Now she know the secret key s, too!
- Like Bob, she decrypts the message by computing $N := M^s \mod (n)$, which is, of course, m again.

So, one has to prevent Eve from being able to factor n. This one does, in practice, by choosing p and q very big, e.g. of size around 2^{2048}, so that p and q have each more than 600 decimal digits. Then the currently best known algorithms for factoring n would be too slow to yield a result in less than a couple of millions of years.
Of course, one does not know whether there is not a much faster algorithm. This insecurity, one has to live with.

3 Finite fields

If p is a prime number, then $\mathbb{F}_p := \mathbb{Z}/(p)$ is a finite field with p elements. But, these are not the only ones. In fact, in this part of the lecture we are going to establish that for each prime power p^n there is a finite field having p^n elements, called $\mathbb{F}_{p^n}$, and up to isomorphism these are the only finite fields. It is very important to remember that $\mathbb{F}_{p^n} \neq \mathbb{Z}/(p^n)$, as soon as $n > 1$ (for instance, in $\mathbb{Z}/(p^n)$ the equality $0 = pp^{n-1}$ shows that $0 \neq p$ is a non-unit, but in fields all non-zero elements are units).

First we treat the example of the finite field with 4 elements in order to show that there are other finite fields than $\mathbb{F}_p$ with p a prime. Consider $f(X) := X^2 + X + 1 \in \mathbb{F}_2[X]$. It is an irreducible polynomial. This one can check by testing that it does not have any zeros in $\mathbb{F}_2$: $f(0) = 1 \neq 0$ and $f(1) = 1 \neq 0$ (always remember that this way of testing irreducibility is only valid for polynomials of degrees 2 and 3, since from degree 4 onwards, a polynomial f could factor as $f = gh$ with both g and h having no zero). We recall the notation $(f(X))$ for the principal ideal generated by $f(X)$, which consists of all multiples of $f(X)$.
We put $K := \mathbb{F}_2[X]/(X^2 + X + 1)$. We represent its elements as

$$\overline{0} := 0 + (f), \overline{1} := 1 + (f), \overline{X} := X + (f), \overline{1 + X} := 1 + X + (f).$$

It is very simple to write down the addition and the multiplication table explicitly (we did this in the lecture). It becomes obvious that every element of K different from $\overline{0}$ has a multiplicative inverse. As we already know from the general theory of quotient rings that K is a ring, the existence of the multiplicative inverses shows that K is a field. It has 4 elements and is denoted $\mathbb{F}_4$.

Definition 3.1. *Let R be a commutative ring. If there is a positive integer m such that*

$$\underbrace{1_R + 1_R + \cdots + 1_R}_{m \text{ times}} = 0_R$$

in R (where for the sake of clarity we write 0_R (resp. 1_R) for the neutral element of addition (resp. multiplication) of R – we shall not do this at any other place), then the characteristic of *R is defined to be the minimum such m.*
If no such m exists, then we say that R has characteristic 0.

Example 3.2. *$\mathbb{Q}$ has characteristic 0 and for a prime number p, the finite field $\mathbb{F}_p$ has characteristic p. The characteristic of $\mathbb{F}_4$ is 2 (this is clear).*

Proposition 3.3. *Let R be an integral domain (e.g. a field). Then the characteristic is either 0 or a prime number.*

Proof. Suppose the characteristic of R is $m > 0$ and $m = ab$ with $1 < a, b < m$. Then

$$0 = \underbrace{1 + 1 + \cdots + 1}_{m \text{ times}} = (\underbrace{1 + 1 + \cdots + 1}_{a \text{ times}}) \cdot (\underbrace{1 + 1 + \cdots + 1}_{b \text{ times}}).$$

As R is an integral domain, it follows $\underbrace{1 + 1 + \cdots + 1}_{a \text{ times}} = 0$ or $\underbrace{1 + 1 + \cdots + 1}_{b \text{ times}} = 0$ and both contradicts the minimality of m. □

We are now going to construct many more finite fields in a more conceptual way. Our approach is a generalisation of our construction of $\mathbb{F}_4$. The key is – again – the extended Euclid's algorithm, now applied in the polynomial ring.

Theorem 3.4 (Euclid, Bézout). *Let K be a field and let $f(X), g(X) \in K[X]$ not both zero. Then* Euclid's algorithm *computes the greatest common divisor $d(X)$ of $f(X), g(X)$, notation $d(X) = \gcd(f(X), g(X))$, that is:*

- *$d(X) \neq 0$ is monic (i.e. highest coefficient equal to 1),*
- *$d(X) \mid f(X)$, $d(X) \mid g(X)$,*
- *for any $e(X) \neq 0$ such that $e(X) \mid f(X)$ and $e(X) \mid g(X)$, one has $e(X) \mid d(X)$.*

Moreover, the extended Euclid's algorithm *gives $r(X), s(X) \in K[X]$ such that*

$$d(X) = f(X)r(X) + g(X)s(X).$$

The proof is again completely algorithmic.
We presented the theorem about Euclid's algorithm in $\mathbb{Z}$ and $K[X]$ in a completely analogous manner. In fact, most of the theory can be developed for all rings, in which one has a Euclidean division (i.e. a division with remainder). Such rings are called *Euclidean rings*. You may or may not have seen them in your algebra classes. In this lecture we just need $\mathbb{Z}$ and the polynomial ring over a field, so we will not go into Euclidean rings in general. On Exercise Sheet 3, you will prove an analogue of Gauß' fundamental theorem of elementary number theory for $K[X]$ (the general statement, which you may have seen, is: Every Euclidean ring is a unique factorisation domain.).
We start with a simple, but extremely useful consequence:

Lemma 3.5. *Let K be a field and $f(X) \in K[X]$ be a non-zero polynomial. Then the following statements hold:*

(a) Suppose there is $\alpha \in K$ such that $f(\alpha) = 0$ (such α is called a zero *or a* root *of f). Then there is a polynomial $g(X) \in K[X]$ such that*

$$f(X) = (X - \alpha)g(X).$$

(b) $f(X)$ has at most $\deg(f)$ many zeros.

(c) Let $f'(X)$ be the formal derivative of $f(X)$; that is, for $f(X) = \sum_{i=0}^{n} a_i X^i$, we let $f'(X) = \sum_{i=1}^{n} a_i i X^{i-1}$. If $f(X) = g(X)h(X)^2$ with $g(X), h(X) \in K[X]$ non-zero polynomials, then $h(X)$ divides the $\gcd(f(X), f'(X))$.

Proof. (a) We use Euclidean division:

$$f(X) = q(X) \cdot (X - \alpha) + r(X),$$

where the rest $r(X)$ has degree strictly smaller than the degree of the divisor $(X - \alpha)$, whence the degree of $r(X)$ is 0. Thus, $r(X) = c$ is a constant polynomial. Now, we plug in α for X and obtain:

$$0 = f(\alpha) = q(\alpha) \cdot (\alpha - \alpha) + c = 0 + c = c,$$

showing that the rest $r(X)$ is zero, so that $(X - \alpha)$ divides f.
(b) follows by induction from (a).
(c) It is easily checked that the Leibniz rule holds for the formal derivative (see Exercise on Sheet 4):

$$f'(X) = g'(X)h(X)^2 + 2g(X)h'(X)h(X) = h(X)\big(g'(X)h(X) + 2g(X)h'(X)\big),$$

showing that $h(X)$ divides $f'(X)$ and thus it divides the greatest common divisor of $f(X)$ and $f'(X)$.
□

We now turn to the construction of finite fields. The fundamental result is the following, which we first phrase in some generality and then specialise to finite fields in the corollary.

Proposition 3.6. *Let K be a field and $f \in K[X]$ an irreducible polynomial of degree $n > 0$. Then $K[X]/(f(X))$ is a field. Its elements can be represented as*

$$\overline{\sum_{i=0}^{n-1} a_i X^i} := (\sum_{i=0}^{n-1} a_i X^i) + (f(X)) \text{ with } a_0, a_1, \dots, a_{n-1} \in K.$$

Proof. We already know that $K[X]/(f(X))$ is a ring. Now we show that every non-zero element has a multiplicative inverse. Let $g + (f(X)) \in K[X]/(f(X))$ be a non-zero element. Being non-zero means that $g(X) + (f(X)) \neq 0 + (f(X))$, which is equivalent to $g(X) \notin (f(X))$, which is the same as g not being a multiple of f, i.e. $f(X)$ does not divide $g(X)$.
It follows that the greatest common divisor of $f(X)$ and $g(X)$ is equal to 1, whence there are $r(X), s(X) \in K[X]$ such that

$$1 = f(X)r(X) + g(X)s(X).$$

Taking residue classes in $K[X]/(f(X))$ we obtain

$$\overline{1} = 1 + (f(X)) = \big(g(X) + (f(X))\big)\big(s(X) + (f(X))\big) = \overline{gs},$$

exhibiting the desired inverse of $\overline{g} = g(X) + (f(X))$.
The representatives listed in the assertion are just the remainders for division by f. □

Corollary 3.7. *Let p be a prime number and $f \in \mathbb{F}_p[X]$ an irreducible polynomial of degree $n = \deg(f) > 0$.*
Then $\mathbb{F}_p[X]/(f(X))$ is a finite field having p^n elements, which can be represented as

$$\overline{\sum_{i=0}^{n-1} a_i X^i} := (\sum_{i=0}^{n-1} a_i X^i) + (f(X)) \text{ with } 0 \leq a_0, a_1, \dots, a_{n-1} \leq p - 1.$$

Proof. In view of the previous proposition, this is clear. □

Now we have a big supply of finite fields – under the assumption that there are many irreducible polynomials in $\mathbb{F}_p[X]$. It is possible to give a brute force proof that for every $n \in \mathbb{N}$, there is an irreducible monic polynomial $f(X) \in \mathbb{F}_p[X]$ of degree n. This can be done by counting the number of reducible monic polynomials of degree n and observing that this number is smaller than p^n (which is the total number of monic polynomials of degree n), so that there must at least be one irreducible monic polynomial. We will, however, go a slightly smarter way, which uses the notion of a splitting field of a polynomial.
The central role in the construction of the field with p^n elements is played by the polynomial $X^{p^n} - X \in \mathbb{F}_p[X]$. For $n > 1$ it is not irreducible, so we cannot apply the previous corollary. Instead, we will take its splitting field. Although splitting fields may be known to you from a course in algebra, we shall construct them here again (in a quick and concise way).

Theorem 3.8. *Let K be a field and $f(X) \in K[X]$ a monic polynomial of degree n. Then there is a field L satisfying the following properties:*

(1) $K \subseteq L$.

(2) There are $\alpha_1, \dots, \alpha_n \in L$ such that (in $L[X]$):

$$f(X) = (X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n).$$

(3) If $K \subseteq L_1 \subseteq L$ and L_1 satisfies (1) and (2), then $L = L_1$ (i.e. L is the smallest field containing K, over which $f(X)$ factors into a product of linear polynomials).

The field L is called the splitting field (corps de décomposition, Zerfällungskörper) of f.

Proof. We show the following assertion by induction on n.

> For every field K and every monic polynomial $f(X) \in K[X]$ of degree at most n, there is a field L such that
>
> (I) $K \subseteq L$.
>
> (II) There are $\alpha_1, \dots, \alpha_n \in L$ such that (in $L[X]$):
>
> $$f(X) = (X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n).$$

If $n = 1$, then f is already linear and $L = K$ trivially satisfies (I) and (II).
Now assume that the assertion has been established for all polynomials of degrees up to $n - 1$. We now want to establish it for the polynomial $f \in K[X]$ of degree n. For this, we distinguish two cases:
f is reducible: In this case, we factor $f(X) = g(X)h(X)$ with $g(X), h(X) \in K[X]$ of degrees strictly less than n. From the induction hypothesis applied for $g(X) \in K[X]$ we deduce the existence of a field L_1 satisfying (I) and (II). We apply the induction hypothesis again for $h(X) \in L_1[X]$ (we can, of course, view $h(X)$ as a polynomial of $L_1[X]$ because K is a subfield of L_1) and obtain a field L satisfying (I) and (II) (for the polynomial $h(X)$). We have $L \supseteq L_1 \supseteq K$, showing (I) for $f \in K[X]$. Moreover, it is clear that $f(X)$ factors into linear factors over $L[X]$ because the roots of $g(X)$ lie in $L_1 \subseteq L$ and those of $h(X)$ lie in L.
f is irreducible: From Proposition 3.6 we know that $L_1 := K[X]/(f(X))$ is a field. It contains K (the classes of the constant polynomials) and the class $\alpha := \overline{X} = X + (f(X))$ is a zero of $f(X) \in L_1[X]$. To see this, let us write $f(X) = \sum_{i=0}^{n} a_i X^i$. Then:

$$f(\overline{X}) = \sum_{i=0}^{n} a_i \overline{X}^i = \sum_{i=0}^{n} a_i \big(X + (f(X))\big)^i = \sum_{i=0}^{n} a_i X^i + (f(X)) = f(X) + (f(X))$$
$$= 0 + (f(X)) = \overline{0}.$$

(Note the small ambiguity in the notation: $a = a + (f(x)) = \overline{a}$ for $a \in K$.) Hence, over $L_1[X]$ we have $f(X) = (X - \alpha)g(X)$ with $g(X) \in L_1[X]$ of degree $n - 1$. This allows us to apply the induction hypothesis for $g(X) \in L_1[X]$, yielding a field $L \supseteq L_1 \supseteq K$ over which $g(X)$ factors as a product of linear polynomials. Consequently, over L the polynomial $f(X)$ factors into a product of linear polynomials, establishing the assertion for n.

We now prove the theorem. The above assertion gives us a field M satisfying (1) and (2). We now want to show that there is a field L for which (3) also holds. This is very easy. Namely, it suffices to let L be the smallest subfield of M which contains $\alpha_1, \dots, \alpha_n$. □

We are now ready for the construction of a finite field with p^n elements.

Proposition 3.9. *Let p be a prime number and $n \in \mathbb{N}_{>0}$. Consider $f(X) = X^{p^n} - X \in \mathbb{F}_p[X]$. Then the splitting field L of $f(X)$ over $\mathbb{F}_p$ is a finite field with p^n elements.*

Proof. As L is the splitting field, there are elements $\alpha_1, \dots, \alpha_{p^n} \in L$ such that $f(X) = \prod_{i=1}^{p^n}(X - \alpha_i)$. By Lemma 3.5 (c), the α_i are pairwise distinct because

$$\gcd(f(X), f'(X)) = \gcd(f(X), p^n X^{p^n - 1} - 1) = \gcd(f(X), -1) = 1$$

(if $\alpha_i = \alpha_j$ for $i \neq j$, then take $h(X) = (X - \alpha_i)$ and $g(X) = f(X)/(h(X)^2)$). So, the set $M = \{\alpha_1, \dots, \alpha_{p^n}\}$ has p^n elements and it consists precisely of the zeros (in L) of $f(X)$.
We now show that M is a subfield of L. Let $\alpha, \beta \in M$, hence $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$.

- $0, 1 \in M$ because they clearly satisfy $f(0) = 0 = f(1)$.
- Suppose $\alpha \neq 0$. Then $\alpha^{p^n} = \alpha$ implies $(\frac{1}{\alpha})^{p^n} = \frac{1}{\alpha}$, showing that M contains the multiplicative inverse of any non-zero element in M.
- From $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$, it follows $(\alpha\beta)^{p^n} = \alpha\beta$, showing that M contains the product of any two elements of M.
- From $\alpha^{p^n} = \alpha$, it follows $(-\alpha)^{p^n} = (-1)^{p^n}\alpha = -\alpha$ (note that for $p = 2$ this equation is also true), showing that M contains the negative of any of its elements.
- From $\alpha^{p^n} = \alpha$ and $\beta^{p^n} = \beta$, it follows $(\alpha + \beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$ (see Exercise on Sheet 4), showing that M contains the sum of any two elements of M.

Due to (3) of the definition of a splitting field, one has $L = M$ and this finishes the proof. □

We have thus shown that there is a field with p^n elements by constructing it as the splitting field of the polynomial $X^{p^n} - X \in \mathbb{F}_p[X]$. Next, we prove that all finite fields with p^n elements are of this type. From that we shall deduce that any two finite fields with the same number of elements are isomorphic, so that we will obtain a complete classification of all finite fields.

Lemma 3.10. *Let K be a finite field and let p be its characteristic. Then p is a prime number and there is $n \in \mathbb{N}$ such that the number of elements of K is p^n.*

Proof. The characteristic of K cannot be 0 because in that case K would contain infinitely many elements, namely $\mathbb{N}$ and hence $\mathbb{Q}$. So, the characteristic of K is p. That means that the kernel of the ring homomorphism

$$\mathbb{Z} \to K, \quad z \mapsto \begin{cases} \underbrace{1+1+\dots+1}_{z \text{ times}} & \text{if } z \geq 0, \\ \underbrace{-1-1-\dots-1}_{|z| \text{ times}} & \text{if } z \leq 0. \end{cases}$$

is the prime ideal (p), whence by the homomorphism theorem (1er théorème d'isomorphisme) we obtain an injection $\mathbb{F}_p \hookrightarrow K$. So, $\mathbb{F}_p$ is a subfield of K and, thus, K is an $\mathbb{F}_p$-vector space of some dimension n. Hence, K has p^n elements. □

Proposition 3.11. *Let p be a prime number, $n \in \mathbb{N}_{>0}$, and K a finite field with p^n elements. Then K is a splitting field of the polynomial $X^{p^n} - X$ over $\mathbb{F}_p$.*

Proof. This is actually very easy. We check conditions (1), (2) and (3) in the definition of a splitting field:
(1) $\mathbb{F}_p \subseteq K$; this is clear due to Lemma 3.10.
(2) Let $a \in K$. If $a = 0$, then clearly $a^{p^n} = a$. If $a \neq 0$, then $a^{(p^n-1)} = 1$ because the multiplicative group $K^\times = K \setminus \{0\}$ has order $p^n - 1$. Hence, we also find $a^{p^n} = a$. Consequently, all elements of K are zeros of $f(X) = X^{p^n} - X \in \mathbb{F}_p[X]$. As we have $\deg(f)$ zeros of f in K, f factors into linear factors over K.
(3) Of course, no proper subfield of a field with p^n elements can contain all the zeros of f because their number is p^n. □

Lemma 3.12. *Let A be a finite abelian group. The* exponent $\exp(A)$ *of A is defined as the minimal positive integer e such that $a^e = 1$ for all elements $a \in A$. Then the following statements hold:*

(a) Let $a, b \in A$. Suppose that $1 = \gcd(\mathrm{ord}(a), \mathrm{ord}(b))$, then $\mathrm{ord}(ab) = \mathrm{ord}(a)\,\mathrm{ord}(b)$.

(b) Let $a, b \in A$. Then there are $i, j \in \mathbb{N}$ such that $\mathrm{ord}(a^i b^j) = \mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b))$ (lcm: lowest common multiple; ppcm: plus petit commun multiple, kgV: kleinstes gemeinsames Vielfaches).

(c) There is $a \in A$ such that $\mathrm{ord}(a) = \exp(A)$.

(d) A is cyclic $\Leftrightarrow \exp(A) = \#A$.

Proof. (a) Let $e \geq 1$ such that $a^e b^e = 1$. Since $1 = \gcd(\mathrm{ord}(a^e), \mathrm{ord}(b^e))$, it follows from $a^e = b^{-e}$ that $a^e = 1 = b^e$. Thus, $\mathrm{ord}(a) \mid e$ and $\mathrm{ord}(b) \mid e$, hence, $\mathrm{ord}(a)\,\mathrm{ord}(b) = \mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b)) \mid e$. Of course, $(ab)^{\mathrm{ord}(a)\,\mathrm{ord}(b)} = 1$.
(b) Let

$$\mathrm{ord}(a) = p_1^{m_1} \cdot \ldots \cdot p_k^{m_k} \text{ and } \mathrm{ord}(b) = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$$

be the prime factorisations (i.e. the $p_1, \ldots, p_k$ are pairwise distinct prime numbers), where we sort the primes in such a way that $m_1 \geq n_1, \ldots, m_s \geq n_s$ and $m_{s+1} < n_s, \ldots, m_k < n_k$. Let

$$a' := a^{p_{s+1}^{m_{s+1}} \cdot \ldots \cdot p_k^{m_k}} \text{ and } b' := b^{p_1^{n_1} \cdot \ldots \cdot p_s^{n_s}}.$$

It is clear that we have

$$\mathrm{ord}(a') = p_1^{m_1} \cdot \ldots \cdot p_s^{m_s} \text{ and } \mathrm{ord}(b') = p_{s+1}^{n_{s+1}} \cdot \ldots \cdot p_k^{n_k}.$$

Hence, (a) implies that the order of $a'b'$ is

$$p_1^{m_1} \cdot \ldots \cdot p_s^{m_s} \cdot p_{s+1}^{n_{s+1}} \cdot \ldots \cdot p_k^{n_k} = \mathrm{lcm}(\mathrm{ord}(a), \mathrm{ord}(b)).$$

Of course, $(ab)^{\mathrm{lcm}(\mathrm{ord}(a),\mathrm{ord}(b))} = 1$.
(c) Let e denote the lowest common multiple of the orders of all elements in A. It is an immediate consequence of (b) that there is an element $a \in A$ whose order is e. So, $e = \mathrm{ord}(a) \mid \exp(A)$. Clearly, $\exp(A)$ is less than or equal to e, showing the desired equality.
(d) is an immediate consequence of (c). □

Proposition 3.13. *Let K be a finite field. Then the group of units $K^\times = K \setminus \{0\}$ (group with respect to multiplication and neutral element 1) is a cyclic group of order $\#K - 1$.*

Proof. Let $\#K = p^n$. Let $e := \exp(K^\times)$. Due to Lemma 3.12 it suffices to show that $e = p^n - 1$. Suppose $e < p^n - 1$. Then every element $a \in K$ satisfies $a^{e+1} = a$, so that the p^n elements are all zeros of the polynomial $X^{e+1} - X$, which has degree $e + 1$. This is, of course, impossible because a polynomial of degree $e + 1$ has at most $e + 1$ zeros (since the coefficients of the polynomial are in a field). □

Definition 3.14. *Let K be a field, L a field containing K, and $\alpha \in L$. Consider the evaluation map $\mathrm{ev}_a : K[X] \xrightarrow{f(X) \mapsto f(\alpha)} L$.*
Let $g(X)$ be the unique monic generator of the principal ideal $\ker(\mathrm{ev}_a)$ (recall: $K[X]$ is a principal ideal domain). In particular, any other polynomial $f(X) \in K[X]$ with $f(\alpha) = 0$ is a multiple of $g(X)$.
One calls $g(X)$ the minimal polynomial of a over K.

Proposition 3.15. *Let p be a prime number, $n \in \mathbb{N}_{>0}$, and K and L finite fields with p^n elements. Then K and L are isomorphic, i.e. there is a field isomorphism $\Phi : K \to L$.*

Proof. By Proposition 3.13, the unit group $K^\times$ is cyclic of order $p^n - 1$. Let $\alpha \in K^\times$ be a generator, i.e. an element of $K^\times$ of order $p^n - 1$. Let $g(X) \in \mathbb{F}_p[X]$ be the minimal polynomial of α. It has degree n, for, if it had a smaller degree m, then the order of α would be a divisor of $p^m - 1$, which is impossible.
The evaluation map $\mathrm{ev}_a : \mathbb{F}_p[X] \xrightarrow{f(X) \mapsto f(\alpha)} K$ defines an isomorphism (via the homomorphism theorem) $\mathbb{F}_p[X]/(g(X)) \cong K$. We show that also $\mathbb{F}_p[X]/(g(X)) \cong L$.
Note that $g(X) \mid X(X^{p^n-1} - 1) = X^{p^n} - X$ (in $\mathbb{F}_p[X]$) because α is a zero of both polynomials, so that $X^{p^n} - X$ is in the principal ideal generated by $g(X)$. We know by Proposition 3.11 that L is a splitting field of $X^{p^n} - X$ over $\mathbb{F}_p$. Hence, also $g(X)$ splits in L into linear factors and, thus, there is $\beta \in L$ such that $g(\beta) = 0$. This means that the evaluation map $\mathrm{ev}_\beta : \mathbb{F}_p[X] \xrightarrow{f(X) \mapsto f(\beta)} L$ defines the desired isomorphism (via the homomorphism theorem) $\mathbb{F}_p[X]/(g(X)) \cong L$. □

Now we can state and prove the complete classification result of finite fields up to isomorphism.

Theorem 3.16. *(a) The number of elements of any finite field K is of the form p^n, where p is a prime number and the characteristic of K, and $n \in \mathbb{N}_{>0}$.*

(b) For any prime p and any $n \in \mathbb{N}_{>0}$, there is a finite field having p^n elements. Any two such are isomorphic. We use the notation $\mathbb{F}_{p^n}$.

(c) Let K be a subfield of $\mathbb{F}_{p^n}$. Then $\#K = p^e$ for some divisor e of n.

(d) For every divisor $e \mid n$, there is a unique subfield $K \subseteq \mathbb{F}_{p^n}$ having p^e elements.

Proof. (a) and (b) have been proved above.
(c) The field $\mathbb{F}_{p^n}$ is a field extension of K, hence, $\mathbb{F}_{p^n}$ is a K-vector space of some dimension d. Thus, $p^n = \#\mathbb{F}_{p^n} = (\#K)^d = p^{ed}$.
(d) Let $n = ed$. Then (geometric sum)

$$p^n - 1 = (p^e - 1)\underbrace{(p^{e(d-1)} + p^{e(d-2)} + \ldots + 1)}_{=:m}$$

and (again geometric sum)

$$X^{p^n-1} - 1 = (X^{p^e-1} - 1)(X^{(p^e-1)(m-1)} + X^{(p^e-1)(m-2)} + \ldots + 1),$$

showing $f(X) := (X^{p^e} - X) \mid (X^{p^n} - X)$.
The zeros of $f(X)$ form a subfield K of $\mathbb{F}_{p^n}$ with p^e-elements: it is the splitting field of $f(X)$ over $\mathbb{F}_p$.
If $L \subseteq \mathbb{F}_{p^n}$ is a subfield with p^e elements, then all its elements are zeros of $f(X)$, whence $L \subseteq K$, hence $L = K$. □

4 Diffie-Hellman and El Gamal for finite fields

Symmetric encryption

Alice and Bob want to communicate secretly. A *message* is, as before, a positive integer $1 \leq m \leq N$ (for some fixed big N). A *key* is a positive integer $K \in \mathbb{N}$.
A *symmetric encryption function* (for the key K) is a pair of maps:

$$f_1 : \{1, 2, \ldots, N\} \times \mathbb{N} \to \{1, 2, \ldots, N\}$$

$$f_2 : \{1, 2, \ldots, N\} \times \mathbb{N} \to \{1, 2, \ldots, N\}$$

such that $f_2(f_1(m, K), K) = m$ and both $f_1(m, K)$ and $f_2(n, K)$ can be computed quickly for all $m, n \in \{1, 2, \ldots, N\}$. One also wants that m cannot (easily) be computed from $f_1(m, K)$ if K is unknown. One calls $f_1(m, K)$ the *encryption* of the message m for the key K.
Just to give an idea of a symmetric encryption system (this one is not perfect). Suppose the key is

$$K = \sum_{i=0}^{d-1} a_i 10^i \text{ with } a_i \in \{0, 1, \ldots, 9\}$$

and the message is

$$m = \sum_{i=0}^{e} m_i 10^i \text{ with } m_i \in \{0, 1, \ldots, 9\},$$

where we imagine that e is much bigger than d. Then we could take:

$$f_1(m, K) = \sum_{i=0}^{e} M_i 10^i,$$

where the M_i are computed as follows:

$$\begin{aligned} M_0 &\equiv m_0 + a_0 \mod (10), \ldots, & M_{d-1} &\equiv m_{d-1} + a_{d-1} \mod (10) \\ M_d &\equiv m_d + a_0 \mod (10), \ldots, & M_{2d-1} &\equiv m_{2d-1} + a_{d-1} \mod (10) \\ M_{2d} &\equiv m_{2d} + a_0 \mod (10), \ldots, & M_{3d-1} &\equiv m_{3d-1} + a_{d-1} \mod (10), \end{aligned}$$

and so on, until M_e. The function f_2 is defined in the same way, replacing $+$ by $-$.
Assumption: Alice and Bob have a common secret: a big integer $K \in \mathbb{N}$.
If Alice wants to send message m to Bob, all she has to do is compute $M := f_1(m, K)$ and send M to Bob. He can read the message by computing $m = f_2(M, K)$. Our assumptions imply that Eve, who knows M (and also f_1 and f_2), cannot deduce m. But, this all relies on the above assumption that Alice and Bob have this common secret key K. If they are far away (Bob is in New York and Alice in Luxembourg, they can only speak on the phone, and Eve listens to all their conversations), it is not so clear how they can get a common secret. That it is possible was demonstrated by Diffie and Hellman.

Diffie-Hellman key exchange

The players are the same as for RSA: Alice, Bob and Eve.
Task: Alice and Bob want to agree on a secret key, which both of them know, but which is unknown to Eve. They want to do this, even though Eve is listening to their conversation.
A revolutionary method was found by Diffie and Hellman. In order to illustrate the method, we first present the idea in a simpler setting, where it turns out to fail, and then present the right version.

First (wrong) attempt

(1) Alice and Bob agree on a big prime number p and an integer $1 < g < p$. Eve may know p and g.

(2) Alice chooses secretly $a \in \mathbb{N}$, computes $A := ag \mod (p)$ and sends A to Bob.

(3) Bob chooses secretly $b \in \mathbb{N}$, computes $B := bg \mod (p)$ and sends B to Alice.

(4) Alice receives B from Bob and computes $K_{\text{Alice}} := aB \equiv abg \mod (p)$.

(5) Bob receives A from Alice and computes $K_{\text{Bob}} := bA \equiv abg \mod (p)$.

Note: $K_{\text{Alice}} = K_{\text{Bob}}$.

Eve listened to their conversation. She knows: A, B, p and g. She now uses the Euclidean algorithm to compute $1 < h < p$ such that $gh \equiv 1 \mod (p)$ (i.e. an inverse to g in $\mathbb{F}_p^\times$). This allows her to compute

$$Ah \equiv agh \equiv a \mod (p) \text{ and } K := aB \mod (p),$$

so that $K = K_{\text{Alice}} = K_{\text{Bob}}$. Thus, Eve knows the common 'secret' K.
A slight modification of the above turns out to prevent Eve from obtaining the secret!

Correct realisation

The idea is to replace computations in $(\mathbb{F}_p, +)$ by computations in $(\mathbb{F}_{p^n}^\times, \cdot)$ (where we may, but need not, choose $n = 1$).

(1) Alice and Bob agree on a big finite field $\mathbb{F}$ (e.g. $\mathbb{F}_p$ or any $\mathbb{F}_{p^n}$) and a generator g of the cyclic group $\mathbb{F}^\times$. Eve may know $\mathbb{F}$ and g.

(2) Alice chooses secretly $a \in \mathbb{N}$, computes $A := g^a \in \mathbb{F}^\times$ and sends A to Bob.

(3) Bob chooses secretly $b \in \mathbb{N}$, computes $B := g^b \in \mathbb{F}^\times$ and sends B to Alice.

(4) Alice receives B from Bob and computes $K_{\text{Alice}} := B^a = (g^a)^b = g^{ab} \in \mathbb{F}^\times$.

(5) Bob receives A from Alice and computes $K_{\text{Bob}} := A^b = (g^b)^a = g^{ab} \in \mathbb{F}^\times$.

Note: $K_{\text{Alice}} = K_{\text{Bob}}$.

Eve again listened to their conversation. She again knows: A, B, p and g. But, in order to compute a from A (and p and g) she would have to solve the discrete logarithm problem in the finite field $\mathbb{F}$, which is defined as follows:

> Given a finite field $\mathbb{F}$ and a generator g of the cyclic group $\mathbb{F}^\times$ (with respect to multiplication).
>
> For $A \in \mathbb{F}^\times$, find a such that $g^a = A \in \mathbb{F}^\times$.
>
> The solution a is called a (discrete) logarithm of A (for the basis/generator g) because $g^a = A$.

Up to this day, no efficient algorithm is known to compute a discrete logarithm in a big finite field. Hence, Eve cannot compute a and, thus, cannot obtain the common secret $K_{\text{Alice}} = K_{\text{Bob}}$, although she has seen everything that Alice and Bob exchanged!
As a variant, one can replace the discrete logarithm problem in finite fields by the discrete logarithm problem in elliptic curves, and obtain an elliptic curves Diffie-Hellman key exchange. This is used, for instance, in the authentication procedure for the communication between the German passport and a reader.

El Gamal encryption

A slight variation of the order of step in the Diffie-Hellman key exchange gives rise to a public key encryption system, which works similarly to RSA: Bob wants to receive messages (in particular, but, not only from Alice), and for that purpose he produces a public key, which can be looked up in a phone book, and a secret key. People (like Alice) who have looked up the public key can send encrypted messages to Bob which only he can decrypt using his secret key.

Bob's preparation step

- Bob chooses a big finite field $\mathbb{F}$ (e.g. $\mathbb{F}_p$ or any $\mathbb{F}_{p^n}$) and a generator g of the cyclic group $\mathbb{F}^\times$. Eve may know $\mathbb{F}$ and g.
- Bob chooses secretly $b \in \mathbb{N}$ and computes $B := g^b \in \mathbb{F}^\times$.
- Bob publishes B (and $\mathbb{F}$ and g) in the phone book.

Alice's message encryption

- Alice looks up Bob's B (and $\mathbb{F}$ and g) in the phone book.
- Alice chooses secretly $a \in \mathbb{N}$ and computes $A := g^a \in \mathbb{F}^\times$ (just like in the Diffie-Hellman key exchange).
- Alice computes $K_{\text{Alice}} := B^a = (g^a)^b = g^{ab} \in \mathbb{F}^\times$.
- Alice encrypts the message $M := f_1(m, K_{\text{Alice}})$.
- Alice sends M and A to Bob.

Bob's message decryption

- Bob receives M and A from Alice.
- Bob computes $K_{\text{Bob}} = A^b = (g^a)^b = g^{ab} \in \mathbb{F}^\times$. Note that again $K_{\text{Alice}} = K_{\text{Bob}}$.
- Bob decypts the message $m = f_2(M, K_{\text{Bob}})$.

And Eve?

Eve knows A, B (and $\mathbb{F}$ and g) and M. As in the Diffie-Hellman key exchange she is faced with computing b from B or a from A in order to get hold of $K_{\text{Alice}} = K_{\text{Bob}}$ (which we assume is necessary for the message decryption). This is the same discrete logarithm problem in the finite field $\mathbb{F}$, and, hence, currently undoable if the field is big enough.

5 Legendre symbol

We first prove two lemmas to be used later on. They could already have been treated at earlier places in the lecture.

Lemma 5.1. *(a) Let $m \in \mathbb{N}_{\geq 2}$. There is a group isomorphism*

$$(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}.$$

The factors are generated by the classes of -1 and 5 in $(\mathbb{Z}/2^m\mathbb{Z})^\times$, respectively.

(b) Let $p > 2$ be a prime number and $m \in \mathbb{N}_{\geq 1}$. There is a group isomorphism

$$(\mathbb{Z}/p^m\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{p-1}\mathbb{Z}.$$

Proof. Exercise. □

Lemma 5.2. *Let $p > 2$ be a prime number. There are $\frac{p-1}{2}$ squares in $\mathbb{F}_p^\times$ (a square in $\mathbb{F}_p^\times$ is an element a such that there is $b \in \mathbb{F}_p^\times$ such that $a = b^2$) and there are equally many nonsquares.*

Proof. We consider the group homomorphism

$$\varphi : \mathbb{F}_p^\times \xrightarrow{x \mapsto x^2} \mathbb{F}_p^\times.$$

Its kernel is clearly $\{-1, 1\}$ and its image is the set of squares $\mathbb{F}_p^{\times 2}$ in $\mathbb{F}_p^\times$. Thus the homomorphism theorem (1st isomorphism theorem) gives the isomorphism

$$\overline{\varphi} : \mathbb{F}_p^\times/\{1, -1\} \cong \mathbb{F}_p^{\times 2},$$

from which the claimed formula follows. □

Definition 5.3. *Let $N \in \mathbb{N}_{\geq 1}$. An integer $a \in \mathbb{Z}$ is called* quadratic residue modulo N *if there is $b \in \mathbb{Z}$ such that*

$$a \equiv b^2 \mod N.$$

Otherwise, we call it a quadratic nonresidue.

Lemma 5.4. *(a) Let $N \in \mathbb{N}_{\geq 1}$. Whether or not a is a quadratic residue modulo N only depends on the class of a in $\mathbb{Z}/N\mathbb{Z}$.*

(b) Suppose $N = \prod_{i=1}^k p_i^{n_i}$ in its factorisation into prime powers (that is, the p_i are distinct primes). Then a is a quadratic residue modulo N if and only if it is a quadratic residue modulo $p_i^{n_i}$ for all $i \in \{1, \dots, k\}$.

(c) Let $p \geq 2$ be a prime number, $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ such that $p \nmid a$. Then the following statements are equivalent:

(i) a is a quadratic residue modulo p^n.

(ii) a is a quadratic residue modulo p.

(d) Let $a \in \mathbb{Z}$ be odd. Then the following statements are equivalent:

(i) a is a quadratic residue modulo 2^n.

(ii) $n = 1$ or ($n = 2$ and $a \equiv 1 \mod 4$) or ($n \geq 3$ and $a \equiv 1 \mod 8$).

Proof. (a) is clear since it is an assertion about the ring $\mathbb{Z}/N\mathbb{Z}$.
(b) This follows immediately from the Chinese Remainder Theorem which gives the isomorphism

$$\begin{aligned}\Psi : \mathbb{Z}/N\mathbb{Z} \to& \mathbb{Z}/p_i^{n_i}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{n_k}\mathbb{Z}\\ a \mapsto& (a_1, \dots, a_k)\\ b \mapsto& (b_1, \dots, b_k).\end{aligned}$$

'$\Rightarrow$': If $a = b^2$, then $a_i = b_i^2$ for all $i \in \{1, \dots, k\}$, showing that a_i is a square modulo $p_i^{n_i}$.
'$\Leftarrow$': Suppose now $a_i = b_i^2$ for all $i \in \{1, \dots, k\}$. Then $\Psi(a) = (a_1, \dots, a_k) = (b_1^2, \dots, b_k^2) = \Psi(b^2)$.
(c) '(i) $\Leftarrow$ (ii)': If $a \equiv b^2 \mod p^n$, that is, $p^n \mid (b^2 - a)$, hence $p \mid (b^2 - a)$, thus $a \equiv b^2 \mod p$.
'(ii) $\Rightarrow$ (i)': Suppose $a \equiv b^2 \mod p$. As $p \nmid a$, it follows $p \nmid b$, thus b is a unit in $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Hence, there is $c \in \mathbb{Z}$ such that $a \equiv b^2 c \mod p^n$ and $c \equiv 1 \mod p$.
Claim: For all $i \geq 0$ we have $c^{p^i} \equiv 1 \mod p^{i+1}$.
We show that claim by induction. The case $i = 0$ is true by assumption. Suppose the assertion is true for i, we want to prove it for $i + 1$. So, we know $c^{p^i} = 1 + p^{i+1}x$ for some $x \in \mathbb{Z}$. We take the p-th power and expand it

$$\begin{aligned}c^{p^{i+1}} &= (c^{p^i})^p = (1 + p^{i+1}x)^p = \sum_{k=0}^{p} \binom{p}{k} p^{(i+1)k} x^k\\ &= 1 + \binom{p}{1} p^{i+1} x + \sum_{k=2}^{p} \binom{p}{k} p^{(i+1)k} x^k \equiv 1 \mod p^{i+2}.\end{aligned}$$

Thus, $c^{p^{n-1}} \equiv 1 \mod p^n$. We exploit this as follows. Set $d := c^{\frac{p^{n-1}+1}{2}}$. Then

$$d^2 = (c^{\frac{p^{n-1}+1}{2}})^2 = c^{p^{n-1}+1} = c^{p^{n-1}} \cdot c \equiv c \mod p^n.$$

Hence, $a \equiv b^2 c \equiv b^2 d^2 = (bd)^2 \mod p^n$.
(d) '(i) $\Rightarrow$ (ii)': Let $a = 2m + 1$ be any odd number (with $m \in \mathbb{Z}$). Then its square is congruent to 1 modulo 8 (hence also 1 modulo 4 and 1 modulo 2):

$$a^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 4m(m + 1) + 1 \equiv 1 \mod 8,$$

where we used that $m(m + 1)$ is necessarily even as it is the product of two consecutive integers.
'(ii) $\Rightarrow$ (i)': The cases $n = 1$ and $n = 2$ are trivial as $1 = 1^2$ is a square. Let us hence assume $n \geq 3$ and $a \equiv 1 \mod 8$. From Lemma 5.1 it follows that $a \equiv 5^{2k} \mod 2^n$ for some $k \in \mathbb{N}$: in general we know $a \equiv (-1)^r 5^s \mod 2^n$ for some $r, s \in \mathbb{Z}$; thus $1 \equiv a \equiv (-1)^r 5^s \mod 8$, implying $2 \mid r$ and $2 \mid s$. □

This lemma reduces the calculation whether or not a is a quadratic residue modulo N to the calculation whether or not a is a quadratic residue modulo p for the primes p dividing N. This leads to the introduction of the Legendre symbol.

Definition 5.5. *Let $p > 2$ be a prime number and $a \in \mathbb{Z}$. The* Legendre symbol *is defined as*

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

Note that the definition only depends on the class of a modulo p.

Proposition 5.6 (Euler)**.** *Let $p > 2$ be a prime number and $a \in \mathbb{Z}$. Then the congruence*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$$

holds.

Proof. If $p \mid a$, the result is straight forward:

$$\left(\frac{a}{p}\right) = 0 \text{ and } a^{\frac{p-1}{2}} \equiv 0^{\frac{p-1}{2}} = 0 \mod p.$$

We now assume $p \nmid a$, that is $a \in \mathbb{F}_p^\times$. We consider the group homomorphism

$$\varphi : \mathbb{F}_p^\times \xrightarrow{x \mapsto x^{\frac{p-1}{2}}} \mathbb{F}_p^\times.$$

Recall that $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$ and note that $\varphi(x^2) = (\varphi(x))^2 = x^{p-1} = 1$ for all $x \in \mathbb{F}_p^\times$. This implies that the image is $\{1, -1\} \subseteq \mathbb{F}_p^\times$ and that the squares $\mathbb{F}_p^{\times 2}$ are in the kernel. The homomorphism theorem (1st isomorphism theorem) gives an isomorphism

$$\overline{\varphi} : \mathbb{F}_p^\times / \ker(\varphi) \cong \operatorname{im}(\varphi) = \{-1, 1\},$$

showing that the order of $\ker(\varphi)$ is $\frac{p-1}{2}$. By Lemma 5.2 there are $\frac{p-1}{2}$ squares in $\mathbb{F}_p^\times$, hence $\ker(\varphi) = \mathbb{F}_p^{\times 2}$. This proves the proposition. □

Corollary 5.7. *Let $p > 2$ be a prime number. The Legendre symbol defines a group homomorphism*

$$\mathbb{F}_p \to \{-1, 1\}, \quad a \mapsto \left(\frac{a}{p}\right).$$

In particular, for all $a, b \in \mathbb{Z}$ one has

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Proof. This follows immediately from Proposition 5.6. □

6 Gauß' reciprocity law

We first state Gauß' reciprocity law. Its proof will be given later.

Theorem 6.1 (Gauß' reciprocity law)**.** *Let $p \neq q$ be two distinct odd prime numbers.*

(a) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4, \\ -1 & \text{if } p \equiv 3 \mod 4. \end{cases}$

(b) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv 1,7 \mod 8, \\ -1 & \text{if } p \equiv 3,5 \mod 8. \end{cases}$

(c) $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$*. In particular, if* $p \equiv 1 \mod 4$ *or* $q \equiv 1 \mod 4$*, then* $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$.

Let us remark that (a) is a direct consequence of Euler's result Proposition 5.6.

Example 6.2. *In the following examples we apply Gauß' reciprocity law and the fact that the Legendre symbol $\frac{n}{p}$ only depends on the residue class of n modulo p.*

- $\left(\frac{100}{101}\right) = \left(\frac{4\cdot 25}{101}\right) = \left(\frac{4}{101}\right)\left(\frac{25}{101}\right) = 1 \cdot 1 = 1.$
- $\left(\frac{500}{101}\right) = \left(\frac{4\cdot 125}{101}\right) = \left(\frac{4}{101}\right)\left(\frac{25}{101}\right)\left(\frac{5}{101}\right) = \left(\frac{101}{5}\right) = \left(\frac{1}{5}\right) = 1.$
- $\left(\frac{127}{31}\right) = \left(\frac{3}{31}\right) = -\left(\frac{31}{3}\right) = -\left(\frac{1}{3}\right) = -1.$

A generalisation of the Legendre Symbol is the Jacobi Symbol. We will use it for primality testing later this term.

Definition 6.3. *Let $m \geq 3$ be an odd natural number and write $m = p_1 \cdot \dots \cdot p_k$ for its factorisation into (not necessarily distinct) prime numbers. For $a \in \mathbb{Z}$, the* Jacobi symbol *is defined as*

$$\left(\frac{a}{m}\right) := \prod_{i=1}^{k} \left(\frac{a}{p_i}\right),$$

where the Legendre symbol is used on the right hand side.

If m is a prime number, then the Jacobi symbol $\left(\frac{a}{m}\right)$ equals the Legendre symbol. However, if m is not a prime number, then one must not interpret the Jacobi symbol like the Legendre symbol. For instance,

$$\left(\frac{-1}{21}\right) = \left(\frac{-1}{3}\right)\left(\frac{-1}{7}\right) = (-1)\cdot(-1) = 1,$$

but -1 is not a square modulo 21 (see Lemma 5.4).

Lemma 6.4. *Let $m = \prod_{i=1}^{k} p_i \geq 3$ be an odd integer (and the p_i are primes) and let $a, b \in \mathbb{Z}$.*

(a) The Jacobi symbol $\left(\frac{a}{m}\right)$ only depends on the residue class of a modulo m.

(b) $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$.

Proof. (a) This follows immediately from the Chinese Remainder Theorem: If $a \equiv b \mod m$, then $a \equiv b \mod p_i$ for all $i \in \{1, \ldots, k\}$. But we already know for the Legendre symbol that $\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right)$, which gives the assertion.
(b) $\left(\frac{ab}{m}\right) = \prod_{i=1}^k \left(\frac{ab}{p_i}\right) = (\prod_{i=1}^k \left(\frac{a}{p_i}\right)) \cdot (\prod_{i=1}^k \left(\frac{a}{p_i}\right)) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$. □

We will now extend Gauß' reciprocity law from the Legendre to the Jacobi symbol. For this we first include a lemma.

Lemma 6.5. *(a) The map*

$$\epsilon : (\mathbb{Z}/4\mathbb{Z})^\times \to \{+1, -1\}, \quad m \mapsto (-1)^{\frac{m-1}{2}}$$

is a group homomorphism.

(b) The map

$$w : (\mathbb{Z}/8\mathbb{Z})^\times \to \{+1, -1\}, \quad m \mapsto (-1)^{\frac{m^2-1}{8}}$$

is a group homomorphism.

Proof. (a) We have $\frac{mk-1}{2} - \left(\frac{m-1}{2} + \frac{k-1}{2}\right) = 2 \cdot \frac{m-1}{2}\frac{k-1}{2} \equiv 0 \mod 2$. This shows $(-1)^{\frac{mk-1}{2}} = (-1)^{\frac{m-1}{2}}(-1)^{\frac{k-1}{2}}$.
(b) We have $\frac{m^2k^2-1}{8} - \left(\frac{m^2-1}{8} + \frac{k^2-1}{8}\right) = 8 \cdot \frac{m^2-1}{8}\frac{k^2-1}{8} \equiv 0 \mod 2$. This shows $(-1)^{\frac{m^2k^2-1}{8}} = (-1)^{\frac{m^2-1}{8}}(-1)^{\frac{k^2-1}{8}}$. □

Theorem 6.6 (Jacobi's reciprocity law)**.** *Let $m \neq k$ be two distinct odd integers at least 3.*

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

(b) $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} = w(m)$.

(c) $\left(\frac{k}{m}\right) = \left(\frac{m}{k}\right)(-1)^{\frac{k-1}{2}\frac{m-1}{2}}$.

Proof. Let $m = \prod_{i=1}^r p_i$ and $k = \prod_{i=1}^s q_i$ be the factorisations of m and k into prime numbers (not necessarily distinct).
(a) $\left(\frac{-1}{m}\right) = \prod_{i=1}^r \left(\frac{-1}{p_i}\right) = \prod_{i=1}^r \epsilon(p_i) = \epsilon(\prod_{i=1}^r p_i) = \epsilon(m)$, where we used Gauß' reciprocity law Theorem 6.1 (a) and Lemma 6.5 (a).
(b) $\left(\frac{2}{m}\right) = \prod_{i=1}^r \left(\frac{2}{p_i}\right) = \prod_{i=1}^r w(p_i) = w(\prod_{i=1}^r p_i) = w(m)$, where we used Gauß' reciprocity law Theorem 6.1 (b) and Lemma 6.5 (b).
(c) We now use Gauß' reciprocity law Theorem 6.1 (c) and Lemma 6.5 (a):

$$\begin{aligned}\left(\frac{k}{m}\right)\left(\frac{m}{k}\right) &= (\prod_{i=1}^r \left(\frac{k}{p_i}\right))(\prod_{j=1}^s \left(\frac{m}{q_j}\right)) = (\prod_{i=1}^r \prod_{j=1}^s \left(\frac{q_j}{p_i}\right))(\prod_{j=1}^s \prod_{i=1}^r \left(\frac{p_i}{q_j}\right)) \\ &= \prod_{j=1}^s \prod_{i=1}^r (\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right)) = \prod_{j=1}^s \prod_{i=1}^r (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} = \prod_{j=1}^s \prod_{i=1}^r \epsilon(p_i)^{\frac{q_j-1}{2}} = \prod_{j=1}^s \epsilon(m)^{\frac{q_j-1}{2}} \\ &= \begin{cases} 1 & \text{if } \epsilon(m) = 1 \\ \prod_{j=1}^s (-1)^{\frac{q_j-1}{2}} = \prod_{j=1}^s \epsilon(q_j) = \epsilon(k) & \text{if } \epsilon(m) = -1 \end{cases}.\end{aligned}$$

This shows $\left(\frac{k}{m}\right)\left(\frac{m}{k}\right) = (-1)^{\frac{k-1}{2}\frac{m-1}{2}}$. □

Example 6.7. $\left(\frac{888}{1999}\right) = \left(\frac{2}{1999}\right)\left(\frac{4}{1999}\right)\left(\frac{111}{1999}\right) = \left(\frac{111}{1999}\right) = -\left(\frac{1999}{111}\right) = -\left(\frac{1}{111}\right) = -1$. *We used that* $1999 \equiv 7 \mod 8$ *(hence* $\left(\frac{2}{1999}\right) = 1$*) and* $111 \equiv 3 \mod 4$, $1999 \equiv 3 \mod 4$, $1999 = 111 \cdot 18 + 1$. *We have thus computed the Legendre symbol* $\left(\frac{888}{1999}\right)$ *using the rules of the Jacobi symbol without factoring* 111*, just doing division with remainder. This is an important advantage because it is very hard to factor big numbers in practice!*

Next we will prove Gauß' reciprocity law Theorem 6.1 by using Gauß sums, which allow to write down a closed formula for $\left(\frac{p}{q}\right)$ for distinct odd primes p, q.

Lemma 6.8. *Let* p *be a prime number and* $n \in \mathbb{N}_{\geq 1}$ *not divisible by* p*. There is a finite field extension* $\mathbb{F}_p(n)$ *of* $\mathbb{F}_p$ *such that* $\mathbb{F}_p(n)^\times$ *contains a cyclic subgroup of order* n*.*

Proof. Define $\mathbb{F}_p(n)$ as the splitting field over $\mathbb{F}_p$ of the polynomial $X^n - 1 \in \mathbb{F}_p[X]$, which is separable as $\gcd(X^n - 1, nX^{n-1}) = 1$. Thus it has n distinct roots, all of which are elements of order dividing n. We know that $\mathbb{F}_p(n)^\times$ is a cyclic group by Proposition 3.13, hence there are precisely n elements or order dividing n and these form a cyclic subgroup of order n, as required. □

For the rest of this section and the proof of Theorem 6.1 we fix two distinct odd prime numbers p, q.

Lemma 6.9. *For any* $1 \neq \beta \in \mathbb{F}_p(q)$ *of order* q *we have*

$$\sum_{k=0}^{q-1} \beta^k = 0 \in \mathbb{F}_p(q).$$

Proof. $(1-\beta)\sum_{k=0}^{q-1}\beta^k = \sum_{k=0}^{q-1}\beta^k - \sum_{k=1}^{q}\beta^k = \beta^0 - \beta^q = 1 - 1 = 0.$ □

We now fix an element α of $\mathbb{F}_p(q)^\times$ of order equal to q, which exists by Lemma 6.8.

Definition 6.10. *The* Gauß sum for q modulo p *(with respect to* α*) is defined as:*

$$S_p(q) := \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \alpha^k \in \mathbb{F}_p(q).$$

Proposition 6.11. $S_p(q)^2 = \left(\frac{-1}{q}\right) \cdot q \in \mathbb{F}_p(q)^\times$.

Proof. We first have by definition

$$S_p(q)^2 = (\sum_{n=1}^{q-1} \left(\frac{n}{q}\right) \alpha^n) \cdot (\sum_{m=1}^{q-1} \left(\frac{m}{q}\right) \alpha^m) = \sum_{n=1}^{q-1}\sum_{m=1}^{q-1} \left(\frac{nm}{q}\right) \alpha^{n+m}.$$

We rewrite this as

$$S_p(q)^2 = \sum_{n \in (\mathbb{Z}/q\mathbb{Z})^\times} \sum_{m \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{nm}{q}\right) \alpha^{n+m}.$$

Note now that multiplication by $n \in (\mathbb{Z}/q\mathbb{Z})^\times$ defines a group automorphism of $(\mathbb{Z}/q\mathbb{Z})^\times$; that is, every element $m \in (\mathbb{Z}/q\mathbb{Z})^\times$ can be written as $m = nr$ for a unique $r \in (\mathbb{Z}/q\mathbb{Z})^\times$. Thus we may make the variable substitution $m = nr$:

$$S_p(q)^2 = \sum_{n \in (\mathbb{Z}/q\mathbb{Z})^\times} \sum_{r \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{n(rn)}{q}\right) \alpha^{n+rn} = \sum_{r \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{r}{q}\right) \sum_{n \in (\mathbb{Z}/q\mathbb{Z})^\times} (\alpha^{1+r})^n.$$

We now use Lemma 6.9 to obtain

$$S_p(q)^2 = \sum_{r \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{r}{q}\right) \cdot \begin{cases} -1 & \text{if } \alpha^{1+r} \neq 1, \\ q-1 & \text{if } \alpha^{1+r} = 1. \end{cases}$$

Thus we obtain

$$S_p(q)^2 = (q-1)\left(\frac{-1}{q}\right) - \sum_{r=1}^{q-2} \left(\frac{r}{q}\right) = q\left(\frac{-1}{q}\right) - \sum_{r=1}^{q-1} \left(\frac{r}{q}\right) = q\left(\frac{-1}{q}\right),$$

where we used $\left(\frac{-1}{q}\right) = \left(\frac{q-1}{q}\right)$ and the fact that in $(\mathbb{Z}/q\mathbb{Z})^\times$ contains as many squares as non-squares (Lemma 5.2), whence the finial sum cancels out. □

Proposition 6.12 (Closed formula for the Legendre symbol with Gauß sums)**.**

$$\left(\frac{p}{q}\right) = \frac{S_p(q)^p}{S_p(q)} \in \mathbb{F}_p(q).$$

Proof. We first have by definition

$$S_p(q)^p = (\sum_{n=1}^{q-1} \left(\frac{n}{q}\right) \alpha^n)^p = \sum_{n=1}^{q-1} \left(\frac{n}{q}\right) \alpha^{np} = \sum_{n=1}^{q-1} \left(\frac{np^2}{q}\right) \alpha^{np},$$

where we used 'little Fermat' Corollary 1.12 and the fact that $(-1)^p = -1$; the final equality is trivial. Note now that multiplication by p defines a group automorphism of $(\mathbb{Z}/q\mathbb{Z})^\times$; that is, every element $r \in (\mathbb{Z}/q\mathbb{Z})^\times$ can be written as $r = np$ for a unique $n \in (\mathbb{Z}/q\mathbb{Z})^\times$. Thus we may make the variable substitution $np = r$:

$$S_p(q)^p = \sum_{r \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{rp}{q}\right) \alpha^r.$$

Next we exploit the multiplicativity of the Legendre symbol

$$S_p(q)^p = \left(\frac{p}{q}\right) \sum_{r \in (\mathbb{Z}/q\mathbb{Z})^\times} \left(\frac{r}{q}\right) \alpha^r = \left(\frac{p}{q}\right) S_p(q),$$

which is the claimed result, since $S_p(q)$ is invertible by Proposition 6.11. □

We can now do the main part of the proof of Gauß' reciprocity law.

Proof of Theorem 6.1 (c). We first combine Proposition 6.11 with Euler's result 5.6:

$$S_p(q)^2 = q \cdot \left(\frac{-1}{q}\right) = q \cdot (-1)^{\frac{q-1}{2}} \in \mathbb{F}_p(q)^\times.$$

We obtain from this equality the following equivalence:

$$\left(\frac{q \cdot (-1)^{\frac{q-1}{2}}}{p}\right) = 1 \Leftrightarrow S_p(q) \in \mathbb{F}_p$$

because on the one hand if $S_p(q) \in \mathbb{F}_p$, then $q \cdot (-1)^{\frac{q-1}{2}}$ is a square in $\mathbb{F}_p$; on the other hand, as square roots in fields are unique up to sign, if $q \cdot (-1)^{\frac{q-1}{2}}$ is a square in $\mathbb{F}_p$, then $S_p(q)$ must belong to $\mathbb{F}_p$. Now recall that an element x in some finite extension of $\mathbb{F}_p$ lies in $\mathbb{F}_p$ if and only if $x^p = x$. Thus we have the equivalence

$$\left(\frac{q \cdot (-1)^{\frac{q-1}{2}}}{p}\right) = 1 \Leftrightarrow S_p(q) = S_p(q)^p,$$

which by Proposition 6.12 gives the equivalence

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

As the only possible values for the Legendre symbols in question here are -1 or 1, we have shown the equality

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

It suffices to interpret this in the desired way:

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

by Theorem 6.1 (a), which we already proved above. □

We must still give the proof of part (b) of Gauß' reciprocity law. It is essentially the same arguments again with q replaced by 8.

Proof of Theorem 6.1 (b). Let us fix a generator γ of the group of elements of order dividing 8 in $\mathbb{F}_p(8)$, which exists by Lemma 6.8.
The *Gauß sum for* 2 *modulo* p is defined as

$$S_p(2) = \gamma + \gamma^{-1} \in \mathbb{F}_p(8).$$

Note that $\gamma^4 = -1$. We use this in the following calculation:

$$\gamma^2 + \gamma^{-2} = \gamma^2 + \gamma^6 = \gamma^2 + \gamma^4\gamma^2 = \gamma^2 - \gamma^2 = 0.$$

This implies

$$S_p(2)^2 = (\gamma + \gamma^{-1})^2 = \gamma^2 + 2 + \gamma^{-2} = 2 \in \mathbb{F}_p(8)^\times.$$

As in the proof of Theorem 6.1 (c) this gives the equivalences:

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow S_p(2) \in \mathbb{F}_p \Leftrightarrow S_p(2) = S_p(2)^p.$$

We hence also calculate the p-th power of $S_p(2)$. Assume first $p \equiv 1, -1 \mod 8$. Then (using again 'Little Fermat' Corollary 1.12)

$$S_p(2)^p = (\gamma + \gamma^{-1})^p = \gamma^p + \gamma^{-p} = \gamma + \gamma^{-1} = S_p(2).$$

Assume now $p \equiv 5, -5 \mod 8$. Then we have

$$S_p(2)^p = \gamma^p + \gamma^{-p} = \gamma^5 + \gamma^{-5} = \gamma^4\gamma + (\gamma^4)^{-1}\gamma^{-1} = -(\gamma + \gamma^{-1}) = -S_p(2).$$

Thus, we obtain $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1, -1 \mod 8$, which can be equivalently expressed as $(-1)^{\frac{p^2-1}{8}} = 1$. This consequently yields the claimed equality $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. □

7 Carmichael numbers

Let us recall 'little Fermat': *For a prime p one has*

$$a^{p-1} \equiv 1 \mod p \text{ for all } a \in \mathbb{Z} \text{ such that } p \nmid a.$$

Does the converse also hold? That is: Let $n \in \mathbb{N}_{\geq 2}$ not be prime. Is there $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$ such that

$$a^{n-1} \not\equiv 1 \mod n?$$

The answer is no. Let $n = 561$. Then $a^{560} \equiv 1 \mod 561$ for all $a \in \mathbb{Z}$ such that $\gcd(a, 561) = 1$. The proof is given below.

Definition 7.1. *A natural number $n \in \mathbb{N}$ is called* Carmichael number *if n is not prime and*

$$a^{n-1} \equiv 1 \mod n$$

for all $a \in \mathbb{Z}$ such that $\gcd(a, n) = 1$.

We are now going to characterise Carmichael numbers.

Proposition 7.2. *Let $N \in \mathbb{N}_{\geq 2}$. The following statements are equivalent:*

(i) N is a prime or a Carmichael number.

(ii) The exponent of $(\mathbb{Z}/N\mathbb{Z})^\times$ is a divisor of $N - 1$.

(iii) For every prime number p such that p divides N

- *$p^2 \nmid N$ (numbers that are not divisible by the square of any prime are called* squarefree*) and*

- $(p-1) \mid (N-1)$.

Before the proof let us check that 561 is indeed a Carmichael number:

$$n = 561 = 3 \cdot 11 \cdot 17.$$

We have

$$(3-1) \mid 560, \quad (11-1) \mid 560 \text{ and } (17-1) \mid 560 = 16 \cdot 35.$$

Other Carmichael numbers are $5 \cdot 13 \cdot 17$ and $7 \cdot 13 \cdot 19$.

Proof. '(i) $\Leftrightarrow$ (ii)': This equivalence is by definition of Carmichael numbers and the exponent.
'(ii) $\Rightarrow$ (iii)': We assume that the exponent of $(\mathbb{Z}/N\mathbb{Z})^\times$ is a divisor of $N-1$. Let $N = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$ be the factorisation of N into distinct prime powers, where $r_i \geq 1$ for $i \in \{1, \dots, s\}$. The Chinese Remainder Theorem reads

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{r_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s^{r_s}\mathbb{Z})^\times.$$

We know that the order of $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$ is $(p_i-1)p_i^{r_i-1}$, and that this group contains an element of order $p_i - 1$ by Lemma 5.1. Thus the exponent of $(\mathbb{Z}/N\mathbb{Z})^\times$ is divisible by $p_i - 1$ for all $i \in \{1, \dots, s\}$.
Suppose now that N is not squarefree. Then without loss of generality $r_1 > 1$. Then there is an element of order p_1 in $(\mathbb{Z}/p_1^{r_1}\mathbb{Z})^\times$. Thus also it follows that $(\mathbb{Z}/N\mathbb{Z})^\times$ contains such an element, whence p_1 divides the exponent of $(\mathbb{Z}/N\mathbb{Z})^\times$, hence p_1 divides $N-1$. As p_1 also divides N, it divides 1, which is a contradiction.
'(iii) $\Rightarrow$ (ii)': Let $N = p_1 p_2 \cdots p_s$ be the factorisation of N into distinct primes, which is possible since N is squarefree. The Chinese Remainder Theorem

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong (\mathbb{Z}/p_1\mathbb{Z})^\times \times (\mathbb{Z}/p_2\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s\mathbb{Z})^\times$$

together with with fact that $(\mathbb{Z}/p_i\mathbb{Z})^\times$ is cyclic (Proposition 3.13) implies that for each $i \in \{1, \dots, s\}$ there is an element $g_i \in (\mathbb{Z}/N\mathbb{Z})^\times$ of order $p_i - 1$. Lemma 3.12 implies that there is $g \in (\mathbb{Z}/N\mathbb{Z})^\times$ of order $\mathrm{lcm}(p_1 - 1, p_2 - 1, \dots, p_s - 1) =: e$. As $a^e \equiv 1 \mod N$ for all $a \in \mathbb{Z}$ such that $\gcd(a, N) = 1$, it follows that e is the exponent of $(\mathbb{Z}/N\mathbb{Z})^\times$.
Since $(p_i - 1) \mid (N-1)$ for all $i \in \{1, \dots, s\}$, it follows that $\mathrm{lcm}(p_1 - 1, p_2 - 1, \dots, p_s - 1)$ and hence the exponent of $(\mathbb{Z}/N\mathbb{Z})^\times$ divides $N-1$. □

Proposition 7.3. *Every Carmichael number is odd and has at least three prime divisors.*

Proof. Let N be a Carmichael number.
If N were even, then $N-1$ would be odd. But $(p-1)|(N-1)$ for all $p \mid N$ would imply that only 2 can be a prime divisor of N. As N is squarefree, it follows $N = 2$. This is a contradiction because 2 is prime.
Assume $N = pq$ with two distinct prime numbers p and q. We know that $p-1$ divides $N - 1 = pq - 1 = (p-1)q + (q-1)$, whence $p-1$ divides $q-1$. Exchanging the roles of p and q we obtain that $q-1$ divides $p-1$, so that we get $p = q$, a contradiction again. □

8 The Solovay-Strassen primality test

We have seen that the cryptographic systems RSA, Diffie-Hellman, El Gamal, etc. need ‘big’ prime numbers. How does one find ‘big’ prime numbers? How does one know whether a ‘big’ number is prime?

A *deterministic primality test* is an algorithm:

Input: $m \in \mathbb{N}_{\geq 2}$

Output: `true` ⇒ m is a prime number.

`false` ⇒ m is not a prime number.

A *probabilistic primality test* is an algorithm:

Input: $m \in \mathbb{N}_{\geq 2}$

Output: `true` ⇒ m is a prime number with ‘high probability’.

`false` ⇒ m is not a prime number.

A prime number test does *not* compute a factorisation of m. The idea is to decide whether m is a prime number or not *without* factorising m. The reason for this is that factorisation of a big number is in practice often undoable (recall that the security of RSA relies precisely on this). In practice probabilistic primality tests are usually faster than deterministic ones, and for everyday cryptographic purposes probabilistic tests suffice: if the probability that my banking application is corrupted is less than 10^{-1000}, I shouldn’t be worried.

In this section we present the so-called Solovay-Strassen primality test. It is a probabilistic one. We, however, start with a different primality test, which is deterministic.

Let us recall ‘little Fermat’ again: *For all $a \in \mathbb{Z}$ we have $a^{p-1} \equiv 1 \mod p$ if p is prime and $p \nmid a$.* Recall that the proof is just that $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p \setminus \{0\}$ is a group of cardinality $p-1$, and any element raised to the order of the group equals the neutral element. But, we know more: $\mathbb{F}_p^\times$ is even a cyclic group. Let b be a generator of it. Then $c := b^{\frac{p-1}{2}}$ satisfies $c^2 = 1 \in \mathbb{F}_p^\times$, hence

$$c = b^{\frac{p-1}{2}} = -1 \in \mathbb{F}_p^\times.$$

This can be turned around to provide a deterministic primality test.

Proposition 8.1. *Let $N \in \mathbb{N}_{\geq 3}$ be odd. Suppose that for all $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ we have $a^{\frac{N-1}{2}} \equiv \pm 1 \mod N$. We suppose that one of the two following statements holds:*

(1) $N \equiv 3 \mod 4$.

(2) There is $b \in (\mathbb{Z}/N\mathbb{Z})^\times$: $b^{\frac{N-1}{2}} \equiv -1 \mod N$.

Then N is a prime number.

Proof. Exercise. □

Corollary 8.2. *Let $N \in \mathbb{N}_{\geq 3}$ be odd. Then the following two statements are equivalent:*

(i) N is prime.

(ii) For all $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ we have (for the Jacobi symbol):

$$a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \mod N$$

Proof. '(i) $\Rightarrow$ (ii)': This is just Euler's result: Proposition 5.6.
'(ii) $\Rightarrow$ (i)': Assume that N is not prime. Squaring (ii) shows that N is Carmichael number and hence squarefree. Let p be a prime divisor of N (necessarily odd) and let $g \in \mathbb{Z}$ be a generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Note that the Legendre symbol $\left(\frac{g}{p}\right)$ is -1 (Exercise). By the Chinese Remainder Theorem there exists $b \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $b \equiv g \mod p$ and $b \equiv 1 \mod q$ for any prime divisor $q \mid N$, $q \neq p$. Hence, the Jacobi symbol $\left(\frac{b}{N}\right)$ equals -1. Thus Proposition 8.1 shows that N is prime, a contradiction. □

Lemma 8.3. *Let $N \in \mathbb{N}_{\geq 3}$ be odd and suppose N is not a prime. Consider the set*

$$A := \{a \in (\mathbb{Z}/N\mathbb{Z})^\times \mid a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \mod N\}.$$

Then $\#A \leq \frac{1}{2}\varphi(N) = \frac{1}{2}\#(\mathbb{Z}/N\mathbb{Z})^\times$.

Proof. We consider the group homomorphism

$$\psi : (\mathbb{Z}/N\mathbb{Z})^\times \to (\mathbb{Z}/N\mathbb{Z})^\times, \quad a \mapsto a^{\frac{N-1}{2}} \cdot \left(\frac{a}{N}\right).$$

Note that A is equal to $\ker(\psi)$. By Corollary 8.2 and the assumption that N is not prime, there is $b \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that $b^{\frac{N-1}{2}} \not\equiv \left(\frac{b}{N}\right) \mod N$, thus $\mathrm{im}(\psi) \supsetneq \{1\}$, so $\#\,\mathrm{im}(\psi) \geq 2$. The isomorphism theorem implies $\mathrm{im}(\psi) \cong (\mathbb{Z}/N\mathbb{Z})^\times/A$, thus by Lagrange's theorem $2 \geq \#\,\mathrm{im}(\psi) = \varphi(N)/\#A$, implying the assertion. □

We can now describe the Solovay-Strassen primality test:

Algorithm 8.4 (Solovay-Strassen primality test)**.**

<u>*Input:*</u> $N \in \mathbb{N}_{\geq 3}$ *odd*, $B \in \mathbb{N}$ *(the 'bound').*
<u>*Output:*</u> `true` *or* `false`.

```
(1) Set $i = 0$.
(2) Choose a 'random' $a \in (\mathbb{Z}/N\mathbb{Z})^\times$.
(3) Calculate the Jacobi symbol $g := \left(\frac{a}{N}\right)$.
(4) Calculate $a^{\frac{N-1}{2}} \mod N$ by fast exponentiation modulo $N$.
(5) If $g \equiv h \mod N$,
      • then replace $i$ by $i + 1$.
        If $i > B$, then return true and stop. If $i \leq B$, then go back to step (2).
      • otherwise, return false and stop.
```

Remark 8.5. *Let $N \in \mathbb{N}_{\geq 3}$ be odd.*

(a) If the Solovay-Strassen algorithm for (N, B) returns `false`*, then N is not a prime number by Corollary 8.2.*

(b) *If the Solovay-Strassen algorithm for (N, B) returns* `true`*, then N is a prime number with 'probability' at least $1 - \frac{1}{2^B}$, in the following (slightly imprecise) sense: If N is not prime, then by Lemma 8.3 the 'probability' that the 'random' element a satisfies the congruence $a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \mod N$ is less than $\frac{1}{2}$. If the 'random' choice of a is really random (like tossing a coin) and independent of this congruence condition, then the probability of satisfying the congruence B consecutive times is at most $\frac{1}{2^B}$.*

In this course we did not and we are not going to treat 'random numbers' and generators of random numbers. The reader should be aware that it is impossible to generate really random numbers by a deterministic device like a computer. So randomness will only be some 'fake randomness', which is – if well done – sufficient for all practical purposes.

9 The Riemann ζ-function and prime numbers

In the rest of the lecture we will prove the prime number theorem. The exposition will follow the book *Funktionentheorie* by Freitag and Busam.

Definition 9.1. *Denote by $\mathbb{P}$ the set of prime numbers.*
Define the prime counting function *as*

$$\pi : \mathbb{R}_{\geq 0} \to \mathbb{N}, \quad x \mapsto \#\{p \in \mathbb{P} \mid p \leq x\},$$

that is, the function that counts the number of primes less than or equal to x.

Theorem 9.2 (Prime number theorem; Hadamard, de la Vallée-Poussin)**.**

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log(x)} = 1.$$

In words: Asymptotically, the prime number function $\pi(x)$ is described by $\frac{x}{\log(x)}$.

The proof of this theorem will occupy the rest of the lecture.
In order to explain the meaning of this theorem, let us look at the following subsets of $\mathbb{N}$:

- $\{n \in \mathbb{N} \mid 2 \mid n\}$, the set of even numbers,
- $\{n \in \mathbb{N} \mid \exists\, m \in \mathbb{N} : n = m^2\}$, the set of squares,
- $\mathbb{P}$, the set of primes.

All three sets are infinite and countable. Can we distinguish nevertheless 'how infinite' they are? In order to do so, we count the number of elements in this set up to the bound x and then compare how these numbers behave for $x \to \infty$.

- $\#\{n \leq x \mid 2 \mid n\} = \lfloor x \rfloor = x + r(x)$ with $|r(x)| \leq 1$, numbers,
- $\#\{n \in \mathbb{N} \mid \exists\, m \in \mathbb{N} : n = m^2\} = \lfloor \sqrt{x} \rfloor = \sqrt{x} + r(x)$ with $|r(x)| \leq 1$,
- $\pi(x) = \frac{x}{\log(x)} + r(x)$ with $\lim_{x \to \infty} r(x) \frac{\log(x)}{x} = 0$.

In this sense, the set of even numbers is much bigger than the set of primes, which in turn is much bigger than the set of squares.
But, there is even more contained in the prime number theorem: Suppose one knows all prime numbers up to x; this knowledge is not enough to predict the next prime number; in order to find it, one has to check all numbers starting from x for primality. This is to say that 'locally' (in a small interval) primes behave very randomly. The prime number theorem, however, says that if one looks 'globally', then the set of prime numbers has much more structure (we know its growth!).
This statement can be made more precise if one takes error bounds into account, which we are not really going to do because of time constraints. Very importantly, the famous still unproved Riemann Hypothesis predicts a very strong error term, which in turn would mean that the set of primes is even more regular than we know as of today.

Definition 9.3. *The* Riemann ζ-function *is defined as*

$$\zeta(s) := \sum_{n=1}^{\infty} n^{-s}$$

for $s \in \mathbb{C}$ *such that* $\mathrm{Re}(s) > 1$. *Here* $n^{-s} = \exp(-s\log(n))$.

Lemma 9.4. *The series defining the Riemann ζ-function converges absolutely and uniformly on* $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > 1+\delta\}$ *for any* $\delta > 0$ *and thus defines a holomorphic function* $\zeta : \{s \in \mathbb{C} \mid \mathrm{Re}(s) > 1\} \to \mathbb{C}$.

Proof. One has the estimate

$$|n^{-s}| = |\exp(-(\sigma+it)\log(n))| = |\exp(-\sigma\log(n))| = |n^{-\sigma}| \leq |\frac{1}{n^{1+\delta}}|.$$

It is easy to prove that $\sum_{n=1}^{\infty}\frac{1}{n^{1+\delta}}$ converges (of course, absolutely, since all terms are positive anyway). General theory about complex power series implies the assertions. □

The relation to prime numbers is established by the following great insight of Euler:

Proposition 9.5. *For any* $s \in \mathbb{C}$ *with* $\mathrm{Re}(s) > 1$, *we have*

$$\zeta(s) = \prod_{p\in\mathbb{P}} (1-p^{-s})^{-1}.$$

In particular, $\zeta(s) \neq 0$ *for all* $s \in \mathbb{C}$ *such that* $\mathrm{Re}(s) > 1$.

Proof. Note that $1 = (1-p^{-s}) \cdot (\sum_{k=0}^{\infty} p^{-ks})$, whence we find (geometric series)

$$(1-p^{-s})^{-1} = \sum_{k=0}^{\infty} p^{-ks}.$$

Let us multiply these together for the first m primes, where we number the primes $p_1, p_2, \ldots$ in the natural way.

$$\prod_{r=1}^{m}(1-p_r^{-s})^{-1} = \prod_{r=1}^{m}\sum_{k=0}^{\infty} p_r^{-ks} = \sum_{k_1,\ldots,k_m=0}^{\infty} (p_1^{k_1}p_2^{k_2}\cdots p_m^{k_m})^{-s}.$$

Since every positive integer is uniquely the product of prime numbers (Theorem 1.3), we find

$$\prod_{r=1}^{m}(1-p_r^{-s})^{-1} = \sum_{n\in\mathcal{A}_m} n^{-s},$$

where $\mathcal{A}_m$ is the subset of $\mathbb{N}_{\geq 1}$ consisting of those integers only divisible by the first m primes. We clearly have $\mathbb{N}_{\geq 1} = \bigcup_{m=1}^{\infty}\mathcal{A}_m$. Thus we obtain

$$\lim_{m\to\infty}\prod_{r=1}^{m}(1-p_r^{-s})^{-1} = \sum_{n=1}^{\infty} n^{-s},$$

where we use that the series converges absolutely and may hence be reordered. As furthermore

$$\sum_{p\in\mathbb{P}} |1-(1-p^{-s})^{-1}| = \sum_{p\in\mathbb{P}}\sum_{k=1}^{\infty}|p^{-ks}| \leq \sum_{n=1}^{\infty}|n^{-s}|,$$

we find (using an exercise on Sheet 11) that the infinite product does not have any zeros for $s\in\mathbb{C}$ such that $\mathrm{Re}(s)>1$. □

Definition 9.6. *The* Mangoldt function *is defined as*

$$\Lambda(n) := \begin{cases} \log(p) & \text{if } n = p^r \text{ with } p \text{ prime and } r\in\mathbb{N}_{\geq 1},\\ 0 & \text{otherwise.}\end{cases}$$

The Chebychev function *is defined as*

$$\psi(x) := \sum_{1\leq n\leq x}\Lambda(n).$$

Proposition 9.7. *For $s\in\mathbb{C}$ with $\mathrm{Re}(s)>1$ we have*

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty}\Lambda(n)n^{-s}.$$

Proof. We first compute the derivative of $f(s) := 1-p^{-s} = 1-\exp(-s\log(p))$:

$$f'(s) = \log(p)\exp(-s\log(p)) = \log(p)p^{-s}.$$

Hence we find for the logarithmic derivative

$$\log(f(s))' = \frac{f'(s)}{f(s)} = \frac{\log(p)p^{-s}}{1-p^{-s}} = \log(p)p^{-s}\sum_{k=0}^{\infty}p^{-ks} = \log(p)\sum_{k=1}^{\infty}p^{-ks}.$$

Thus

$$-\big(\log(\zeta(s))\big)' = -\frac{\zeta(s)'}{\zeta(s)} = -\log(\prod_{p\in\mathbb{P}}(1-p^{-s})^{-1})' =$$

$$-\sum_{p\in\mathbb{P}}\log((1-p^{-s})^{-1})' = \sum_{p\in\mathbb{P}}\log(1-p^{-s})' = \sum_{p\in\mathbb{P}}\log(p)\sum_{k=1}^{\infty}p^{-ks},$$

where we used that $\sum_{p\in\mathbb{P}}\log(1-p^{-s})$ is absolutely converging by an Exercise on Sheet 11. Write $s=\sigma+it$ with $\sigma>1$. Choose $0<\epsilon<\sigma-1$. There is N such that for all $n>N$ we have $\log(n)<n^{\epsilon}$, hence $\frac{\log(n)}{n^s}\leq\frac{1}{n^{s-\epsilon}}$. Thus we have the estimate

$$\sum_{p\in\mathbb{P}}\sum_{k=1}^{\infty}|\log(p)p^{-ks}|\leq\sum_{n=1}^{\infty}\frac{\log(n)}{n^{\sigma}}\leq\sum_{n=N+1}^{\infty}\frac{1}{n^{\sigma-\epsilon}}+\sum_{n=1}^{N}\frac{\log(n)}{n^{\sigma}};$$

the series hence converges absolutely and may be reordered. But, reordering precisely yields the assertion. □

The next lemma shows that the contribution of the proper prime powers p^n for $n\geq 2$ to the Chebychev function ψ is 'small' in a precise sens:

Lemma 9.8. *Define*

$$\Theta(x):=\sum_{p\in\mathbb{P},p\leq x}\log(p).$$

Then

$$\psi(x)=\Theta(x)+O(\log(x)\sqrt{x})$$

(i.e. $\Psi(x)-\Theta(x)=O(\log(x)\sqrt{x})$*).*

Proof. We bound the number of proper prime powers p^n for $n\geq 2$ up to x, that is $\#\{p^n\leq x\mid p\text{ prime },n\geq 2\}$. If $p^n\leq x$, then $p\leq x^{1/n}$ and consequently $\log(2)\leq\log(p)\leq\frac{1}{n}\log(x)$, which implies the upper bound

$$n\leq\frac{\log(x)}{\log(2)}.$$

We have

$$\begin{aligned}\#\{p^n\leq x\mid p\text{ prime },n\geq 2\}\leq\sum_{2\leq n\leq\frac{\log(x)}{\log(2)}}\ \sum_{p\leq x^{1/n}}1=\sum_{2\leq n\leq\frac{\log(x)}{\log(2)}}x^{1/n}\\ =\sqrt{x}+\sum_{3\leq n\leq\frac{\log(x)}{\log(2)}}x^{1/n}=O(\sqrt{x})\end{aligned}$$

because $\frac{\log(x)}{\log(2)}x^{1/3}=O(\sqrt{x})$ as $\log(x)=O(x^{\alpha})$ for any $\alpha>0$. The assertion of the lemma now follows immediately from $\log(p)\leq\log(x)$. □

Proposition 9.9. *(a) The following statements are equivalent:*

(i) $\Theta(x)=\sum_{p\in\mathbb{P},p\leq x}\log(p)=x+o(x)$.

(ii) $\psi(x)=\sum_{1\leq n\leq x}\Lambda(n)=x+o(x)$.

(b) The validity of any of the two implies the prime number theorem 9.2.

Proof. (a) The equivalence of (i) and (ii) is immediate from Lemma 9.8 in view of $\log(x)\sqrt{x} = o(x)$.
(b) We define the remainder function as

$$r(x) = \frac{\Theta(x) - x}{x}, \text{ so that } \Theta(x) = x(1 + r(x)).$$

Assertion (i) is equivalent to $\lim_{x\to\infty} r(x) = 0$. The crude estimate $\log(p) \leq \log(x)$ for any prime $p \leq x$ gives

$$\Theta(x) \leq \pi(x)\log(x)$$

and thus

$$\pi(x) \geq \frac{x}{\log(x)}(1 + r(x)).$$

We also need show an inequality in the other way. Let $0 < q < 1$, which we will choose later specifically. We have the trivial inequality $\pi(x^q) \leq x^q$. It implies

$$\Theta(x) \geq \sum_{x^q \leq p \leq x} \log(p) \geq \log(x^q)\cdot(\pi(x) - \pi(x^q)) = q\log(x)(\pi(x) - \pi(x^q)) \geq q\log(x)(\pi(x) - x^q).$$

We thus obtain

$$\pi(x) \leq \frac{\Theta(x)}{q\log(x)} + x^q = \frac{x}{\log(x)} \cdot \frac{1 + r(x)}{q} + x^q = \frac{x}{\log(x)} \cdot \left(1 + \frac{1 - q + r(x)}{q} + \frac{\log(x)}{x^{1-q}}\right),$$

which is valid for all $0 < q < 1$ and all x. The idea now is to choose q in dependence of x such that $q \to 1$ (for $x \to \infty$) and such that the term on the right still tends to zero for $x \to \infty$. This can be achieved by $q := 1 - 1/\sqrt{\log(x)}$. The only non-trivial thing to check is:

$$\frac{\log(x)}{x^{1-q}} = \frac{\log(x)}{x^{1/\sqrt{\log(x)}}} = o(1)$$

by an exercise from Sheet 11. □

In order to prove the prime number theorem in the next two sections, we shall prove the statement from Proposition 9.9.

10 On the analytic continuation of the Riemann zeta function

We have verified (and the verification was really easy) that $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ defines a holomorphic function on $\{\mathrm{Re}(s) > 1\}$. You also know from your first course in analysis that the harmonic series $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges, hence, it does not make sense to evaluate the series defining ζ at 1.
The key to the prime number theorem is in fact to continue ζ meromorphically just a little bit left of $\{\mathrm{Re}(s) \geq 1\}$ in such a way that the only pole is at 1 (that manifests itself in the divergence of the harmonic series).
Since we are going to use it a lot, let us remark

$$\begin{aligned} |t^s| = |\exp(s\log(t))| = |\exp(\sigma\log(t) + i\tau\log(t))| &= |\exp(\sigma\log(t))| \cdot |\exp(i\tau\log(t))| \\ &= |\exp(\sigma\log(t))| = t^\sigma, \end{aligned}$$

where $s = \sigma + i\tau$ and $t \in \mathbb{R}_{>0}$.

Proposition 10.1. *(a) Define $\beta : \mathbb{R} \to \mathbb{R}$ as $\beta(t) := t - \lfloor t \rfloor - 1/2$ (draw sketch). The integral*

$$F(s) := \int_1^\infty \frac{\beta(t)}{t^{1+s}} dt$$

converges absolutely for $\mathrm{Re}(s) > 0$ and defines a holomorphic function in this area.

(b) For $\mathrm{Re}(s) > 1$ we have the equality

$$\zeta(s) = \frac{1}{2} + \frac{1}{s-1} - sF(s).$$

Proof. (a) We use the estimate $|\frac{\beta(t)}{t^{1+s}}| < |\frac{1}{t^{1+\sigma}}|$. It implies that (with $s = \sigma i + \tau$)

$$|\int_a^b \frac{\beta(t)}{t^{1+s}}|dt \leq \int_a^b \frac{1}{t^{1+\sigma}} dt \leq -\frac{1}{\sigma} t^{-\sigma}|_a^b = \frac{1}{\sigma}\left(\frac{1}{a^\sigma} - \frac{1}{b^\sigma}\right).$$

In particular, $|F(s)| \leq \frac{1}{\sigma}$ and the integral converges. From general facts it follows that the function $F_N(s) := \int_1^N \frac{\beta(t)}{t^{1+s}} dt$ is holomorphic (this is not very difficult to prove). Note that

$$|F(s) - F_N(s)| = |\int_N^\infty \frac{\beta(t)}{t^{1+s}} dt| \leq \frac{1}{\sigma N^\sigma} \leq \frac{1}{\beta N^\beta}$$

for any $\beta > 0$. Hence in any open neighbourhood of s which is contained in $\{\mathrm{Re}(z) \geq \beta\}$ the sequence of holomorphic functions F_N converges to F uniformly, implying that F is holomorphic there, since locally uniformly convering sequences of holomorphic functions are holomorphic.
(b) The maybe at first sight strange choice of β is explained by the formula

$$\int_n^{n+1} \beta(t) \left(t^{-s}\right)' dt = \frac{1}{2}\big((n+1)^{-s} + n^{-s}\big) - \int_n^{n+1} t^{-s} dt,$$

which is just integration by parts, using that on the open interval $(n, n+1)$ we have $\beta(t) = t-(n+\frac{1}{2})$. Hence (recalling the well known formulas $(t^{-s})' = -s\frac{1}{t^{s+1}}$ and $\int t^{-s} dt = \frac{1}{1-s} t^{1-s}$),

$$\begin{aligned} -sF_N(s) &= \sum_{n=1}^{N-1} \int_n^{n+1} \beta(t) \left(t^{-s}\right)' dt \\ &= \frac{1}{2} \sum_{n=1}^{N-1} \big((n+1)^{-s} + n^{-s}\big) - \int_1^N t^{-s} dt \\ &= \sum_{n=1}^{N} \frac{1}{n^s} - \frac{1}{2}\big(N^{-s} + 1\big) + \frac{N^{1-s} - 1}{s-1} \end{aligned}$$

Taking the limit $N \to \infty$ yields the proposition, as $\mathrm{Re}(s) > 1$. □

Corollary 10.2. *The function $s \mapsto (s-1)\zeta(s)$ can be continued to a holomorphic function on the open set $\{\mathrm{Re}(s) > 0\}$. Its value at 1 is 1.*
Thus, the Riemann-zeta function $\zeta(s)$ can be continued to a meromorphic function on the open set $\{\mathrm{Re}(s) > 0\}$ (still denoted ζ) having a single pole at $s = 1$ of order 1 and residue 1.

Proof. This is clear since we have $(s-1)\zeta(s) = 1 + \frac{s-1}{2} - s(s-1)F(s)$ by Proposition 10.1. □

Proposition 10.3. *For every $m \in \mathbb{N}$ there is a constant $C_m > 0$ such that the m-th derivative of the Riemann-zeta function satisfies*

$$\left|\zeta^{(m)}(s)\right| \leq C_m\,|s|$$

for all s such that $\operatorname{Re}(s) > 1$ *and* $|\operatorname{Im}(s)| \geq 1$.

Proof. Let us first take $\sigma = \operatorname{Re}(s) \geq 2$. Then

$$|\zeta(s)| \leq \sum_{n=1}^{\infty} |\frac{1}{n^s}| = \sum_{n=1}^{\infty} \frac{1}{n^\sigma} \leq \sum_{n=1}^{\infty} \frac{1}{n^2} = \zeta(2),$$

so the Riemann-zeta function is bounded there. By the way, the value $\zeta(2)$ is $\pi^2/6$, as one usually shows in a course on real analysis. In the same way one gets $|\zeta^{(m)}(s)| \leq \zeta^{(m)}(2)$.
Thus we assume now $1 < \sigma < 2$ and $|\tau| \geq 1$ with $\tau = \operatorname{Im}(s)$. We use $\zeta(s) = \frac{1}{2} + \frac{1}{s-1} - sF(s)$ from Proposition 10.1. It is clear that in this area $\frac{1}{2} + \frac{1}{s-1}$ is bounded by a constant; the same statement is true for all its derivatives. It suffices thus to show that for every $m \in \mathbb{N}$ the m-th derivative $|F^{(m)}(s)|$ is bounded by a constant. Note that for $t \geq 1$ one has $|\log(t)| \leq c_m t^{\frac{1}{2m}}$ for some constant c_m. Thus we obtain

$$|F^{(m)}(s)| = \left|\int_1^\infty (-\log(t))^m \frac{\beta(t)}{t^{s+1}} dt\right| \leq c_m \int_1^\infty \frac{1}{t^{\frac{3}{2}}} dt < \infty,$$

a converging integral. This finishes the proof. □

Proposition 10.4. *The meromorphically continued Riemann-zeta function $\zeta(s)$ has no zero on the closed half plane $\{\operatorname{Re}(s) \geq 1\}$. Moreover, there is $\delta > 0$ such that for all $s = \sigma i + \tau \in \mathbb{C}$ with $\sigma > 1$ and $|\tau| \geq 1$ one has*

$$|\zeta(s)| \geq \delta \frac{1}{|\tau|^4}.$$

Proof. We show this proposition in a number of steps.

(1) Let us first remark that the statement is true for $\sigma > 2$ because then

$$|\zeta(s)| \geq 1 - |\zeta(s) - 1| \geq 1 - \sum_{n=2}^{\infty} \frac{1}{n^2} = 2 - \zeta(2) = 2 - \frac{\pi^2}{6} > 0.35.$$

So, we can restrict to $1 < \sigma \leq 2$, which we will use below.

(2) We take the logarithm of the Euler product of the Riemann-zeta function and use the well-known Taylor expansion of $\log(1-z)$ valid for $|z| < 1$:

$$\log(\zeta(s)) = \log\left(\prod_{p\in\mathbb{P}} (1-p^{-s})^{-1}\right) = \sum_{p\in\mathbb{P}} -\log(1-p^{-s}) = \sum_{p\in\mathbb{P}} \sum_{m=1}^{\infty} \frac{p^{-ms}}{m} = \sum_{n=1}^{\infty} b_n n^{-s},$$

where $b_n = \begin{cases} \frac{1}{m} & \text{if } n = p^m \text{ for } p \in \mathbb{P}, m \in \mathbb{N}, \\ 0 & \text{otherwise.} \end{cases}$

(3) Let $a \in \mathbb{C}$ such that $|a| = 1$. Then $\operatorname{Re}(a^4) + 4\operatorname{Re}(a^2) + 3 \geq 0$.

Note $(a + \bar(a))^4 = a^4 + \bar(a)^4 + 4(a^2 + \bar(a)^2) + 6$ (using $a\bar{a} = |a|^2 = 1$). We rewrite this and obtain

$$0 \leq \big(2\operatorname{Re}(a)\big)^4 = 2\operatorname{Re}(a^4) + 8\operatorname{Re}(a^2) + 6,$$

yielding the claim.

(4) Applying (1) with $a = n^{-i\tau/2}$ gives

$$\operatorname{Re}(n^{-2i\tau}) + 4\operatorname{Re}(n^{-i\tau}) + 3 \geq 0.$$

Multiplying with the real number $n^{-\sigma}$ yields

$$\operatorname{Re}(n^{-(\sigma+2i\tau)}) + 4\operatorname{Re}(n^{-(\sigma+i\tau)}) + 3n^{-\sigma} \geq 0.$$

(5) Taking the sum $\sum_{n=1}^{\infty} b_n \bullet$ we get

$$\operatorname{Re}(\sum_{n=1}^{\infty} b_n n^{-(\sigma+2i\tau)}) + 4\operatorname{Re}(\sum_{n=1}^{\infty} b_n n^{-(\sigma+i\tau)}) + 3\sum_{n=1}^{\infty} b_n n^{-\sigma} \geq 0.$$

Using $|\exp(z)| = \exp(\operatorname{Re}(z))$ we get for $\operatorname{Re}(s) = \sigma > 1$ by taking $\exp$ (in order to get rid of $\log$):

$$|\zeta(\sigma + i2\tau)| \cdot |\zeta(\sigma + i\tau)|^4 \cdot |\zeta(\sigma)|^3 \geq 1. \tag{10.1}$$

(6) From the Euler product it follows that $\zeta(s) \neq 0$ for all $s \in \mathbb{C}$ with $\operatorname{Re}(s) > 1$. Let us now assume $\operatorname{Re}(s) = 1$ in order to derive the first assertion. Let us suppose that $\zeta(s) = 0$ for $s = 1 + it$. Then we rewrite Equation (10.1) as

$$\left| \frac{\zeta(\sigma + it) - \overbrace{\zeta(1 + it)}^{=0}}{\sigma - 1} \right|^4 \cdot |\zeta(\sigma + i2t)| \cdot |\zeta(\sigma)(\sigma - 1)|^3 \geq \frac{1}{|\sigma - 1|}.$$

Letting σ tend to 1 from the right, we obtain on the left hand side the value $|\zeta'(1 + it)| \cdot |\zeta(1+i2t)|$, whereas the right hand side diverges. This contradiction shows that ζ does not possess a zero on the vertical axis $\operatorname{Re}(s) = 1$.

(7) Rewriting Equation (10.1) gives

$$|\zeta(s)| \geq (\sigma - 1)^{3/4} \left(\frac{1}{|\zeta(\sigma + i2\tau)|} \right)^{1/4} \cdot \left(\frac{1}{\zeta(\sigma)(\sigma - 1)} \right)^{3/4}.$$

By Corollary 10.2 we know that $\zeta(\sigma)(\sigma - 1)$ is a continuous function on the closed interval $1 \leq \sigma \leq 2$, whence it is bounded above by some positive constant $C_1 > 0$. By Proposition 10.3 we have

$$|\zeta(\sigma + i2\tau)| \leq C_2|\tau|$$

for some constant $C_2 > 0$ Putting these estimates together we have

$$|\zeta(s)| \geq C_3(\sigma - 1)^{3/4} \frac{1}{|\tau|^{1/4}}$$

with some constant $C_3 > 0$.

(8) In view of the formula we aim at, we put

$$\sigma(\tau) := 1 + \epsilon \frac{1}{|\tau|^5},$$

for some $\epsilon > 0$ to be chosen below. With this definition we get for $\sigma \geq \sigma(\tau)$

$$|\zeta(s)| \geq C_3 \cdot \frac{\epsilon^{3/4}}{|\tau|^{15/4}} \cdot \frac{1}{|\tau|^{1/4}} = C_3 \cdot \epsilon^{3/4} \cdot \frac{1}{|\tau|^4}.$$

This inequality is precisely of the required form (that's why $\sigma(\tau)$ was chosen this way); note that it holds for any choice of $\epsilon > 0$.

(9) We still have to treat the case $\sigma < \sigma(\tau)$. Due to the existence of the derivative we have

$$\zeta(\sigma + i\tau) = \zeta(\sigma(\tau) + i\tau) - \int_{\sigma}^{\sigma(\tau)} \zeta'(u + i\tau) du.$$

By Proposition 10.3 we have (since $|s| \geq |\tau|$)

$$|\zeta'(\sigma + i\tau)| \leq C_4 |\tau|.$$

Thus we obtain the estimate

$$|\zeta(\sigma + i\tau)| \geq |\zeta(\sigma(\tau) + i\tau)| - C_4 \cdot (\sigma(\tau) - 1) \cdot |\tau|.$$

Using the estimate from (6) we get

$$\begin{aligned} |\zeta(\sigma + i\tau)| &\geq C_3(\sigma(\tau) - 1)^{3/4} \frac{1}{|\tau|^{1/4}} - C_4 \cdot (\sigma(\tau) - 1) \cdot |\tau| \\ &= C_3(\epsilon \frac{1}{|\tau|^5})^{3/4} \frac{1}{|\tau|^{1/4}} - C_4 \cdot (\epsilon \frac{1}{|\tau|^5}) \cdot |\tau| = (C_3 \epsilon^{3/4} - C_4 \epsilon) \frac{1}{|\tau|^4}. \end{aligned}$$

We now choose $\epsilon > 0$ small enough such that $\delta := C_3 \epsilon^{3/4} - C_4 \epsilon > 0$. This finishes the estimate also for $\sigma < \sigma(\tau)$.

□

These estimates will be applied to the function (defined as in Proposition 9.7)

$$D(s) := -\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \Lambda(n) n^{-s}.$$

It will play the major role in the proof of the prime number theorem.

Corollary 10.5. *The function $D(s)$ has a pole of first order at 1 of residue 1 and the function $(s - 1)D(s)$ can be continued analytically to an open set that contains $\{z \in \mathbb{C} \mid \operatorname{Re}(z) \geq 1\}$. Moreover, there is a constant $C > 0$ such that*

$$|D(s)| \leq C |\tau|^5$$

for all $s = \sigma + i\tau$ with $\sigma > 1$ and $|\tau| \geq 1$.

Proof. We have

$$(s-1)D(s) = -\frac{(s-1)\zeta(s)'}{\zeta(s)} = -\frac{\big((s-1)\zeta(s)\big)' - \zeta(s)}{\zeta(s)} = 1 - \frac{\big((s-1)\zeta(s)\big)'}{\zeta(s)}.$$

Using Corollary 10.2 and the first assertion of Proposition 10.4, this function has the value 1 at 1 and is analytic everywhere on $\{\mathrm{Re}(s) > 0\}$, where $\zeta(s) \neq 0$, that is, at least for $\mathrm{Re}(s) \geq 1$. The estimate follows immediately from the estimates in Propositions 10.3 and 10.4. □

11 A Tauberian Theorem

In this section we will prove the prime number theorem 9.2 by proving that the remainder term $r(x) = \frac{\psi(x)-x}{x}$ in

$$\psi(x) = \sum_{1 \leq n \leq x} \Lambda(n) = x(1 + r(x))$$

tends to 0 as x tends to ∞. That this suffices was proved in Proposition 9.9.
For $k \in \mathbb{N}$ we define for real positive x

$$A_k(x) := \frac{1}{k!} \sum_{n \leq x} \Lambda(n)(x-n)^k.$$

We have the following obvious statements:

- $\psi(x) = A_0(x)$,
- $A'_{k+1}(x) = A_k(x)$ for all $k \in \mathbb{N}$,
- $A_{k+1}(x) = \int_1^x A_k(t)dt$, and
- $A_k(x)$ is continuous if $k \geq 1$ and piece-wise continuous for all $k \in \mathbb{N}$.

We also generalise the remainder term by defining it by the equation

$$A_k(x) = \frac{x^{k+1}}{(k+1)!}(1 + r_k(x)).$$

Note that $r_0(x) = r(x)$ and that $r_k(x)$ is continous if $k \geq 1$.
The strategy is to conclude the convergence of $r_0(x)$ from the convergence of $r_k(x)$ by descending the k down to 0. We will even be able to obtain an error term. This is done by the following proposition.

Proposition 11.1. *Let $k \in \mathbb{N}$. If $r_{k+1}(x) = O(1/\log(x)^{1/N})$, then $r_k(x) = O(1/\log(x)^{1/(2N)})$*

Proof. As all $\Lambda(n)$ are positive, the functions $A_k(x)$ are monotonously increasing (for the variable x). Thus one has for all $0 < h < 1$:

$$\begin{aligned} hxA_k(x) &= hx \cdot \frac{x^{k+1}}{(k+1)!}(1 + r_k(x)) = h(k+2) \cdot \frac{x^{k+2}}{(k+2)!}(1 + r_k(x)) \\ &\leq \int_x^{x+hx} A_k(t)dt = A_{k+1}(x+hx) - A_{k+1}(x) \\ &= \frac{1}{(k+2)!}\Big((x+hx)^{k+2}(1 + r_{k+1}(x+hx)) - x^{k+2}(1 + r_{k+1}(x))\Big). \end{aligned}$$

Rewriting gives:

$$1 + r_k(x) \leq \frac{1}{h(k+2)} \Big((1+h)^{k+2} \big(1 + r_{k+1}(x+hx)\big) - \big(1 + r_{k+1}(x)\big) \Big).$$

Let now $\epsilon(x) := \sum_{0 \leq \xi \leq 1} |r_{k+1}(x + \xi x)| < \infty$ (for, $r_{k+1}(x)$ is continuous). From the assumption $r_{k+1}(x) = O(1/\log(x)^{1/N})$ we obtain $\epsilon(x) = O(1/\log(x)^{1/N})$; in particular, for $x \to \infty$, $\epsilon(x)$ tends to 0. Plugging in the definition of $\epsilon(x)$ yields

$$\begin{aligned} r_k(x) &\leq \frac{1}{h(k+2)} \Big((1+h)^{k+2} \big(1 + \epsilon(x)\big) - \big(1 - \epsilon(x)\big) \Big) - 1 \\ &= \frac{\big((1+h)^{k+2} + 1\big)\,\epsilon(x)}{h(k+2)} + \frac{(1+h)^{k+2} - (1 + h(k+2))}{h(k+2)} \\ &= \frac{\big((1+h)^{k+2} + 1\big)\,\epsilon(x)}{h(k+2)} + \frac{\sum_{m=2}^{k+2} \binom{k+2}{m} h^m}{h(k+2)}. \end{aligned}$$

We now specialise $h := \sqrt{\epsilon(x)}$. This is less than 1 for x big enough. We obtain

$$r_k(x) \leq C_1 \cdot \sqrt{\epsilon(x)}$$

for some constant $C_1 > 0$.
In a very similar way (we omit the details) one also obtains

$$r_k(x) \geq -C_2 \cdot \sqrt{\epsilon(x)}$$

for some constant $C_2 > 0$. Thus, $|r_k(x)| \leq C\sqrt{\epsilon(x)} = O(1/\log(x)^{1/(2N)})$. □

The final aim is to prove the following proposition.

Proposition 11.2. *For* $\mathbb{N} \ni k \geq 7$ *we have* $r_k(x) = O(1/\log(x))$.

Corollary 11.3. *We have* $r(x) = O(1/\log(x)^{1/128})$.
In particular, $\lim_{x\to\infty} r(x) = 0$ *and the prime number theorem follows.*

Proof. We start with $r_7(x) = O(1/\log(x))$ from Proposition 11.2 and apply Proposition 11.1 seven times (note $128 = 2^7$). □

We keep writing $s = \sigma + i\tau$ with $\sigma, \tau \in \mathbb{R}$. We also introduce the notation

$$\int_{\sigma - i\infty}^{\sigma + i\infty} f(s) ds := \int_{-\infty}^{\infty} f(\sigma + i\tau) d\tau.$$

We start with a very useful lemma; it is based on the residue theorem and exploits it in order to get a function that is constant zero for real values on $(0, 1]$ and positive for all $a > 1$. It will allow to ‘cut off’ an infinite series.

Lemma 11.4. *For* $k \in \mathbb{N}_{\geq 2}$ *and all* $\sigma > 0$ *we have*

$$\frac{1}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} \frac{a^s}{s \cdot (s+1) \cdot \ldots \cdot (s+k)} ds = \begin{cases} 0 & \text{if } 0 < a \leq 1, \\ \frac{1}{k!}(1 - \frac{1}{a})^k & \text{if } 1 < a. \end{cases}$$

Proof. In order to compute the integral $\int_{\sigma-i\infty}^{\sigma+i\infty}$ we compute $\int_{\sigma-iR}^{\sigma+iR}$ and then let R tend to infinity. In order to abbreviate, let us write

$$f(z) := \frac{a^z}{z \cdot (z+1) \cdot \ldots \cdot (z+k)}.$$

Note that $f(z)$ is meromorphic with poles only at $0, -1, -2, \ldots, -k$. We have to distinguish the two cases.

(1) $0 < a \leq 1$.

In this case, the absolute value $|a^z| = a^{\mathrm{Re}(z)}$ is bounded by $a^\sigma > 0$ for all $z \in \mathbb{C}$ with $\mathrm{Re}(z) \geq \sigma$. Moreover, for all $z \in \mathbb{C}$ with $|z| = R$ we have $|f(z)| \leq \frac{a^\sigma}{R(R-1)}$. Since f does not have any poles on the right half plane, Cauchy's integral theorem tells us that the integral $\int_{\sigma-iR}^{\sigma+iR} f(z)dz + \int_{\gamma_R} f(z)dz$ vanishes, where γ_R is the arc on the circle of radius R around 0 starting at $\sigma + iR$ and running through the right half plane to $\sigma - iR$. The above estimate shows $\lim_{R\to\infty} \int_{\gamma_R} f(z)dz = 0$, thus $\lim_{R\to\infty} \int_{\sigma-iR}^{\sigma+iR} f(z)dz = 0$.

(2) $1 < a$.

In this case we cannot argue as before, as the integral along the arc on the circle of radius R through the right half plane 'explodes'. We thus have to take the other way, through the left half plane. By the very same arguments as above, the integral along the circle through the left half plane tends to 0 for $R \to \infty$.

However, there are poles in the left half plane! This explains the great difference in the behaviour. We may not use Cauchy's integral theorem. Instead, the answer is given by the residue theorem: For $R > k$ (so as to see all poles) we obtain

$$\lim_{R\to\infty} \int_{\sigma-iR}^{\sigma+iR} f(z)dz = 2\pi i \sum_{m=0}^{k} \mathrm{Res}(f; -m) = 2\pi i \sum_{m=0}^{k} \frac{(-a)^{-m}}{m!(k-m)!} = 2\pi i \frac{1}{k!}(1 - \frac{1}{a})^k,$$

as required. (We used the standard formula for computing residues of functions with a simple pole of order 1.)

□

We use the previous lemma in order to give a description of $A_k(x)$ in terms of an integral, which we subsequently will estimate.

Proposition 11.5. *For all $k \in \mathbb{N}_{\geq 1}$ and all $\sigma > 1$ we have*

$$A_k(x) = \frac{1}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} \frac{D(s)x^{s+k}}{s \cdot (s+1) \cdot \ldots \cdot (s+k)} ds.$$

Proof. We obtain the proposition from the following calculation (based on Lemma 11.4).

$$\begin{aligned}
A_k(x) &= \sum_{1\le n\le x} \Lambda(n)\frac{1}{k!}(n-x)^k \\
&= \sum_{n=1}^{\infty} \Lambda(n)x^k \begin{cases} \frac{1}{k!}(1-\frac{n}{x})^k & \text{if } x > n, \\ 0 & \text{if } x \le n \end{cases} \\
&= \sum_{n=1}^{\infty} \Lambda(n)x^k \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} \frac{\left(\frac{x}{n}\right)^s}{s\cdot(s+1)\cdot\ldots\cdot(s+k)}ds \\
&\overset{(*)}{=} \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} \frac{\sum_{n=1}^{\infty}\Lambda(n)x^k\left(\frac{x}{n}\right)^s}{s\cdot(s+1)\cdot\ldots\cdot(s+k)}ds \\
&= \frac{1}{2\pi i}\int_{\sigma-i\infty}^{\sigma+i\infty} \frac{D(z)x^{s+k}}{s\cdot(s+1)\cdot\ldots\cdot(s+k)}ds.
\end{aligned}$$

For the equality $\overset{(*)}{=}$ one uses that

$$\int_{\sigma-i\infty}^{\sigma+i\infty}\left|\frac{\left(\sum_{n=N+1}^{\infty}\Lambda(n)\frac{1}{n^s}\right)x^s}{s\cdot(s+1)\cdot\ldots\cdot(s+k)}\right|ds \le \int_{\sigma-i\infty}^{\sigma+i\infty}\frac{\left(\sum_{n=N+1}^{\infty}\Lambda(n)\frac{1}{n^\sigma}\right)x^\sigma}{|s\cdot(s+1)\cdot\ldots\cdot(s+k)|}ds$$

tends to 0 for $N\to\infty$ (note that the infinite sum in the numerator does not involve the integration variable!). This implies that

$$\left|\int_{\sigma-i\infty}^{\sigma+i\infty}\frac{\sum_{n=1}^{\infty}\Lambda(n)x^k\left(\frac{x}{n}\right)^s}{s\cdot(s+1)\cdot\ldots\cdot(s+k)}ds - \sum_{n=1}^{N}\Lambda(n)x^k\int_{\sigma-i\infty}^{\sigma+i\infty}\frac{\left(\frac{x}{n}\right)^s}{s\cdot(s+1)\cdot\ldots\cdot(s+k)}ds\right|$$

tends to 0 for $N\to\infty$, showing $\overset{(*)}{=}$. □

Now it remains to estimate the integral of Proposition 11.5. For this, one uses the following general result due to Riemann and Lebesgue.

Proposition 11.6. *Let $I=(a,b)\subseteq\mathbb{R}$ an open, but not necessarily finite, interval of the real line and $f: I\to\mathbb{C}$ a function satisfying*

- *f is bounded on I,*
- *f is continously differentiable, and*
- *f and f' are absolutely integrable on I.*

Then for any $x\in\mathbb{R}_{>0}$ the function $g(t):=f(t)x^{it}$ is absolutely integrable on I and one has

$$\int_a^b f(t)x^{it}dt = O(1/\log(x)).$$

Proof. We choose sequences (a_n) and (b_n) such that

$$a_n \xrightarrow{n\to\infty} a,\quad b_n \xrightarrow{n\to\infty} b,\ \text{and } a<a_n<b_n<b \text{ for all } n.$$

Then we have by definition and integration by parts

$$\begin{aligned}\int_a^b f(t)x^{it}dt &= \lim_{n\to\infty}\int_{a_n}^{b_n} f(t)x^{it}dt\\ &= \frac{1}{i\log(x)}\lim_{n\to\infty}\int_{a_n}^{b_n} f(t)e^{it}dt\\ &= \frac{1}{\log(x)}\lim_{n\to\infty}\int_{a_n}^{b_n} f(t)\left(\frac{1}{i}e^{it}\right)'dt\\ &= \frac{1}{\log(x)}\lim_{n\to\infty}\left(\left(f(b_n)e^{ib_n}-f(a_n)e^{ia_n}\right)-\int_{a_n}^{b_n} f'(t)e^{it}dt\right).\end{aligned}$$

As f is bounded, $\lim_{n\to\infty}|f(b_n)e^{ib_n}-f(a_n)e^{ia_n}|$ is bounded above by a constant. Furthermore, since f' is absolutely integrable on I, also $\lim_{n\to\infty}\left|\int_{a_n}^{b_n} f'(t)e^{it}dt\right|$ is bounded above by a constant, implying the proposition. □

We can now finish the proof of the prime number theorem.

Proof of Proposition 11.2. We must prove

$$A_k(x) = \frac{x^{k+1}}{(k+1)!} + O(x^{k+1}/\log(x)).$$

We proceed in several steps.

(1) Let γ be the path starting at $1-iR$, going in a straight line up to $1-i$, then going right to $2-i$, then going straight down to $2-iR$ and finally left back to $1-iR$. As the function $f(s) := \frac{a^s}{s\cdot(s+1)\cdot\ldots\cdot(s+k)}$ is analytic inside and on this curve, Cauchy's integral theorem tells us that $\int_\gamma f(s)ds$ vanishes. Note that inside the area of this path we have the estimate (for fixed x)

$$\left|\frac{D(s)x^{s+k}}{s\cdot(s+1)\cdot\ldots\cdot(s+k)}\right| \le C_1|\tau|^{5-7-1} \le C_1|\tau|^{-3}.$$

In particular, the integral along the lower horizontal segment tends to 0 as R tends to ∞.

Making a similar argument on the upper part, we obtain from Proposition 11.5

$$A_k(x) = \frac{1}{2\pi i}\int_L \frac{D(s)x^{s+k}}{s\cdot(s+1)\cdot\ldots\cdot(s+k)}ds,$$

where L is the path starting at $1-i\infty$, going up in a straight line to $1-i$, then going right to $2-i$, then going up in a straight line to $2+i$, then going left to $1+i$, and finally going up in a straight line to $1+i\infty$.

(2) We now estimate the integral on the vertical part from $1-i\infty$ up to $1-i$ by Proposition 11.6. It yields (in view of the boundedness of $f(s)$ proved in (1)):

$$\left|\int_{1-i\infty}^{1-i}\frac{D(s)x^{k+s}}{s\cdot(s+1)\cdot\ldots\cdot(s+k)}ds\right| = O(x^{k+1}/\log(x)).$$

So, this part will vanish in the error term. The same argument applies to give

$$\left|\int_{1+i}^{1+i\infty} \frac{D(s)x^{k+s}}{s\cdot(s+1)\cdot\ldots\cdot(s+k)}ds\right| = O(x^{k+1}/\log(x)).$$

(3) It remains to evaluate the integral on the path starting at $1-i$, going right to $2-i$, then going up in a straight line to $2+i$, and finally going left to $1+i$. We shall again use the residue theorem to do so. As $(s-1)D(s)$ has an analytic continuation to an open set containing $\{z \in \mathbb{C} \mid \mathrm{Re}(z) \geq 1\}$, there is $0 < \sigma < 1$ such that $D(s)$ is a meromorphic function on $\{z \in \mathbb{C} \mid \sigma/2 < \mathrm{Re}(z) < 3, |\tau| \leq 2\}$ having a unique pole at $z = 1$ with residue 1. Thus,

$$\mathrm{Res}(\frac{D(s)x^{k+s}}{s\cdot(s+1)\cdot\ldots\cdot(s+k)};1) = \frac{x^{k+1}}{(k+1)!}.$$

Let δ be the path starting at $\sigma - i$, going right to $2 - i$, going up to $2 + i$, going left to $\sigma + i$ and going back down to $\sigma - i$. The residue theorem gives:

$$\frac{1}{2\pi i}\int_\delta \frac{D(s)x^{k+s}}{s\cdot(s+1)\cdot\ldots\cdot(s+k)}ds = \frac{x^{k+1}}{(k+1)!}.$$

This looks like the result we are aiming at! So, it remains to prove that the contribution of the part of the path δ that is left of the vertical line at 1 only contributes to the error term.

(4) We first take care of the integral over the vertical line from $\sigma + i$ to $\sigma - i$ by Proposition 11.6. It yields:

$$\left|\int_{\sigma+i}^{\sigma-i} \frac{D(s)x^{k+s}}{s\cdot(s+1)\cdot\ldots\cdot(s+k)}ds\right| = O(x^{k+\sigma}/\log(x)).$$

So, this part will vanish in the error term, as required.

(5) It remains to treat the integrals over the vertical lines from $1 + i$ to $\sigma + i$ and from $\sigma - i$ to $1 - i$. As the second one works precisely as the first one, we focus on the first one. On this part the continous function $\frac{D(s)x^{k+s}}{s\cdot(s+1)\cdot\ldots\cdot(s+k)}$ can be bounded above by some constant. Thus, it remains to estimate

$$x^{k+1}\int_\sigma^1 x^u du = \frac{x^{k+1}}{\log(x)}\int_\sigma^1 e^u du = \frac{x^{k+1}}{\log(x)}(e - e^\sigma),$$

which also vanishes in the error term.

□

Théorie des nombres et applications à la cryptographie

Semestre d'été 2013

Université du Luxembourg **Feuille 1**
Prof. Dr. Gabor Wiese 19/02/2013

Ces exercices sont à rendre le 26/02/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 05/03/2013.

1. (a) Calculer $d := \mathrm{pgcd}(252, 225)$ par l'algorithme d'Euclide.
   Trouver $a, b \in \mathbb{Z}$ tels que $d = 252 \cdot a + 225 \cdot b$ (identité de Bézout).

   (b) Soient $n = 252$ et $e = 71$. Trouver $s \in \mathbb{N}$ tel que $1 \leq s \leq 252$ et $es \equiv 1 \mod (n)$.

2. Soient $p_1, p_2, \ldots, p_r$ des nombres premiers distincts. On pose $n = p_1 \cdot p_2 \cdots p_r$. Soit $m \equiv 1$ mod $(\varphi(n))$, où $\varphi(n)$ est la fonction d'Euler, c'est-à-dire, le nombre d'unités de l'anneau $\mathbb{Z}/(n)$.
   Démontrer que pour tout $x \in \mathbb{Z}/(n)$ on a : $x^m = x$ (égalité dans $\mathbb{Z}/(n)$).

Théorie des nombres et applications à la cryptographie

Semestre d'été 2013

Université du Luxembourg **Feuille 2**
Prof. Dr. Gabor Wiese 26/02/2013

Ces exercices sont à rendre le 05/03/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 12/03/2013.

1. Dans cet exercice nous allons voir comment transformer une phrase (pour simplifier en majuscules sans accents) en un entier. Pour ceci, nous allons utiliser le tableau suivant.

Lettre	0	1	...	9	A	B	...	Z	.	,	:	;	!	?	espace
Entier	0	1	...	9	10	11	...	35	36	37	38	39	40	41	42

La phrase « Tu es. » est transformée en un entier ainsi :
T=29, U=30, espace=42, E=14, S=28 , .=36

$$29 + 30 \cdot 43 + 42 \cdot 43^2 + 14 \cdot 43^3 + 28 \cdot 43^4 + 36 \cdot 43^5 = 5389222451.$$

(a) Décrire en détail la procédure inverse pour transformer un entier en phrase.
Indication : Utiliser la division euclidienne.

(b) Quelle phrase est représentée par l'entier 9965219185703 ?

2. Dans cet exercice nous voyons comment marche « l'exponentiation rapide ».
Soit n un entier positif donné en notation binaire $n = (a_r, a_{r-1}, \dots, a_1, a_0)_2$ avec des chiffres $a_i \in \{0, 1\}$ pour $i = 0, \dots, r$, c'est-à-dire

$$n = \sum_{i=0}^{r} a_i 2^i.$$

Exemples : $3 = (1,1)_2 = 1 \cdot 2^1 + 1 \cdot 2^0$, $10 = (1,0,1,0)_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$.
Soit $x \in \mathbb{Z}$ (ou dans n'importe quel autre anneau). Nous voulons calculer x^n en faisant aussi peu de multiplications que possible. Observer :

$$x^n = x^{(\sum_{i=0}^{r} a_i 2^i)} = (x^{(2^0)})^{a_0} \cdot (x^{(2^1)})^{a_1} \cdot (x^{(2^2)})^{a_2} \cdot \ldots \cdot (x^{(2^r)})^{a_r}.$$

Nous calculons x^{10} : Si l'on le fait de la manière naive $x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x$, on a besoin de 9 multiplications. Nous pouvons y arriver avec seulement 4 multiplications, notamment :

$$e_1 := x \cdot x = x^2, \;\; e_2 := e_1 \cdot e_1 = x^4, \;\; e_3 := e_2 \cdot e_2 = x^8, \;\; e_1 \cdot e_3 = x^{10}$$

(a) Imiter le calcul de x^{10} pour calculer x^{20}. Combien de multiplications vous faut-il ?

(b) Soit $n = (a_r, a_{r-1}, \dots, a_1, a_0)_2$. Démontrer qu'on n'a jamais besoin de plus de $2r$ multiplications.

Théorie des nombres et applications à la cryptographie

Semestre d'été 2013

Université du Luxembourg **Feuille 3**

Prof. Dr. Gabor Wiese 05/03/2013

Ces exercices sont à rendre le 12/03/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 19/03/2013.

1. Dans cet exercice vous allez construire un corps de cardinal 9.
   (a) Trouver un couple $a, b \in \mathbb{F}_3$ tels que $X^2 + aX + b$ est un polynôme irréductible dans $\mathbb{F}_3[X]$.
   (b) Soit $K := \mathbb{F}_3[X]/(X^2 + aX + b)$ pour le couple (a, b) de (a). Dresser la liste de tous les éléments de K.
   (c) Calculer un inverse pour tout élément non nul de K.
   (Cela montre que K est un corps commutatif, car nous savons que K est un anneau commutatif.)
2. Soit K un corps. Dans cet exercice vous allez démontrer un analogue pour l'anneau des polynômes $K[X]$ du théorème principal de la théorie élémentaire des nombres. Vous pouvez le déduire de l'algorithme d'Euclide et de l'identité de Bézout ainsi :
   (a) Soit $f \in K[X]$ un polynôme de degré $n := \deg(f) > 0$. Démontrer qu'il existe une famille finie de polynômes irréductibles $p_1(X), \ldots, p_r(X) \in K[X]$ tels que
   $$f(X) = p_1(X) \cdot p_2(X) \cdot \ldots \cdot p_r(X).$$
   (b) Soit $p(X) \in K[X]$ un polynôme de degré $n := \deg(p) > 0$. Démontrer que les assertions suivantes sont équivalentes :
      (i) $p(X)$ est un polynôme irréductible.
      (ii) $p(X)$ est un élément premier dans l'anneau $K[X]$.
      (Se rappeler que, par définition, $p(X)$ est un élément premier dans $K[X]$ si et seulement si pour tout $g(X), h(X) \in K[X]$ tels que $p(X) \mid g(X)h(X)$, on a que $p(X)$ divise $g(X)$ ou $h(X)$.)
   (c) Soit $f(X) \in K[X]$ un polynôme unitaire (c'est-à-dire que le coefficient du monôme dominant est égal à 1) de degré $n := \deg(f) > 0$.
   Démontrer que $f(X)$ s'écrit comme produit fini de polynômes unitaires et irréductibles : Il existe $r \in \mathbb{N}$ et de polynômes unitaires et irréductibles $p_1(X), \ldots, p_r(X)$ tels que
   $$f(X) = p_1(X) \cdot p_2(X) \cdot \ldots \cdot p_r(X).$$
   Démontrer aussi qu'à numérotation près, les polynômes unitaires et irréductibles apparaissant dans le produit sont uniques, c'est-à-dire : Si $f(X) = q_1(X) \cdot q_2(X) \cdot \ldots \cdot q_s(X)$ est un autre tel produit, alors $r = s$ et il existe σ dans le groupe symétrique sur les lettres $\{1, \ldots, r\}$ (c'est-à-dire, le groupe de toutes les permutations de $\{1, \ldots, r\}$) tel que $q_i(X) = p_{\sigma(i)}(X)$ pour tout $i \in \{1, \ldots, r\}$.

Théorie des nombres et applications à la cryptographie

Semestre d'été 2013

Université du Luxembourg **Feuille 4**
Prof. Dr. Gabor Wiese 12/03/2013

Ces exercices sont à rendre le 19/03/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 26/03/2013.

1. Cet exercice vérifie la règle de Leibniz (c'est-à-dire la règle du produit) pour la dérivée d'un polynôme. Soit K un corps. La dérivée formelle du polynôme $f(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$ est définie par $f'(X) = \sum_{i=1}^{n} a_i i X^{i-1}$.
   Soient $f(X), g(X) \in K[X]$ et $h(X) = f(X)g(X)$. Démontrer :
   $$h'(X) = f'(X)g(X) + f(X)g'(X).$$

2. Soit K un corps fini de cardinal p^n où p est premier.
   (a) Démontrer : $(\alpha + \beta)^p = \alpha^p + \beta^p$ pour tout $\alpha, \beta \in K$.
   (b) Déduire de (a) : $(\alpha + \beta)^{p^d} = \alpha^{p^d} + \beta^{p^d}$ pour tout $d \in \mathbb{N}$.
   (c) Démontrer que l'application
   $$F : K \to K, \quad x \mapsto x^p$$
   définit un isomorphisme de corps (que l'on appelle *morphisme de Frobenius*).
   (d) Calculer l'ordre de F (dans le groupe des automorphismes de corps de K).
   (e) Soient $1 \leq d \leq n$ et $F^d = \underbrace{F \circ F \circ \cdots \circ F}_{d \text{ fois}}$. Démontrer que $K^{\langle F^d \rangle} := \{x \in K \mid F^d(x) = x\}$ est un sous-corps de K et calculer le cardinal de $K^{\langle F^d \rangle}$.

Théorie des nombres et applications à la cryptographie

Semestre d'été 2013

Université du Luxembourg **Feuille 5**
Prof. Dr. Gabor Wiese 19/03/2013

Ces exercices sont à rendre le 26/03/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 09/04/2013.

1. (a) Démontrer que le polynôme $f(X) = X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$ est irréductible.

   (b) Considérer $K = \mathbb{F}_2[X]/(f(X))$. Nous savons que c'est un corps de cardinal 16, donc $K^\times$ est un groupe cyclique d'ordre 15.

   Trouver un générateur de $K^\times$.

2. *Le « protocole sans clé » de Shamir.* Shamir a trouvé une méthode permettant à Alice d'envoyer un message à Bob qui ne puisse être lu par personne d'autre. Sa méthode a la propriété très spéciale qu'Alice et Bob n'ont pas besoin d'une clé commune.

   D'abord on décrit la méthode avec les outils du quotidien. Alice met son message dans une boîte et elle ferme la boîte avec un cadenas à elle (elle seule possède la clé pour l'ouvrir). Alice est donc la seule personne qui peut ouvrir la boîte à ce moment-là. Elle envoie la boîte à Bob. Bob ajoute une cerrure à lui pour fermer la boîte une deuxième fois (seul Bob possède la clé pour ouvrir son cadenas). Il envoie la boîte (maintenant ayant deux cadenas) à Alice. Elle utilise sa clé pour enlever son cadenas. Elle envoie la boîte, qui est à ce moment-là fermée seulement par le cadenas de Bob, à Bob qui peut l'ouvrir avec sa clé et récupérer le message. Noter que la boîte est fermée pendant tous ses trajets par au moins un cadenas.

   Soit p un « grand » nombre premier et $1 \leq m \leq p-1$ le message (on devrait aussi supposer que $m \in \mathbb{F}_p^\times$ est d'ordre $p-1$ pour des raisons de sécurité, mais nous négligeons ce point). Alice veut envoyer m à Bob.

   (a) Décrire une version du protocole sans clé de Shamir dans $\mathbb{F}_p^\times$ dont la sécurité repose sur le problème du logarithme discret.

   (b) Supposons qu'Eve sait résoudre le problème du logarithme discret dans $\mathbb{F}_p$ et qu'elle connaît toute la conversation entre Alice et Bob. Démontrer qu'Eve peut calculer m.

Théorie des nombres et applications à la cryptographie

Semestre d'été 2013

Université du Luxembourg **Feuille 6**
Prof. Dr. Gabor Wiese 26/03/2013

Ces exercices sont à rendre le 09/04/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 16/04/2013.

1. (a) Démontrer par récurrence : $5^{2^k} = (1+4)^{2^k} \equiv 1 + 2^{k+2} \mod 2^{k+3}$ pour tout $k \in \mathbb{N}_{\geq 0}$.

   (b) Conclure de (a) que l'ordre de 5 dans $(\mathbb{Z}/2^m\mathbb{Z})^\times$ est égal à 2^{m-2} pour tout $m \in \mathbb{N}_{\geq 2}$.

   (c) Soit $p > 2$ un nombre premier. Démontrer par récurrence : $(1+p)^{p^k} \equiv 1 + p^{k+1} \mod p^{k+2}$ pour tout $k \in \mathbb{N}_{\geq 0}$.

   (d) Conclure de (c) que l'ordre de $1+p$ dans $(\mathbb{Z}/p^m\mathbb{Z})^\times$ est égal à p^{m-1} pour tout $m \in \mathbb{N}_{\geq 1}$.

2. (a) Soit $m \in \mathbb{N}_{\geq 2}$. Démontrer l'existence d'un isomorphisme de groupes

$$(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}.$$

   Les facteurs sont engendrés par -1 et 5 dans $(\mathbb{Z}/2^m\mathbb{Z})^\times$, respectivement.

   Indication : Nous savons que $\varphi(2^m) = (2-1)2^{m-1} = 2^{m-1}$. Montrer qu'aucune puissance de 5 n'est égale à -1 dans $(\mathbb{Z}/2^m\mathbb{Z})^\times$.

   (b) Soient $p > 2$ un nombre premier et $m \in \mathbb{N}_{\geq 1}$. Démontrer l'existence d'un isomorphisme de groupes

$$(\mathbb{Z}/p^m\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{p-1}\mathbb{Z}.$$

   Indication : Nous savons que $\varphi(p^m) = (p-1)p^{m-1}$. Utiliser la classe de $1+p$, le fait que $\mathbb{F}_p^\times = \mathbb{Z}/p\mathbb{Z}^\times$ et le fait que p et $p-1$ sont premiers entre eux.

Théorie des nombres et applications à la cryptographie

Semestre d'été 2013

Université du Luxembourg **Feuille 7**
Prof. Dr. Gabor Wiese 09/04/2013

Ces exercices sont à rendre le 16/04/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 23/04/2013.

1. Calculer les symboles de Legendre en utilisant la réciprocité de Gauß :

$$\left(\frac{313}{367}\right); \qquad \left(\frac{367}{401}\right); \qquad \left(\frac{401}{313}\right); \qquad \left(\frac{3}{401}\right).$$

   Indication : Les nombres $3, 313, 367, 401$ sont tous premiers.

2. Soit $p \geq 5$ un nombre premier. Démontrer :

   (a) $\left(\frac{3}{p}\right) = \begin{cases} +1, & \text{si } p \equiv \pm 1 \pmod{12}, \\ -1, & \text{si } p \equiv \pm 5 \pmod{12}. \end{cases}$

   (b) On suppose que $2^p - 1$ est un nombre premier. Alors $\left(\frac{3}{2^p-1}\right) = -1$.

Théorie des nombres et applications à la cryptographie

Semestre d'été 2013

Université du Luxembourg **Feuille 8**
Prof. Dr. Gabor Wiese 16/04/2013

Ces exercices sont à rendre le 23/04/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 30/04/2013.

1. Démontrer le *Théorème de Wilson :* Soit $n \in \mathbb{N}_{\geq 2}$. Alors les assertions suivantes sont équivalentes :

   (i) n est un nombre premier.

   (ii) $(n-1)! \equiv -1 \mod n$.

   Indication : Si n est premier, la classe de $(n-1)!$ dans le groupe multiplicatif du corps fini $\mathbb{F}_n$ est le produit de tous les éléments de $\mathbb{F}_n^\times$, et si $x \in \mathbb{F}_n^\times \setminus \{\pm 1\}$, alors $x \neq x^{-1}$.

2. Soit $n \in \mathbb{N}_{\geq 3}$ impair. Calculer le symbole de Jacobi $\left(\frac{(n-1)!}{n}\right)$.
   Indication : Utiliser le théorème de Wilson.

Théorie des nombres et applications à la cryptographie

Semestre d'été 2013

Université du Luxembourg **Feuille 9**

Prof. Dr. Gabor Wiese 23/04/2013

Ces exercices sont à rendre le 30/04/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 07/05/2013.

1. *Test de primalité de Pépin pour les nombres de Fermat.*

   (a) Soit $n \in \mathbb{N}_{\geq 1}$. On pose $F_n := 2^{2^n} + 1$. Démontrer que les assertions suivantes sont équivalentes :

   (i) F_n est un nombre premier (dit *de Fermat*).

   (ii) $3^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}$.

   Indication : Pour « (i) ⇒ (ii) » utiliser le résultat d'Euler $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ pour un nombre premier p et exercice 2(a) de la feuille 7. Pour « (ii) ⇒ (i) » calculer l'ordre de 3 dans $(\mathbb{Z}/F_n\mathbb{Z})^\times$ et comparer avec le cardinal de ce groupe si F_n n'est pas premier.

   (b) Utiliser une calculatrice/un ordinateur et le critère de (a) pour démontrer que 257 est un nombre premier. Si vous voulez, démontrer que 65537 est aussi un nombre premier. Dans ce cas, vous avez vérifié la primalité de tous les nombres premiers de Fermat connus, c'est-à-dire 3, 5, 17, 257, 65537.

   Indication : Exponentiation rapide (carré de carré de carré de carré... mais prendre le reste mod F_n à chaque étape) !

2. Soit $N \in \mathbb{N}_{\geq 3}$ impair et $N - 1 = R \cdot \prod_{i=1}^{s} p_i^{k_i}$ où $p_1, \dots, p_s$ sont des nombres premiers distincts et $R \in \mathbb{N}$ tel que $p_i \nmid R$ pour tout $i \in \{1, \dots, s\}$.

   (a) On suppose que pour tout $i \in \{1, \dots, s\}$ il existe $a_i \in \mathbb{Z}$ tel que

   (i) $a_i^{N-1} \equiv 1 \pmod{N}$ et

   (ii) $\mathrm{pgcd}(a_i^{(N-1)/p_i} - 1, N) = 1$.

   Démontrer que tout premier q qui divise N est de la forme

   $$q = m \cdot \prod_{i=1}^{s} p_i^{k_i} + 1 \qquad (1)$$

   pour un $m \in \mathbb{N}$ convenable.

   (b) Démontrer : si $\prod_{i=1}^{s} p_i^{k_i} > R$, alors N est un nombre premier.

   (c) Démontrer : si N est un nombre premier, alors tout générateur a de $(\mathbb{Z}/N\mathbb{Z})^\times$ satisfait les hypothèses de (a) pour tout i.

   Indications : Pour (a) démontrer d'abord

   (i) $a_i^{N-1} \equiv 1 \pmod{q}$, et

   (ii) $a_i^{(N-1)/p_i} \not\equiv 1 \pmod{q}$

   pour tout diviseur premier $q \mid N$. Conclure de (i) que $p_i^{k_i+1}$ ne divise pas l'ordre de a_i dans $\mathbb{F}_q^\times$. Conclure de (ii) que $p_i^{k_i}$ divise l'ordre de a_i dans $\mathbb{F}_q^\times$. En déduire la forme (1) pour q en utilisant que $\mathbb{F}_q^\times$ est un groupe cyclique de cardinal $q - 1$.

Théorie des nombres et applications à la cryptographie

Semestre d'été 2013

Université du Luxembourg **Feuille 10**

Prof. Dr. Gabor Wiese 30/04/2013

Ces exercices sont à rendre le 07/05/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 14/05/2013.

1. Soit $p \neq 2$ un nombre premier. Soit $g \in \mathbb{Z}$ dont la classe mod p engendre le groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^\times$. Démontrer que le symbole de Legendre $\left(\frac{g}{p}\right)$ est égal à -1.
2. Soit $N \in \mathbb{N}_{\geq 3}$ impair. On suppose que pour tout $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ on a $a^{\frac{N-1}{2}} \equiv \pm 1 \mod N$.

   Le but de cet exercice est de démontrer que N est un nombre premier, si on impose une hypothèse supplémentaire (celle de (e) ou celle de (f)). On raisonne par l'absurde et on suppose que N n'est pas premier. Soit $N = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ sa factorisation en nombres premiers. On procède en plusieurs étapes :

   (a) Démontrer : N est un nombre de Carmichael, donc par le cours N est sans carré (squarefree), $k \geq 3$ et $(p_i - 1) \mid (N-1)$ pour $i = 1, \ldots, k$.

   (b) Le théorème chinois donne un isomorphisme

   $$\Psi : (\mathbb{Z}/N\mathbb{Z})^\times \to \prod_{i=1}^{k} (\mathbb{Z}/p_i\mathbb{Z})^\times.$$

   Décrire les images des classes $\overline{1} \in (\mathbb{Z}/N\mathbb{Z})^\times$ et $\overline{-1} \in (\mathbb{Z}/N\mathbb{Z})^\times$ par Ψ.

   (Cette question est facile. Son unique but est de vous faire réviser le théorème chinois car il faut l'utiliser dans ce qui suit.)

   (c) On suppose qu'il existe $j \in \{1, \ldots, k\}$ tel que $\frac{N-1}{p_j-1}$ est impair. Soit g_j un générateur de $(\mathbb{Z}/p_j\mathbb{Z})^\times$ (qui existe car nous savons que le groupe multiplicatif de tout corps est cyclique).

   Calculer

   $$(\overline{1}, \ldots, \overline{1}, g_j, \overline{1}, \ldots, \overline{1})^{\frac{N-1}{2}} \in \prod_{i=1}^{k} (\mathbb{Z}/p_i\mathbb{Z})^\times$$

   (g_j est à la j-ième place) et en déduire une contradiction.

   (d) On fait l'hypothèse supplémentaire que $N \equiv 3 \mod 4$. Déduire de (a)–(c) que N est premier.

   (e) On fait l'hypothèse supplémentaire qu'il existe $b \in (\mathbb{Z}/N\mathbb{Z})^\times$ tel que $b^{\frac{N-1}{2}} \equiv -1 \mod N$.

   Déduire de (a)–(c) que N est premier.

   Indication : Si pour tous $i \in \{1, \ldots, k\}$ on a que $\frac{N-1}{p_i-1}$ est pair, alors pour $a \in (\mathbb{Z}/N\mathbb{Z})^\times$ calculer

   $$(\overline{a}, \ldots, \overline{a})^{\frac{N-1}{2}} \in \prod_{i=1}^{k} (\mathbb{Z}/p_i\mathbb{Z})^\times$$

   et en déduire une contradiction.

Théorie des nombres et applications à la cryptographie

Semestre d'été 2013

Université du Luxembourg **Feuille 11**
Prof. Dr. Gabor Wiese 07/05/2013

Ces exercices sont à rendre le 14/05/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 21/05/2013.

1. Soit $(a_n)_{n=1}^{\infty}$ une suite de nombres complexes telle que $\sum_{n=1}^{\infty} a_n$ converge absolument. Démontrer :
   (a) Il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$: $|a_n| < 1$.
   (b) La série $\sum_{n=N}^{\infty} \log(1 + a_n)$ converge absolument, où le logarithme complexe est défini par
   $$\log(1+z) = -\sum_{n=1}^{\infty}(-1)^n \frac{z^n}{n}$$
   pour $z \in \mathbb{C}$ avec $|z| < 1$.
   (c) On définit $\prod_{n=1}^{\infty}(1 + a_n)$ par $\lim_{m\to\infty} \prod_{n=1}^{m}(1 + a_n)$. On a
   $$\prod_{n=1}^{\infty}(1+a_n) = (1+a_1)(1+a_2)\cdots(1+a_{N-1}) \cdot \exp\big(\sum_{n=N}^{\infty}\log(1+a_n)\big).$$
   (d) $\prod_{n=1}^{\infty}(1 + a_n) = 0$ si et seulement s'il existe $n \in \mathbb{N}$ tel que $1 + a_n = 0$.
2. Soient $f, g : [x_0, \infty) \to \mathbb{C}$ deux fonctions. On considère les deux définitions suivantes (due à Landau) :
   – $f(x) = O(g(x))$ si et seulement s'il existe $C > 0$ et $x_1 > x_0$ tels que $|f(x)| \leq C \cdot |g(x)|$ pour tout $x > x_1$.
   – $f(x) = o(g(x))$ si et seulement si pour tout $\epsilon > 0$ il existe $x_\epsilon > x_0$ tel que $|f(x)| \leq \epsilon \cdot |g(x)|$ pour tout $x > x_\epsilon$.
   Démontrer :
   (a) $f(x) = O(1)$ si et seulement s'il existe x_1 tel que $|f|$ est bornée dans l'interval $[x_1, \infty)$.
   (b) $f(x) = o(1)$ si et seulement si $\lim_{x\to\infty} f(x) = 0$.
   (c) Pour tout $\epsilon > 0$ on a $\log(x) = O(x^\epsilon)$.
   (d) $\log(x)x^{-1/\sqrt{\log(x)}} = o(1)$.
   (e) On définit $\mathrm{Li}(x) := \int_2^x \frac{1}{\log(t)}dt$. Montrer par intégration par parties $\mathrm{Li}(x) = \frac{x}{\log(x)}(1 + s(x))$ avec $s(x) = O(1/\log(x))$.

Théorie des nombres et applications à la cryptographie

Semestre d'été 2013

Université du Luxembourg **Feuille 12**
Prof. Dr. Gabor Wiese 14/05/2013

Ces exercices sont à rendre le 21/05/2013 au début du cours. L'un/une d'entre vous présentera un des exercices lors du cours du 28/05/2013.

---

1. On peut définir la fonction de Möbius $\mu : \mathbb{N} \to \{-1, 0, 1\}$ par l'égalité

$$\frac{1}{\zeta(s)} \overset{\text{produit d'Euler}}{=} \prod_{p \in \mathbb{P}} (1 - p^{-s}) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s},$$

de fonctions holomorphes dans $\{\mathrm{Re}(s) > 1\}$ (ne pas démontrer l'holomorphie). Démontrer :

$$\mu(n) = \begin{cases} 1 & \text{si } n = 1, \\ (-1)^k & \text{si } n = p_1 \cdot p_2 \cdot \ldots \cdot p_k \text{ avec des premiers distincts } p_1, p_2, \ldots, p_k, \\ 0 & \text{sinon.} \end{cases}$$

Indication : Vous pouvez utiliser que $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ est localement uniformément absolument convergente dans $\{\mathrm{Re}(s) > 1\}$, donc on peut échanger l'ordre des termes.

2. On numérote les nombres premiers par leur taille : $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc. Démontrer l'équivalences des deux assertions suivantes :

   (i) Le théorème des nombres premiers est correct, c'est-à-dire $\lim_{x\to\infty} \pi(x) \frac{\log(x)}{x} = 1$.

   (ii) $\lim_{n\to\infty} \frac{p_n}{n \log(n)} = 1$.

Indication : Pour $\Rightarrow$ montrer $\frac{\log(\pi(x))}{\log(x)} \xrightarrow{x\to\infty} 1$. Pour $\Leftarrow$ montrer $\frac{\log(p_n)}{\log(n)} \xrightarrow{n\to\infty} 1$, $\frac{p_{n+1}}{n \log(n)} \xrightarrow{n\to\infty} 1$, et considérer $p_n \leq x < p_{n+1}$.