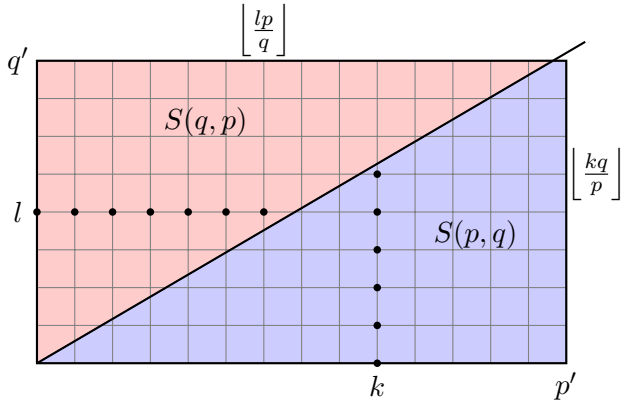
Elementary Number Theory

Benjamin Sambale
Leibniz Universität Hannover

Version: April 4, 2026



Contents

Warning: This is an AI-translated version of my German lecture notes, performed by *Gemini 3 Flash Preview*. I have not checked whether Gemini introduced errors. Use with care!

Preface

Number theory is, alongside geometry, one of the oldest subfields of pure mathematics. At the center of the investigation are the natural numbers $1, 2, \ldots$ and their arithmetic properties. In contrast to other mathematical fields, number theory allows for the statement of seemingly simple problems that have remained unsolved for centuries. This particularly concerns the distribution of prime numbers. Mention should be made of the *Goldbach conjecture* (every even number greater than 2 is the sum of two prime numbers), the *twin prime conjecture* (there are infinitely many pairs of prime numbers (p, q) with $q = p + 2$) or the Millennium Problem, the *Riemann hypothesis* (the non-trivial zeros of the ζ-function have real part $1/2$). In this lecture, we will cover what are, in my view, the most beautiful chapters of number theory. In many places, I provide application examples. Prior knowledge of linear algebra and analysis 1 is assumed. Knowledge of algebra 1 is helpful but not strictly necessary. I would like to thank Annika Bartelt and Claude Sonnet (4.6) for pointing out errors.

Literature:

- Bundschuh, *Einführung in die Zahlentheorie*, 6th edition, Springer, 2008
- Scheid, *Zahlentheorie*, 3rd edition, 2003
- Leutbecher, *Zahlentheorie*, Springer, 1996
- Schmidt, *Einführung in die algebraische Zahlentheorie*, Springer, 2007

1 Divisibility

Remark 1.1. We use the usual number sets:

- Natural numbers: $\mathbb{N} = \{1, 2, \ldots\}$, $\mathbb{N}_0 = \{0, 1, \ldots\}$.
- Integers: $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$.
- Rational numbers: $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z},\ b \neq 0\}$.
- Real numbers: $\mathbb{R}$ (Analysis).
- Complex numbers: $\mathbb{C} = \{a + b\mathrm{i} : a, b \in \mathbb{R}\}$.

Theorem 1.2 (Euclidean division)**.** *For $a \in \mathbb{Z}$ and $d \in \mathbb{N}$, there exist uniquely determined $q, r \in \mathbb{Z}$ with $a = qd + r$ and $0 \leq r < d$.*

Proof. Obviously, the set $M := \{a - cd : c \in \mathbb{Z} \text{ with } a - cd \geq 0\} \subseteq \mathbb{N}_0$ is not empty and therefore possesses a minimal element $r := a - qd \geq 0$ with $q \in \mathbb{Z}$. In the case $r \geq d$, then $a - (q+1)d = r - d \in M$ would also hold, in contradiction to the minimality of r. Thus $0 \leq r < d$. Now let $q', r' \in \mathbb{Z}$ with $a = q'd + r'$ and $0 \leq r' < d$. From $d|q - q'| = |dq - dq'| = |r' - r| < d$ it then follows that $q = q'$ and $r = r'$. □

Remark 1.3. One calls r in Theorem 1.2 the *remainder* in the division of a by d.

Example 1.4. The division of 20 by 7 leaves remainder 6, because $20 = 2 \cdot 7 + 6$.

Theorem 1.5 (b-adic expansion)**.** *Let $b \in \mathbb{N}$ with $b \geq 2$. For every $n \in \mathbb{N}$ there exist uniquely determined numbers $k \in \mathbb{N}$ and $0 \leq n_0, n_1, \ldots, n_k \leq b-1$ with*

$$n = n_k b^k + n_{k-1} b^{k-1} + \ldots + n_1 b + n_0 =: [n_k, \ldots, n_0]_b.$$

and $n_k > 0$.

Proof. Induction on n: For $n = 1$, it is obvious that $k = 0$ and $n_0 = 1$ must hold. Now let $n \geq 2$. Euclidean division by b yields $n = qb + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < b$. In the case $q < 0$, it would follow that $n \leq -b + r < 0$. Thus $0 \leq q < n$. By induction, there exist $0 \leq q_0, q_1, \ldots, q_l \leq b-1$ with $q = q_0 + \ldots + q_l b^l$ (in the case $q = 0$ let $l = 0 = q_0$). We can now define $k := l + 1$, $n_0 := r$ and $n_i := q_{i-1}$ for $i = 1, \ldots, k$. Then $n = qb + r = n_k b^k + \ldots + n_1 b + n_0$ holds.

Assume that $n = n'_{k'} b^{k'} + \ldots + n'_0$ also holds with $0 \leq n'_0, n'_1, \ldots, n'_{k'} \leq b-1$ and $n_{k'} > 0$. Then $n_0 = n'_0$ is the uniquely determined remainder of the division of n by b. From this one obtains

$$n_k b^{k-1} + \ldots + n_2 b + n_1 = \frac{n - n_0}{b} = n'_{k'} b^{k'} + \ldots + n'_2 b + n'_1 < n.$$

By induction, $k = k'$ and $n_i = n'_i$ for $i = 1, \ldots, k$ hold. □

Example 1.6.

(i) The 10-adic expansion is exactly the usual decimal notation. The 3-adic expansion of 100 is: $100 = 81 + 18 + 1 = 3^4 + 2 \cdot 3^2 + 3^0 = [1, 0, 2, 0, 1]_3$.

(ii) We will later expand (positive) real numbers into an infinite p-adic series (see Theorem 5.2).

(iii) On computers, one calculates in the *binary system* thus with 2-adic expansions.

(iv) (Nim game) Euler and Gauss play the following game: Given are n piles with m_i coins each for $i = 1, \ldots, n$. The players take turns in each move taking any positive number of coins from one of the piles (it is also allowed to take the entire pile). Whoever takes the last coin wins. Can Euler as the starting player force a victory? In the case $m_1 = \ldots = m_n = 1$, Euler obviously wins if and only if n is odd. For $n = 2$ and $(m_1, m_2) = (3, 2)$, Euler can win as follows:

$$(3,2) \xrightarrow{\text{E}} (2,2) \begin{cases} \xrightarrow{\text{G}} (2,0) \xrightarrow{\text{E}} (0,0) \\ \xrightarrow{\text{G}} (2,1) \xrightarrow[\text{E}]{} (1,1) \xrightarrow[\text{G}]{} (1,0) \xrightarrow[\text{E}]{} (0,0) \end{cases}$$

Let $m_i = \sum_{j \geq 0} m_{ij} 2^j$ be the 2-adic expansion and $\alpha_j := \sum_{i=1}^n m_{ij}$ for $j \geq 0$ (for sufficiently large j, $\alpha_j = 0$ holds). We claim:

Euler can force a victory if and only if an α_j is odd.

Proof. Let $j_1 < j_2 < \ldots < j_k$ be the indices for which α_j is odd. Then there exists an i with $m_{ij_k} = 1$. Euler takes exactly

$$2^{j_k} + \sum_{l=1}^{k-1} (-1)^{m_{ij_l}} 2^{j_l} > 0$$

coins from pile i. This changes each of the α_{j_l} by ± 1. After Euler's move, all α_j are thus even. Example:

$$\begin{array}{lll} m_1 = 12 & = [0,1,1,0,0]_2 & [0,1,1,0,0]_2 \\ m_2 = 17 & = [1,0,0,0,1]_2 \xrightarrow{-(2^4-2^2)} & [0,0,1,0,1]_2 = 5 \\ m_3 = 9 & = [0,1,0,0,1]_2 & [0,1,0,0,1]_2 \\ \hline [\alpha_5,\ldots,\alpha_0] & = [1,2,1,0,2] & [0,2,2,0,2] \end{array}$$

Since Gauss can and must change only one pile, after his move an α_j will again be odd. After finitely many moves, we reach the situation with only one pile left, say $m_1 > 0$. Obviously, then an $\alpha_j = m_{ij} = 1$, i. e. it is Euler's turn and he wins by taking the entire pile.

Now let us assume that at the beginning all α_j are even. As just seen, Euler's move will make at least one α_j odd. But now Gauss can force the victory.[1] □

Definition 1.7. For $a, b \in \mathbb{Z}$ one says a *divides* b (or a is a *divisor* of b or b is *divisible* by a), if there exists a $c \in \mathbb{Z}$ with $ac = b$. One then writes $a \mid b$.

Lemma 1.8. *For $a, b, c, d, e \in \mathbb{Z}$ the following holds*

(i) $\pm 1 \mid a \mid 0$,

(ii) $0 \mid a \iff a = 0$,

(iii) $a \mid b \mid c \implies a \mid c$,

(iv) $a \mid b \mid a \implies a = \pm b$,

(v) $a \mid b, c \implies a \mid (bd + ce)$,

(vi) $a \mid b \neq 0 \implies |a| \leq |b|$.

Proof. All statements are easy. We prove (iv) as a sample. Because of $a \mid b \mid a$ there exist $c, d \in \mathbb{Z}$ with $ac = b$ and $bd = a$. Thus $a = bd = cda$. In the case $a = 0$, $b = ac = 0$ also holds. Otherwise $cd = 1$ and $c = \pm 1$. Then $a = \pm b$. □

Definition 1.9. For $a_1, \ldots, a_n \in \mathbb{Z}$ let

$$\operatorname{cd}(a_1, \ldots, a_n) := \{d \in \mathbb{Z} : d \mid a_1, \ldots, a_n\}$$

be the set of *common divisors* of $a_1, \ldots, a_n$. A $g \in \operatorname{cd}(a_1, \ldots, a_n)$ is called *greatest common divisor* of $a_1, \ldots, a_n$, if $g \geq 0$ and $d \mid g$ for all $d \in \operatorname{cd}(a_1, \ldots, a_n)$ holds. One then writes $\gcd(a_1, \ldots, a_n) := g$. In the case $\gcd(a_1, \ldots, a_n) = 1$ one calls $a_1, \ldots, a_n$ *coprime*.

Remark 1.10.

(i) If g and g' are greatest common divisors of $a_1, \ldots, a_n$, then $g \mid g' \mid g$ and $g = \pm g'$ holds according to Lemma 1.8(iv). Because of $g, g' \geq 0$, it follows that $g = g'$, i. e. there exists at most one common divisor of $a_1, \ldots, a_n$ (this justifies the notation gcd).

(ii) The term "greatest common divisor" is misleading, because $\operatorname{cd}(0, 0) = \mathbb{Z}$, but $\gcd(0, 0) = 0$.

[1] Since with probability $\frac{2^n-1}{2^n}$ at least one α_j is odd, it is sufficient against inexperienced players to play randomly at first until a known situation occurs (cf. Exercise 2).

(iii) For the calculation of $\gcd(a_1, \ldots, a_n)$, one can obviously assume $a_1 > \ldots > a_n > 0$. For $d \in \mathrm{cd}(a_1, \ldots, a_n)$, it holds that $d \mid a_1$ and $d \mid \gcd(a_2, \ldots, a_n)$. Thus

$$\mathrm{cd}(a_1, \ldots, a_n) \subseteq \mathrm{cd}(a_1, \gcd(a_2, \ldots, a_n)).$$

Conversely, for $d \in \mathrm{cd}(a_1, \gcd(a_2, \ldots, a_n))$, it holds that $d \mid \gcd(a_2, \ldots, a_n) \mid a_i$ for $i = 2, \ldots, n$, hence $d \in \mathrm{cd}(a_1, \ldots, a_n)$. This shows

$$\gcd(a_1, \ldots, a_n) = \gcd(a_1, \gcd(a_2, \ldots, a_n)).$$

It is therefore sufficient to be able to calculate the gcd of two natural numbers.

(iv) Let $a > b > 0$. Euclidean division yields $a = bq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < b$. According to Lemma 1.8(v), $\mathrm{cd}(a, b) = \mathrm{cd}(bq + r, b) = \mathrm{cd}(r, b)$ and therefore $\gcd(a, b) = \gcd(r, b)$. In the case $r > 0$, one can divide b by r with remainder and thereby obtain increasingly smaller numbers. At the end, $\gcd(a, b) = \gcd(r, b) = \ldots = \gcd(d, 0) = d$. In particular, the gcd always exists. The following theorem provides more precise information.

Theorem 1.11 (Extended Euclidean algorithm)**.**
Input: $a, b \in \mathbb{N}$.
Initialization: $(x_0, y_0, z_0) := (1, 0, a)$, $(x_1, y_1, z_1) := (0, 1, b)$ *and* $k := 0$.
While $z_{k+1} > 0$ *repeat:*
Euclidean division: $z_k = q_{k+1} z_{k+1} + r_{k+1}$ *with* $0 \leq r_{k+1} < z_{k+1}$.
Set $(x_{k+2}, y_{k+2}, z_{k+2}) := (x_k - x_{k+1} q_{k+1}, y_k - y_{k+1} q_{k+1}, r_{k+1})$ *and* $k := k + 1$.
Output: $z_k = x_k a + y_k b = \gcd(a, b)$.

Proof. Because of $z_1 > r_1 = z_2 > r_2 = z_3 > \ldots$, the algorithm terminates. At the end, it holds that

$$\begin{aligned} z_k &= \gcd(z_k, 0) = \gcd(z_k, z_{k+1}) = \gcd(z_k, r_k) = \gcd(z_k, z_{k-1} - q_k z_k) \\ &= \gcd(z_k, z_{k-1}) = \ldots = \gcd(z_0, z_1) = \gcd(a, b). \end{aligned}$$

For $i = 0, 1$, it holds that $x_i a + y_i b = z_i$. Inductively, it follows that

$$\begin{aligned} x_{i+1} a + y_{i+1} b &= (x_{i-1} - x_i q_i) a + (y_{i-1} - y_i q_i) b = x_{i-1} a + y_{i-1} b - (x_i a + y_i b) q_i \\ &= z_{i-1} - z_i q_i = r_i = z_{i+1}. \end{aligned}$$

Therefore $\gcd(a, b) = z_k = x_k a + y_k b$. □

Example 1.12. For $a := 45$ and $b := 24$, one obtains:

x_i	y_i	z_i	q_i
1	0	45	
0	1	24	1
1	-1	21	1
-1	2	$\boxed{3}$	7
		0	

Thus $\gcd(45, 24) = 3 = -45 + 2 \cdot 24$.

Corollary 1.13. *For* $a_1, \ldots, a_n, b \in \mathbb{Z}$*, it holds that*

$$\gcd(a_1, \ldots, a_n) \mid b \iff \exists b_1, \ldots, b_n \in \mathbb{Z} : a_1 b_1 + \ldots + a_n b_n = b.$$

Proof. Let $g := \gcd(a_1, \ldots, a_n)$.

$\Rightarrow$: Let $gd = b$. According to Remark 1.10(iii) and Theorem 1.11, there exist $c_1, \ldots, c_n \in \mathbb{Z}$ with $g = a_1c_1 + \ldots + a_nc_n$. The claim follows with $b_i := dc_i$ for $i = 1, \ldots, n$.

$\Leftarrow$: Because $g \mid a_i$ for $i = 1, \ldots, n$, it holds that $g \mid a_1b_1 + \ldots + a_nb_n = b$. □

Definition 1.14. One calls $v \in \mathbb{Z}$ a *common multiple* of $a_1, \ldots, a_n \in \mathbb{Z}$ if $a_i \mid v$ holds for $i = 1, \ldots, n$. A common multiple $v \in \mathbb{N}_0$ is called the *least common multiple* if v divides every common multiple of $a_1, \ldots, a_n$. One then writes $\operatorname{lcm}(a_1, \ldots, a_n) := v$.

Remark 1.15. As with the gcd, one shows that at most one lcm exists. Furthermore,

$$\operatorname{lcm}(a_1, \ldots, a_n) = \operatorname{lcm}(a_1, \operatorname{lcm}(a_2, \ldots, a_n)).$$

We calculate the lcm via a detour.

2 Prime numbers

Definition 2.1. One calls $p \in \mathbb{N}$ a *prime number* if p has exactly two positive divisors, namely 1 and p. We denote the set of prime numbers by $\mathbb{P}$. One calls $p \in \mathbb{P}$ a *prime divisor* of $a \in \mathbb{Z}$ if $p \mid a$.

Remark 2.2.

(i) Note: 1 is *not* a prime number!

(ii) Two distinct prime numbers are always coprime.

Lemma 2.3.

(i) For $a, b \in \mathbb{Z}$ and $p \in \mathbb{P}$, it holds that $p \mid ab \Longrightarrow p \mid a \vee p \mid b$.

(ii) Every $a \in \mathbb{N} \setminus \{1\}$ possesses a prime divisor.

Proof.

(i) Let $p \mid ab$ and $p \nmid a$. According to the Euclidean algorithm, there exist $c, d \in \mathbb{Z}$ with $1 = \gcd(a, p) = ac + pd$. It follows that $p \mid abc + pbd = b1 = b$.

(ii) Let $p > 1$ be a smallest possible divisor of a (if necessary $p = a$). In the case $p \notin \mathbb{P}$, there exists $1 < q < p$ with $q \mid p \mid a$ in contradiction to the choice of p. Thus $p \in \mathbb{P}$. □

Theorem 2.4 (Euclid)**.** *There are infinitely many prime numbers.*

Proof (Hermite). Assumption: p is the largest prime number. For a prime divisor q of $n = p! + 1$, it holds that $q \leq p$ and one obtains the contradiction $q \mid (n - p!) = 1$. □

Remark 2.5 (Sieve of Eratosthenes)**.** If $n \geq 2$ is not a prime number, then there always exists a prime divisor $p \leq \sqrt{n}$ (if $p > \sqrt{n}$ choose instead a prime divisor of $n/p < \sqrt{n}$). With this consideration, one can easily create a table of all "small" prime numbers:

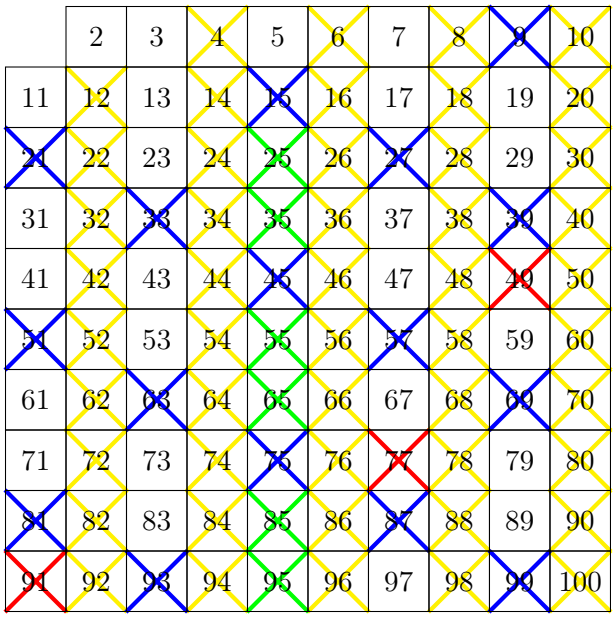
(1) Create a list of numbers from 2 to n.

(2) Let $p \leq \sqrt{n}$ be the smallest number in the list that has not yet been crossed out (initially $p = 2$).

(3) Cross out all multiples pq with $q \geq p$ from the list (initially $4, 6, 8, \ldots$).

(4) Repeat steps 2 and 3 until no suitable p exists anymore.

The numbers in the list that are not crossed out are exactly the prime numbers between 1 and n. For $n = 100$ one obtains the following list:



Theorem 2.6 (Unique Prime Factorization)**.** *For every $n \in \mathbb{N}$ there exist uniquely determined $a_p \in \mathbb{N}_0$ for $p \in \mathbb{P}$ with*

$$n = \prod_{p \in \mathbb{P}} p^{a_p}.$$

Proof. Induction on n: In the case $n = 1$, $a_p = 0$ for all $p \in \mathbb{P}$. Now let $n \geq 2$ and p be a prime divisor of n. By induction, n/p possesses a prime factorization and therefore so does $n = p \cdot n/p$. Let $n = \prod p^{a_p} = \prod p^{b_p}$ and $a_q < b_q$ for some $q \in \mathbb{P}$. Then

$$q \mid \frac{n}{q^{a_q}} = \prod_{p \neq q} p^{a_p}$$

and Lemma 2.3(i) shows $q = p$ for some $p \in \mathbb{P} \setminus \{q\}$. Contradiction. □

Example 2.7. Let $k \geq 2$ and $n \in \mathbb{N}$ not be the k-th power of a natural number. Then $\sqrt[k]{n}$ is irrational, because otherwise there exist coprime $a, b \in \mathbb{N}$ with $\sqrt[k]{n} = a/b$. Then $nb^k = a^k$. The unique prime factorization shows $b^k = 1$ and one obtains the contradiction $n = a^k$. In particular, $\sqrt{2}$ is irrational.

Remark 2.8.

(i) The divisors of $n = \prod_{p\in\mathbb{P}} p^{a_p}$ have the form $n = \prod_{p\in\mathbb{P}} p^{a'_p}$ with $0 \le a'_p \le a_p$ for all $p \in \mathbb{P}$. For $m = \prod_{p\in\mathbb{P}} p^{b_p}$ it therefore holds that

$$\boxed{\gcd(n,m) = \prod_{p\in\mathbb{P}} p^{\min\{a_p,b_p\}}, \quad \operatorname{lcm}(n,m) = \prod_{p\in\mathbb{P}} p^{\max\{a_p,b_p\}}.}$$

This shows

$$\boxed{nm = \gcd(n,m)\operatorname{lcm}(n,m),}$$

since $a_p + b_p = \min\{a_p, b_p\} + \max\{a_p, b_p\}$. Since no fast algorithm for prime factorization is known, the Euclidean algorithm for calculating gcd and lcm is generally to be preferred.

(ii) For $x \in \mathbb{Q} \setminus \{0\}$ there exist uniquely determined $x_p \in \mathbb{Z}$ with $x = \pm\prod_{p\in\mathbb{P}} p^{x_p}$.

(iii) Theorem 2.6 allows the following generalization of Lemma 2.3(i): If $a, b \in \mathbb{Z}$ are coprime and $a \mid bc$, then $a \mid c$ follows.

(iv) Euclid's theorem can be generalized in many respects. The following theorem is a special case of Dirichlet's prime number theorem (see Theorem 9.26).

Theorem 2.9. *There are infinitely many prime numbers of the form $p = 4k - 1$ with $k \in \mathbb{N}$.*

Proof. Assume there are only finitely many such prime numbers, say $p_1, \dots, p_n$. Then all prime divisors of $q := 4p_1 \dots p_n - 1$ have the form $4k + 1$. However, a product of such numbers must also have the form $4k + 1$. Contradiction. □

Theorem 2.10 (Euler)**.** *It holds that $\sum_{p\in\mathbb{P}} \frac{1}{p} = \infty$.*

Proof (Erdős). Assume the series converges. Then there exists an $N \ge 2$ with

$$\sum_{\substack{p\in\mathbb{P}\\ p>N}} \frac{1}{p} < \frac{1}{2}.$$

Let n_1 be the number of all numbers $n \le 2^{4N}$ that possess a prime divisor $p > N$. There are at most $2^{4N}/p$ such numbers that are divisible by a fixed p. This shows

$$n_1 \le 2^{4N} \sum_{\substack{p\in\mathbb{P}\\ p>N}} \frac{1}{p} < 2^{4N-1}.$$

Thus there are at least $2^{4N} - n_1 \ge 2^{4N-1}$ numbers $n \le 2^{4N}$ that are only divisible by prime numbers $p \le N$. Every such number has the form $n = ab^2$ with $\gcd(a, b) = 1$, where a is a product of pairwise distinct prime numbers. Since there are at most N prime numbers $p \le N$, one has at most 2^N possibilities for a. On the other hand, $b \le \sqrt{n} \le 2^{2N}$. Consequently, there are at most $2^N 2^{2N} = 2^{3N} < 2^{4N-1}$ possibilities for n. Contradiction. □

Lemma 2.11. *Let $n \in \mathbb{N}$. Then it holds that*

(i) If $2^n - 1$ is a prime number, then n is a prime number.

(ii) If $2^n + 1$ is a prime number, then n is a power of 2.

Proof.

(i) Obviously $n \geq 2$ holds. Let p be a prime divisor of n and $m := 2^{n/p}$. According to the geometric series, it holds that

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

Since $2^n - 1$ is a prime number, it follows that $m = 2$ and $n = p \in \mathbb{P}$.

(ii) If n has an odd divisor $q > 1$, then

$$2^n + 1 = (2^{n/q} + 1) \sum_{i=0}^{q-1} (-2^{n/q})^i$$

is not a prime number. □

Definition 2.12. One calls $M_n := 2^n - 1$ the n-th MERSENNE *number* and $F_n := 2^{2^n} + 1$ the n-th FERMAT *number*.

Remark 2.13.

(i) The first Mersenne *prime* numbers are

$$M_2 = 3, \quad M_3 = 7, \quad M_5 = 31, \quad M_7 = 127, \quad M_{13} = 8191, \quad M_{17} = 131071, \quad M_{19} = 524287.$$

In contrast, $M_{11} = 2047 = 23 \cdot 89$ is not a prime number. So far, 52 Mersenne prime numbers are known, where $M_{136,279,841}$ with $41,024,320$ decimal places is currently the largest known prime number overall.[2] The Mersenne prime M_{19937} is used for the random number generator *Mersenne Twister*.

(ii) The only known Fermat *prime* numbers are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$. It holds that

$$\begin{aligned} &641 = 5^4 + 2^4 \mid 2^{28}(5^4 + 2^4) = 5^4 \cdot 2^{28} + 2^{32}, \\ &641 = 5 \cdot 2^7 + 1 \mid (5 \cdot 2^7 + 1)(5 \cdot 2^7 - 1)(5^2 \cdot 2^{14} + 1) = 5^4 \cdot 2^{28} - 1, \\ &641 \Big| (5^4 \cdot 2^{28} + 2^{32}) - (5^4 \cdot 2^{28} - 1) = 2^{32} + 1 = F_5 \notin \mathbb{P}. \end{aligned}$$

More generally, it is known that $F_n \notin \mathbb{P}$ for $n = 5, \ldots, 32$.[3] We will learn efficient primality tests for Mersenne and Fermat numbers in Chapter 8.

Definition 2.14. A number $n \in \mathbb{N}$ is called *perfect* if it is the sum of its proper positive divisors, i. e. $\sigma(n) := \sum_{d|n} d = 2n$ (in the following, the sum is always taken only over the positive divisors).

Theorem 2.15 (EULER)**.** *An even number n is perfect if and only if $n = 2^{p-1}M_p$ for a Mersenne prime M_p.*

[2] See `https://en.wikipedia.org/wiki/Largest_known_prime_number`
[3] See `https://www.fermatsearch.org`

Proof. If $M_p \in \mathbb{P}$, then every divisor of $n = 2^{p-1}M_p$ has the form $2^i M_p^j$ with $0 \leq i \leq p-1$ and $j \in \{0,1\}$. This shows

$$\sum_{d|n} d = (M_p+1)\sum_{i=0}^{p-1} 2^i = 2^p(2^p-1) = 2n.$$

Conversely, let $n = 2^a m$ be perfect with $a \geq 0$ and $2 \nmid m$. Because $\gcd(2^a, m) = 1$, it holds that

$$2^{a+1}m = 2n = \sum_{d|n} d = \Big(\sum_{i=0}^{a} 2^i\Big)\Big(\sum_{d|m} d\Big) = (2^{a+1}-1)\sigma(m).$$

It follows that

$$\frac{2^{a+1}}{2^{a+1}-1} = \frac{\sigma(m)}{m}.$$

Since the fraction on the left side is fully reduced (numerator and denominator are coprime), the fraction on the right side must be an expansion. Thus there exists $b \in \mathbb{N}$ with $m = (2^{a+1}-1)b$ and $\sigma(m) = 2^{a+1}b$. In the case $b > 1$, it would be

$$\sigma(m) \geq 1 + b + m = 2^{a+1}b + 1 > \sigma(m).$$

Therefore $m = 2^{a+1}-1$ and $\sigma(m) = 2^{a+1}$ holds. If m were not a prime number, then $\sigma(m) > 1+m = 2^{a+1}$ would hold. Therefore $m = M_{a+1}$ is a Mersenne prime and $n = 2^a M_{a+1}$ as desired. □

Example 2.16. The smallest perfect numbers are $6 = 1+2+3 = 2^{2-1}M_2$ and $28 = 1+2+4+7+14 = 2^{3-1}M_3$. So far, no odd perfect number is known.

Theorem 2.17. *The gaps between two consecutive prime numbers can become arbitrarily large.*

Proof. For $2 \leq k \leq n$, $n!+k$ is divisible by k and thus not a prime number. This yields $n-1$ consecutive composite numbers. [4] □

Definition 2.18. For $x \in \mathbb{R}$, let $\pi(x) := |\{p \in \mathbb{P} : p \leq x\}|$.

Lemma 2.19. *For $2 \leq x \in \mathbb{R}$, it holds that $\prod_{p \leq x} p \leq 4^{x-1}$, where the product runs over the prime numbers $p \leq x$.*

Proof. Wlog. let $x \in \mathbb{P}$. For $x = 2$, the assertion is trivial. So let $x = 2m+1$ and the assertion be already proven for smaller values. Then $\prod_{p \leq m+1} p \leq 4^m$ and

$$\prod_{m+1<p\leq 2m+1} p \leq \frac{(2m+1)!}{m!(m+1)!} = \binom{x}{m} = \frac{1}{2}\left(\binom{x}{m} + \binom{x}{m+1}\right) \leq \frac{1}{2}(1+1)^x = 2^{2m} = 4^m.$$

Overall it follows that

$$\prod_{p\leq x} p = \prod_{p\leq m+1} p \prod_{m+1<p\leq 2m+1} p \leq 4^m 4^m = 4^{x-1}.$$ □

Lemma 2.20. *For $n \in \mathbb{N}$, it holds that $\binom{2n}{n} \geq \frac{4^n}{2n}$.*

[4] If $n+1$ is not a prime number, then $n!+n+1$ cannot be a prime number either. If on the other hand $n+1 \in \mathbb{P}$, then $n+1 \mid n!+1$ according to Exercise 22. For $n \geq 3$, one even obtains n consecutive composite numbers in both cases.

Proof. For $0 \le k \le n-1$, it holds that

$$\binom{2n}{k} < \frac{n+1}{n}\binom{2n}{k} \le \frac{2n-k}{k+1}\binom{2n}{k} = \binom{2n}{k+1} < \ldots < \binom{2n}{n}$$

and $\binom{2n}{k} = \binom{2n}{2n-k}$ (cf. PASCAL's triangle). It follows that

$$4^n = (1+1)^{2n} = \sum_{k=0}^{2n}\binom{2n}{k} = 2 + \sum_{k=1}^{2n-1}\binom{2n}{k} \le 2n\binom{2n}{n}. \qquad \square$$

Lemma 2.21 (LEGENDRE)**.** *For $n \in \mathbb{N}$ we have*

$$n! = \prod_{p\in\mathbb{P}} p^{\left\lfloor \frac{n}{p}\right\rfloor + \left\lfloor \frac{n}{p^2}\right\rfloor + \ldots},$$

where $\lfloor\alpha\rfloor := \max\{z \in \mathbb{Z} : z \le \alpha\}$ for $\alpha \in \mathbb{R}$.

Proof. Among the numbers $1, 2, \ldots, n$, exactly $\left\lfloor \frac{n}{p}\right\rfloor$ are divisible by p, $\left\lfloor \frac{n}{p^2}\right\rfloor$ are divisible by p^2, and so on. $\square$

Lemma 2.22. *Let $n \ge 3$ and $p \le n$ be a prime divisor of $\binom{2n}{n}$. Then $p \le \frac{2}{3}n$. If p^2 is a divisor of $\binom{2n}{n}$, then $p \le \sqrt{2n}$.*

Proof. According to Legendre, p occurs with multiplicity

$$m := \sum_{k=1}^{\infty}\Big(\Big\lfloor\frac{2n}{p^k}\Big\rfloor - 2\Big\lfloor\frac{n}{p^k}\Big\rfloor\Big)$$

in the prime factorization of $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$. Here we have

$$\Big\lfloor\frac{2n}{p^k}\Big\rfloor - 2\Big\lfloor\frac{n}{p^k}\Big\rfloor < \frac{2n}{p^k} - 2\Big(\frac{n}{p^k} - 1\Big) \le 2$$

and $m \le \max\{k \in \mathbb{N}_0 : p^k \le 2n\}$. This shows $p^m \le 2n$. In particular, $p \le \sqrt{2n}$ if $m \ge 2$. In the case $3p > 2n \ge 6$, we have $p \ge 3$ and $p^2 > 2n$. Therefore, p occurs exactly twice in the numerator and denominator of $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$. Consequently, $m = 0$. $\square$

Theorem 2.23 (BERTRAND's Postulate)**.** *For all $n \in \mathbb{N}$, there exists a prime p with $n < p \le 2n$.*

Proof (ERDŐS). One easily checks that

$$p_1, \ldots, p_{11} = 2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 521$$

are primes, where $p_{i+1} < 2p_i$ for $i = 1, \ldots, 10$ holds. For $p_i \le n < p_{i+1}$, we have $p_{i+1} < 2p_i \le 2n$. Therefore, we may assume $n \ge 521$.

Let $\rho(n) := \pi(2n) - \pi(n)$ for $n \in \mathbb{N}$. Then we have

$$\frac{4^n}{2n} \overset{2.20}{\leq} \binom{2n}{n} \overset{2.22}{\leq} \prod_{p \leq \sqrt{2n}} 2n \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \prod_{n < p \leq 2n} p \overset{2.19}{\leq} (2n)^{\sqrt{2n}} \cdot 4^{2n/3} \cdot (2n)^{\rho(n)}$$

$$4^{n/3} < (2n)^{\sqrt{2n}+1+\rho(n)}$$

$$\rho(n) > \frac{2n}{3\log_2(2n)} - (\sqrt{2n}+1).$$

To verify $\rho(n) > 0$, it suffices to show

$$3\log_2(2n) < \frac{2n-1}{\sqrt{2n}+1} = \sqrt{2n} - 1.$$

For $n = 2^9 = 512$, one obtains $30 < 31$. For $x > 38 > 18\log_2(e)^2$, we have

$$(3\log_2(2x))' = (3\log_2(e)\ln(2x))' = \frac{3\log_2(e)}{x} < \frac{1}{\sqrt{2x}} = (\sqrt{2x}-1)',$$

i.e., the function $3\log_2(2x)$ grows slower than $\sqrt{2x} - 1$. Since we have already assumed $n \geq 521$, the claim holds. □

Remark 2.24. It is not yet known whether for $n \geq 2$ there is always a prime between n^2 and $(n+1)^2$.

Theorem 2.25 (Tschebyschow[5])**.** *There exist constants $\alpha, \beta > 0$, such that*

$$\alpha\frac{x}{\log x} \leq \pi(x) \leq \beta\frac{x}{\log x}$$

holds for $x \geq 2$.

Proof. Because of $\pi(x) \geq \pi(2) = 1$, we can assume that x is "large enough". Furthermore, the base of the logarithm does not matter. As before, let always $p \in \mathbb{P}$. From Lemma 2.19 it follows that

$$\sqrt{x}^{\pi(x)-\pi(\sqrt{x})} \leq \prod_{\sqrt{x} < p \leq x} p \leq 4^x.$$

Taking the logarithm yields

$$\pi(x) \leq \frac{4x}{\log_2 x} + \pi(\sqrt{x}) \leq \frac{4x}{\log_2 x} + \sqrt{x} \leq \frac{5x}{\log_2 x}$$

for x sufficiently large.

Now let $n \in \mathbb{N}$ be minimal with $x \leq 2n$. Let $\binom{2n}{n} = p_1^{a_1} \dots p_s^{a_s}$ be the prime factorization. In the proof of Lemma 2.22, we showed $p_i^{a_i} \leq 2n$ for $i = 1, \dots, s$. This implies $\binom{2n}{n} \leq (2n)^s$ and

$$\pi(x) \geq \pi(2n) - 1 \geq s - 1 \geq \frac{\log_2\binom{2n}{n}}{\log_2(2n)} - 1 \overset{2.20}{\geq} \frac{2n - \log_2(2n)}{\log_2(2n)} - 1 = \frac{2n}{\log_2(2n)} - 2.$$

Since the function $\frac{x}{\log_2(x)}$ is monotonically increasing for $x > e$, $\pi(x) \geq \frac{x}{2\log_2 x}$ holds for large x. □

[5] According to Wikipedia, the common transcriptions Tschebyschef, Tschebyscheff, Tschebyschew or Tschebyschev are incorrect.

Remark 2.26. Asymptotically, the *Gauss Prime Number Theorem* holds:[6]

$$\lim_{x\to\infty} \frac{\pi(x)\ln x}{x} = 1,$$

i. e. $\pi(x)$ grows approximately as fast as $\frac{x}{\ln x}$ (without proof). In contrast to Theorem 2.25, one cannot replace the natural logarithm $\ln x$ here with the logarithm with respect to another base. Thus, there is a connection between the prime numbers and Euler's number e.

3 Modulo Arithmetic

Definition 3.1. For $a, b \in \mathbb{Z}$ and $d \in \mathbb{N}$, we write $a \equiv b \pmod{d}$, if $d \mid (a-b)$. One then says: a and b are *congruent modulo* d.

Example 3.2.

(i) In the decimal system, one calculates modulo 10 and in the binary system modulo 2.

(ii) One considers seconds and minutes modulo 60 and hours modulo 12 or 24.

(iii) Days of the week are counted modulo 7.

(iv) Euro cents are calculated modulo 100.

(v) In music, one considers notes modulo 8 (*c, d, e, f, g, a, h*) or 12 (*c, cis, d, ..., h*).

Theorem 3.3. *The congruence modulo $d \in \mathbb{N}$ is an equivalence relation on $\mathbb{Z}$, i. e. it holds that*

(i) $a \equiv a \pmod{d}$ (*reflexive*),

(ii) $a \equiv b \pmod{d} \Longrightarrow b \equiv a \pmod{d}$ (*symmetric*),

(iii) $a \equiv b \equiv c \pmod{d} \Longrightarrow a \equiv c \pmod{d}$ (*transitive*).

Furthermore, it holds that

(iv)

$$\left.\begin{array}{ll} a \equiv a' & \pmod{d} \\ b \equiv b' & \pmod{d} \end{array}\right\} \Longrightarrow a \dot{+} b \equiv a' \dot{+} b' \pmod{d}.$$

Proof.

(i) $d \mid 0 = a - a$.

(ii) $d \mid a-b \Longrightarrow d \mid -(a-b) = b-a$.

(iii) $d \mid a-b \wedge d \mid b-c \Longrightarrow d \mid (a-b)+(b-c) = a-c$.

(iv) Let $d \mid a-a'$ and $d \mid b-b'$. Then it follows that $d \mid (a-a')+(b-b') = (a+b)-(a'+b')$ as well as $d \mid (a-a')b + (b-b')a' = ab - a'b'$. □

[6] proven by Hadamard and Vallée Poussin

Remark 3.4. The equivalence classes in the situation of Theorem 3.3 are called *residue classes* modulo d. They have the form $a + d\mathbb{Z} := \{a + db : b \in \mathbb{Z}\}$ for $a \in \mathbb{Z}$ (all elements in $a + d\mathbb{Z}$ leave the same remainder upon division by d). The set of all residue classes modulo d is denoted by $\mathbb{Z}/d\mathbb{Z}$. Apparently,

$$\mathbb{Z}/d\mathbb{Z} = \{0 + d\mathbb{Z} = d\mathbb{Z},\, 1 + d\mathbb{Z}, \ldots, d - 1 + d\mathbb{Z}\}$$

and $|\mathbb{Z}/d\mathbb{Z}| = d$.

Example 3.5.

(i) Equation (iv) simplifies many calculations. We check whether $7^{90} + 111^7$ is divisible by 5:

$$7^{90} + 111^7 \equiv 2^{90} + 1^7 \equiv 4^{45} + 1 \equiv (-1)^{45} + 1 \equiv 0 \pmod 5.$$

In Corollary 4.8 we show that one may also reduce the exponents, however modulo 4.

(ii) (*Freshman's Dream*) Let $p \in \mathbb{P}$ and $1 \le k \le p - 1$. Then p is a divisor of $\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{k!}$. The binomial theorem shows

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} \equiv a^p + b^p \pmod p.$$

Lemma 3.6 (Cancellation of congruences)**.** *For $a, b \in \mathbb{Z}$ and $d, e \in \mathbb{N}$ it holds that*

$$\boxed{ae \equiv be \pmod d \iff a \equiv b \left(\mathrm{mod}\, \frac{d}{\gcd(d, e)}\right).}$$

Proof. Let $ae \equiv be \pmod d$ and $g := \gcd(d, e)$. Then $d \mid (a - b)e$ and $\frac{d}{g} \mid (a - b)\frac{e}{g}$. Because of $\gcd(\frac{d}{g}, \frac{e}{g}) = 1$ it follows that $\frac{d}{g} \mid (a - b)$ (Remark 2.8(iii)) and $a \equiv b \pmod{\frac{d}{g}}$. Conversely, if $a \equiv b \pmod{\frac{d}{g}}$, then $d \mid d\frac{e}{g} = \frac{d}{g}e \mid (a - b)e$, thus $ae \equiv be \pmod d$. □

Example 3.7. An ISBN for indexing books consists of nine digits $z_1, \ldots, z_9 \in \{0, \ldots, 9\}$ as well as a check digit $s \in \{0, \ldots, 9, X\}$ with

$$s \equiv \sum_{k=1}^{9} k z_k \pmod{11},$$

where 10 is replaced by X. Because of

$$\begin{aligned} kz_k \equiv kz'_k \pmod{11} &\iff z_k \equiv z'_k \pmod{11}, \\ kz_k + lz_k \equiv kz_l + lz_k \pmod{11} &\iff (k - l)z_k \equiv (k - l)z_l \pmod{11} \iff z_k \equiv z_l \pmod{11} \end{aligned}$$

the check digit detects a faulty digit or a transposition of two digits (but not both simultaneously).

Theorem 3.8 (Congruence equations)**.** *Let $a, b \in \mathbb{Z}$ and $d \in \mathbb{N}$. An $x \in \mathbb{Z}$ with $ax \equiv b \pmod d$ exists if and only if $\gcd(a, d) \mid b$. If applicable, these x form a residue class modulo $\frac{d}{\gcd(a,d)}$.*

Proof. First statement:

$$\exists x \in \mathbb{Z} : ax \equiv b \pmod d \iff \exists x, c \in \mathbb{Z} : b = ax + cd \overset{1.13}{\iff} \gcd(a, d) \mid b.$$

Second statement:

$$ax \equiv ay \pmod d \overset{3.6}{\iff} x \equiv y \left(\mathrm{mod}\, \frac{d}{\gcd(a, d)}\right).$$ □

Remark 3.9. Theorem 3.8 states that the equation $ax \equiv b \pmod{d}$ is equivalent to an equation of the form $x \equiv c \pmod{d/\gcd(a,d)}$ in the case of solvability.

Example 3.10. How valuable is a 124.76 g pile of 1- and 2-cent coins? A 1-cent coin weighs 2300 mg and a 2-cent coin 3060 mg. Approach: $2300x + 3060y = 124,760$. We divide by $\gcd(2300, 3060) = 20$ and obtain $115x + 153y = 6238$. Modulo 115 this yields

$$38y \equiv 28 \pmod{115}.$$

According to the Euclidean algorithm, $1 = \gcd(38, 115) = -3 \cdot 38 + 115 \equiv -3 \cdot 38 \pmod{115}$. Substitution yields $38y \equiv 28 \cdot (-3 \cdot 38) \pmod{115}$. Lemma 3.6 shows

$$y \equiv -3 \cdot 28 \equiv 31 \pmod{115}.$$

For $y \geq 31 + 115$, $3060y \geq 446,760 > 124,760$ would hold. Thus $y = 31$ is the only solution and $x = \frac{6238-153y}{115} = 13$ follows.

Answer: $13 + 2 \cdot 31 = 75$ cents.

Theorem 3.11 (Chinese Remainder Theorem)**.** *Let $a_1, \ldots, a_n \in \mathbb{Z}$ and $d_1, \ldots, d_n \in \mathbb{N}$ be pairwise coprime. Then the solutions $x \in \mathbb{Z}$ of the system of equations $x \equiv a_i \pmod{d_i}$ for $i = 1, \ldots, n$ form a residue class modulo $d_1 \ldots d_n$. In particular, there exists exactly one solution $0 \leq x < d_1 \ldots d_n$.*

Proof. According to the prime factorization, $D_i := \prod_{j \neq i} d_j$ is coprime to d_i. According to Theorem 3.8, there exists an $x_i \in \mathbb{Z}$ with $x_i D_i \equiv a_i \pmod{d_i}$ for $i = 1, \ldots, n$. For $x := x_1 D_1 + \ldots + x_n D_n$, it holds that $x \equiv x_i D_i \equiv a_i \pmod{d_i}$ for $i = 1, \ldots, n$. Obviously, every element of the residue class $x + d_1 \ldots d_n \mathbb{Z}$ is also a solution of the system of equations. Conversely, let $y \in \mathbb{Z}$ also be a solution. Then $x - y \equiv a_i - a_i \equiv 0 \pmod{d_i}$ for $i = 1, \ldots, n$. Since $d_1, \ldots, d_n$ are pairwise coprime, it follows that $d_1 \ldots d_n \mid x - y$, i. e. $y \in x + d_1 \ldots d_n \mathbb{Z}$. □

Remark 3.12. Attention: Coprime numbers are not necessarily *pairwise* coprime (consider $6, 10, 15$).

Example 3.13.

(i) Consider the system

$$\begin{aligned} x &\equiv 3 \pmod{7}, \\ x &\equiv 4 \pmod{11}, \\ x &\equiv 5 \pmod{13}. \end{aligned}$$

The approach $x = 3 + 7a$ initially solves the first equation and yields $7a \equiv 1 \pmod{11}$ in the second equation. According to Theorem 3.8, this is equivalent to $a \equiv -3 \pmod{11}$ (the solution -3 can be easily guessed). We now set $a = -3 + 11b$ and obtain $x = -18 + 77b$. This solves the first two equations. The third equation yields $77b \equiv 23 \pmod{13}$, thus $b \equiv 3 \pmod{13}$. The general solution of the system is therefore $x = -18 + 77(3 + 13c) = 213 + 1001c$ with $c \in \mathbb{Z}$.

(ii) What are the last two decimal digits of 47^{88}? We are looking for $0 \leq x \leq 99$ with

$$x \equiv 47^{88} \pmod{100}.$$

Because $\operatorname{lcm}(4, 25) = 100$, this congruence is equivalent to the system

$$\begin{aligned} x &\equiv 47^{88} \pmod 4, \\ x &\equiv 47^{88} \pmod{25} \end{aligned}$$

according to Theorem 3.11. It holds that $47^{88} \equiv (-1)^{88} \equiv 1 \pmod 4$ and

$$47^{88} \equiv (-3)^{3\cdot 29+1} \equiv (-2)^{29}(-3) \equiv (-2)^{7\cdot 4+1}(-3) \equiv (-3)^4 6 \equiv 11 \pmod{25}.$$

The approach $x = 1 + 4a$ solves the first equation and results in $4a \equiv 10 \pmod{25}$ in the second equation. It follows that $2a \equiv 5 \pmod{25}$ and $a \equiv 13 \cdot 2a \equiv 13 \cdot 5 \equiv 15 \pmod{25}$. Thus $x = 1 + 4 \cdot 15 = 61$.

Definition 3.14. One calls

$$\begin{aligned} \varphi\colon \mathbb{N} &\to \mathbb{N}, \\ n &\mapsto |\{1 \le k \le n : \gcd(n, k) = 1\}| \end{aligned}$$

Euler's *φ-function*.

Remark 3.15. For $b \in a + n\mathbb{Z}$, it holds that $\gcd(b, n) = \gcd(a, n)$. Since $a + n\mathbb{Z}$ has exactly one representative b with $1 \le b \le n$, it holds that

$$\varphi(n) = |\{a + n\mathbb{Z} : \gcd(a, n) = 1\}|.$$

Theorem 3.16. *It holds that*

(i) $\varphi(nm) = \varphi(n)\varphi(m)$, *if* $\gcd(n, m) = 1$.

(ii) $\varphi(p^n) = p^n - p^{n-1}$ *for every prime power* $p^n \neq 1$.

Proof.

(i) Let $1 \le a \le n$ and $1 \le b \le m$ with $\gcd(a, n) = 1 = \gcd(b, m)$. According to the Chinese Remainder Theorem, there exists exactly one $1 \le c \le nm$ with $c \equiv a \pmod n$ and $c \equiv b \pmod m$. Obviously, then $\gcd(c, nm) = 1$. Conversely, if $1 \le c \le nm$ with $\gcd(c, nm) = 1$ is given, then also $\gcd(c, n) = 1 = \gcd(c, m)$. Therefore, the sets

$$\{1 \le a \le n : \gcd(a, n) = 1\} \times \{1 \le b \le m : \gcd(b, m) = 1\}$$

and $\{1 \le c \le nm : \gcd(c, nm) = 1\}$ have the same cardinality and the claim follows.

(ii) It holds that $\gcd(p^n, k) = 1$ if and only if $p \nmid k$. Between 1 and p^n there are exactly p^{n-1} multiples of p, namely $p, 2p, \ldots, p^{n-1}p$. This shows the claim. □

Remark 3.17. Let $n = \prod_{p\in\mathbb{P}} p^{a_p} \in \mathbb{N}$. According to Theorem 3.16, then

$$\boxed{\varphi(n) = \prod_{p\in\mathbb{P}} \varphi(p^{a_p}) = \prod_{\substack{p\in\mathbb{P} \\ a_p>0}} (p^{a_p} - p^{a_p-1}).}$$

Example 3.18. It holds that

$$\varphi(36) = \varphi(2^2 \cdot 3^2) = (2^2 - 2^1)(3^2 - 3^1) = 2 \cdot 6 = 12$$

and

$$\{1 \leq a \leq 36 : \gcd(a, 36) = 1\} = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}.$$

Definition 3.19. One calls

$$\mu \colon \mathbb{N} \to \mathbb{Z},$$
$$n \mapsto \begin{cases} (-1)^s & \text{if } n = p_1 \dots p_s \text{ with pairwise distinct } p_1, \dots, p_s \in \mathbb{P}, \\ 0 & \text{otherwise} \end{cases}$$

the MÖBIUS *function*. Here $\mu(1) = 1$ $(s = 0)$.

Remark 3.20. If $p_1, \dots, p_s$ are the distinct prime divisors of $n > 1$, then

$$\sum_{d|n} \mu(d) = \sum_{k=0}^{s} \sum_{q_1,\dots,q_k \in \{p_1,\dots,p_s\}} \mu(q_1 \dots q_k) = \sum_{k=0}^{s} \sum_{\substack{M \subseteq \{p_1,\dots,p_s\} \\ |M|=k}} (-1)^k = \sum_{k=0}^{s} (-1)^k \binom{s}{k} = (1-1)^s = 0.$$

Theorem 3.21 (MÖBIUS inversion)**.** *For $f, F \colon \mathbb{N} \to \mathbb{C}$, the following are equivalent:*

(1) $F(n) = \sum_{d|n} f(d)$ *for all* $n \in \mathbb{N}$.

(2) $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d}) = \sum_{d|n} \mu(\frac{n}{d}) F(d)$ *for all* $n \in \mathbb{N}$.

Proof.

(1) $\Rightarrow$ (2):

$$\sum_{d|n} \mu(d) F(n/d) \overset{(1)}{=} \sum_{d|n} \sum_{e|\frac{n}{d}} \mu(d) f(e) = \sum_{de|n} \mu(d) f(e) = \sum_{e|n} f(e) \sum_{d|\frac{n}{e}} \mu(d) \overset{3.20}{=} f(n).$$

(2) $\Rightarrow$ (1):

$$\sum_{d|n} f(d) \overset{(2)}{=} \sum_{d|n} \sum_{e|d} \mu(d/e) F(e) = \sum_{e|n} F(e) \sum_{d|\frac{n}{e}} \mu(d) \overset{3.20}{=} F(n). \qquad \square$$

Example 3.22. For $n = \prod_{p \in \mathbb{P}} p^{a_p} \in \mathbb{N}$, it holds that

$$\sum_{d|n} \varphi(d) \overset{2.8}{=} \prod_{p \in \mathbb{P}} \sum_{k=0}^{a_p} \varphi(p^k) \overset{3.16}{=} \prod_{p \in \mathbb{P}} (1 + (p-1) + (p^2 - p) + \dots + (p^{a_p} - p^{a_p - 1})) = \prod_{p \in \mathbb{P}} p^{a_p} = n.$$

For $f = \varphi$, we thus have $F = \mathrm{id}_{\mathbb{N}}$ in Theorem 3.21 and obtain

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

for all $n \in \mathbb{N}$.

4 Residue Class Rings

Remark 4.1. We already know from Theorem 3.3 that congruences can be added, subtracted, and multiplied. In this chapter, we investigate the interplay of these operations on the set of residue classes $\mathbb{Z}/n\mathbb{Z}$.

Theorem 4.2. *Let $n \in \mathbb{N}$. With the operations*

$$(a + n\mathbb{Z}) \dot{+} (b + n\mathbb{Z}) := (a \dot{+} b) + n\mathbb{Z}$$

$\mathbb{Z}/n\mathbb{Z}$ becomes a commutative ring*, i. e., the following axioms hold:*

(i) $(\mathbb{Z}/n\mathbb{Z}, +)$ *is an abelian group with neutral element* $0 + n\mathbb{Z} = n\mathbb{Z}$.

(ii) $(a + n\mathbb{Z}) \cdot ((b + n\mathbb{Z}) \cdot (c + n\mathbb{Z})) = ((a + n\mathbb{Z}) \cdot (b + n\mathbb{Z})) \cdot (c + n\mathbb{Z})$ (*associative law*).

(iii) $(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = (b + n\mathbb{Z}) \cdot (a + n\mathbb{Z})$ (*commutative law*).

(iv) $(1 + n\mathbb{Z}) \cdot (a + n\mathbb{Z}) = a + n\mathbb{Z}$ (*neutral element w.r.t.* $\cdot$).

(v) $(a + n\mathbb{Z}) \cdot ((b + n\mathbb{Z}) + (c + n\mathbb{Z})) = ((a + n\mathbb{Z}) \cdot (b + n\mathbb{Z})) + ((a + n\mathbb{Z}) \cdot (c + n\mathbb{Z}))$ (*distributive law*).

Proof. The well-definedness of addition and multiplication was shown in Theorem 3.3. The axioms follow immediately from the corresponding rules in $\mathbb{Z}$ ($\mathbb{Z}$ is a commutative ring). □

Remark 4.3.

(i) As usual, we often omit the multiplication dot when calculating with residue classes and use "multiplication before addition". If misunderstandings are excluded, we write 0 for $0 + n\mathbb{Z}$ and 1 for $1 + n\mathbb{Z}$. In the (uninteresting) special case $n = 1$, $0 = 1$ holds.

(ii) In contrast to a field, in a ring not every element different from 0 is invertible w.r.t. multiplication. For example, there exists no $a + 4\mathbb{Z}$ with $(2 + 4\mathbb{Z})(a + 4\mathbb{Z}) = 1 + 4\mathbb{Z}$. According to Theorem 3.8, the invertible elements in $\mathbb{Z}/n\mathbb{Z}$ have the form $a + n\mathbb{Z}$ with $\gcd(a, n) = 1$. They form a group of order $\varphi(n)$ w.r.t. multiplication (Remark 3.15).

Definition 4.4. For $n \in \mathbb{N}$, one calls

$$(\mathbb{Z}/n\mathbb{Z})^\times := \{a + n\mathbb{Z} : \gcd(a, n) = 1\}$$

the *prime residue class group modulo n.*

Example 4.5. We want to determine the inverse of $7 + 31\mathbb{Z}$ in $(\mathbb{Z}/31\mathbb{Z})^\times$. The Euclidean algorithm yields $1 = \gcd(7, 31) = 9 \cdot 7 - 2 \cdot 31$. Thus $(7 + 31\mathbb{Z})^{-1} = 9 + 31\mathbb{Z}$.

Theorem 4.6. *$\mathbb{Z}/n\mathbb{Z}$ is a field if and only if $n \in \mathbb{P}$.*

Proof. For $n = p \in \mathbb{P}$, $|(\mathbb{Z}/p\mathbb{Z})^\times| = \varphi(p) = p - 1 = |(\mathbb{Z}/n\mathbb{Z}) \setminus (0 + n\mathbb{Z})|$, i. e. every element different from 0 is invertible. Thus $\mathbb{Z}/p\mathbb{Z}$ is a field. If $n \notin \mathbb{P}$, then there exists a prime divisor p of n. Because of $\gcd(p, n) = p \neq 1$, $0 \neq p + n\mathbb{Z}$ is not invertible in $(\mathbb{Z}/n\mathbb{Z})^\times$. Therefore $\mathbb{Z}/n\mathbb{Z}$ is not a field. □

Definition 4.7. For a prime number p, one sets $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

Corollary 4.8 (Euler-Fermat)**.** *For $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $\gcd(a,n) = 1$, it holds that*

$$\boxed{a^{\varphi(n)} \equiv 1 \pmod{n}.}$$

In particular, $a^{p-1} \equiv 1 \pmod{p}$ for $p \in \mathbb{P}$ with $p \nmid a$.

Proof. Let $G := (\mathbb{Z}/n\mathbb{Z})^\times$. As in every group, $gx = gy \iff x = g^{-1}gx = g^{-1}gy = y$ for $g, x, y \in G$. Thus, as g runs through G, gx also runs through all elements of G (only in a different order). Since G is commutative, it follows that

$$\prod_{g \in G} g = \prod_{g \in G} (xg) = x^{|G|} \prod_{g \in G} g = x^{\varphi(n)} \prod_{g \in G} g.$$

By multiplying with the inverse of $\prod g$, one obtains the first claim. The second statement follows from $\varphi(p) = p - 1$. □

Remark 4.9. The equation $a^{p-1} \equiv 1 \pmod{p}$ is called *Fermat's little theorem*. From it follows $a^p \equiv a \pmod{p}$ even for all $a \in \mathbb{Z}$. We investigate the converse of this statement in Theorem 4.24.

Definition 4.10. A group $(G, \cdot)$ is called *cyclic* if an element $g \in G$ exists with $G = \{g^k : k \in \mathbb{Z}\}$. If applicable, g is called a *generator* of G.

Example 4.11. The group $(\mathbb{Z}/n\mathbb{Z}, +)$ is cyclic with generator $1 + n\mathbb{Z}$, since $a + n\mathbb{Z} = a(1 + n\mathbb{Z})$ for $a = 1, \ldots, n$ (the power g^k becomes the multiple here, since the operation is $+$ and not $\cdot$). In the group $G := (\mathbb{Z}/8\mathbb{Z})^\times$, however, $a^2 \equiv 1 \pmod{8}$ holds for all $a + 8\mathbb{Z} \in G$. Therefore G is not cyclic.

Definition 4.12. For $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$, there exists by Euler-Fermat a smallest natural number $k \in \mathbb{N}$ with $a^k \equiv 1 \pmod{n}$. One calls $\operatorname{ord}_n(a) := k$ the *order* of a modulo n.

Lemma 4.13. *Let $a + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ with $d := \operatorname{ord}_n(a)$. Then it holds that*

(i) $a^k \equiv 1 \pmod{n} \iff d \mid k$. *In particular, $d \mid \varphi(n)$.*

(ii) $a^k \equiv a^l \pmod{n} \iff k \equiv l \pmod{d}$ *for $k, l \in \mathbb{N}$.*

(iii) For $k \in \mathbb{N}$,

$$\boxed{\operatorname{ord}_n(a^k) = \frac{d}{\gcd(d,k)}.}$$

Proof.

(i) Euclidean division yields $k = dq + r$ with $q, r \in \mathbb{Z}$ and $0 \le r < d$. Now it holds that

$$a^r \equiv (a^d)^q a^r \equiv a^{dq+r} \equiv a^k \equiv 1 \pmod{n} \iff r = 0 \iff d \mid k.$$

(ii) Let wlog. $k \le l$. From (i) it follows that

$$a^k \equiv a^l \pmod{n} \iff a^{l-k} \equiv 1 \pmod{n} \iff d \mid l - k \iff k \equiv l \pmod{d}.$$

(iii) It holds that

$$\begin{aligned}\operatorname{ord}_n(a^k) &= \min\{s \in \mathbb{N} : a^{ks} = (a^k)^s \equiv 1 \pmod n\} \overset{\text{(i)}}{=} \min\{s \in \mathbb{N} : ks \equiv 0 \pmod d\} \\ &\overset{3.6}{=} \min\left\{s \in \mathbb{N} : s \equiv 0 \left(\mathrm{mod}\ \frac{d}{\gcd(d,k)}\right)\right\} = \frac{d}{\gcd(d,k)}.\end{aligned}$$

□

Example 4.14. How long is the (minimal) *period* of the decimal expansion of a rational number $r = \frac{n}{k}$ with $\gcd(n,k) = 1$ (the existence of this period is proven in a more general context in Theorem 5.2)? Example:

$$\frac{1}{3} = 0{,}\overline{3}, \qquad \frac{1}{7} = 0{,}\overline{142857}, \qquad \frac{1}{22} = 0{,}0\overline{45}.$$

Let $k = 2^a 5^b k'$ with $\gcd(10, k') = 1$. Then it holds that

$$10^{a+b} r = \frac{2^b 5^a n}{k'}.$$

Since the period does not change by multiplication with 10^{a+b} (only the starting position of the period changes), we can assume $\gcd(10, k) = 1$.

Theorem 4.15 (Period length)**.** *Let $n, k \in \mathbb{N}$ with $\gcd(n,k) = 1 = \gcd(10,k)$. Then $\operatorname{ord}_k(10)$ is the period length of $\frac{n}{k}$.*

Proof. By multiplying $r = \frac{n}{k}$ with a suitable power of 10, we can assume that the period begins directly after the decimal point. So let $r = \ldots,\overline{d_1 \ldots d_\rho}$, i. e. the period length is $\rho \geq 0$. Then it holds that

$$10^\rho r - r = \ldots d_1 \ldots d_\rho,\overline{d_1 \ldots d_\rho} - \ldots,\overline{d_1 \ldots d_\rho} \in \mathbb{N}$$

and it follows that $10^\rho n - n \equiv 0 \pmod k$. Due to $\gcd(n,k) = 1$, this is equivalent to $10^\rho \equiv 1 \pmod k$. This shows $t := \operatorname{ord}_k(10) \mid \rho$. Conversely, $10^t \equiv 1 \pmod k$ holds and it follows that $10^t r - r \in \mathbb{N}$. For the decimal places $d_1, d_2, \ldots$ this means $d_{i+t} = d_i$ for all $i \in \mathbb{N}$. Thus $\rho \leq t$. □

Remark 4.16. The period length of $\frac{n}{k}$ is therefore at most $\varphi(k)$. In the following, we investigate when the maximum is attained.

Lemma 4.17. *Let K be a field, $n \in \mathbb{N}$ and $a_0, a_1, \ldots, a_{n-1} \in K$. Then the polynomial equation*

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

has at most n distinct solutions $x \in K$.

Proof. Suppose there exist $n+1$ pairwise distinct solutions $x_0, x_1, \ldots, x_n \in K$. As is well known, the Vandermonde matrix

$$A := \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^n \\ 1 & x_1 & x_1^2 & \cdots & x_1^n \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^n \end{pmatrix} \in K^{(n+1)\times(n+1)}$$

is then invertible (it holds that $\det(A) = \prod_{0 \leq i < j \leq n}(x_j - x_i) \neq 0$). On the other hand, $v := (a_0, a_1, \ldots, a_{n-1}, 1)$ is a non-trivial solution of the linear system of equations $Av = 0$. Contradiction. □

Theorem 4.18. *For $p \in \mathbb{P}$, $\mathbb{F}_p^\times$ is cyclic, i. e. there exists an $a \in \mathbb{Z}$ with*

$$\mathbb{F}_p^\times = \{a^k + p\mathbb{Z} : k = 1, \dots, p-1\}.$$

Proof. Let $f(d)$ be the number of elements $a + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$ of order d. In the case $d \nmid \varphi(p) = p - 1$, $f(d) = 0$ according to Lemma 4.13. Now let $\operatorname{ord}_p(a) = d \mid p - 1$. Then the residue classes $a^k + p\mathbb{Z}$ for $k = 1, \dots, d$ are pairwise distinct and it holds that

$$(a^k)^d - 1 = a^{kd} - 1 = (a^d)^k - 1 \equiv 1^k - 1 \equiv 0 \pmod{p}.$$

According to Lemma 4.17, the residue classes of $a, a^2, \dots, a^d$ are thus the only solutions of the equation $x^d = 1$ in the field $\mathbb{F}_p$. According to Lemma 4.13, it also holds that $\operatorname{ord}_p(a^k) = \frac{d}{\gcd(d,k)}$. Therefore, only the elements a^k with $\gcd(d, k) = 1$ have order d. This shows $f(d) \leq \varphi(d)$. Since every element of $\mathbb{F}_p^\times$ has an order $d \mid p - 1$, it holds that

$$p - 1 = \sum_{d \mid p-1} f(d) \leq \sum_{d \mid p-1} \varphi(d) \overset{3.22}{=} p - 1.$$

It follows that $f(d) = \varphi(d)$ for all $d \mid p - 1$. In particular, $f(p - 1) = \varphi(p - 1) > 0$. If $a + p\mathbb{Z}$ has order $p - 1$, then indeed $\mathbb{F}_p^\times = \{a^k + p\mathbb{Z} : k = 1, \dots, p - 1\}$ according to Lemma 4.13. □

Remark 4.19. A generator $a \in \mathbb{Z}$ of $\mathbb{F}_p^\times$ is called a *primitive root* modulo p. The proof of Theorem 4.18 shows that there are exactly $\varphi(p - 1)$ primitive roots, without however constructing such a root. In fact, no formula is known for the calculation of primitive roots, but as a rule one finds "small" primitive roots[7].

Lemma 4.20. *For every prime $p > 2$ and $n \in \mathbb{N}$, it holds that* $\operatorname{ord}_{p^n}(1 + p) = p^{n-1}$.

Proof. For $n = 1$, the statement is trivial. We prove inductively

$$(1 + p)^{p^{n-2}} \equiv 1 + p^{n-1} \pmod{p^n} \tag{4.1}$$

for $n \geq 2$. In the case $n = 2$, one obtains $1 + p \equiv 1 + p \pmod{p^2}$. Now let $n \geq 3$. By induction, there exists a $k \in \mathbb{Z}$ with $(1 + p)^{p^{n-3}} = 1 + p^{n-2} + kp^{n-1}$. It follows

$$\begin{aligned}(1 + p)^{p^{n-2}} &= (1 + p^{n-2} + kp^{n-1})^p = \sum_{k=0}^{p} \binom{p}{k} (p^{n-2} + kp^{n-1})^k \\ &\equiv 1 + p^{n-1} + \sum_{k=2}^{p} \binom{p}{k} p^{(n-2)k} (1 + kp)^k \pmod{p^n}.\end{aligned}$$

For $2 \leq k < p$, $\binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{k!}$ is divisible by p and $(n - 2)k \geq 2n - 4 \geq n - 1$. Therefore, the sum over $2 \leq k \leq p$ is divisible by p^n and the induction is finished. For $n + 1$, (4.1) becomes

$$(1 + p)^{p^{n-1}} \equiv 1 + p^n \equiv 1 \pmod{p^n}.$$

This shows $\operatorname{ord}_{p^n}(1 + p) \mid p^{n-1}$. On the other hand, because of $1 + p^{n-1} \not\equiv 1 \pmod{p^n}$, $\operatorname{ord}_{p^n}(1 + p) > p^{n-2}$ according to (4.1). Thus $\operatorname{ord}_{p^n}(1 + p) = p^{n-1}$ holds. □

[7] See appendix and `https://oeis.org/A001918`

Theorem 4.21 (Gauss). *The group $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if $n \in \{4, p^m, 2p^m\}$ for an odd prime p and $m \in \mathbb{N}_0$.*

Proof. Let $G := (\mathbb{Z}/n\mathbb{Z})^\times$ and wlog. let $n \geq 3$.

$\Rightarrow$: According to Remark 3.17, $2 \mid \varphi(n)$. Let $a + n\mathbb{Z}$ be a generator of G. According to Lemma 4.13, $a^{\varphi(n)/2} + n\mathbb{Z}$ is the only element of order 2 in G. This shows $a^{\varphi(n)/2} + n\mathbb{Z} = -1 + n\mathbb{Z}$. Let $n = p_1^{m_1} \dots p_k^{m_k}$ be the prime factorization of n. According to the Chinese Remainder Theorem, for each $1 \leq i \leq k$ there exists an $x_i \in \mathbb{Z}$ with $x_i \equiv -1 \pmod{p_i^{m_i}}$ and $x_i \equiv 1 \pmod{p_j^{m_j}}$ for all $j \neq i$. Obviously $x_i^2 \equiv 1 \pmod{n}$, i. e. $\operatorname{ord}_n(x_i) \leq 2$. In the case $k \geq 2$, n has an odd prime divisor, say p_1. Now $-1 \not\equiv 1 \pmod{p_1^{m_1}}$ and $\operatorname{ord}_n(x_i) = 2$. This shows $x_i \equiv -1 \pmod{n}$. But then $-1 \equiv x_i \equiv 1 \pmod{p_i^{m_i}}$ must hold for $i \geq 2$. This yields $k = 2$ and $p_2^{m_2} = 2$.

Now let $k = 1$ and $n = 2^m$. In the case $m \geq 3$, $-1 + 2^{m-1} + n\mathbb{Z}$ would be another element of order 2 besides $-1 + n\mathbb{Z}$, because $(-1 + 2^{m-1})^2 = 1 + 2^m + 2^{2m-2} \equiv 1 \pmod{n}$.

$\Leftarrow$: Let $n = p^m \geq p$ for a prime $p > 2$. Let b be a primitive root modulo p and $a = (1+p)b^n$. Because of $\gcd(b, p) = 1$, we also have $\gcd(a, n) = 1$. Let $d := \operatorname{ord}_n(a)$. From $a^d \equiv 1 \pmod{n}$ it follows that

$$b^{nd} \equiv (1+p)^d b^{nd} \equiv a^d \equiv 1 \pmod{p}.$$

According to Lemma 4.13, $p - 1 \mid d$ holds. Therefore $\varphi(n) = p^{m-1}(p-1) \mid nd$ and $b^{nd} \equiv 1 \pmod{n}$. It follows that $(1+p)^d \equiv a^d \equiv 1 \pmod{n}$. According to Lemma 4.20, $p^{m-1} \mid d$ now holds. Overall, one obtains $\varphi(n) = \operatorname{lcm}(p^{m-1}, (p-1)) \mid d \mid \varphi(n)$. This shows that $a + n\mathbb{Z}$ is a generator of G.

Finally, according to the Chinese Remainder Theorem, there exists a $c \in \mathbb{Z}$ with $c \equiv a \pmod{n}$ and $c \equiv 1 \pmod{2}$. Then $\operatorname{ord}_{2n}(c) \geq \operatorname{ord}_n(c) = \varphi(n) = \varphi(2)\varphi(n) = \varphi(2n)$ holds. Thus $c + 2n\mathbb{Z}$ is a generator of $(\mathbb{Z}/2n\mathbb{Z})^\times$. □

Remark 4.22. The period length of $\frac{n}{k}$ can only be $\varphi(k)$ if $10 + k\mathbb{Z}$ is a generator of $(\mathbb{Z}/k\mathbb{Z})^\times$. Because of $\gcd(10, k) = 1$, only $k = p^m$ for a prime $p > 2$ is possible for this. Assume 10 is not a primitive root of p. Then there exist $d < p - 1$ and $a \in \mathbb{Z}$ with $10^d = 1 + pa$. With the binomial formula it follows that

$$10^{dp^{m-1}} = (1 + ap)^{p^{m-1}} \equiv 1 \pmod{p^m}$$

as in Lemma 4.20. Thus $\operatorname{ord}_k(10) < \varphi(k)$. On the other hand, an open conjecture by Gauss states that there are infinitely many primes p with $\operatorname{ord}_p(10) = \varphi(p)$. In the vast majority of cases, $\operatorname{ord}_{p^2}(10) = \varphi(p^2)$ then also holds (the smallest exceptions are $p = 487$ and $56,598,313$).[8] Exercise 33 shows that, if applicable, the period length of $\frac{n}{p^m}$ is also maximal for all $m \geq 1$.

Definition 4.23. One calls $n \in \mathbb{N} \setminus \mathbb{P}$ a Carmichael *number*, if $n \geq 1$ and $a^{n-1} \equiv 1 \pmod{n}$ holds for all $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$.

Theorem 4.24 (Korselt). *$n \in \mathbb{N}$ is a Carmichael number if and only if n is a product of at least three pairwise distinct odd prime numbers $p_1, \dots, p_k$ and $n \equiv 1 \pmod{p_i - 1}$ holds for $i = 1, \dots, k$.*

[8] see `https://oeis.org/A045616`

Proof. Let $p > 2$ be a prime divisor of n and p^m the maximal p-power that divides n. According to Gauss, there exists a generator $a + p^m\mathbb{Z}$ of $(\mathbb{Z}/p^m\mathbb{Z})^\times$. By the Chinese Remainder Theorem, we can assume $\gcd(a, n) = 1$. From $a^{n-1} \equiv 1 \pmod{p^m}$ it follows that $p - 1 \mid \varphi(p^m) = \mathrm{ord}_{p^m}(a) \mid n - 1$, i. e. $n \equiv 1 \pmod{p-1}$. In the case $m \geq 2$, one would have the contradiction $p \mid n - 1$. From $n \equiv 1 \pmod{p-1}$ it also follows that $\gcd(p - 1, n) = 1$. Thus n can only be even if $n = 2^m$ with $m \geq 2$ holds ($m = 1$ is excluded since Carmichael numbers are not prime numbers). In this case, however, $-1 \equiv (-1)^{n-1} \equiv 1 \pmod{4}$ would hold. Thus n is a product of pairwise distinct odd prime numbers. Suppose $n = pq$ with prime numbers $p < q$. Then

$$p - 1 \equiv n - 1 \equiv 0 \pmod{q-1}$$

and one obtains the contradiction $q - 1 \leq p - 1 < p - 1$.

Conversely, let $n = p_1 \dots p_k$ with prime numbers $p_1 < \dots < p_k$ and $n \equiv 1 \pmod{p_i - 1}$ for $i = 1, \dots, k$. Let $\gcd(a, n) = 1$. Because of $\varphi(p_i) \mid n - 1$, it holds that $a^{n-1} \equiv 1 \pmod{p_i}$. From this it follows that $a^{n-1} \equiv 1 \pmod{n}$. Thus n is a Carmichael number (the conditions $p_1 > 2$ and $k \geq 3$ are not required). □

Example 4.25. Let $n = pqr$ be a Carmichael number with odd prime numbers $p < q < r$. For $p = 3$, $n \equiv 1 \pmod{p-1}$ is obviously satisfied. For $q = 5$, one obtains $15 \equiv 15r \equiv n \equiv 1 \pmod{r-1}$. There is no r for this. The case $q = 7$ is likewise excluded, because here $\gcd(n, 6) = 1$ would hold. Finally, let $q = 11$. Then $3r \equiv 1 \pmod{10}$, so $r \equiv 7 \pmod{10}$. The choice $r = 17$ requires $33 \equiv n \equiv 1 \pmod{16}$, which is correct. Thus $n = 3 \cdot 11 \cdot 17 = 561$ is a (the smallest) Carmichael number.

Remark 4.26. Since Carmichael numbers are relatively rare, the Fermat equation $a^{p-1} \equiv 1 \pmod{p}$ is suitable as a (necessary but not sufficient) primality test (Exercise 30). Alford-Granville-Pomerance have shown, however, that there are infinitely many Carmichael numbers. The following refinement provides a better primality test.

Theorem 4.27 (Miller-Rabin Test)**.** *Let $n \in \mathbb{N}$ and $n - 1 = 2^k m$ with $k \geq 1$ and $2 \nmid m$.*

(i) If there exist numbers $a \in \mathbb{N}$ and $0 \leq l < k$ with $a^{2^l m} \not\equiv \pm 1 \pmod{n}$ and $a^{2^{l+1}m} \equiv 1 \pmod{n}$, then n is not a prime number.

(ii) If n is not a prime number, then there exist at most $\frac{1}{4}n$ numbers $a \in \{2, \dots, n-1\}$ for which $a^m \equiv 1 \pmod{n}$ or $a^{2^l m} \equiv -1 \pmod{n}$ holds for some $l < k$.

Proof. First, let $n \in \mathbb{P}$. Then $G := (\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic of order $n - 1$. In particular, $-1 + n\mathbb{Z}$ is the only element of order 2 in G. For a with $a^{2^l m} \not\equiv 1 \pmod{n}$ and $a^{2^{l+1}m} \equiv 1 \pmod{n}$, it must therefore hold that $a^{2^l m} \equiv -1 \pmod{n}$. This shows (i).

Now let $n \notin \mathbb{P}$ and a as in (ii). Let A be the number of these elements a. Because of $a^{n-1} = a^{2^k m} \equiv 1 \pmod{n}$, we have $\overline{a} := a + n\mathbb{Z} \in G$ and $t := |\langle \overline{a} \rangle|$ divides $\gcd(\varphi(n), n - 1)$. Let $n = p_1^{r_1} \dots p_s^{r_s}$ be the prime factorization of n. Because of $\gcd(n - 1, p_1 \dots p_s) = 1$, we have $t \mid (p_1 - 1) \dots (p_s - 1)$. Since n is odd, the groups $G_i := (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$ are cyclic for $i = 1, \dots, s$. According to the Chinese Remainder Theorem, $G = G_1 \times \dots \times G_s$ holds. We write $\overline{a} = (\overline{a}_1, \dots, \overline{a}_s)$ with $\overline{a}_i \in G_i$. Then there are at most $p_i - 1$ possibilities for $\overline{a}_i$. In the case $r_i > 1$, it holds that

$$A \leq (p_1 - 1) \dots (p_s - 1) \leq \frac{p_i - 1}{p_i^2} n \leq \frac{2}{9} n < \frac{1}{4} n.$$

We can therefore assume $r_1 = \ldots = r_s = 1$. In particular, $s \geq 2$ because of $n \notin \mathbb{P}$.

Let $p_i - 1 = 2^{d_i} q_i$ with $d_i \geq 1$ and $2 \nmid q_i$ for $i = 1, \ldots, s$. In the case $a^m \equiv 1 \pmod{n}$, $\overline{a}$ has odd order. Here there are at most $q_1 \ldots q_s$ possibilities for a. Now let $a^{2^l m} \equiv -1 \pmod{n}$ for some $l < k$. Then $a^{2^l m} \equiv -1 \pmod{p_i}$ also holds for $i = 1, \ldots, s$. For $\overline{a}_i$, there are therefore at most $\varphi(2^{l+1}) q_i = 2^l q_i$ possibilities (with equality if $q_i \mid m$). Consequently, there are at most $2^{ls} q_1 \ldots q_s$ possibilities for a. With $d := \max\{d_1, \ldots, d_s, k\}$, one obtains

$$A \leq q_1 \ldots q_s + q_1 \ldots q_s \sum_{l=0}^{d-1} 2^{ls} = \Big(1 + \frac{2^{sd} - 1}{2^s - 1}\Big) q_1 \ldots q_s.$$

In the case $s \geq 3$, we have

$$A \leq \frac{2^{sd} + 6}{7} q_1 \ldots q_s \leq \frac{2^{sd}}{4} q_1 \ldots q_s \leq \frac{1}{4}(p_1 - 1) \ldots (p_s - 1) < \frac{1}{4} n.$$

The case $s = 2$ remains. If $d_1 \neq d_2$, one obtains

$$A \leq \frac{2^{2d} + 2}{3} q_1 q_2 \leq \frac{2^{2d-1} + 1}{3} (p_1 - 1)(p_2 - 1) \leq 2^{2d-2} (p_1 - 1)(p_2 - 1) < \frac{1}{4} n.$$

Therefore, let $d_1 = d_2 = d$. Wlog. let $q_1 < q_2$. Then it holds that

$$2^k m = n - 1 = (2^d q_1 + 1)(2^d q_2 + 1) - 1 \equiv 2^d q_1 \not\equiv 0 \pmod{q_2}$$

and $q_2 \nmid m$. For $\overline{a}_2$, only at most $\frac{1}{3} 2^d q_2$ elements are possible. This yields

$$A \leq \frac{2^{2d} + 2}{9} q_1 q_2 < \frac{1}{4} n. \qquad \square$$

Remark 4.28.

(i) In practice, one chooses random numbers $a_1, \ldots, a_s \in \{2, \ldots, n-1\}$. If $a_i^{n-1} \not\equiv 1 \pmod{n}$ for some i, then n is not a prime number according to Fermat. If Theorem 4.27(i) holds for some a_i, then n is likewise not a prime number. Otherwise, we can conclude according to Theorem 4.27(ii) that n is not a prime number with probability $\leq 4^{-s}$. It is therefore a *probabilistic* primality test. A definitive answer is obtained by testing more than $\frac{1}{4} n$ many a_i, which is however impractical.[9] For the success of the Miller-Rabin test, the randomness of the a_i is indispensable, because for any given set $\{a_1, \ldots, a_s\}$, composite numbers n can be constructed that pass the Miller-Rabin test with respect to the a_i (without proof).

(ii) Under the assumption of the Riemann Hypothesis, one can show that the Miller-Rabin test already provides a definitive answer for relatively "small" a_i. Thus, the algorithm has a runtime of $O(\log(n)^4)$. With the *AKS test*, a deterministic algorithm with polynomial runtime (in $\log(n)$) that does not depend on unproven conjectures was found for the first time in 2002 (Exercise 26). Note that primality tests usually do not provide a concrete divisor of n if n is not a prime number. Prime factorization is a much more difficult problem from an algorithmic point of view (see Chapter 10).

Example 4.29.

(i) For the Carmichael number $n = 561$, we have $n - 1 = 2^4 \cdot 75$. For $a = 2$, we calculate $a^{4 \cdot 75} \equiv 67 \not\equiv \pm 1 \pmod{n}$ and $a^{8 \cdot 75} \equiv 1 \pmod{n}$. Thus n is not a prime number.

[9] Due to possible hardware defects, one cannot expect a one hundred percent statement in computer calculations anyway.

(ii) For the Mersenne number $n = M_{11} = 2047$, we have $n - 1 = 2 \cdot 1023$. For $a = 2$, $a^{1023} \equiv 1 \pmod{n}$, i.e., the Miller-Rabin test does not recognize for this a that n is not a prime number. However, because of $3^{1023} \equiv 1565 \pmod{n}$, the test with $a = 3$ is sufficient.

5 Continued Fractions

Remark 5.1. Irrational numbers are characterized by the fact that their (infinite) decimal expansion has no period. For certain irrational numbers, we will nevertheless construct a regular sequence. First, we generalize the b-adic expansion (Theorem 1.5) and the decimal expansion of rational numbers (Theorem 4.15).

Theorem 5.2. *Let $b \in \mathbb{N} \setminus \{1\}$ and $x \in \mathbb{R}$ with $x > 0$. Then there exists exactly one $n \in \mathbb{Z}$ and exactly one infinite sequence $x_n, x_{n+1}, \ldots \in \{0, \ldots, b-1\}$ with the following properties:*

(i) The series $\sum_{k=n}^{\infty} x_k b^{-k}$ converges to x.

(ii) $x_n \neq 0$ and infinitely many x_i are not equal to $b - 1$.

(iii) $x \in \mathbb{Q}$ if and only if there exist $p, n_0 \in \mathbb{N}$ with $x_{k+p} = x_k$ for all $k \geq n_0$. If applicable, the sequence (x_i) is called periodic. *If p is chosen minimally, then $x_{n_0}, x_{n_0+1}, \ldots, x_{n_0+p-1}$ is called the* period *of* length *p of x.*

Proof. Let $n \in \mathbb{Z}$ be minimal and $x_n \in \{1, \ldots, b-1\}$ maximal with $x_n b^{-n} \leq x$ (exists since $x > 0$). Let $n_1 > n$ be minimal and $x_{n_1} \in \{1, \ldots, b-1\}$ maximal with $x_n b^{-n} + x_{n_1} b^{-n_1} \leq x$ etc. For $k \neq n_i$ we set $x_k := 0$. Because of

$$|x - x_n b^{-n} - \ldots - x_{n_k} b^{-n_k}| < b^{-n_k}$$

for $k \in \mathbb{N}$, the sequence of partial sums $\sum_{k=n}^{m} x_k b^{-k}$ converges to x. Suppose only finitely many x_i are not equal to $b - 1$. Then there exists an $N \in \mathbb{N}$ with $x_k = b - 1$ for $k > N$. In the case $N \geq n$ let $x_N < b - 1$. Then it would be

$$x = \sum_{k=n}^{\infty} x_k b^{-k} = \sum_{k=n}^{N} x_k b^{-k} + \sum_{k=N+1}^{\infty} (b-1) b^{-k} = \sum_{k=n}^{N-1} x_k b^{-k} + (x_N + 1) b^{-N}$$

in contradiction to the construction of x_N.

Let also $x = \sum_{k=n'}^{\infty} x'_k b^{-k}$ with $n' \in \mathbb{Z}$ and $0 \leq x'_k \leq b - 1$. Let $m \in \mathbb{Z}$ be minimal with $x_m \neq x'_m$, wlog. $x_m > x'_m$ (where we set $x_k := 0$ and $x'_k := 0$ for $k < n$ resp. $k < n'$). Then one obtains

$$0 \leq b^{-m} - \sum_{k=m+1}^{\infty} (b-1) b^{-k} \leq \sum_{k=m}^{\infty} (x_k - x'_k) b^{-k} = x - x = 0.$$

Equality can only hold if $x_k = 0$ and $x'_k = b - 1$ for $k \geq m + 1$. But then only finitely many of the x'_k would be not equal to $b - 1$. This contradiction shows the uniqueness of the x_k.

Now let us assume that $x_{k+p} = x_k$ holds for all $k \geq n_0$. Then

$$x(b^{-p} - 1) = xb^{-p} - x = \sum_{k=n}^{\infty} x_k (b^{-k-p} - b^{-k}) = \sum_{k=n}^{n_0-1} x_k (b^{-k-p} - b^{-k}) - \sum_{k=n_0}^{n_0+p-1} x_k b^{-k} \in \mathbb{Q}.$$

This shows $x \in \mathbb{Q}$. Conversely, let $x = \frac{r}{s} \in \mathbb{Q}$ with $r, s \in \mathbb{N}$. Multiplication by a power of b causes an index shift of the sequence (x_k). We can thus assume $\gcd(s, b) = 1$ and $n \leq 0$. For $t := \varphi(s)$ it then holds $b^t \equiv 1 \pmod{s}$. Thus

$$\sum_{k=n}^{\infty}(x_{k+t} - x_k)b^{-k} = b^t \sum_{k=n}^{\infty} x_{k+t}b^{-k-t} - x = x(b^t - 1) - \sum_{k=n}^{n+t-1} x_k b^{-k+t} \in \mathbb{N}.$$

From the b-adic expansion it follows $x_{k+t} = x_k$ for $k \geq 1$, i.e., (x_k) is periodic with length $\leq t$ (cf. Theorem 4.15). □

Example 5.3.

$$\frac{1}{3} = \frac{4^{-1}}{1 - 4^{-1}} = \sum_{k=1}^{\infty} 2^{-2k} = 0{,}\overline{01}_2.$$

Definition 5.4. For $n \in \mathbb{N}$, the FAREY *sequence* $\mathcal{F}_n$ consists of the increasingly ordered reduced fractions of the form $\frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $0 \leq a \leq b \leq n$.

Example 5.5.

$$\mathcal{F}_5 = \left\{\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}\right\}.$$

Lemma 5.6. *Let $\frac{a}{b} < \frac{a'}{b'} < \frac{a''}{b''}$ be consecutive members of $\mathcal{F}_n$. Then*

(i) $\frac{a}{b} < \frac{a+a'}{b+b'} < \frac{a'}{b'}$, $b + b' > n$ *and* $b \neq b'$.

(ii) $a'b - ab' = 1$.

(iii) $\frac{a'}{b'} = \frac{a+a''}{b+b''}$.

Proof.

(i) From $ab' < a'b$ follows $a(b + b') < b(a + a')$ and $b'(a + a') < a'(b + b')$. This shows $\frac{a}{b} < \frac{a+a'}{b+b'} < \frac{a'}{b'}$. By assumption $\frac{a+a'}{b+b'} \notin \mathcal{F}_n$ and thus $b + b' > n$. In the case $b = b'$ it would be

$$\frac{a}{b} < \frac{a}{b-1} < \frac{a+1}{b} \leq \frac{a'}{b} = \frac{a'}{b'}.$$

(ii) Because of $\gcd(a, b) = 1$ there exist coprime $c, d \in \mathbb{Z}$ with $bc - ad = 1$. By replacing (c, d) with $(c + \lambda a, d + \lambda b)$ with a suitable $\lambda \in \mathbb{Z}$, one can assume $n - b < d \leq n$. It holds

$$\frac{a}{b} < \frac{a}{b} + \frac{1}{bd} = \frac{ad+1}{bd} = \frac{c}{d}.$$

In the case $\frac{c}{d} = \frac{a'}{b'}$ it follows $c = a'$ and $d = b'$ from $\gcd(c, d) = 1$. Because of $d \leq n$ we can thus assume $\frac{c}{d} > \frac{a'}{b'}$. It follows

$$\frac{c}{d} - \frac{a'}{b'} = \frac{cb' - a'd}{db'} \geq \frac{1}{db'},$$
$$\frac{a'}{b'} - \frac{a}{b} = \frac{a'b - ab'}{bb'} \geq \frac{1}{bb'}.$$

This yields the contradiction

$$\frac{1}{bd} = \frac{bc - ad}{bd} = \frac{c}{d} - \frac{a'}{b'} + \frac{a'}{b'} - \frac{a}{b} \geq \frac{1}{db'} + \frac{1}{bb'} = \frac{b+d}{bb'd} > \frac{n}{bb'd} \geq \frac{1}{bd}.$$

(iii) From (ii) follows $a'b - ab' = 1 = a''b' - a'b''$ and

$$b'(a''b - ab'') = (a'b - ab')b'' + (a''b' - a'b'')b = b + b''$$
$$a'(a''b - ab'') = (a'b - ab')a'' + (a''b' - a'b'')a = a + a''.$$

This shows the assertion. □

Remark 5.7. The proof provides a procedure for calculating the successor of $\frac{a}{b} \in \mathcal{F}_n$: Determine $c, d \in \mathbb{Z}$ with $bc - ad = 1$ and $n - b < d \leq n$. Then $\frac{c}{d}$ is the successor of $\frac{a}{b}$. Example: $\frac{3}{7} \in \mathcal{F}_{10}$. Because of $7 \cdot 1 - 3 \cdot 2 = 1 = 7 \cdot (1 + 3) - 3 \cdot (2 + 7)$ it holds $\frac{a'}{b'} = \frac{4}{9}$.

Theorem 5.8 (Dirichlet's approximation theorem)**.** *For $n \in \mathbb{N}$ and $x \in \mathbb{R}$ there exist $a, b \in \mathbb{Z}$ with $1 \leq b \leq n$ and*

$$\left|x - \frac{a}{b}\right| \leq \frac{1}{b(n+1)} \leq \frac{1}{b(b+1)} < \frac{1}{b^2}.$$

Proof. Wlog. let $0 < x < 1$. Then x lies between two consecutive members of the Farey sequence $\mathcal{F}_n$:

$$\frac{a}{b} < x \leq \frac{a'}{b'}.$$

According to Lemma 5.6, it holds that

$$\frac{a}{b} < x \leq \frac{a + a'}{b + b'} \qquad \text{or} \qquad \frac{a + a'}{b + b'} < x \leq \frac{a'}{b'}$$

with

$$\frac{a + a'}{b + b'} - \frac{a}{b} = \frac{a'b - ab'}{b(b + b')} = \frac{1}{b(b + b')} \leq \frac{1}{b(n + 1)},$$
$$\frac{a'}{b'} - \frac{a + a'}{b + b'} = \frac{a'b - ab'}{b'(b + b')} \leq \frac{1}{b'(n + 1)}.$$

□

Remark 5.9. Attention: Not for every $b \in \mathbb{N}$ does there exist an $a \in \mathbb{N}$ with $|x - \frac{a}{b}| < \frac{1}{b^2}$. For $x = \frac{1}{2}$ and $b = 3$, for example, $|\frac{1}{2} - \frac{a}{3}| \geq \frac{1}{6} > \frac{1}{9}$.

Example 5.10. If one chooses the obvious approximation $\frac{a}{b} = \frac{314}{100} = \frac{157}{50}$ for $\pi \approx 3{,}14$, one only obtains

$$\left|\pi - \frac{a}{b}\right| = 0{,}0015 > \frac{1}{1000} > \frac{1}{2550} = \frac{1}{50 \cdot 51}.$$

Better is the approximation $\frac{a}{b} = \frac{355}{113}$ with

$$\left|\pi - \frac{a}{b}\right| = 2{,}7 \cdot 10^{-7} < 10^{-5} < \frac{1}{113 \cdot 114}.$$

In the following, we construct such *convergents* systematically.

Remark 5.11. For $a \in \mathbb{Z}$ and $b \in \mathbb{N}$, the Euclidean algorithm yields sequences $q_1, q_2, \ldots, q_n = \gcd(a, b)$ and $r_1, \ldots, r_n$ with $a = q_1 b + r_1$, $b = q_2 r_1 + r_2$, $r_1 = q_2 r_2 + r_3, \ldots, r_{n-1} = q_n r_n$. This can be written in the form

$$\frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_1}} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots \cfrac{}{\frac{1}{q_n}}}}.$$

Definition 5.12. For $a_0 \in \mathbb{R}$ and $a_1, \ldots \in \mathbb{R} \setminus \{0\}$, we define $[a_0] := a_0$ and $[a_0, \ldots, a_n] := [a_0, \ldots, a_{n-2}, a_{n-1} + \frac{1}{a_n}]$ for $n \geq 1$. Thus, it holds that

$$[a_0, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{}{\ddots \; \cfrac{}{\frac{1}{a_n}}}}}.$$

In the case $a_0 \in \mathbb{Z}$ and $a_1, \ldots \in \mathbb{N}$, one calls $[a_0, \ldots, a_n]$ a *continued fraction*.

Theorem 5.13. *Every $x \in \mathbb{Q}$ can be represented in exactly one way as a continued fraction $x = [a_0, \ldots, a_n]$, where $a_n \geq 2$ if $n \geq 1$.*

Proof. Let $x = \frac{a}{b}$ with $\gcd(a, b) = 1$. From Remark 5.11, one obtains natural numbers $q_1, \ldots, q_n = 1$ with $x = [q_1, \ldots, q_n]$. In the case $n \geq 1$, $x = [q_1, \ldots, q_{n-1} + 1]$ with $q_{n-1} + 1 \geq 2$ is also possible. For uniqueness, let $x = [a_0, \ldots, a_n] = [b_0, \ldots, b_m]$. For $n = 0$, $x = a_0 \in \mathbb{Z}$. Then $m = 0$ and $a_0 = b_0$ as well, because otherwise $0 < x - b_0 < 1$ due to $b_m > 1$. Now let $n, m \geq 1$. Because $0 \leq x - a_0 < 1$ and $0 \leq x - b_0 < 1$, it follows that $a_0 = b_0$. From $[a_1, \ldots, a_n] = \frac{1}{x - a_0} = [b_1, \ldots, b_m]$, it follows inductively that $n = m$ and $a_i = b_i$ for $i = 0, \ldots, n$. □

Example 5.14.

(i)
$$\frac{19}{7} = 2 + \frac{1}{\frac{7}{5}} = 2 + \cfrac{1}{1 + \cfrac{1}{\frac{5}{2}}} = \ldots = [2, 1, 2, 2].$$

(ii) The orbital period of the Earth around the Sun is approximately 365,24219 days. This corresponds to the continued fraction $[365, 4, 7, 1, 3, 24, 6, 2, 2]$. The convergent $[365, 4] = 265 + \frac{1}{4}$ leads to the leap year rule of the Julian calendar (one additional day every 4 years). The approximation

$$[365, 4, 7, 1, 3] = 365 + \frac{31}{128}$$

provides a more precise rule: 31 leap days every 128 years. The currently valid rule of the Gregorian calendar (97 leap days every 400 years) is less precise, but easier to remember.

Lemma 5.15. *Let $a_0 \in \mathbb{R}$, $a_1, \ldots \in \mathbb{R} \setminus \{0\}$ and*

$$\begin{aligned}(p_0, q_0) &:= (a_0, 1),\\ (p_1, q_1) &:= (a_0 a_1 + 1,\ a_1),\\ (p_k, q_k) &:= (a_k p_{k-1} + p_{k-2},\ a_k q_{k-1} + q_{k-2})\end{aligned}$$

for $k \geq 2$. Then $[a_0, \ldots, a_k] = \frac{p_k}{q_k}$ holds for $k = 0, \ldots, n$.

Proof. Induction on k: For $k = 0, 1$ the assertion holds, because $\frac{p_1}{q_1} = \frac{a_0 a_1 + 1}{a_1} = a_0 + \frac{1}{a_1} = [a_0, a_1]$. For $k \geq 2$ we have

$$[a_0, \ldots, a_{k+1}] = \left[a_0, \ldots, a_k + \frac{1}{a_{k+1}}\right] = \frac{(a_k + \frac{1}{a_{k+1}})p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}})q_{k-1} + q_{k-2}}$$
$$= \frac{p_k + \frac{1}{a_{k+1}}p_{k-1}}{q_k + \frac{1}{a_{k+1}}q_{k-1}} = \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}. \qquad \square$$

Example 5.16. We calculate the continued fraction $[1, 1, \ldots, 1]$ using Lemma 5.15:

a_k	1	1	1	1	1	$\cdots$
p_k	1	2	3	5	8	$\cdots$
q_k	1	1	2	3	5	$\cdots$

Here $p_k = q_{k+1}$ are the terms of the well-known FIBONACCI *sequence* (Exercise 3).

Corollary 5.17. *Let $[a_0, \ldots, a_n]$ be a continued fraction. With the notation from Lemma 5.15, the following hold:*

(i) $1 \leq q_1 < q_2 < \ldots$ *and* $q_k \geq k$ *for* $k \in \mathbb{N}$.

(ii) $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k+1}$ *and*

$$\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k+1}}{q_k q_{k-1}}$$

for $k = 1, \ldots, n$. *In particular,* $\gcd(p_k, q_k) = 1$ *for* $k \geq 0$.

(iii) $p_k q_{k-2} - p_{k-2} q_k = (-1)^k a_k$ *and*

$$\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{(-1)^k a_k}{q_k q_{k-2}}$$

for $k = 2, \ldots, n$.

Proof.

(i) By definition $q_0 = 1$, $q_1 = a_1 \geq 1$ and inductively $q_k = a_k q_{k-1} + q_{k-2} \geq q_{k-1} + q_{k-2} > q_{k-1} \geq k - 1$.

(ii) One can interpret the definition of p_k and q_k as a matrix equation:

$$\begin{pmatrix} p_1 & p_0 \\ q_1 & q_0 \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix},$$
$$\begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} = \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix}.$$

Then it holds that

$$P_k := \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} = \prod_{i=0}^{k} \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix}$$

and $p_k q_{k-1} - p_{k-1} q_k = \det P_k = (-1)^{k+1}$. The second equation follows after division by $q_{k-1} q_k$. Furthermore, it follows that $\gcd(p_k, q_k) = 1$ for $k \geq 0$.

(iii) It holds that

$$p_k q_{k-2} - p_{k-2} q_k = \det \begin{pmatrix} p_k & p_{k-2} \\ q_k & q_{k-2} \end{pmatrix} = \det \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} \det \begin{pmatrix} a_k & 0 \\ 1 & 1 \end{pmatrix} = (-1)^k a_k. \qquad \square$$

Lemma 5.18. *Let $a_0 \in \mathbb{Z}$ and $a_1, \ldots \in \mathbb{N}$. For $k \in \mathbb{N}_0$ let $\alpha_k := [a_0, \ldots, a_k]$. Then it holds that*

$$\alpha_0 < \alpha_2 < \ldots < \alpha_{2k} < \alpha_{2k-1} < \alpha_{2k-3} < \ldots < \alpha_1.$$

In particular, the limit $[a_0, \ldots] := \lim_{k\to\infty} \alpha_k$ exists.

Proof. According to Corollary 5.17, $\alpha_{2k} - \alpha_{2k-2} = \frac{a_{2k}}{q_{2k} q_{2k-2}} > 0$ and analogously $\alpha_{2k-1} - \alpha_{2k} < 0$ as well as $\alpha_{2k-1} - \alpha_{2k-3} < 0$. For $k < l$ it holds that $\alpha_{2k} < \alpha_{2l} < \alpha_{2l-1} \leq \alpha_{2k+1} < \alpha_{2k-1}$. This shows

$$|\alpha_l - \alpha_k| \leq |\alpha_{k+1} - \alpha_k| \leq \frac{1}{q_{k+1} q_k} < \frac{1}{k^2} \xrightarrow{k\to\infty} 0.$$

Thus $(\alpha_k)_k$ is a Cauchy sequence that converges in the complete space $\mathbb{R}$. $\square$

Remark 5.19. In the situation of Lemma 5.18, $\alpha = [a_0, \ldots]$ is called an (infinite) *continued fraction* and α_k is called the k-th *convergent* of α.

Theorem 5.20. *For all $x \in \mathbb{R} \setminus \mathbb{Q}$ there exist uniquely determined numbers $a_0 \in \mathbb{Z}$ and $a_1, \ldots \in \mathbb{N}$ with $x = [a_0, \ldots]$.*

Proof. Because of $x \notin \mathbb{Q}$, there exist $a_k \in \mathbb{Z}$ and $0 < \epsilon_k < 1$ with $x = a_0 + \epsilon_0$ and $\epsilon_{k-1}^{-1} = a_k + \epsilon_k$ for $k \geq 1$. Because of $\epsilon_{k-1}^{-1} > 1$, it follows that $a_k \in \mathbb{N}$ for $k \geq 1$. Furthermore,

$$x = a_0 + \epsilon_0 = [a_0, \epsilon_0^{-1}] = [a_0, a_1 + \epsilon_1] = [a_0, a_1, \epsilon_1^{-1}] = \ldots = [a_0, \ldots, a_k, \epsilon_k^{-1}].$$

for $k \geq 1$. From Lemma 5.15 it follows that

$$\begin{aligned} |x - [a_0, \ldots, a_k]| &= \Big| \frac{\epsilon_k^{-1} p_k + p_{k-1}}{\epsilon_k^{-1} q_k + q_{k-1}} - \frac{p_k}{q_k} \Big| = \Big| \frac{(\epsilon_k^{-1} p_k + p_{k-1}) q_k - p_k (\epsilon_k^{-1} q_k + q_{k-1})}{(\epsilon_k^{-1} q_k + q_{k-1}) q_k} \Big| \\ &= \Big| \frac{p_{k-1} q_k - p_k q_{k-1}}{(\epsilon_k^{-1} q_k + q_{k-1}) q_k} \Big| \overset{5.17}{<} \frac{1}{q_k^2} \leq \frac{1}{k^2}. \end{aligned}$$

This shows $x = [a_0, \ldots]$. Let $x = [b_0, \ldots]$ also be a continued fraction. Then $x = b_0 + \tau_0$ with $\tau_0 = [b_1, \ldots]^{-1}$. From $0 < \tau_0 < 1$ it follows that $\tau_0 = \epsilon_0$ and $a_0 = b_0$. Now $[a_1, \ldots] = \epsilon_0^{-1} = \tau_0^{-1} = [b_1, \ldots]$ holds and one obtains $a_1 = b_1$ etc. $\square$

Example 5.21.

(i) For $\pi = 3{,}1415926\ldots$, the algorithm from the proof of Theorem 5.20 yields:

$$\begin{aligned} a_0 &= 3, & \epsilon_0^{-1} &= 7{,}0625, \\ a_1 &= 7, & \epsilon_1^{-1} &= 15{,}9965\ldots, \\ a_2 &= 15, & \epsilon_2^{-1} &= 1{,}0034\ldots, \\ a_3 &= 1, & \epsilon_3^{-1} &= 292{,}6345\ldots. \end{aligned}$$

Thus $\pi = [3, 7, 15, 1, 292, \ldots]$ (due to rounding errors, more decimal places than those given are required). Due to the high value 292, one obtains a particularly good convergent through $[3, 7, 15, 1] = \frac{355}{113} \approx 3{,}1415929$.

(ii) For Euler's number e, the continued fraction exhibits an obvious pattern:

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, \ldots]$$

(without proof). For π, there is at least one regular "continued fraction" of a different kind:

$$\pi = 3 + \cfrac{1^2}{6 + \cfrac{3^2}{6 + \cfrac{5^2}{6 + \ldots}}}$$

(found by Lange, 1999).

(iii) For the *golden ratio* $\varphi = \frac{1+\sqrt{5}}{2}$, it holds that $\varphi = 1 + \frac{1}{\varphi} = [1, \varphi] = [1, 1, \ldots] = [\bar{1}]$. The convergents are formed from the Fibonacci numbers $\frac{f_{n+1}}{f_n}$ (Example 5.16).

(iv) The next theorem improves Dirichlet's approximation theorem.

Theorem 5.22 (Hurwitz)**.** *Let $x \in \mathbb{R}$ and $n \in \mathbb{N}$. Then there exists $\frac{p}{q} \in \mathbb{Q}$ with $q \geq n$ and*

$$\left| x - \frac{p}{q} \right| < \frac{1}{\sqrt{5} q^2}.$$

Proof. Wlog. let $x > 0$ (otherwise consider $x + m > 0$ for an $m \in \mathbb{N}$). In the case $x \in \mathbb{Q}$, one can choose $\frac{p}{q} = x$ and guarantee $q \geq n$ by expanding. So let $x = [a_0, \ldots]$ be irrational with convergents $\alpha_k = \frac{p_k}{q_k}$. Wlog. let $n \geq 5$ be odd. According to Lemma 5.15 and Lemma 5.18, it holds that $n \leq q_{n-1} \leq q_n \leq q_{n+1}$ and $\alpha_{n-1} < \alpha_{n+1} < x < \alpha_n$. Assume indirectly that $|x - \alpha_k| > \frac{1}{\sqrt{5} q_k^2}$ for $k = n - 1, n, n + 1$. Then

$$\frac{1}{q_k q_{k+1}} = |\alpha_{k+1} - \alpha_k| > \frac{1}{\sqrt{5} q_k^2} + \frac{1}{\sqrt{5} q_{k+1}^2}$$

holds for $k = n - 1, n$ according to Corollary 5.17. Multiplication by $\sqrt{5} q_{k+1}^2$ yields

$$\left(\frac{q_{k+1}}{q_k} \right)^2 - \sqrt{5} \frac{q_{k+1}}{q_k} + 1 < 0.$$

The roots of $X^2 - \sqrt{5} X + 1$ are $(\sqrt{5} - 1)/2$ and the golden ratio $\varphi = (\sqrt{5} + 1)/2$. In particular, $\frac{q_{k+1}}{q_k} < \varphi$ holds for $k = n - 1, n$. With Lemma 5.15, one obtains the contradiction

$$\frac{q_{n+1}}{q_n} \geq \frac{q_n + q_{n-1}}{q_n} = 1 + \frac{q_{n-1}}{q_n} > 1 + \varphi^{-1} = \varphi. \qquad \square$$

Example 5.23. The estimate of Hurwitz is optimal in two respects:

(i) Let $\varphi = (\sqrt{5} + 1)/2$ and $c > \sqrt{5}$. Suppose there are infinitely many $\frac{p}{q} \in \mathbb{Q}$ with $\gcd(p, q) = 1$ and

$$\left| \varphi - \frac{p}{q} \right| < \frac{1}{c q^2}.$$

Let $\varphi = \frac{p}{q} + \frac{\epsilon}{q^2}$ with $|\epsilon| < 1/c$. Then it follows that

$$\frac{\epsilon^2}{q^2} - \epsilon \sqrt{5} = \left(\frac{\epsilon}{q} - \frac{1}{2} q \sqrt{5} \right)^2 - \frac{5}{4} q^2 = \left(\frac{1}{2} q - p \right)^2 - \frac{5}{4} q^2 = p^2 - pq - q^2.$$

For large q, the left side lies strictly between -1 and 1. Since the right side is an integer, it follows that $p^2 - pq - q^2 = 0$. But then $p \mid q$ would hold, in contradiction to $\gcd(p, q) = 1$. Therefore, the constant $\sqrt{5}$ cannot be improved in general. One also obtains that φ can be approximated particularly "badly" by rational numbers.

(ii) Let $x \in \mathbb{R}$ be a root of a non-constant integer polynomial (e. g. $x = \sqrt{2}$). The THUE-SIEGEL-ROTH theorem states that for every $\epsilon > 0$, there exist only finitely many $\frac{p}{q} \in \mathbb{Q}$ with

$$\left| x - \frac{p}{q} \right| < \frac{1}{q^{2+\epsilon}}.$$

Corollary 5.24. *For every number $a \in \mathbb{N}$, there exists a power of 2 that begins with the digits of a.*

Proof. We are looking for $n, k \in \mathbb{N}$ with $a \cdot 10^k \leq 2^n < (a+1)10^k$, i. e.

$$\log_{10}(a) \leq n \log_{10}(2) - k < \log_{10}(a+1). \tag{5.1}$$

According to Exercise 9, $\log_{10}(2)$ is irrational. According to Theorem 5.22, there exist $p, q \in \mathbb{N}$ with $\frac{1}{q} < \log_{10}(a+1) - \log_{10}(a)$ and $0 < \log_{10}(2) - \frac{p}{q} < \frac{1}{q^2}$ (since the distance from p/q to the following convergent is smaller than $1/q^2$, one can assume $p/q < \log_{10}(2)$). It follows that

$$0 < q \log_{10}(2) - p < \frac{1}{q} < \log_{10}(a+1) - \log_{10}(a).$$

Now there exists an $s \in \mathbb{N}$ with $\log_{10}(a) < s(q \log_{10}(2) - p) < \log_{10}(a+1)$. Thus (5.1) holds for $n := sq$ and $k := sp$. □

Example 5.25. Which power of 2 begins with $a = 7$? The first two convergents for $\log_{10}(2) \approx 0{,}30$ are $\frac{1}{3}$ and $\frac{3}{10}$. It holds that

$$0 < 10 \log_{10}(2) - 3 < \log_{10}(8) - \log_{10}(7) \approx 0{,}058.$$

In the proof above, one can choose $s = 83$ and obtains 2^{830}. However, 2^{46} already begins with a 7.

Remark 5.26. Let $q \in \mathbb{Q}$ with $\sqrt{q} \notin \mathbb{Q}$. Then $\mathbb{Q}(\sqrt{q}) := \mathbb{Q} + \mathbb{Q}\sqrt{q}$ is a 2-dimensional $\mathbb{Q}$-vector space with basis $1, \sqrt{q}$. Because of

$$(a_1 + b_1\sqrt{q})(a_2 + b_2\sqrt{q}) = (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{q} \in \mathbb{Q}(\sqrt{q})$$

$\mathbb{Q}(\sqrt{q})$ is closed under multiplication. For $x := a + b\sqrt{d} \in \mathbb{Q}(\sqrt{q})$ let $x^* := a - b\sqrt{q}$ (in the case $q < 0$, $x^* = \bar{x}$ is the complex conjugate of x). It holds that $xx^* = a^2 - b^2q \in \mathbb{Q}$. From the unique prime factorization, it follows easily that $xx^* \neq 0$ for $x \neq 0$. If necessary, $x^{-1} = \frac{x^*}{xx^*} \in \mathbb{Q}(\sqrt{q})$. This shows that $\mathbb{Q}(\sqrt{q})$ is a field. As with complex conjugation, it holds that

$$(x \dot{+} y)^* = x^* \dot{+} y^*$$

for $x, y \in \mathbb{Q}(\sqrt{q})$.

Theorem 5.27 (EULER-LAGRANGE)**.** *Let $x = [a_0, \ldots] \in \mathbb{R} \setminus \mathbb{Q}$ be as in Theorem 5.20. x is the solution of a quadratic equation with coefficients in $\mathbb{Q}$ if and only if the sequence $a_0, \ldots$ becomes periodic.*

Proof. First, let $x = [\overline{a_0, \ldots, a_n}]$ be a *purely* periodic continued fraction. Then $x = [\overline{a_0, \ldots, a_n}, x]$ holds and with Corollary 5.17 it follows that $x = \frac{xp_k + p_{k-1}}{xq_k + q_{k-1}}$ with $p_k, p_{k-1}, q_k, q_{k-1} \in \mathbb{N}$. By rearranging, one obtains a quadratic equation in x. Now let $x = [a_0, \ldots, a_n, \overline{b_1, \ldots, b_m}]$ and $y := [\overline{b_1, \ldots, b_m}]$. Then $x = [a_0, \ldots, a_n, y]$ and $x = \frac{yp_k + p_{k-1}}{yq_k + q_{k-1}}$ with $p_k, p_{k-1}, q_k, q_{k-1} \in \mathbb{N}$. According to the first part, y is a solution of a quadratic equation, say $y = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$ and $d \in \mathbb{N}$ (p-q-formula). According to Remark 5.26, it follows that $x \in \mathbb{Q}(\sqrt{d})$ and there exist $a', b' \in \mathbb{Q}$ with $x = a' + b'\sqrt{d}$. Thus x is a solution of a quadratic equation.

Conversely, let x be a solution of a quadratic equation. Then there exist $a, b \in \mathbb{Z}$ and $d \in \mathbb{N}$ with $x = \frac{a+\sqrt{d}}{b} = \frac{ab+\sqrt{db^2}}{b^2}$. By replacing (a, b, d) with $(ab, b^2, b^2 d)$, we can assume $b \mid d - a^2$. Define

$$k_0 := a, \quad m_0 := b, \quad \alpha_i := \frac{k_i + \sqrt{d}}{m_i}, \quad a_i := \lfloor \alpha_i \rfloor, \quad k_{i+1} := a_i m_i - k_i, \quad m_{i+1} := \frac{d - k_{i+1}^2}{m_i} \quad (i \geq 0).$$

Because of $m_0 = b \mid d - a^2 = d - k_0^2$ and

$$d - k_{i+1}^2 = d - a_i m_i^2 + 2a_i m_i k_i - k_i^2 = m_i(m_{i-1} - a_i m_i + 2a_i k_i)$$

$m_i \in \mathbb{Z}$ for $i \in \mathbb{N}_0$. Because of $x \notin \mathbb{Q}$, d is not a square number and $m_i \neq 0$. From $0 < \alpha_0 - a_0 < 1$ and

$$\alpha_{i+1} = \frac{k_{i+1} + \sqrt{d}}{m_{i+1}} = \frac{m_i(k_{i+1} + \sqrt{d})}{d - k_{i+1}^2} = \frac{m_i}{\sqrt{d} - k_{i+1}} = \frac{m_i}{\sqrt{d} - a_i m_i + k_i} = \frac{1}{\alpha_i - a_i} > 1$$

it follows inductively that $a_i \geq 1$ for $i \geq 1$. This shows

$$x = \alpha_0 = a_0 + \frac{1}{\alpha_1} = \ldots = [a_0, \ldots].$$

With the usual notation, it holds that

$$x = \frac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}}, \qquad x^* \overset{5.26}{=} \frac{\alpha_k^* p_{k-1} + p_{k-2}}{\alpha_k^* q_{k-1} + q_{k-2}}$$

for all $k \geq 2$. As before, one calculates with Lemma 5.15

$$\begin{aligned} \alpha_k^* q_{k-1}\Big(x^* - \frac{p_{k-1}}{q_{k-1}}\Big) &= \alpha_k^* \frac{q_{k-1}(\alpha_k^* p_{k-1} + p_{k-2}) - p_{k-1}(\alpha_k^* q_{k-1} + q_{k-2})}{\alpha_k^* q_{k-1} + q_{k-2}} = \frac{-\alpha_k^*(-1)^k}{\alpha_k^* q_{k-1} + q_{k-2}} \\ &= \frac{-(\alpha_k^* p_{k-1} + p_{k-2})q_{k-2} + p_{k-2}(\alpha_k^* q_{k-1} + q_{k-2})}{\alpha_k^* q_{k-1} + q_{k-2}} = -q_{k-2}\Big(x^* - \frac{p_{k-2}}{q_{k-2}}\Big). \end{aligned}$$

Because of $q_k > 0$ and $\lim_{k\to\infty} \frac{p_k}{q_k} = x \neq x'$, an $N \in \mathbb{N}$ with $\alpha_i^* < 0$ for all $i \geq N$ must exist. Then $\frac{2\sqrt{d}}{m_i} = \alpha_i - \alpha_i^* > 0$ and $m_i > 0$. Because of $m_i m_{i-1} = d - k_{i+1}^2$, it follows that $0 < m_i < d$ and $k_{i+1}^2 < d$ for all $i \geq N$. In particular, the numbers $m_0, m_1, \ldots$ and $k_0, k_1 \ldots$ can only take finitely many values. Therefore, there exist $s < t$ with $\alpha_s = \alpha_t$. Then

$$x = [a_0, \ldots, a_{s-1}, \alpha_t] = [a_0, \ldots, a_{t-1}, \alpha_t] = [a_0, \ldots, a_{s-1}, \overline{a_s, \ldots, a_{t-1}}]. \qquad \square$$

Theorem 5.28. *$x \in \mathbb{R} \setminus \mathbb{Q}$ is the root of a rational number > 1 if and only if the continued fraction has the form*

$$x = [a_0, \overline{a_1, \ldots, a_d, 2a_0}] = [a_0, \overline{a_d, a_{d-1}, \ldots, a_1, 2a_0}].$$

Proof.

$\Rightarrow$: Let $r \in \mathbb{Q}$, $r > 1$, $\sqrt{r} = a_0 + \epsilon_0$ and $\epsilon_{k-1}^{-1} = a_k + \epsilon_k$ with $0 < \epsilon_k < 1$ as in the proof of Theorem 5.20. By Remark 6.12, it holds that $-\sqrt{r} = a_0 + \epsilon_0^*$ and $(\epsilon_{k-1}^*)^{-1} = a_k + \epsilon_k^*$. Because $\epsilon_0^* = -a_0 - \sqrt{r} < -1$, we have $-1 < (\epsilon_0^*)^{-1} < 0$. Let $-1 < (\epsilon_{k-1}^*)^{-1} < 0$ be already shown by induction. Then $\epsilon_k^* = (\epsilon_{k-1}^*)^{-1} - a_k < -1$ and $-1 < (\epsilon_k^*)^{-1} < 0$. This shows $a_k = (\epsilon_{k-1}^*)^{-1} - \epsilon_k^* = \lfloor -\epsilon_k^* \rfloor$ for $k \geq 1$.

According to Theorem 5.27, $\sqrt{r} = [a_0, \ldots, a_k, \epsilon_k^{-1}]$ is periodic, say $\epsilon_k = \epsilon_l$ with $k < l$. In the case $k > 1$, we have $a_k = \lfloor -\epsilon_k^* \rfloor = \lfloor -\epsilon_l^* \rfloor = a_l$ and $\epsilon_{k-1} = \epsilon_{l-1}$. Inductively, one obtains $\epsilon_1 = \epsilon_s$, i. e. $\sqrt{r} = [a_0, \overline{a_1, \ldots, a_s}]$ with $s := l - k + 1$. Because $\epsilon_0^{-1} = [\overline{a_1, \ldots, a_s}] = [a_1, \ldots, a_s, \epsilon_0^{-1}]$, it holds that

$$\epsilon_0^{-1} = \frac{\epsilon_0^{-1} p_s + p_{s-1}}{\epsilon_0^{-1} q_s + q_{s-1}} = \frac{p_s + p_{s-1}\epsilon_0}{q_s + q_{s-1}\epsilon_0} \tag{5.2}$$

with the usual notation. Let $\sigma := [\overline{a_s, a_{s-1}, \ldots, a_1}]$. As in the proof of Corollary 5.17, let

$$P_s := \begin{pmatrix} p_s & p_{s-1} \\ q_s & q_{s-1} \end{pmatrix} = \prod_{i=1}^{s} \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix}$$

Then

$$\begin{pmatrix} p_s & q_s \\ p_{s-1} & q_{s-1} \end{pmatrix} = P_s^{\mathrm{t}} = \prod_{i=0}^{s-1} \begin{pmatrix} a_{s-i} & 1 \\ 1 & 0 \end{pmatrix}$$

and

$$\sigma = \frac{\sigma p_s + q_s}{\sigma p_{s-1} + q_{s-1}}.$$

From this, one obtains quadratic equations with the same coefficients:

$$\begin{aligned} p_{s-1}\epsilon_0^2 + (p_s - q_{s-1})\epsilon_0 - q_s &= \epsilon_0(p_s + p_{s-1}\epsilon_0) - (q_s + q_{s-1}\epsilon_0) \overset{(5.2)}{=} 0, \\ p_{s-1}(-\sigma)^2 + (p_s - q_{s-1})(-\sigma) - q_s &= \sigma(\sigma p_{s-1} + q_{s-1}) - (\sigma p_s + q_s) = 0. \end{aligned}$$

Along with ϵ_0, $\epsilon_0^* \neq \epsilon_0$ is also a solution of this equation by Remark 5.26. Because $\sigma > 0 > -\epsilon_0$, it therefore holds that

$$[\overline{a_s, \ldots, a_1}] = \sigma = -\epsilon_0^* = a_0 + \sqrt{r} = 2a_0 + \epsilon_0 = [2a_0, \overline{a_1, \ldots, a_s}].$$

Thus $a_s = 2a_0$ and $a_i = a_{s-i}$ for $i = 1, \ldots, s-1$.

$\Leftarrow$: Let x be as specified. By Theorem 5.27, there exist $s, t \in \mathbb{Q}$ with $x = s + \sqrt{t}$. With the notation from above, $\epsilon_0^{-1} = [\overline{a_1, \ldots, a_d, 2a_0}]$ and

$$-\epsilon_0^* = \sigma = [\overline{2a_0, a_d, \ldots, a_1}] = [2a_0, \epsilon_0^{-1}] = 2a_0 + \epsilon_0.$$

This shows

$$s - \sqrt{t} = x^* = a_0 + \epsilon_0^* = -a_0 - \epsilon_0 = -x = -s - \sqrt{t}$$

and $s = 0$. Because $2a_0 = a_{d+1} \geq 1$, we have $t > 1$. □

Remark 5.29. If $0 < x = [a_0, \ldots] < 1$, then $x^{-1} = [0, a_0, a_1, \ldots] >$. If $x = \sqrt{r}$ for some $r \in \mathbb{Q}$, then one can apply Theorem 5.28 to x^{-1} and thus also obtains the continued fraction for x.

Example 5.30. Let $n = d^2 + 1$ with $d \in \mathbb{N}$. Then

$$\sqrt{n} = d + \frac{1}{\sqrt{n} + d} = d + \frac{1}{2d + \frac{1}{\sqrt{n}+d}} = [d, \overline{2d}].$$

Specifically, $\sqrt{2} = [1, \overline{2}]$, $1 + \sqrt{2} = [\overline{2}]$ and $\sqrt{5} = [2, \overline{4}]$. On the other hand, $\sqrt{14} = [3, \overline{1, 2, 1, 6}]$.

Theorem 5.31 (Pell's Equation)**.** *Let $n \in \mathbb{N}$ not be a square number and $P := \{(p, q) \in \mathbb{N}^2 : p^2 - nq^2 = 1\}$. Then $P \neq \varnothing$. If $(p_1, q_1) \in P$ with p_1 as small as possible, then*

$$P = \left\{(p, q) \in \mathbb{N}^2 : \exists k \in \mathbb{N} : p + \sqrt{n}q = (p_1 + \sqrt{n}q_1)^k\right\}.$$

Proof. Let $\sqrt{n} = [a_0, \overline{a_1, \ldots, a_d}]$ be the continued fraction from Theorem 5.28 (the structure of the period is not required). Let e be an even multiple of d. For $\beta := (\sqrt{n} - a_0)^{-1} = [\overline{a_1, \ldots, a_e}]$, it holds that $\sqrt{n} = [a_0, a_1, \ldots, a_e, \beta]$. From Lemma 5.15 it follows that

$$\sqrt{n} = \frac{\beta p_e + p_{e-1}}{\beta q_e + q_{e-1}} = \frac{p_e + p_{e-1}(\sqrt{n} - a_0)}{q_e + q_{e-1}(\sqrt{n} - a_0)}.$$

Multiplying by the denominator yields

$$nq_{e-1} + (q_e - q_{e-1}a_0)\sqrt{n} = p_e - p_{e-1}a_0 + p_{e-1}\sqrt{n}.$$

Since $\sqrt{n}$ is irrational, 1 and $\sqrt{n}$ are linearly independent over $\mathbb{Q}$. One can therefore compare coefficients:

$$nq_{e-1} = p_e - p_{e-1}a_0, \qquad q_e - q_{e-1}a_0 = p_{e-1}.$$

This shows

$$p_{e-1}^2 - nq_{e-1}^2 = (q_e - q_{e-1}a_0)p_{e-1} - (p_e - p_{e-1}a_0)q_{e-1} = p_{e-1}q_e - p_e q_{e-1} \overset{5.17}{=} (-1)^e = 1,$$

i. e. $(p_{e-1}, q_{e-1}) \in P$. Now let $(p_1, q_1) \in P$ with p_1 minimal. Let $k, s, t \in \mathbb{N}$ with

$$(p_1 + \sqrt{n}q_1)^k = s + \sqrt{n}t.$$

Then it also holds that

$$s^2 - nt^2 = (s + \sqrt{n}t)(s + \sqrt{n}t)^* = (p_1 + \sqrt{n}q_1)^k((p_1 + \sqrt{n}q_1)^*)^k = (p_1^2 - nq_1^2)^k = 1^k = 1,$$

i. e. $(s, t) \in P$. Assume there exists a solution $(p, q) \in \mathbb{N}^2$ with $p + \sqrt{n}q \neq (p_1 + \sqrt{n}q_1)^k$ for all $k \in \mathbb{N}$. Then there exists a $k \in \mathbb{N}$ with $(p_1 + \sqrt{n}q_1)^k < p + \sqrt{n}q < (p_1 + \sqrt{n}q_1)^{k+1}$. It follows that

$$1 = (p_1 + \sqrt{n}q_1)^k(p_1 - \sqrt{n}q_1)^k < (p + \sqrt{n}q)(p_1 - \sqrt{n}q_1)^k < p_1 + \sqrt{n}q_1.$$

There exist $s, t \in \mathbb{Z}$ with $(p + \sqrt{n}q)(p_1 - \sqrt{n}q_1)^k = s + \sqrt{n}t$. As above, $s^2 - nt^2 = 1$. In the case $t < 0$, then $0 < (s + \sqrt{n}t)^{-1} = s - \sqrt{n}t < 1$ and $s < 0$. But then $s + \sqrt{n}t < 0$. Thus $t > 0$. In the case $s < 0$, then $-s + \sqrt{n}t = -(s + \sqrt{n}t)^{-1} < 0$ with $-s, t > 0$. Thus $s, t \in \mathbb{N}$ and $(s, t) \in P$. This contradicts the minimality of p_1. This proves the second assertion. □

Remark 5.32. As in the proof, let d be the period length of the continued fraction of $\sqrt{n}$ and $e = \operatorname{lcm}(2, d)$. One can show that the pair $(p, q) \in P$ with minimal p is given by (p_{e-1}, q_{e-1}). All further pairs in P also appear as convergents (without proof).

Example 5.33.

(i) The longer the period of the continued fraction for $\sqrt{n}$ is, the larger the pairs (p, q) with $p^2 - nq^2 = 1$ become. For $\sqrt{2} = [1, \overline{2}]$, every second convergent works, so

$$(p, q) \in \{(3, 2), (17, 12), (99, 70), \ldots\}.$$

For $\sqrt{61} = [7, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14]$, the smallest solution is

$$(p, q) = (1766319049, 226153980).$$

(ii) (HERON method) For $n \in \mathbb{N}$, $\sqrt{n}$ is the side length of a square Q with area n. We approximate Q by rectangles with area n. In the first step, one chooses the side lengths $x_1 := 1$ and $y_1 := n$. If the side lengths $x_k < y_k$ are already determined, one obtains a better side length through the mean value $x_{k+1} := \frac{x_k + y_k}{2}$. The other side length must be $y_{k+1} := \frac{n}{x_{k+1}}$. For $n = 2$, one obtains some of the convergents for $\sqrt{2}$:

$$x_i = 1, \frac{3}{2}, \frac{12}{17}, \frac{577}{408}.$$

This method results from the NEWTON method for finding roots of $f(x) = x^2 - n$.

6 Quadratic Number Fields

Remark 6.1.

(i) We will extend the unique prime factorization of $\mathbb{Z}$ to certain subrings R of $\mathbb{C}$. As with residue class rings, let $R^\times$ always be the set of invertible elements of R.

(ii) For $d \in \mathbb{Q}$ with $\sqrt{d} \notin \mathbb{Q}$, we introduced the field $\mathbb{Q}(\sqrt{d})$ in Remark 5.26. Let $d = \frac{r}{s}$ with $r, s \in \mathbb{Z}$. Then $\sqrt{d} = \frac{\sqrt{rs}}{s}$ and $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{rs})$. Thus, one can always assume $d \in \mathbb{Z}$. Because of $\sqrt{de^2} = \sqrt{d}e$, one can furthermore assume that d is square-free, i.e., d is not divisible by the square of a prime number. One calls $\mathbb{Q}(\sqrt{d})$ a *quadratic number field*. In the case $d > 0$ or $d < 0$, one speaks of *real quadratic* or *imaginary quadratic* number fields.

Definition 6.2. For $d \in \mathbb{Z}$ square-free, let

$$\begin{aligned} S &\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}, \qquad a + b\sqrt{d} \mapsto 2a, \\ N &\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}, \qquad a + b\sqrt{d} \mapsto a^2 - b^2 d \end{aligned}$$

be the *trace* or *norm*.

Remark 6.3.

(i) In the case $d < 0$, $N(x) = x\bar{x} = |x|^2$ for $x \in \mathbb{Q}(\sqrt{d})$.

(ii) For $x = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, it holds that

$$x^2 - S(x)x + N(x) = a^2 + b^2 d + 2ab\sqrt{d} - 2a(a + b\sqrt{d}) + a^2 - b^2 d = 0.$$

Lemma 6.4. *In every quadratic number field $\mathbb{Q}(\sqrt{d})$, $S(x+y) = S(x) + S(y)$ and $N(xy) = N(x)N(y)$ hold for $x, y \in \mathbb{Q}(\sqrt{d})$.*

Proof. The equation $S(x+y) = S(x) + S(y)$ is trivial. Furthermore, $N(xy) = xy(xy)^* = xyx^*y^* = xx^*yy^* = N(x)N(y)$ according to Remark 5.26. □

Definition 6.5. One calls $x \in \mathbb{Q}(\sqrt{d})$ *algebraic integer*, if $S(x), N(x) \in \mathbb{Z}$ holds. Let $\mathbb{Z}_d$ be the set of algebraic integers in $\mathbb{Q}(\sqrt{d})$.

Remark 6.6. According to Remark 6.3, an algebraic integer x is a root of the monic integer polynomial $X^2 - S(x)x + N(x)$.

Theorem 6.7. *For $d \in \mathbb{Z} \setminus \{0,1\}$ square-free, it holds that*

$$\mathbb{Z}_d = \begin{cases} \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4, \\ \mathbb{Z} + \mathbb{Z}\sqrt{d} & \text{otherwise.} \end{cases}$$

In particular, $\mathbb{Z}_d$ is a ring.

Proof. First, obviously $\mathbb{Z} + \mathbb{Z}\sqrt{d} \subseteq \mathbb{Z}_d$ holds. Conversely, let $x = a + b\sqrt{d} \in \mathbb{Z}_d$. From $S(x) = 2a \in \mathbb{Z}$ and $N(x) = a^2 - b^2 d \in \mathbb{Z}$ follows $(2b)^2 d = S(x)^2 - 4N(x) \in \mathbb{Z}$ and $2b \in \mathbb{Z}$, since d is square-free. Thus, let $x = \frac{a_1 + b_1\sqrt{d}}{2}$ with $a_1, b_1 \in \mathbb{Z}$. Because of $N(x) = \frac{a_1^2 - b_1^2 d}{4} \in \mathbb{Z}$, it holds that $a_1^2 \equiv b_1^2 d \pmod 4$ with $d \not\equiv 0 \pmod 4$. If $d \equiv 2, 3 \pmod 4$, then a_1 and b_1 must be even, because $a_1^2 \equiv 0, 1 \pmod 4$. In this case, $x \in \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Now let $d \equiv 1 \pmod 4$. If a_1 is odd, then b_1 must also be odd. In this case

$$a + b\sqrt{d} = \frac{a_1 - b_1}{2} + b_1 \frac{1+\sqrt{d}}{2} \in \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}.$$

Conversely, $\mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2} \subseteq \mathbb{Z}_d$ also holds here.

For the second assertion, only the closure with respect to multiplication in the case $d \equiv 1 \pmod 4$ needs to be shown:

$$\left(a_1 + b_1\frac{1+\sqrt{d}}{2}\right)\left(a_2 + b_2\frac{1+\sqrt{d}}{2}\right) = a_1a_2 + b_1b_2\frac{d-1}{4} + (a_1b_1 + a_2b_1 + b_1b_2)\frac{1+\sqrt{d}}{2}. \qquad \square$$

Definition 6.8. One calls $\mathbb{Z}_d$ the *ring of integers* of $\mathbb{Q}(\sqrt{d})$. The elements of $\mathbb{Z}_{-1}$ and $\mathbb{Z}_{-3}$ are called *Gaussian integers* and EISENSTEIN *integers* respectively.

Lemma 6.9. *For $d \in \mathbb{Z} \setminus \{0,1\}$ square-free, it holds that*

$$x \in \mathbb{Z}_d^\times \iff N(x) = \pm 1.$$

Proof. For $x = a + b\sqrt{d} \in \mathbb{Z}_d^\times$, it holds that $N(x) \in \mathbb{Z}$ and $N(x)^{-1} = N(x^{-1}) \in \mathbb{Z}$. This is only possible for $N(x) = \pm 1$. Conversely, let $N(x) = \pm 1$. From $x^{-1} = \frac{1}{N(x)}(a - b\sqrt{d})$ follows $S(x^{-1}) = \pm S(x) \in \mathbb{Z}$ and $N(x^{-1}) = N(x) \in \mathbb{Z}$. Thus $x \in \mathbb{Z}_d^\times$. □

Theorem 6.10. *For $d < 0$ square-free, it holds that*

$$\mathbb{Z}_d^\times = \begin{cases} \langle \mathrm{i} \rangle = \{\pm 1, \pm \mathrm{i}\} & \text{if } d = -1, \\ \left\langle \frac{1+\sqrt{-3}}{2} \right\rangle = \left\{\pm 1, \pm \frac{1 \pm \sqrt{-3}}{2}\right\} & \text{if } d = -3, \\ \langle -1 \rangle = \{\pm 1\} & \text{otherwise.} \end{cases}$$

For $d > 1$, it holds that $|\mathbb{Z}_d^\times| = \infty$.

Proof. Of course, $\pm 1 \in \mathbb{Z}_d^\times$ holds in all cases. Let $x = a + b\sqrt{d} \in \mathbb{Z}_d^\times$. According to Lemma 6.9, $a^2 - b^2 d = N(x) = \pm 1$. In the case $b = 0$, $x = a = \pm 1$. So let $b \neq 0$. First, let $d < 0$. Then $\frac{1}{4}|d| \leq a^2 + b^2|d| = 1$ and $|d| \leq 4$. Since d is square-free, one obtains $d \in \{-1, -2, -3\}$. In the case $d = -1$, $a, b \in \mathbb{Z}$ and it follows that $a, b \in \{\pm 1\}$. In the case $d = -2$, $b \in \mathbb{Z}$ and thus $b = 0$. Finally, let $d = -3$ and $a = a_1/2$ as well as $b = b_1/2$ with $a_1, b_1 \in \mathbb{Z}$. From $a_1^2 + 3b_1^2 = 1$ it follows that $a_1, b_1 \in \{\pm 1\}$. This yields the six specified elements. These form the group of the sixth roots of unity, which is generated by $\frac{1+\sqrt{-3}}{2}$.

Now let $d > 1$. According to Pell's equation, there exist infinitely many $a, b \in \mathbb{Z}$ with $a^2 - b^2 d = 1$. The claim therefore follows from Lemma 6.9. □

Definition 6.11. Let $R \subseteq \mathbb{C}$ be a subring.

- For $a, b \in R$ we write (as usual) $a \mid b$ if there exists a $c \in R$ with $ac = b$. One then says: *a divides b*, *a* is a *divisor* of *b* etc. Furthermore, let $a \equiv b \pmod{c}$ if $c \mid a - b$. Let the set of multiples of a be $Ra = \{ra : r \in R\}$. The *residue classes* modulo a have the form $b + Ra$.
- As defined in Definition 1.9, one defines the set of common divisors $\mathrm{cd}(a, b)$ for $a, b \in R$. If $\mathrm{cd}(a, b)$ consists only of invertible elements, then a and b are called *coprime*. One calls $g \in \mathrm{cd}(a, b)$ a *greatest common divisor* of a, b if $x \mid g$ holds for all $x \in \mathrm{cd}(a, b)$.
- One calls $a, b \in R$ *associated* if $a \mid b \mid a$ holds.
- One calls $p \in R \setminus (R^\times \cup \{0\})$ a *prime element* if for all $a, b \in R$ it holds that: $p \mid ab \Rightarrow p \mid a \vee p \mid b$ (cf. Lemma 2.3).

Remark 6.12.

(i) For $a, b, c, d, e \in R \subseteq \mathbb{C}$, the usual calculation rules hold:

- $\pm 1 \mid a \mid 0$,
- $0 \mid a \iff a = 0$,
- $a \mid b \mid c \implies a \mid c$,
- $a \mid b, c \implies a \mid (bd + ce)$.

(ii) Being associated is an equivalence relation on R. If $a, b \in R$ are associated, then there exist $r, s \in R$ with $ar = b$ and $bs = a$. It follows that $a(1 - rs) = a - ars = a - bs = a - a = 0$. In the case $a = 0$, we also have $b = 0$. Otherwise, $rs = 1$ and $r \in R^\times$. Conversely, if $ar = b$ with $r \in R^\times$, then also $br^{-1} = a$ and one obtains $a \mid b \mid a$. Thus, a, b are associated if and only if there exists an $r \in R^\times$ with $ar = b$.

(iii) In contrast to $\mathbb{Z}$, greatest common divisors do not always exist and even if they exist, they are only uniquely determined up to association (in $\mathbb{Z}$ we had additionally required $\gcd \geq 0$, which makes no sense in $\mathbb{C}$).

(iv) The next lemma justifies the term "prime element".

Lemma 6.13. *Let $R \subseteq \mathbb{C}$ be a subring and $p \in R$ a prime element. If there exist $a, b \in R$ with $p = ab$, then $a \in R^\times$ or $b \in R^\times$.*

Proof. By definition, p is a divisor of a or b, say $p \mid a$. Because of $a \mid p$, a and p are associated. According to Remark 6.12, there exists $r \in R^\times$ with $p = ar$. It follows that $a(b-r) = 0$. Because of $p \neq 0 \neq a$, it holds that $b = r \in R^\times$. □

Lemma 6.14. *Let $R \subseteq \mathbb{C}$ be a subring. Let $p_1, \ldots, p_s, q_1, \ldots, q_t \in R$ be prime elements with $p_1 \ldots p_s = q_1 \ldots q_t$. Then $s = t$ and, with suitable numbering, p_i is associated to q_i for $i = 1, \ldots, s$.*

Proof. Induction on s: In the case $s = 0$, we have $q_1 \ldots q_t = 1$ and $q_1 \in R^\times$. Since prime elements are not invertible, $t = 0$ holds. Now let $s \geq 1$ and assume the statement is already proven for $s-1$. From $p_s \mid p_1 \ldots p_s = q_1 \ldots q_t$ it follows that $p_s \mid q_i$ for some $i \in \{1, \ldots, t\}$, say $i = t$. So let $e \in R$ with $p_s e = q_t$. According to Lemma 6.13, $e \in R^\times$ holds. In particular, p_s and q_t are associated. It follows that

$$(p_1 \ldots p_{s-1} - q_1 \ldots q_{t-1} e) p_s = p_1 \ldots p_s - q_1 \ldots q_t = 0.$$

Because of $p_s \neq 0$, we have $p_1 \ldots p_{s-1} = q_1 \ldots (q_{t-1} e)$. By induction, $s = t$ and, with suitable numbering, p_i is associated to q_i or to $q_{t-1} e$ for $i = 1, \ldots, s-1$. This shows the claim. □

Definition 6.15. A subring $R \subseteq \mathbb{C}$ is called

- *factorial*[10], if every element from $R \setminus (R^\times \cup \{0\})$ is a product of prime elements.
- *Euclidean*, if a map $H \colon R \to \mathbb{N}_0$ with the following property exists: For all $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ with $a = qb + r$ and $H(r) < H(b)$ (Euclidean division).

Remark 6.16.

(i) Let $R \subseteq \mathbb{C}$ be factorial and $P \subseteq R$ a system of representatives for the equivalence classes of associated prime elements (for example the prime numbers in $R = \mathbb{Z}$). According to Lemma 6.14, every $x \in R \setminus \{0\}$ has a unique *prime factorization*

$$x = e \prod_{p \in P} p^{\nu_p(x)}$$

with $e \in R^\times$ and $\nu_p(x) \in \mathbb{N}_0$ for $p \in P$. For $x, y \in R \setminus \{0\}$, $x \mid y$ holds if and only if $\nu_p(x) \leq \nu_p(y)$ for all $p \in P$. For $x_1, \ldots, x_n \in R \setminus \{0\}$ one sets

$$\gcd(x_1, \ldots, x_n) := \prod_{p \in P} p^{\min\{\nu_p(x_1), \ldots, \nu_p(x_n)\}},$$
$$\operatorname{lcm}(x_1, \ldots, x_n) := \prod_{p \in P} p^{\max\{\nu_p(x_1), \ldots, \nu_p(x_n)\}}.$$

(ii) In every Euclidean ring $R \subseteq \mathbb{C}$, a greatest common divisor for $a, b \in R \setminus \{0\}$ can be determined using the extended Euclidean algorithm:

- Set $(x_0, y_0, z_0) := (1, 0, a)$, $(x_1, y_1, z_1) := (0, 1, b)$ and $k := 0$.
- As long as $z_{k+1} \neq 0$ repeat:

$$(x_{k+2}, y_{k+2}, z_{k+2}) := (x_k - x_{k+1} q_{k+1}, y_k - y_{k+1} q_{k+1}, r_{k+1}),$$

where $z_k = q_{k+1} z_{k+1} + r_{k+1}$ with $H(r_{k+1}) < H(z_{k+1})$.

[10] or *UFD* (unique factorization domain)

- For $z_{k+1} = 0$, $z_k = x_k a + y_k b$ is a gcd of a and b.

Because of $H(r_{k+1}) < H(z_{k+1})$, $z_{k+1} = 0$ holds after finitely many steps. As in Theorem 1.11, one shows $\operatorname{cd}(a, b) = \operatorname{cd}(z_k, 0)$. However, it is not clear how to perform the Euclidean division in practice.

Lemma 6.17. *In every Euclidean ring $R \subseteq \mathbb{C}$, one can choose the function H such that for all $a, b \in R$ with $b \neq 0$ the following holds:*

(i) $H(a) \leq H(ab)$.

(ii) If $a \neq 0$, then $H(a) = H(ab) \iff b \in R^\times$.

(iii) $H(a) = H(1) \iff a \in R^\times$.

Proof. Let

$$H'(a) := \min_{b \in R \setminus \{0\}} H(ab)$$

for $a \in R$. Then $H'(a) \leq H(a1) = H(a)$ holds. For $a, b \in R$ with $b \neq 0$, there exists a $c \in R \setminus \{0\}$ with $H'(b) = H(bc)$. Because of $bc \neq 0$, there exist $q, r \in R$ with $a = qbc + r$ and $H'(r) \leq H(r) < H(bc) = H'(b)$. For $q' = qc$, it thus holds that $a = q'b + r$ and $H'(r) < H'(b)$. Thus R is Euclidean with respect to H'.

(i) Let $c \in R$ with $H'(ab) = H(abc)$. Then $H'(a) \leq H(a(bc)) = H'(ab)$ holds.

(ii) If $b \in R^\times$, then $H'(a) \leq H'(ab) \leq H'(abb^{-1}) = H'(a)$ follows from (i). Conversely, let $H'(a) = H'(ab)$. Euclidean division yields $q, r \in R$ with $a = q(ab) + r$ and $H'(r) < H'(ab)$. Thus $H'(a(1 - qb)) = H'(r) < H'(a)$ and $qb = 1$ according to (i). This shows $b \in R^\times$.

(iii) Follows from (ii) with $a = 1$. □

Theorem 6.18. *Euclidean rings are factorial.*

Proof. Let R be Euclidean with H as in Lemma 6.17. We show by induction on $H(x)$ that every $x \in R \setminus (R^\times \cup \{0\})$ is a product of prime elements. Let $p \in R \setminus R^\times$ be a divisor of x such that $H(p)$ is as small as possible (if necessary $p = x$). Let $a, b \in R$ with $p \mid ab$. Assume p is coprime to a and to b. According to the extended Euclidean algorithm, there exist $\alpha, \beta, \gamma, \delta \in R$ with $\alpha p + \beta a = 1 = \gamma p + \delta b$. But then

$$p \mid \beta\delta ab + \beta\gamma ap + \alpha\delta bp + \alpha\gamma p^2 = (\alpha p + \beta a)(\gamma p + \delta b) = 1.$$

So let wlog. $q \in \operatorname{cd}(a, p) \setminus R^\times$. From $q \mid p \mid x$ follows $H(q) = H(p)$. According to Lemma 6.17, p and q are associated and therefore $p \mid q \mid a$. This shows that p is a prime element. Let $y \in R$ with $x = py$. According to Lemma 6.17, $H(y) < H(x)$ holds. By induction, y is a product of prime elements and thus so is x. □

Lemma 6.19. *Let $d \in \mathbb{Z} \setminus \{0, 1\}$ be square-free. If for every $x \in \mathbb{Q}(\sqrt{d})$ there exists an $a \in \mathbb{Z}_d$ with $|N(x - a)| < 1$, then R is Euclidean.*

Proof. Let $R := \mathbb{Z}_d$ and $H(a) := |N(a)|$ for $a \in R$. For $a, b \in R$ with $b \neq 0$, there exists $q \in R$ with $|N(\frac{a}{b} - q)| < 1$. With $r := a - bq \in R$ it follows that

$$H(r) = |N(a - bq)| = |N(b)| \left| N\Big(\frac{a}{b} - q\Big) \right| < |N(b)| = H(b).$$ □

Theorem 6.20. *For $d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 13, 17, 21, 29\}$, $\mathbb{Z}_d$ is Euclidean.*

Proof. We apply Lemma 6.19. Let $x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ with $x, y \in \mathbb{Q}$ be given. For $d \in \{-2, -1, 2, 3\}$, we choose $a, b \in \mathbb{Z}$ with $|x - a|, |y - b| \leq \frac{1}{2}$. Then

$$\left|N\big((x + y\sqrt{d}) - (a + b\sqrt{d})\big)\right| = \left|(x - a)^2 - d(y - b)^2\right| \leq \frac{1}{4}\big(|d| + 1\big)$$

holds and the claim follows (for $d = 3$, the inequality is strict). Now let $d \in \{-11, -7, -3, 5\}$. Then one can choose a, b with

$$\left|N\Big(\Big(x + y\sqrt{d}\Big) - \Big(a + b\frac{1 + \sqrt{d}}{2}\Big)\Big)\right| = \left|\Big(x - a - \frac{b}{2}\Big)^2 - d\Big(y - \frac{b}{2}\Big)^2\right| \leq \frac{1}{4} + \frac{|d|}{16} < 1.$$

For the remaining values, we require a case distinction:

(i) $d \in \{6, 7\}$: Let

$$\begin{aligned} |x - a| \leq \frac{1}{2} \quad &\text{if} \quad |y - b|^2 < \frac{1}{d}, \\ \frac{1}{2} \leq |x - a| \leq 1 \quad &\text{if} \quad \frac{1}{d} < |y - b|^2 < \frac{5}{4d}, \\ 1 \leq |x - a| \leq \frac{3}{2} \quad &\text{if} \quad \frac{5}{4d} < |y - b|^2 \leq \frac{1}{4}. \end{aligned}$$

Then

$$|(x - a)^2 - d(y - b)^2| < \begin{cases} d\frac{1}{d} = 1 & \text{if } |y - b|^2 < \frac{1}{d}, \\ \frac{5}{4} - \frac{1}{4} = 1 & \text{if } \frac{1}{d} < |y - b|^2 < \frac{5}{4d}, \\ \frac{9}{4} - \frac{5}{4} = 1 & \text{if } \frac{5}{4d} < |y - b|^2 \leq \frac{1}{4}. \end{cases}$$

(ii) $d \in \{13, 17, 21, 29\}$: Instead of $|x - a|$ and $|y - b|$, one can choose $|x - a - \frac{b}{2}|$ and $|y - \frac{b}{2}|$ here as in the case $d \in \{6, 7\}$. The estimates then hold in the same way, since one can additionally achieve $|y - \frac{b}{2}| \leq \frac{1}{4}$. □

Example 6.21.

(i) We show that $\mathbb{Z}_{-5} = \mathbb{Z} + \sqrt{-5}\mathbb{Z}$ is not factorial (and thus also not Euclidean). It holds that $2 \mid 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Because of $N(2) = 4$ and $N(1 \pm \sqrt{-5}) = 6$, 2 cannot divide $1 \pm \sqrt{-5}$. Therefore, 2 is not a prime element. Suppose there is a factorization $2 = xy$ with $x, y \in \mathbb{Z}_{-5}$. Because of $N(a + b\sqrt{-5}) = a^2 + 5b^2 \neq 2$ for all $a, b \in \mathbb{Z}$, it must hold that $N(x) = 1$ or $N(y) = 1$. Thus $x \in \mathbb{Z}_{-5}^{\times}$ or $y \in \mathbb{Z}_{-5}^{\times}$. This shows that 2 cannot be written as a product of prime elements.

(ii) One can show that $\mathbb{Z}_d$ is Euclidean with respect to $H(a) = |N(a)|$ if and only if

$$d \in \{-11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

For $d < 0$, there are generally no further Euclidean rings $\mathbb{Z}_d$. On the other hand, $\mathbb{Z}_{14}$ and $\mathbb{Z}_{69}$ are Euclidean and it is conjectured that there are infinitely many further Euclidean rings with $d > 0$.

(iii) HEEGNER showed that $\mathbb{Z}_d$ for negative d is factorial if and only if

$$-d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$$

(*Heegner numbers*). In particular, there are factorial rings that are not Euclidean. This can be used to explain why

$$e^{\pi\sqrt{163}} = 262537412640768743{,}99999999999925\ldots$$

is almost an integer (without proof).

(iv) One calls $x \in \mathbb{C}$ *algebraic* if x is a root of a non-constant polynomial with coefficients in $\mathbb{Q}$. Since these polynomials can be counted, there exist only countably many algebraic numbers. There are therefore uncountably many numbers that are not algebraic. They are called *transcendental*. According to the theorem of LINDEMANN, $\pi \approx 3{,}14$ is transcendental.[11] For a transcendental number $x \in \mathbb{C}$, one obtains according to Exercise 41 a Euclidean ring

$$\mathbb{Z}[x] := \Big\{\sum_{i=0}^{n} a_i x^i : n \in \mathbb{N}, a_0, \ldots, a_n \in \mathbb{Z}\Big\}.$$

Theorem 6.22. *For every prime element $\pi \in \mathbb{Z}_{-1}$, exactly one of the following statements holds:*

(i) π is associated to $1 + \mathrm{i}$.

(ii) π is associated to a prime number $p \equiv 3 \pmod 4$.

(iii) $\pi\overline{\pi} = p \equiv 1 \pmod 4$ for a prime number p and π is not associated to $\overline{\pi}$.

Proof. Let $R := \mathbb{Z}_{-1}$. Since $\pi \notin R^\times$, we have $\pi \mid \pi\overline{\pi} = |\pi|^2 \geq 2$. Therefore π divides a prime factor p of $|\pi|^2$. If π also divides $q \in \mathbb{P} \setminus \{p\}$, then π also divides $\gcd(p, q) = 1$ and one obtains the contradiction $\pi \in R^\times$. Thus p is the only prime number divisible by π. One can therefore determine the prime elements in R by decomposing the prime numbers into prime elements. Every $\pi \in R$ with $|\pi|^2 \in \mathbb{P}$ is a prime element in R due to Lemma 6.13. In particular, $1 + \mathrm{i} \in R$ is a prime element and $2 = -\mathrm{i}(1 + \mathrm{i})^2$ is the prime factorization of 2 (one says: 2 is *ramified*).

Now let $p \equiv 3 \pmod 4$ and $\sigma, \tau \in R$ with $p = \sigma\tau$. Then

$$|\sigma\tau|^2 = p^2. \tag{6.1}$$

Since $a^2 + b^2 \not\equiv 3 \pmod 4$ for all $a, b \in \mathbb{Z}$, the equation $a^2 + b^2 = p$ has no integer solutions. Therefore σ or τ is invertible and p is a prime element in R (one says: p is *inert*).

Finally, let $p \equiv 1 \pmod 4$ and $q := (p-1)/2 \in 2\mathbb{Z}$. According to Wilson (Exercise 22)

$$-1 \equiv (p-1)! \equiv \prod_{k=1}^{q} k(p-k) \equiv (-1)^q (q!)^2 \equiv (q!)^2 \pmod p.$$

This shows $p \mid (q!)^2 + 1 = (q! - \mathrm{i})(q! + \mathrm{i})$. If p were a prime element in R, then $p = \bar{p} \mid q! \pm \mathrm{i}$ and

$$0 \not\equiv 2q! = (q! + \mathrm{i}) + (q! - \mathrm{i}) \equiv 0 \pmod p.$$

Thus p is not a prime element and according to (6.1) there exists a prime factor $\pi \mid p$ with $\pi\overline{\pi} = p$. Wlog. let $\pi \mid q! + \mathrm{i}$. Suppose π and $\overline{\pi}$ are associated. Then π and $\overline{\pi}$ would be divisors of $q! \pm \mathrm{i}$ and therefore also divisors of $2 = \mathrm{i}((q! - \mathrm{i}) - (q! + \mathrm{i}))$. However, we already know that every prime element divides only one prime number. Therefore π and $\overline{\pi}$ are not associated (one says: p is *split*). □

[11] See appendix in Algebra notes

Theorem 6.23 (Girard)**.** *A number $n \in \mathbb{N}$ can be written as a sum of two integer squares if and only if the multiplicity of every prime number $p \equiv 3 \pmod 4$ in the prime factorization of n is even. In particular, every prime number $p \equiv 1 \pmod 4$ is a sum of two squares.*

Proof (Dedekind).

$\Rightarrow$: Let $n = a^2 + b^2 = (a + b\mathrm{i})(a - b\mathrm{i})$ with $a, b \in \mathbb{Z}$. According to Theorem 6.22, one obtains the prime factorization of $a + b\mathrm{i} \in \mathbb{Z}_{-1}$ as follows

$$a + b\mathrm{i} = e(1 + \mathrm{i})^{\delta_2} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 3 \pmod 4}} p^{\delta_p} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod 4}} \pi_p^{\delta_p} \overline{\pi_p}^{\delta'_p}$$

with $e \in \{\pm 1, \pm \mathrm{i}\}$ and $\delta_2, \delta_p, \delta'_p \in \mathbb{N}_0$. Therefore

$$n = |a + b\mathrm{i}|^2 = 2^{\delta_2} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 3 \pmod 4}} p^{2\delta_p} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod 4}} p^{\delta_p + \delta'_p}$$

is the prime factorization of n.

$\Leftarrow$: By assumption

$$n = 2^{\delta_2} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 3 \pmod 4}} p^{2\delta_p} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod 4}} p^{\delta_p} = |\alpha|^2$$

with

$$\alpha = (1 + \mathrm{i})^{\delta_2} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 3 \pmod 4}} p^{\delta_p} \prod_{\substack{p \in \mathbb{P} \\ p \equiv 1 \pmod 4}} \pi_p^{\delta_p} \in \mathbb{Z}_{-1}.$$

Therefore there exist $a, b \in \mathbb{Z}$ with $\alpha = a + b\mathrm{i}$ and $a^2 + b^2 = |\alpha|^2 = n$. □

Lemma 6.24. *Let p be a prime and $a \in \mathbb{F}_p$. Then there exist $x, y \in \mathbb{F}_p$ with $x^2 + y^2 = a$.*

Proof. For $p = 2$ one chooses $x := a$ and $y := 0$. So let p be odd and $q := (p - 1)/2$. For $0 \leq k, l \leq q$ it holds that

$$k^2 \equiv l^2 \pmod p \iff (k + l)(k - l) \equiv 0 \pmod p \iff k \equiv \pm k \pmod p \iff k = l,$$

since $\mathbb{F}_p$ is a field. Thus one has $q + 1$ pairwise distinct residues modulo p. Analogously, $a - k^2$ for $k = 0, \ldots, q$ are also pairwise distinct modulo p. Because of $2(q + 1) = p + 1 > p$, there exist $x, y \in \mathbb{Z}$ with $x^2 \equiv a - y^2 \pmod p$ by the pigeonhole principle. Thus $x^2 + y^2 = a$ holds in $\mathbb{F}_p$. □

Theorem 6.25 (Lagrange's four-square theorem)**.** *Every natural number is the sum of (at most) four squares.*

Proof. By allowing $0 = 0^2$ as a square number, we can show that every $n \in \mathbb{N}$ is the sum of (exactly) four square numbers. Wlog. let $n \geq 3$. Let p be a prime divisor of n. In the case $p < n$, we can assume by induction on n that p and n/p are sums of four squares. Because of the *Euler's identity*

$$\begin{aligned}(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) &= (a_1 b_1 + a_2 b_2 + a_3 b_3 + a_4 b_4)^2 \\ +(a_1 b_2 - a_2 b_1 + a_3 b_4 - a_4 b_3)^2 + (a_1 b_3 - a_3 b_1 + a_4 b_2 - a_2 b_4)^2 &+ (a_1 b_4 - a_4 b_1 + a_2 b_3 - a_3 b_2)^2\end{aligned} \tag{6.2}$$

then n is also a sum of four squares. So let $n = p \in \mathbb{P}$. According to Theorem 6.23, we may assume $p \equiv 3 \pmod 4$. According to Lemma 6.24, there exist $x, y \in \mathbb{Z}$ with $x^2 + y^2 \equiv 0 \pmod p$. By replacing x or y with $-x$ or $-y$ if necessary, one can assume $0 \leq x, y \leq \frac{p-1}{2}$. Then $x^2 + y^2 < \frac{p^2}{2} < p^2$ holds. In particular, the equation $x_1^2 + x_2^2 + x_3^2 + x_4^2 = hp$ is solvable for an $h < p$. Let h be minimal with this property. Let us assume $h > 1$. First, let h be even. Then the number of odd squares x_i^2 is even (possibly 0). With suitable numbering, $2 \mid x_1 \pm x_2$ and $2 \mid x_3 \pm x_4$ hold. It follows that

$$\Big(\frac{x_1 + x_2}{2}\Big)^2 + \Big(\frac{x_1 - x_2}{2}\Big)^2 + \Big(\frac{x_3 + x_4}{2}\Big)^2 + \Big(\frac{x_3 - x_4}{2}\Big)^2 = \frac{1}{2}\big(x_1^2 + x_2^2 + x_3^2 + x_4^2\big) = \frac{h}{2}p$$

in contradiction to the choice of h. Thus $h \geq 3$ is odd. Let $y_1, \ldots, y_4 \in \mathbb{Z}$ with $y_i \equiv x_i \pmod h$ and $|y_i| \leq \frac{h-1}{2}$ for $i = 1, \ldots, 4$. In the case $(y_1, \ldots, y_4) = (0, \ldots, 0)$, $h^2 \mid x_1^2 + \ldots + x_4^2 = hp$ and $h \mid p$. But then $h \geq p$ would hold. Thus $0 < y_1^2 + \ldots + y_4^2 < h^2$ and $y_1^2 + \ldots + y_4^2 \equiv x_1^2 + \ldots + x_4^2 \equiv 0 \pmod h$ hold. Thus there exists a $1 \leq k < h$ with $y_1^2 + \ldots + y_4^2 = kh$. Because of (6.2), $hp \cdot kh = z_1^2 + \ldots + z_4^2$ holds with

$$\begin{aligned}
z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv hp \equiv 0 \pmod h,\\
z_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \equiv x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3 \equiv 0 \pmod h,\\
z_3 &= x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4 \equiv x_1x_3 - x_3x_1 + x_4x_2 - x_2x_4 \equiv 0 \pmod h,\\
z_4 &= x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 \equiv x_1x_4 - x_4x_1 + x_2x_3 - x_3x_2 \equiv 0 \pmod h.
\end{aligned}$$

This yields $kp = \big(\frac{z_1}{h}\big)^2 + \ldots + \big(\frac{z_4}{h}\big)^2$ in contradiction to the choice of h. □

Remark 6.26. There are several related square theorems, which we state without proof:

(i) (Legendre's 3-*Square Theorem*) $n \in \mathbb{N}$ is a sum of three squares if and only if n is *not* of the form $4^a(8b+7)$ with $a, b \in \mathbb{N}_0$. For example, 7 is not the sum of three squares. One direction of the proof is easy (Exercise 44), but the other direction is more difficult than the 4-Square Theorem.

(ii) (Waring's Problem) For every $k \in \mathbb{N}$, there exists a $w_k \in \mathbb{N}$ such that every natural number is the sum of at most w_k non-negative k-th powers. According to the 4-Square Theorem, one can choose $w_2 = 4$. Furthermore, $w_3 = 9$, $w_4 = 19$ and it is generally conjectured that

$$w_k = \Big\lfloor \frac{3^k}{2^k} \Big\rfloor + 2^k - 2$$

for $k \geq 2$ is the smallest w_k (cf. Exercise 39). It is conjectured that every natural number is the sum of four *integer* cubes. Moreover, it is conjectured that, up to finitely many exceptions, every natural number is the sum of four non-negative cubes.

(iii) (Mordell's Problem) Every number $n \equiv 4, 5 \pmod 9$ is not the sum of three integer cubes, because $a^3 \equiv -1, 0, 1 \pmod 9$. It is not known whether all other numbers are the sum of three cubes. This has been verified up to $n \leq 113$. The last outstanding case $n = 42$ was solved in 2019:

$$42 = (-80538738812075974)^3 + 80435758145817515^3 + 12602123297335631^3.$$

(iv) From the proof of Theorem 6.23 and the unique prime factorization in $\mathbb{Z}_{-1}$, it follows that every prime $p \equiv 1 \pmod 4$ can be written as a sum of squares in only one way (up to the order of the squares). The number of possible decompositions of a natural number n as a sum of four squares is given by Jacobi's *formula*

$$\big|\{(a, b, c, d) \in \mathbb{Z}^4 : a^2 + b^2 + c^2 + d^2 = n\}\big| = 8 \sum_{4 \nmid d \mid n} d.$$

For $n = 28$, one obtains

$$\sum_{4 \nmid d \mid 28} d = 1 + 2 + 7 + 14 = 24.$$

Thus, there are $8 \cdot 24 = 192$ possibilities to write 28 as a sum of four squares. However, all these possibilities arise by permutation and choice of signs from

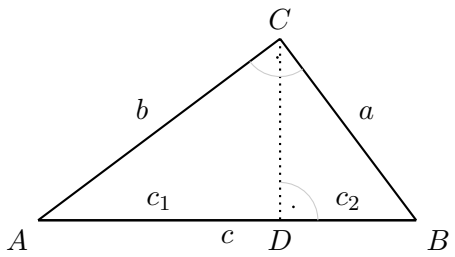
$$28 = 5^2 + 1^2 + 1^2 + 1^2 = 4^2 + 2^2 + 2^2 + 2^2 = 3^2 + 3^2 + 3^2 + 1^2.$$

7 Fermat's Last Theorem

Remark 7.1. In this chapter, we discuss two special cases of the famous Last Theorem of Fermat. The Euclidean ring of Eisenstein integers $\mathbb{Z}_{-3}$ plays a role here.

Theorem 7.2 (Pythagoras)**.** *A triangle with side lengths a, b, and c is right-angled if and only if (with suitable labeling) $a^2 + b^2 = c^2$ holds.*

Proof. All proofs presuppose certain geometric postulates that go back to Euclid's *Elements*. Let ABC be a right-angled triangle with sides a, b, c:



The triangles ABC and ADC have, in addition to the right angle, the angle at A in common. They are therefore similar. Analogously, ABC and DBC are also similar. For the side lengths, it therefore holds that $\frac{a}{c} = \frac{c_2}{a}$ and $\frac{b}{c} = \frac{c_1}{b}$. It follows

$$a^2 + b^2 = cc_2 + cc_1 = c(c_1 + c_2) = c^2.$$

Now let a, b, c be the side lengths of an arbitrary triangle Δ such that $a^2 + b^2 = c^2$ holds. Certainly, there exists a right-angled triangle Δ' with side lengths a, b, c', where c' is the largest side. According to the first part of the proof, $(c')^2 = a^2 + b^2 = c^2$ and thus $c' = c$. Therefore, Δ and Δ' are congruent. Like Δ', Δ is also right-angled. □

Definition 7.3. One calls $(a, b, c) \in \mathbb{N}^3$ a *pythagorean triple*, if $a^2 + b^2 = c^2$.

Theorem 7.4 (Euclid)**.** *Every pythagorean triple has the form*

$$d(2st, t^2 - s^2, t^2 + s^2) \qquad \textit{resp.} \qquad d(t^2 - s^2, 2st, t^2 + s^2)$$

where $d, s, t \in \mathbb{N}$ with $s < t$. Conversely, every choice of these parameters yields a pythagorean triple. In particular, there are infinitely many pythagorean triples.

Proof. Let (a,b,c) be a Pythagorean triple and $d := \gcd(a,b)$. Then d^2 is a divisor of $a^2+b^2=c^2$. By the unique prime factorization, d is a divisor of c. Consequently, $\frac{1}{d}(a,b,c)$ is also a Pythagorean triple. We can therefore assume $\gcd(a,b)=1$. In particular, a or b is odd. If both are odd, then the contradiction $c^2 = a^2+b^2 \equiv 2 \pmod 4$ arises. Wlog. let $a=2k$ and b be odd. Then c is also odd and one obtains

$$\frac{c+b}{2}\frac{c-b}{2} = \frac{c^2-b^2}{4} = \frac{a^2}{4} = k^2. \tag{7.1}$$

Let $e \in \mathbb{N}$ be a common divisor of $\frac{c+b}{2}$ and $\frac{c-b}{2}$. Then e also divides $\frac{c+b}{2}+\frac{c-b}{2}=c$ as well as $\frac{c+b}{2}-\frac{c-b}{2}=b$. Consequently, e^2 also divides $c^2-b^2=a^2$. Because of $\gcd(a,b)=1$, it follows that $e=1$, i. e. $\frac{c+b}{2}$ and $\frac{c-b}{2}$ are coprime. Every prime factor of k thus divides either the first or the second factor in (7.1). This yields $s,t \in \mathbb{N}$ with $s<t$ and

$$\frac{c+b}{2} = t^2, \qquad \frac{c-b}{2} = s^2, \qquad st = k.$$

We calculate

$$\begin{aligned} a &= 2k = 2st, \\ b &= \frac{c+b}{2} - \frac{c-b}{2} = t^2 - s^2, \\ c &= \frac{c+b}{2} + \frac{c-b}{2} = t^2 + s^2. \end{aligned}$$

Conversely, if $d,s,t \in \mathbb{N}$ with $s<t$ are given, then $(a,b,c) := d(2st, t^2-s^2, t^2+s^2) \in \mathbb{N}^3$ with

$$a^2+b^2 = d^2(4s^2t^2 + (t^2-s^2)^2) = d^2(t^4+2s^2t^2+s^4) = d^2(t^2+s^2)^2 = c^2. \qquad \square$$

Example 7.5. For $(d,s,t) \in \{(1,1,2),(1,2,3)\}$ one obtains the Pythagorean triples $(3,4,5)$ and $(5,12,13)$. For $(d,s,t) \in \{(1,1,3),(2,1,2)\}$ one obtains $(6,8,10)$ in each case. One can make the numbers d,s,t in Theorem 7.4 unique by additionally requiring $\gcd(s,t)=1$ and $s \not\equiv t \pmod 2$.

Theorem 7.6 (Fermat's "last" theorem)**.** *For $n \geq 3$ there exists no triple $(a,b,c) \in \mathbb{N}^3$ with $a^n+b^n = c^n$.*

Remark 7.7.

(i) Suppose $a,b,c \in \mathbb{Z}$ satisfy $a^n+b^n=c^n$. If n is even or $a,b,c<0$, then $|a|^n+|b|^n=|c|^n$ also holds. In all other cases, one can if necessary swap c with a or b to achieve $|a|^n+|b|^n=|c|^n$. Fermat's last theorem (short FLT) shows that at least one of the numbers a, b or c must be zero. In $\mathbb{Z}^3$ there are therefore only *trivial* solutions. The same obviously holds over $\mathbb{Q}$ (multiply by common denominator).

(ii) If Theorem 7.6 is proven for n, then also for nk with $k \in \mathbb{N}$, because every solution $a^{nk}+b^{nk} = c^{nk}$ for nk yields a solution $(a^k)^n + (b^k)^n = (c^k)^n$ for n. One therefore "only" needs to prove Theorem 7.6 for $n=4$ and odd prime numbers. Fermat proved his theorem only for $n=4$. This is presumably the most elementary case.

Theorem 7.8 (Fermat)**.** *There exists no triple $(a,b,c) \in \mathbb{N}^3$ with $a^4+b^4=c^4$.*

Proof. Let us assume more generally that $(a, b, c) \in \mathbb{N}^3$ with $a^4 + b^4 = c^2$ exists (this includes the given equation because of $c^4 = (c^2)^2$). Let c be as small as possible. Then $\gcd(a, b) = 1$ holds, because otherwise one could divide by $\gcd(a, b)$ as in the proof of Theorem 7.4. Since (a^2, b^2, c) is a Pythagorean triple, there exist $s, t \in \mathbb{N}$ with $s < t$ and wlog. $(a^2, b^2, c) = (2st, t^2 - s^2, t^2 + s^2)$. Now (b, s, t) is also a Pythagorean triple with $\gcd(b, s) \mid \gcd(b, 2st) = \gcd(b, a^2) = 1$. Since a is even, b is odd. According to Theorem 7.4, there exist $u, v \in \mathbb{N}$ with $(b, s, t) = (v^2 - u^2, 2uv, v^2 + u^2)$. Because of $\gcd(a, b) = 1$, we also have $\gcd(s, t) = 1$. Here $s = 2uv$ is even and t is odd. The prime factorization of $a^2 = 2st$ shows $s = 2x^2$ and $t = y^2$ with $x, y \in \mathbb{N}$ and $\gcd(x, y) = 1$. Finally, $\gcd(u, v) \mid \gcd(b, s) = 1$ also holds. The equation $x^2 = uv$ therefore yields $p, q \in \mathbb{N}$ with $u = p^2$ and $v = q^2$. Overall, one obtains $p^4 + q^4 = u^2 + v^2 = t = y^2$ with $y \leq y^2 = t \leq t^2 < t^2 + s^2 = c$. This contradicts the choice of (a, b, c). □

Remark 7.9. According to Remark 7.7 and Theorem 7.8, it suffices to prove FLT for every odd prime $n = p$. The idea is to transform the sum $a^p + b^p$ into a product and subsequently compare it with the prime factorization of c^p. For this, let $\zeta := e^{2\pi \mathrm{i}/p} \in \mathbb{C}$. Since p is odd, $-\zeta, -\zeta^2, \ldots, -\zeta^p = -1$ are the roots of the monic polynomial $X^p + 1$, i. e.

$$X^p + 1 = \prod_{i=1}^{p} (X + \zeta^i).$$

We substitute $\frac{a}{b}$ for X and subsequently multiply by b^p:

$$a^p + b^p = \prod_{i=1}^{p} (a + \zeta^i b). \tag{7.2}$$

The factors on the right side lie in the ring

$$R := \mathbb{Z}[\zeta] := \{a_2\zeta^{p-2} + a_3\zeta^{p-3} + \ldots + a_p : a_2, \ldots, a_p \in \mathbb{Z}\}.$$

We restrict ourselves from now on to $p = 3$. Then $\zeta = \frac{1}{2}(-1 + \sqrt{-3})$ holds and $R = \mathbb{Z}_{-3}$ is Euclidean according to Theorem 6.20. For $\alpha = a + b\zeta \in R$, we have

$$N(\alpha) = |\alpha|^2 = (a + b\zeta)(a + b\zeta^2) = a^2 + b^2 - ab.$$

We consider $\lambda := 1 - \zeta \in R$. Because of $N(\lambda) = 3$, λ is a prime element. From $3 = \lambda\overline{\lambda} \equiv 0 \pmod{\lambda}$ and $\zeta \equiv 1 \pmod{\lambda}$, it follows that $R/R\lambda \cong \mathbb{F}_3$.

Lemma 7.10. *For $\alpha \in R = \mathbb{Z}_{-3}$ with $\lambda \nmid \alpha$, we have $\alpha^3 \equiv \pm 1 \pmod{\lambda^4}$.*

Proof. By replacing α with $-\alpha$ if necessary, one can assume $\alpha \equiv 1 \pmod{\lambda}$. Let $\beta \in R$ with $\alpha - 1 = \beta\lambda$. Then it holds that

$$\begin{aligned} \alpha - \zeta &= (\alpha - 1) + \lambda = \lambda(\beta + 1), \\ \alpha - \zeta^2 &= (\alpha - \zeta) + (\zeta - \zeta^2) = \lambda(\beta + 1) + \zeta\lambda = \lambda(\beta - \zeta^2). \end{aligned}$$

It follows

$$\alpha^3 - 1 = (\alpha - 1)(\alpha - \zeta)(\alpha - \zeta^2) = \lambda^3\beta(\beta + 1)(\beta - \zeta^2).$$

Because of $\zeta^2 \equiv 1 \pmod{\lambda}$, the numbers β, $\beta + 1$ and $\beta - \zeta^2$ lie in different residue classes modulo λ. One of the numbers must therefore be divisible by λ. This shows the claim. □

Theorem 7.11 (Euler). *There is no triple* $(a,b,c) \in \mathbb{N}^3$ *with* $a^3+b^3=c^3$.

Proof. Let $R := \mathbb{Z}_{-3}$. We assume more generally that $\alpha, \beta, \gamma \in R \setminus \{0\}$ and $\epsilon \in R^\times$ with $\alpha^3+\beta^3 = \epsilon\gamma^3$ exist. Wlog. let α, β and γ be (pairwise) coprime. First let $\lambda \mid \alpha\beta$. Since λ is a prime element, wlog. $\lambda \mid \alpha$ and $\lambda \nmid \beta$ as well as $\lambda \nmid \gamma$ holds. According to Lemma 7.10, then $\pm\epsilon \equiv \epsilon\gamma^3 = \alpha^3+\beta^3 \equiv \pm 1 \pmod{\lambda^2}$ and $\lambda^2 \mid 1 \pm \epsilon$. In the case $\epsilon \neq \mp 1$, it would be $3 = |\lambda^2| \leq |1 \pm \epsilon| \leq 2$ by the triangle inequality. Thus $\epsilon = \mp 1$ and $\beta^3 + (\pm\gamma)^3 = (-\alpha)^3$. By swapping α and γ, one can therefore assume $\lambda \nmid \alpha\beta$.

Among all such counterexamples, we choose γ such that

$$t := \nu(\gamma) := \max\{n \in \mathbb{N}_0 : \lambda^n \mid \gamma\}$$

is as small as possible. In the case $t = 0$, there exist $e, f \in \{\pm 1\}$ with

$$\pm\epsilon \equiv \epsilon\gamma^3 = \alpha^3+\beta^3 \equiv e+f \pmod{\lambda^4}$$

according to Lemma 7.10. Clearly $e = f$ and $\lambda^4 \mid \epsilon \pm 2$. This yields the contradiction $9 = |\lambda^4| \leq |\epsilon \pm 2| \leq 5$. In the case $t = 1$, it is

$$0 \not\equiv \epsilon\gamma^3 = \alpha^3+\beta^3 \equiv \pm 2 \pmod{\lambda^4}$$

and $\lambda \mid \epsilon\gamma^3 + (\pm 2 - \epsilon\gamma^3) = \pm 2$. This yields the contradiction $3 = N(\lambda) \mid N(2) = 4$. Thus $t \geq 2$ and $\nu(\gamma^3) = 3t \geq 6$.

Equation 7.2 becomes

$$(\alpha+\beta)(\alpha+\beta\zeta)(\alpha+\beta\zeta^2) = \epsilon\gamma^3. \tag{7.3}$$

It follows that $\nu(\alpha+\beta) \geq 2$, $\nu(\alpha+\beta\zeta) \geq 2$ or $\nu(\alpha+\beta\zeta^2) \geq 2$. Wlog. let $\nu(\alpha+\beta) \geq 2$ (otherwise replace β by $\beta\zeta$ or $\beta\zeta^2$, respectively). Because of $\lambda \nmid \beta$, it is then

$$\begin{aligned}\nu(\alpha+\beta\zeta) &= \nu(\alpha+\beta-\beta(1-\zeta)) = \nu(\alpha+\beta-\beta\lambda) = 1,\\ \nu(\alpha+\beta\zeta^2) &= \nu(\alpha+\beta-\beta\lambda(1+\zeta)) = \nu(\alpha+\beta+\beta\lambda\zeta^2) = 1.\end{aligned}$$

This shows $\nu(\alpha+\beta) = 3t-2 \geq 4$. Let $\delta \in R$ be a prime element which is not associated with λ. If δ is a common divisor of $\alpha+\beta$ and $\alpha+\beta\zeta$, then δ also divides $\beta(1-\zeta) = \beta\lambda$. It follows that $\delta \mid \beta$ and $\delta \mid \alpha$ in contradiction to $\gcd(\alpha,\beta) \in R^\times$. Analogously, one sees that δ can divide at most one of the numbers $\alpha+\beta$, $\alpha+\beta\zeta$ and $\alpha+\beta\zeta^2$. The prime factorization of (7.3) therefore yields $\alpha_1, \beta_1, \rho \in R$ and $\epsilon_1, \epsilon_2, \epsilon_3 \in R^\times$ with

$$\alpha+\beta = \epsilon_1\lambda^{3t-2}\rho, \qquad \alpha+\beta\zeta = \epsilon_2\lambda\alpha_1^3, \qquad \alpha+\beta\zeta^2 = \epsilon_3\lambda\beta_1^3$$

and $\lambda \nmid \rho\alpha_1\beta_1$. It follows that

$$0 = (\alpha+\beta) + (\alpha+\beta\zeta)\zeta + (\alpha+\beta\zeta^2)\zeta^2 = \epsilon_1\lambda^{3t-2}\rho^3 + \epsilon_2\lambda\alpha_1^3\zeta + \epsilon_3\lambda\beta_1^3\zeta^2.$$

We set $\gamma_1 := \lambda^{t-1}\rho$. Then there exist $\mu_1, \mu_2 \in R^\times$ with

$$\alpha_1^3 + \mu_1\beta_1^3 = \mu_2\gamma_1^3.$$

Because of $t \geq 2$, $\lambda \mid \gamma_1$ and therefore $0 \equiv \pm\mu_2\gamma_1^3 \equiv 1 \pm \mu_1 \pmod{\lambda^2}$ according to Lemma 7.10. As above, it follows that $\mu_1 = \mp 1$. Thus

$$\alpha_1^3 + (\mp\beta_1)^3 = \mu_2\gamma_1^3$$

with $\nu(\gamma_1) = t-1$ in contradiction to the choice of γ. □

Remark 7.12.

(i) LEGENDRE and DIRICHLET proved FLT for $p = 5$.

(ii) Let $p > 2$ be an arbitrary prime and $\zeta = e^{2\pi i/p}$. For $1 \leq k, l \leq q := \frac{p-1}{2}$ it holds that

$$2k \equiv \pm 2l \pmod{p} \overset{3.6}{\iff} k \equiv \pm l \pmod{p} \iff k = l.$$

Because of

$$(X^{p-1} + \ldots + X + 1)(X - 1) = X^p - 1 = \prod_{k=1}^{p}(X - \zeta^k)$$

it follows that

$$p = \prod_{k=1}^{p-1}(1 - \zeta^k) = \prod_{k=1}^{q}(1 - \zeta^{2k})(1 - \zeta^{-2k}) = \prod_{k=1}^{q}(\zeta^k - \zeta^{-k})(\zeta^{-k} - \zeta^k) = (-1)^q \prod_{k=1}^{q}(\zeta^k - \zeta^k)^2.$$

Thus $\sqrt{(-1)^q p} = \prod_{k=1}^{q}(\zeta^k - \zeta^k) \in \mathbb{Z}[\zeta] = R$. This shows $\mathbb{Z}_p \subseteq R$ if $p \equiv 1 \pmod 4$ and $\mathbb{Z}_{-p} \subseteq R$ otherwise. In the first case $|R^\times| = \infty$ according to Theorem 6.10. This also holds in the second case for $p > 3$ according to DIRICHLET's *unit theorem*.

(iii) LAMÉ had believed he could conduct the proof of Theorem 7.11 for all $p > 2$. LIOUVILLE pointed out, however, that $R = \mathbb{Z}[\zeta]$ is no longer a factorial ring for $p > 19$.

(iv) As an alternative, KUMMER showed that at least all *ideals* in R possess a unique factorization into prime ideals (rings with this property are called *Dedekind domains*). By means of the *class number* it can be precisely measured how far R is from being a factorial ring. Kummer proved FLT for *regular* prime numbers p, i.e., the class number of R is not divisible by p. These prime numbers $p > 2$ can be equivalently characterized by the fact that the numerators of the BERNOULLI *numbers* $B_2, B_4, \ldots, B_{p-3}$ are not divisible by p. The Bernoulli numbers appear as coefficients of the power series

$$\frac{X}{\exp(X) - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} X^n$$

and can be calculated by the recursion formula

$$\sum_{k=0}^{n-1} \binom{n}{k} B_k = 0$$

with the starting value $B_0 = 1$. It holds that $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$ and $B_{2n+1} = 0$ for $n \geq 1$ (the *denominator* of B_{2n} is the product of all prime numbers q with $q - 1 \mid 2n$ according to CLAUSEN and VON STAUDT). Thus FLT holds for $p \leq 31$. Unfortunately, JENSEN has shown that there are infinitely many *irregular* prime numbers (where $p = 37$ is the smallest).

(v) If one considers $a^3 + b^3 = c^3$ modulo 9, one sees $p \mid abc$ (this corresponds to the claim $t \geq 1$ in the proof of Theorem 7.11). For $p > 3$ this reasoning is not possible. One therefore distinguishes between the *first case* ($p \nmid abc$) and the *second case* ($p \mid abc$). In the first case, the principal ideals in the factorization

$$(c)^p = \prod_{i=1}^{p}(a + b\zeta)$$

from (7.2) are coprime. Each of the ideals $(a + b\zeta^i)$ is therefore the p-th power of an ideal. If p is regular, then $(a + b\zeta^i)$ is even the p-th power of a principal ideal. This allows for a similar argumentation as in Theorem 7.11. GERMAIN proved the first case for all prime numbers p for which $2p + 1$ is also a prime number (so-called *Germain primes*).

(vi) FALTINGS proved that for a fixed p only at most finitely many coprime solutions (a, b, c) can exist.

(vii) In 1993 WILES presented a 100-page proof for FLT in full generality. This contained a gap, however, which Wiles together with TAYLOR was able to close one year later. In the proof, FLT is interpreted as an elliptic curve (Definition 10.37) and modular forms are used.

8 The Quadratic Reciprocity Law

Remark 8.1. In Theorem 3.8 and Theorem 3.11 we learned how to solve linear equations or systems of equations in residue class rings. To solve quadratic equations, one must first clarify which residue classes possess a square root. We will derive an extremely simple criterion for this using the Jacobi symbol.

Definition 8.2. Let p be a prime number and $n \in \mathbb{Z} \setminus p\mathbb{Z}$. One calls n a *quadratic residue* modulo p if there exists a $k \in \mathbb{Z}$ with $n \equiv k^2 \pmod{p}$. For $n \in \mathbb{Z}$ one defines the *Legendre symbol*

$$\left(\frac{n}{p}\right) := \begin{cases} 1 & \text{if } n \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } n \text{ is not a quadratic residue modulo } p, \\ 0 & \text{if } p \mid n \end{cases}$$

of n *over* p.

Example 8.3. Obviously $\left(\frac{n}{2}\right) \equiv n \pmod{2}$ holds. One can therefore concentrate on odd prime numbers. For $m \equiv n \pmod{p}$ it is furthermore $\left(\frac{n}{p}\right) = \left(\frac{m}{p}\right)$. Thus one can assume $0 < n < p$.

Lemma 8.4 (EULER criterion)**.** *For every odd prime number p and $n \in \mathbb{Z}$ it holds that*

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

Proof. Wlog. let $p \nmid n$. Because of $n^{p-1} \equiv 1 \pmod{p}$ (Euler-Fermat), $n^{\frac{p-1}{2}} \in \{1, -1\}$, since the equation $x^2 = 1$ has only the solutions ± 1 in the field $\mathbb{F}_p$. Let $\zeta \in \mathbb{F}_p^\times$ be a primitive root. If $\left(\frac{n}{p}\right) = 1$, then $n = \zeta^{2i}$ for some $i \in \mathbb{Z}$. It follows that $n^{\frac{p-1}{2}} = \zeta^{p-1} = 1$. Conversely, let $n = \zeta^i$ with $\gamma^{i\frac{p-1}{2}} = n^{\frac{p-1}{2}} = 1$. According to Lemma 4.13, $p - 1 = \mathrm{ord}_p(\gamma) \mid i\frac{p-1}{2}$. Since p is odd, it follows that $2 \mid i$ and $n = \zeta^i$ is a square. □

Example 8.5 (1st Supplement)**.** From the Euler criterion it follows that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv -1 \pmod{4} \end{cases} \tag{8.1}$$

and $\left(\frac{n}{3}\right) \equiv n \pmod{3}$. For $n, m \in \mathbb{Z}$ it furthermore follows that $\left(\frac{nm}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{m}{p}\right)$. It therefore suffices to calculate $\left(\frac{p}{q}\right)$ for prime numbers p and q.

Lemma 8.6 (2nd Supplement)**.** *For every odd prime number p it holds that*

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

Proof. For $p' := (p-1)/2$, $r := \lfloor p'/2 \rfloor$ and $s := \lfloor (p'-1)/2 \rfloor$ it holds that

$$\begin{aligned}(p'!)^2 &\equiv (-1)^{p'} \prod_{k=1}^{p'} k(p-k) \equiv (-1)^{p'}(p-1)! \equiv (-1)^{p'}\big(1 \cdot 3 \cdot \ldots \cdot (p-2)\big)\big(2 \cdot 4 \cdot \ldots \cdot (p-1)\big) \\ &\equiv (-2)^{p'}(p'!)\big(1 \cdot 3 \cdot \ldots \cdot (p-2)\big) \overset{8.4}{\equiv} (-1)^{p'}\left(\frac{2}{p}\right)(p'!)\big(1 \cdot 3 \cdot \ldots \cdot (2s+1)\big)\big((p-2)\ldots(p-2r)\big) \\ &\equiv (-1)^{p'+r}(p'!)\left(\frac{2}{p}\right)\big(1 \cdot 3 \cdot \ldots \cdot (2s+1)\big)(2 \cdot 4 \cdot \ldots \cdot 2r) \equiv (-1)^{p'+r}(p'!)^2\left(\frac{2}{p}\right) \pmod p.\end{aligned}$$

This shows $\left(\frac{2}{p}\right) = (-1)^{p'+r}$. A simple case distinction yields $p'+r \equiv 0 \pmod 2 \iff p \equiv \pm 1 \pmod 8$. Simultaneously, it holds that

$$\frac{p^2-1}{8} \equiv 0 \pmod 2 \overset{3.6}{\iff} (p-1)(p+1) \equiv p^2 - 1 \equiv 0 \pmod{16} \iff p \equiv \pm 1 \pmod 8. \qquad \square$$

Definition 8.7. Let $p \in \mathbb{P}$ be odd and $a \in \mathbb{Z}$. Then there exists exactly one $r \in \mathbb{Z}$ with $a \equiv r \pmod p$ and $|r| \leq \frac{p-1}{2}$. In the case $r > 0$ (resp. $r < 0$) we call a a *positive* (resp. *negative*) residue modulo p.

Lemma 8.8 (Gauss)**.** *Let $p \in \mathbb{P}$ be odd and $p \nmid a \in \mathbb{Z}$. Let μ be the number of negative residues modulo p among the numbers $a, 2a, \ldots, \frac{p-1}{2}a$. Then $\left(\frac{a}{p}\right) = (-1)^\mu$ holds.*

Proof. Let $p' := \frac{p-1}{2}$. Let $-p' \leq r_1, \ldots, r_\mu \leq -1$ resp. $1 \leq s_1, \ldots, s_{p'-\mu} \leq p'$ be the negative resp. positive residues among the numbers $a, 2a, \ldots, p'a$ (because $p \nmid a$, no residue is 0). Because $ka \not\equiv la \pmod p$ for $1 \leq k < l \leq p'$, the r_i and the s_i are pairwise distinct among themselves. Let us assume $-r_i = s_j$. Then there exist $1 \leq k, l \leq p'$ with $-ka \equiv -r_i \equiv s_j \equiv la \pmod p$. From $(k+l)a \equiv 0 \pmod p$ and $0 \leq k+l \leq 2p' = p-1$ follows the contradiction $k = l$. This shows $\{-r_1, \ldots, -r_\mu, s_1, \ldots, s_{p'-\mu}\} = \{1, \ldots, p'\}$ and

$$(p')! = (-1)^\mu r_1 \ldots r_\mu s_1 \ldots s_{p'-\mu} \equiv (-1)^\mu \prod_{k=1}^{p'} ka \equiv (-1)^\mu a^{p'}(p')! \pmod p.$$

With the Euler criterion, it follows that $\left(\frac{a}{p}\right) \equiv a^{p'} \equiv (-1)^\mu \pmod p$. $\square$

Lemma 8.9. *Let $p \in \mathbb{P}$ be odd and $a \in \mathbb{Z}$ odd with $p \nmid a$. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{ka}{p} \right\rfloor}.$$

Proof. We use the notation from the proof of Lemma 8.8. For $1 \leq k \leq p'$, it holds that $ka = \left\lfloor \frac{ka}{p} \right\rfloor p + r$ with $r \in \{p+r_1, \ldots, p+r_\mu, s_1, \ldots, s_{p'-\mu}\}$ (Euclidean division). Summing up yields

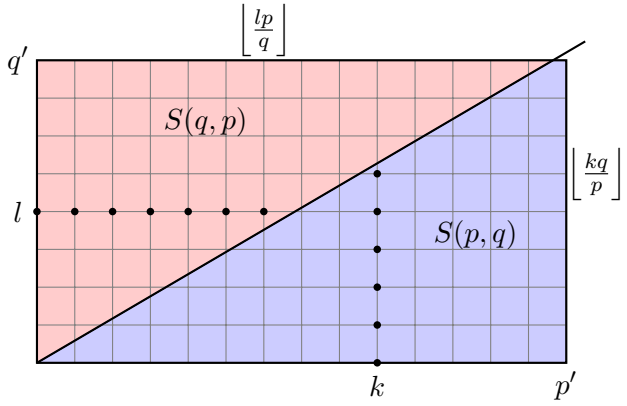
$$a\binom{p'+1}{2} = \sum_{k=1}^{p'} ka = p\sum_{k=1}^{p'} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{i=1}^{\mu}(p+r_i) + \sum_{j=1}^{p'-\mu} s_j = p\sum_{k=1}^{p'} \left\lfloor \frac{ka}{p} \right\rfloor + \mu p + \binom{p'+1}{2}.$$

Since a and p are odd, $\mu \equiv \sum_{k=1}^{p'} \left\lfloor \frac{ka}{p} \right\rfloor \pmod 2$ and the assertion follows from Lemma 8.8. $\square$

Theorem 8.10 (Quadratic Reciprocity Law)**.** *For distinct odd prime numbers p and q, it holds that*

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

Proof (Eisenstein). As before, let $p' := \frac{p-1}{2}$ and $q' := \frac{q-1}{2}$. We count the points with integer coordinates inside the rectangle $(0, p/2) \times (0, q/2) \subseteq \mathbb{R}^2$ in two ways. Obviously, there are exactly $p'q'$ such points, namely (x, y) with $1 \leq x \leq p'$ and $1 \leq y \leq q'$. No points lie on the diagonal $y = \frac{q}{p}x$, because otherwise $pa = qb$ with $a, b \in \mathbb{N}$ and $a < q$ as well as $b < p$. Below the diagonal, the points are distributed on the vertical lines $(k, *)$. The number of points on this line is $\left\lfloor \frac{kq}{p} \right\rfloor$. In total, $S(p, q) := \sum_{k=1}^{p'} \left\lfloor \frac{kq}{p} \right\rfloor$ points lie below the diagonal. An analogous argument with the horizontal lines $(*, k)$ yields exactly $S(q, p)$ points above the diagonal.



This shows $S(p, q) + S(q, p) = p'q'$. With Lemma 8.9 it follows that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S(p,q)+S(q,p)} = (-1)^{p'q'}. \qquad \square$$

Remark 8.11.

(i) According to the reciprocity law, it holds that

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv -1 \pmod 4, \\ \left(\frac{q}{p}\right) & \text{otherwise.} \end{cases} \tag{8.2}$$

In this way, $\left(\frac{n}{p}\right)$ can be calculated for any $n \in \mathbb{Z}$, provided that one knows the prime factorization of n and all smaller numbers. In the following, we show how one can dispense with the (costly) prime factorization.

(ii) More than 300 proofs for the reciprocity law are known. [12]

Definition 8.12. Let $n \in \mathbb{Z}$. Let $a \in \mathbb{N}$ be odd with prime factorization $a = p_1 \dots p_k$ (the case $a = 1$ with $k = 0$ is allowed). One calls

$$\left(\frac{n}{a}\right) := \left(\frac{n}{p_1}\right) \dots \left(\frac{n}{p_k}\right)$$

[12] see Flemmermeyer homepage

the *Jacobi symbol* of n *modulo* a.[13]

Remark 8.13. The Jacobi symbol extends the Legendre symbol. If n is a quadratic residue modulo a, then n is also a quadratic residue modulo p_i for every prime divisor p_i of a. In this case, $\left(\frac{n}{a}\right) = 1$ holds. The converse, however, is false. For example, -1 is not a quadratic residue modulo 9, but $\left(\frac{-1}{9}\right) = \left(\frac{-1}{3}\right)\left(\frac{-1}{3}\right) = 1$. The calculation rules for the Legendre symbol carry over to the Jacobi symbol as follows.

Theorem 8.14. *For $n, m \in \mathbb{Z}$ and odd $a, b \in \mathbb{N}$ it holds:*

(i) $n \equiv m \pmod{a} \Longrightarrow \left(\frac{n}{a}\right) = \left(\frac{m}{a}\right)$.

(ii) $\left(\frac{nm}{a}\right) = \left(\frac{n}{a}\right)\left(\frac{m}{a}\right)$ *and* $\left(\frac{n}{ab}\right) = \left(\frac{n}{a}\right)\left(\frac{n}{b}\right)$.

(iii) $\left(\frac{-1}{a}\right) = \begin{cases} 1 & \text{if } a \equiv 1 \pmod{4}, \\ -1 & \text{if } a \equiv -1 \pmod{4}. \end{cases}$

(iv) $\left(\frac{2}{a}\right) = \begin{cases} 1 & \text{if } a \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } a \equiv \pm 3 \pmod{8}. \end{cases}$

(v) $\left(\frac{a}{b}\right) = \begin{cases} -\left(\frac{b}{a}\right) & \text{if } a \equiv b \equiv -1 \pmod{4}, \\ \left(\frac{b}{a}\right) & \text{otherwise.} \end{cases}$

Proof. Let $a = p_1 \dots p_k$ and $b = q_1 \dots q_l$ be the prime factorizations of a and b.

(i) According to Example 8.3, $\left(\frac{n}{a}\right) = \left(\frac{n}{p_1}\right) \dots \left(\frac{n}{p_k}\right) = \left(\frac{m}{p_1}\right) \dots \left(\frac{m}{p_k}\right) = \left(\frac{m}{a}\right)$.

(ii) According to Example 8.5,

$$\left(\frac{nm}{a}\right) = \left(\frac{nm}{p_1}\right) \dots \left(\frac{nm}{p_k}\right) = \left(\frac{n}{p_1}\right)\left(\frac{m}{p_1}\right) \dots \left(\frac{n}{p_k}\right)\left(\frac{m}{p_k}\right) = \left(\frac{n}{a}\right)\left(\frac{m}{a}\right).$$

The second equation follows directly from the definition.

(iii) For $r := |\{1 \le i \le k : p_i \equiv -1 \pmod{4}\}|$, it holds that

$$a - 1 \equiv (-1)^r - 1 \equiv 2r \equiv \sum_{i=1}^{k} (p_i - 1) \pmod{4}.$$

This shows $\frac{a-1}{2} \equiv \sum_{i=1}^{k} \frac{p_i - 1}{2} \pmod{2}$ according to Lemma 3.6. From (8.1) it follows that

$$\left(\frac{-1}{a}\right) = \left(\frac{-1}{p_1}\right) \dots \left(\frac{-1}{p_k}\right) = \prod_{i=1}^{k} (-1)^{\frac{p_i - 1}{2}} = (-1)^{\sum_{i=1}^{k} \frac{p_i - 1}{2}} = (-1)^{\frac{a-1}{2}}.$$

(iv) For $r := |\{1 \le i \le k : p_i \equiv \pm 3 \pmod{8}\}|$, it holds that

$$a^2 - 1 \equiv 9^r - 1 \equiv 8r \equiv \sum_{i=1}^{k} (p_i^2 - 1) \pmod{16}$$

[13] The more general *Kronecker symbol* also allows even denominators, although the property $n \equiv m \pmod{a} \Longrightarrow \left(\frac{n}{a}\right) = \left(\frac{m}{a}\right)$ is lost.

and $\frac{a^2-1}{8} \equiv \sum_{i=1}^{k} \frac{p_i^2-1}{8} \pmod 2$. From Lemma 8.6 it follows that

$$\left(\frac{2}{a}\right) = \left(\frac{2}{p_1}\right) \dots \left(\frac{2}{p_k}\right) = \prod_{i=1}^{k} (-1)^{\frac{p_i^2-1}{8}} = (-1)^{\sum_{i=1}^{k} \frac{p_i^2-1}{8}} = (-1)^{\frac{a^2-1}{8}}.$$

(v) Wlog. let $\gcd(a,b) = 1$, because otherwise both sides are 0. As in (iii), it holds that

$$\begin{aligned}\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) &\overset{\text{(ii)}}{=} \prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}} \\ &= (-1)^{\sum_{i=1}^{k}\frac{p_i-1}{2}\sum_{j=1}^{l}\frac{q_j-1}{2}} = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}.\end{aligned}$$

□

Remark 8.15. Let $n \in \mathbb{Z}$ and $a \in \mathbb{N}$ be odd. The following algorithm computes $\left(\frac{n}{a}\right)$:

(1) Set $\epsilon := 1$.

(2) As long as $a > 1$ repeat:

- Reduce n modulo a, such that $|n| \leq \frac{a-1}{2}$.
- If $n = 0$, then output 0. End.
- If $n < 0$, then
  - replace n by $-n$ (now $n \in \mathbb{N}$),
  - if $a \equiv -1 \pmod 4$, then multiply ϵ by -1.
- As long as $4 \mid n$, divide n by 4.
- If $2 \mid n$, then
  - divide n by 2 (now n is odd),
  - if $a \equiv \pm 3 \pmod 8$, then multiply ϵ by -1.
- Swap n and a.
- If $n \equiv a \equiv -1 \pmod 4$, then multiply ϵ by -1.

(3) Output: ϵ.

The runtime is logarithmic in the input, as with the Euclidean algorithm (Exercise 5). The condition $a \equiv 1 \pmod 4$ (or $a \equiv \pm 1 \pmod 8$) can be read from the last two (or three) decimal digits of a, because $4 \mid 100$ (or $8 \mid 1000$).

Example 8.16. Because of

$$\begin{aligned}\left(\frac{12346}{7787}\right) &= \left(\frac{-3408}{7787}\right) = -\left(\frac{3408}{7787}\right) = -\left(\frac{852}{7787}\right) = -\left(\frac{213}{7787}\right) = -\left(\frac{7787}{213}\right) = -\left(\frac{-94}{213}\right) \\ &= -\left(\frac{94}{213}\right) = \left(\frac{47}{213}\right) = \left(\frac{213}{47}\right) = \left(\frac{-22}{47}\right) = -\left(\frac{22}{47}\right) = -\left(\frac{11}{47}\right) = \left(\frac{47}{11}\right) = \left(\frac{3}{11}\right) \\ &= -\left(\frac{11}{3}\right) = -\left(\frac{-1}{3}\right) = \left(\frac{1}{3}\right) = 1\end{aligned}$$

12346 is a quadratic residue modulo the prime number 7787.

Remark 8.17. In the following, we use the Jacobi symbol to construct primality tests for Mersenne and Fermat prime numbers. In Remark 2.13, we have verified the prime divisor $641 = 5 \cdot 2^7 + 1$ of $F_5 = 2^{2^5} + 1$.

Theorem 8.18 (Lucas)**.** *Let $n \geq 2$. For every prime divisor p of F_n, $2^{n+2} \mid p - 1$ holds.*

Proof. Certainly $p > 2$. From $2^{2^n} \equiv -1 \pmod{p}$, it follows that $2^{n+1} = \operatorname{ord}_p(2) \mid p - 1$. Because $p \equiv 1 \pmod{2^{n+1}}$, we have $p \equiv 1 \pmod 8$ and $\left(\frac{2}{p}\right) = 1$ by the second supplementary law. Euler's criterion shows $2^{\frac{p-1}{2}} = 1 \pmod{p}$, i. e. $2^{n+1} = \operatorname{ord}_p(2) \mid \frac{p-1}{2}$. Thus 2^{n+2} is a divisor of $p - 1$. □

Theorem 8.19 (Pépin-Test)**.** *Let $n \in \mathbb{N}$. F_n is a prime number if and only if $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ holds.*

Proof. Let $F_n \in \mathbb{P}$. According to Euler's criterion and the reciprocity law, we have

$$3^{(F_n-1)/2} \equiv \left(\frac{3}{F_n}\right) \equiv \left(\frac{F_n}{3}\right) \equiv \left(\frac{4^{2^{n-1}} + 1}{3}\right) \equiv \left(\frac{2}{3}\right) \equiv -1 \pmod{F_n}.$$

Conversely, let $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ and p be a prime divisor of F_n. From $3^{F_n-1} \equiv 1 \pmod{p}$, it follows that $2^{2^n} = F_n - 1 = \operatorname{ord}_p(3) \mid p - 1$. This shows $F_n \leq p \leq F_n$, i. e. $F_n = p \in \mathbb{P}$. □

Theorem 8.20. *Let $p \equiv 3 \pmod 4$ be a Germain prime (i. e. $2p + 1 \in \mathbb{P}$). Then $2p + 1 \mid M_p$. In particular, $M_p \notin \mathbb{P}$ if $p > 3$.*

Proof. Let $q := 2p + 1 \in \mathbb{P}$. According to Euler-Fermat,

$$M_p(M_p + 2) = (2^p - 1)(2^p + 1) = 2^{q-1} - 1 \equiv 0 \pmod{q}.$$

Suppose $q \mid M_p + 2$. Then

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

From the second supplementary law, it follows that $2p + 1 = q \equiv \pm 3 \pmod 8$ and $p \equiv 1 \pmod 4$ in contradiction to the assumption. Thus $q \mid M_p$. In the case $p > 3$, $q < M_p \notin \mathbb{P}$. □

Example 8.21. From Theorem 8.20, it follows that $M_p \notin \mathbb{P}$ for $p = 11, 23, 83, 131, \ldots$.

Theorem 8.22. *Let $p \in \mathbb{P}$ be odd and d be a divisor of M_p. Then $d \equiv \pm 1 \pmod 8$ and $d \equiv 1 \pmod{p}$ hold.*

Proof. Wlog. let $d \in \mathbb{P} \setminus \{2\}$. From $2^p \equiv 1 \pmod{d}$ it follows that $1 \neq \operatorname{ord}_d(2) \mid p$ and $p = \operatorname{ord}_d(2) \mid \varphi(d) = d - 1$. Thus $d \equiv 1 \pmod{p}$ holds. Because $p > 2$, there exists a $k \in \mathbb{N}$ with $d - 1 = 2kp$. From Euler's criterion it follows that

$$\left(\frac{2}{d}\right) \equiv 2^{\frac{d-1}{2}} \equiv 2^{kp} \equiv 1 \pmod{d}.$$

The second supplement yields $d \equiv \pm 1 \pmod 8$. □

Example 8.23. As a prime divisor of M_{13}, according to Theorem 8.22, only 79 comes into consideration, because $\sqrt{M_{13}} < 91$. However, $79 \nmid M_{13}$ and M_{13} must be a prime number.

Definition 8.24. The LUCAS *sequence* is defined by $L_0 := 4$, $L_{k+1} := L_k^2 - 2$ for $k \geq 0$.

Remark 8.25.

(i) In the following, we consider the Euclidean ring $\mathbb{Z}_3 = \mathbb{Z} + \mathbb{Z}\sqrt{3}$ (Theorem 6.20) with $\omega := 2 + \sqrt{3}$. Because $N(\omega) = \omega\omega^* = (2+\sqrt{3})(2-\sqrt{3}) = 1$, ω is invertible. Obviously, $\omega + \omega^* = 4 = L_0$ holds. Let $\omega^{2^k} + (\omega^*)^{2^k} = L_k$ be shown inductively. Then

$$L_{k+1} = L_k^2 - 2 = \omega^{2^{k+1}} + 2(\omega\omega^*)^{2^k} + (\omega^*)^{2^{k+1}} - 2 = \omega^{2^{k+1}} + (\omega^*)^{2^{k+1}}.$$

Thus $\omega^{2^k} + (\omega^*)^{2^k} = L_k$ holds for all $k \in \mathbb{N}_0$.

(ii) For a prime number q, let $\mathbb{Z}_3 q = \mathbb{Z}q + \mathbb{Z}q\sqrt{3}$. One easily shows that the residue classes modulo $\mathbb{Z}_3 q$ form the ring

$$R_q := \mathbb{Z}_3/\mathbb{Z}_3 q = \mathbb{F}_q + \mathbb{F}_q\sqrt{3}.$$

The map $\mu\colon \mathbb{Z}_3 \to R_q$, $x \mapsto x + \mathbb{Z}_3 q$ is obviously a ring homomorphism, i. e. $\mu(x \dot{+} y) = \mu(x) \dot{+} \mu(y)$ for all $x, y \in \mathbb{Z}_3$. In the following, we use that $\operatorname{Ker}(\mu) \cap \mathbb{Z} = q\mathbb{Z}$. Since 0 is not invertible, $|R_q^\times| \leq |R| - 1 = q^2 - 1$ holds. As in the proof of Euler-Fermat, one shows $x^{|R_q^\times|} = 1$ for all $x \in R_q^\times$. In particular, the order of x is bounded by $q^2 - 1$ (cf. Lemma 4.13).

Theorem 8.26 (LUCAS-LEHMER test)**.** *Let $p \in \mathbb{P}\setminus\{2\}$. M_p is a prime number if and only if $M_p \mid L_{p-2}$.*

Proof.

$\Leftarrow$: Let $kM_p = L_{p-2} = \omega^{2^{p-2}} + (\omega^*)^{2^{p-2}}$ for a $k \in \mathbb{Z}$ with the notation from Remark 8.25. Then it follows that

$$\omega^{2^{p-1}} = (kM_p - (\omega^*)^{2^{p-2}})\omega^{2^{p-2}} = kM_p\omega^{2^{p-2}} - 1.$$

Assume $M_p \notin \mathbb{P}$. For the smallest prime divisor q of M_p, it then holds that $q^2 \leq M_p$. Since M_p is odd, q is also odd. Because $\mu(M_p) = 0 \in R_q$, it holds that

$$\mu(\omega^{2^{p-1}}) = \mu(M_p)\mu(k\omega^{2^{p-2}}) - \mu(1) = -1 \in R_q \setminus \{1\}.$$

Thus ω has the order 2^p in R_q. Remark 8.25 yields the contradiction $2^p \leq q^2 - 1 \leq M_p - 1 = 2^p - 2$.

$\Rightarrow$: Let $p = 2k + 1$ and $q := M_p \in \mathbb{P}$. Then $M_p = 2^p - 1 = 2 \cdot 4^k - 1 \equiv 1 \pmod 3$. According to Euler's criterion and the law of quadratic reciprocity, it holds that

$$3^{\frac{q-1}{2}} \equiv \left(\frac{3}{q}\right) \equiv -\left(\frac{q}{3}\right) \equiv -\left(\frac{1}{3}\right) \equiv -1 \pmod q.$$

By the second supplement, we have

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

Together this results in

$$6^{\frac{q-1}{2}} \equiv 2^{\frac{q-1}{2}} 3^{\frac{q-1}{2}} \equiv -1 \pmod q. \tag{8.3}$$

In particular, $\mu(6) \in R_q^\times$. Furthermore, in R_q it holds that

$$(3+\sqrt{3})^q \overset{3.5}{\equiv} 3^q + \sqrt{3}^q \overset{4.8}{\equiv} 3 + \sqrt{3} \cdot 3^{\frac{q-1}{2}} \equiv 3 - \sqrt{3} \pmod{q}$$

Because $(3+\sqrt{3})^2 = 9+3+6\sqrt{3} = 6\omega$, it follows that

$$6 = (3+\sqrt{3})(3-\sqrt{3}) \equiv (3+\sqrt{3})^{q+1} = (6\omega)^{\frac{q+1}{2}} \equiv 6\omega(6\omega)^{\frac{q-1}{2}} \overset{(8.3)}{\equiv} -6\omega^{\frac{q+1}{2}} \pmod{q}.$$

Since $\mu(6) \in R_q^\times$, one may divide by 6 and obtains $\omega^{\frac{q+1}{2}} \equiv -1 \pmod{q}$. From $\omega\omega^* = 1$, it finally follows that

$$L_{p-2} \overset{8.25}{=} \omega^{2^{p-2}} + (\omega^*)^{2^{p-2}} = \omega^{\frac{q+1}{4}} + (\omega^*)^{\frac{q+1}{4}} \equiv \left(\omega^{\frac{q+1}{2}} + 1\right)(\omega^*)^{\frac{q+1}{4}} \equiv 0 \pmod{q}. \qquad \square$$

Example 8.27. In practice, it suffices to calculate the Lucas sequence modulo M_p. For $p = 17$, for example:

k	0	1	2	3	4	5	6	7
$L_k \pmod{M_{17}}$	4	14	194	37634	95799	119121	66179	53645
k	8	9	10	11	12	13	14	15
$L_k \pmod{M_{17}}$	122218	126220	70490	69559	99585	78221	130559	0

Because $L_{15} \equiv 0 \pmod{M_{17}}$, $M_{17} \in \mathbb{P}$.

9 Dirichlet's Prime Number Theorem

Remark 9.1. As is well known, there exist infinitely many odd prime numbers p, i. e. $p \equiv 1 \pmod 2$. In Theorem 2.9 we proved that infinitely many prime numbers have the form $p \equiv 3 \pmod 4$. Dirichlet proved in 1837 that for coprime natural numbers a, d there exist infinitely many prime numbers $p \equiv a \pmod d$. His proof uses deep-seated properties of the Riemann ζ-function and it was long believed that no "elementary" proof (i. e. without function theory) could exist. Such a proof was only found in 1949 by Selberg. Since Selberg's proof is significantly longer and more technical, we follow an analytical approach that manages with elementary properties of the complex logarithm (inspired by Chapman). Only knowledge of Analysis 1 to the extent of Forster's book "Analysis 1" is required.

Definition 9.2. For $s \in \mathbb{R}$ with $s > 1$ we define the *Riemann ζ-function*

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

Remark 9.3. Because of

$$\sum_{n=1}^{\infty} \frac{1}{n^s} \leq 1 + \frac{1}{2^s} + \frac{1}{2^s} + 4\frac{1}{4^s} + \ldots = \sum_{n=0}^{\infty} 2^{n(1-s)} = \frac{1}{1-2^{1-s}} < \infty$$

$\zeta(s)$ converges for $s > 1$. For $s = 1$, however, one obtains the harmonic series $\sum_{n=1}^{\infty} \frac{1}{n} = \infty$.

Lemma 9.4. *For $s > 1$ it holds that $\frac{1}{s-1} < \zeta(s) < \frac{s}{s-1}$. In particular,*

$$\lim_{s\to 1}(s-1)\zeta(s) = 1. \tag{9.1}$$

Proof. For $n \in \mathbb{N}$ it holds that $\frac{1}{n+1} < \int_n^{n+1} x^{-n}\mathrm{d}x < \frac{1}{n}$ (keyword: step function). Summing over n yields

$$\zeta(s) - 1 = \sum_{n=2}^{\infty} \frac{1}{n^s} < \int_1^{\infty} x^{-s}\mathrm{d}x < \zeta(s).$$

We calculate

$$\int_1^{\infty} x^{-s}\mathrm{d}x = \lim_{n\to\infty}\int_1^n x^{-s}\mathrm{d}x = -\lim_{n\to\infty}\frac{x^{-s+1}}{s-1}\Big|_1^n = \frac{1}{s-1}.$$

The claim follows easily from this. □

Theorem 9.5. *Let A be a finite abelian group and $\hat{A} := \mathrm{Hom}(A, \mathbb{C}^\times)$ the set of homomorphisms $A \to \mathbb{C}^\times$. Then:*

(i) By pointwise multiplication, $\hat{A}$ is an abelian group of order $|A|$, which is closed under complex conjugation.

(ii) For $B \leq A$, the restriction map $\hat{A} \to \hat{B}$ is an epimorphism. In particular, every $\lambda \in \hat{B}$ has exactly $|A : B|$ extensions to A.

(iii) For $\lambda, \mu \in \hat{A}$, the first orthogonality relation *holds:*

$$\sum_{a\in A} \lambda(a)\overline{\mu(a)} = \begin{cases} |A| & \text{if } \lambda = \mu, \\ 0 & \text{if } \lambda \neq \mu. \end{cases}$$

(iv) For $a, b \in A$, the second orthogonality relation *holds:*

$$\sum_{\lambda\in\hat{A}} \lambda(a)\overline{\lambda(b)} = \begin{cases} |A| & \text{if } a = b, \\ 0 & \text{if } a \neq b. \end{cases}$$

Proof.

(i) For $\lambda, \mu \in \hat{A}$, $\lambda\mu \in \hat{A}$ with $(\lambda\mu)(a) := \lambda(a)\mu(a)$ for $a \in A$. Obviously, $\hat{A}$ becomes an abelian group in this way. According to the fundamental theorem of finite abelian groups, there exist $a_1, \ldots, a_n \in A$ with $A = \langle a_1\rangle \oplus \ldots \oplus \langle a_n\rangle$. Let $d_i := |\langle a_i\rangle|$ for $i = 1, \ldots, n$. For $\lambda \in \hat{A}$, it holds that $\lambda(a_i)^{d_i} = \lambda(a_i^{d_i}) = \lambda(1) = 1$, i.e., $\lambda(a_i)$ is a d_i-th root of unity. In particular, there are at most d_i possibilities for $\lambda(a_i)$. Since λ is uniquely determined by the images of $a_1, \ldots, a_n$, it follows that $|\hat{A}| \leq d_1 \ldots d_n = |A|$. Every element in A can be uniquely written in the form $a_1^{k_1} \ldots a_n^{k_n}$ with $0 \leq k_i \leq d_i - 1$ for $i = 1, \ldots, n$. Let $\zeta_i \in \mathbb{C}$ be a d_i-th root of unity. Then

$$\lambda(a_1^{k_1} \ldots a_n^{k_n}) := \zeta_1^{k_1} \ldots \zeta_n^{k_n}$$

defines a homomorphism $A \to \mathbb{C}^\times$. Different choices of ζ_i define different λ. This shows $|\hat{A}| \geq |A|$. For $\lambda \in \hat{A}$, $\overline{\lambda} \in \hat{A}$ is also defined by $\overline{\lambda}(a) := \overline{\lambda(a)}$ for $a \in A$.

(ii) The restriction $\Gamma\colon \hat{A} \to \hat{B}$, $\lambda \mapsto \lambda_{|B}$ is obviously a homomorphism. For $\lambda \in \mathrm{Ker}(\Gamma)$, it holds that $B \leq \mathrm{Ker}(\lambda)$. According to the isomorphism theorem, λ can be interpreted as an element of $\widehat{A/B}$. Conversely, every $\hat{\lambda} \in \widehat{A/B}$ defines an element of $\mathrm{Ker}(\Gamma)$ via $a \mapsto \hat{\lambda}(aB)$. From (i) it follows that $|\mathrm{Ker}(\Gamma)| = |\widehat{A/B}| = |A/B|$. According to the isomorphism theorem,

$$|\Gamma(A)| = |\hat{A} : \mathrm{Ker}(\Gamma)| = \frac{|A|}{|A/B|} = |B| = |\hat{B}|,$$

i.e., Γ is surjective. The second statement follows because the preimage of λ is a coset modulo $\mathrm{Ker}(\Gamma)$.

(iii) In the case $\lambda = \mu$, $\lambda(a)\overline{\mu(a)} = |\lambda(a)|^2 = 1$, since $\lambda(a)$ is a root of unity. We can therefore assume $\lambda \neq \mu$. Then there exists a $b \in A$ with $\lambda(b)\overline{\mu(b)} \neq 1$. From

$$\lambda(b)\overline{\mu(b)} \sum_{a\in A} \lambda(a)\overline{\mu(a)} = \sum_{a\in A} \lambda(ab)\overline{\mu(ab)} = \sum_{a\in A} \lambda(a)\overline{\mu(a)}$$

the assertion follows.

(iv) Since the values of $\lambda \in \hat{A}$ are roots of unity, $\overline{\lambda(a)} = \lambda(a^{-1})$ holds. We can therefore assume $b = 1$. For $a = 1$, the assertion is trivial. So let $a \neq 1$ and $B := \langle a \rangle$. According to (ii), it holds that

$$\sum_{\lambda\in\hat{A}} \lambda(a) = |A/B| \sum_{\mu\in\hat{B}} \mu(a).$$

Let $k := |B|$ and $\zeta \in \mathbb{C}^\times$ be a primitive k-th root of unity. The proof of (i) shows

$$\sum_{\mu\in\hat{B}} \mu(a) = 1 + \zeta + \ldots + \zeta^{k-1} = \frac{1-\zeta^k}{1-\zeta} = 0. \qquad \square$$

Definition 9.6. In the following, let $d \geq 2$ always be a natural number. A function $\chi\colon \mathbb{Z} \to \mathbb{C}$ is called a *Dirichlet character* modulo d if for all $a, b \in \mathbb{Z}$ it holds that

- $\chi(a) = 0 \iff \gcd(a, d) > 1$,
- $\chi(ab) = \chi(a)\chi(b)$,
- $\chi(a + d) = \chi(a)$.

Let the set of Dirichlet characters modulo d be Ψ_d. The *L-series* associated with χ is defined by

$$L(s, \chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

for $s \in \mathbb{R}$ with $s > 1$.

Remark 9.7.

(i) Let $A := (\mathbb{Z}/d\mathbb{Z})^\times$. By restriction, one obtains a monomorphism $\Gamma\colon \Psi_d \to \hat{A} = \mathrm{Hom}(A, \mathbb{C}^\times)$. Since every homomorphism $\lambda \in \hat{A}$ can be extended to a Dirichlet character by setting $\lambda(n) := 0$ for $\gcd(n, d) > 1$, Γ is an isomorphism. In particular, $|\Psi_d| = |\hat{A}| = |A| = \varphi(d)$ according to Theorem 9.5.

(ii) With $\chi \in \Psi_d$, we also have $\overline{\chi} \in \Psi_d$ according to Theorem 9.5. In the case $\chi = \overline{\chi}$, we call χ *real*. If applicable, $\chi(\mathbb{Z}) \subseteq \{0, \pm 1\}$ holds. The *trivial* Dirichlet character χ_0 with values 0 and 1 is real.

(iii) For $\chi \in \Psi_d$ and $s > 1$, it holds that

$$\sum_{n=1}^{\infty} \frac{|\chi(n)|}{n^s} \leq \zeta(s).$$

Therefore, $L(s, \chi)$ is absolutely convergent.

Lemma 9.8 (Euler product)**.** *For every Dirichlet character χ and $s > 1$, it holds that*

$$L(s, \chi) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \chi(p)p^{-s}}. \tag{9.2}$$

Proof. Let $\mathbb{P}_N := \{p \in \mathbb{P} : p \leq N\} = \{p_1, \ldots, p_t\}$. Let Z_N be the set of natural numbers whose prime factors lie in $\mathbb{P}_N$. According to the Cauchy product for absolutely convergent series, it holds that

$$\prod_{p \in \mathbb{P}_N} \frac{1}{1 - \chi(p)p^{-s}} = \prod_{i=1}^{t} \sum_{k=0}^{\infty} \frac{\chi(p_i^k)}{p_i^{ks}} = \sum_{k=0}^{\infty} \sum_{k_1 + \ldots + k_t = k} \frac{\chi(p_1^{k_1} \ldots p_t^{k_t})}{(p_1^{k_1} \ldots p_t^{k_t})^s} = \sum_{n \in Z_N} \frac{\chi(n)}{n^s},$$

where the order of the numbers in Z_N does not matter due to absolute convergence. The claim follows with $N \to \infty$. □

Example 9.9. Obviously, $\zeta(s) = \prod_{p \in \mathbb{P}} \frac{1}{1-p^{-s}}$ also holds for $s > 1$. For the trivial Dirichlet character $\chi_0 \in \Psi_d$, it follows that

$$L(s, \chi_0) = \prod_{\substack{p \in \mathbb{P} \\ p \nmid d}} \frac{1}{1 - p^{-s}} = \zeta(s) \prod_{\substack{p \in \mathbb{P} \\ p \mid d}} \frac{p^s - 1}{p^s}$$

and

$$\lim_{s \to 1} L(s, \chi_0)(s-1) = \lim_{s \to 1} \zeta(s)(s-1) \lim_{s \to 1} \prod_{p \mid d} \frac{p^s - 1}{p^s} \overset{(9.1)}{=} \frac{\varphi(d)}{d}. \tag{9.3}$$

In particular, $\lim_{s \to 1} L(s, \chi_0) = \infty$. We will see that non-trivial Dirichlet characters behave differently.

Theorem 9.10. *For $s > 1$, it holds that*

$$\prod_{\chi \in \Psi_d} L(s, \chi) \geq 1. \tag{9.4}$$

Proof. According to (9.2), it holds that

$$P := \prod_{\chi \in \Psi_d} L(s, \chi) = \prod_{\substack{p \in \mathbb{P} \\ p \nmid d}} \prod_{\chi \in \Psi_d} \frac{1}{1 - \chi(p)p^{-s}}$$

(note $|\Psi_d| = \varphi(d) < \infty$). Let e be the order of $p + d\mathbb{Z} \in (\mathbb{Z}/d\mathbb{Z})^\times$ and $f := \varphi(d)/e$. According to Theorem 9.5(ii) (applied to $\langle p + d\mathbb{Z} \rangle \leq (\mathbb{Z}/d\mathbb{Z})^\times$), the numbers $\{\chi(p) : \chi \in \Psi_d\}$ run through all e-th

roots of unity and each root of unity occurs exactly f times. For a primitive e-th root of unity $\omega \in \mathbb{C}$, it holds that $X^e - 1 = \prod_{k=1}^{e}(X - \omega^k)$. This shows

$$\prod_{\chi \in \Psi_d} \frac{1}{1 - \chi(p)p^{-s}} = \Big(\prod_{k=1}^{e} \frac{p^s}{p^s - \omega^k}\Big)^f = \frac{p^{sef}}{(p^{se} - 1)^f} > 1.$$

Thus $P \geq 1$. □

Lemma 9.11 (ABELian Summation)**.** *Let $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{C}$ and $A_k := \sum_{i=1}^{k} a_i$. Then it holds that*

$$\sum_{k=1}^{n} a_k b_k = A_n b_n + \sum_{k=1}^{n-1} A_k (b_k - b_{k+1}). \tag{9.5}$$

Proof. Induction on n: For $n = 1$, we have $\sum_{k=1}^{n} a_k b_k = A_1 b_1$. Now let $n \geq 1$. Then it holds that

$$\begin{aligned}\sum_{k=1}^{n} a_k b_k &= A_{n-1} b_{n-1} + \sum_{k=1}^{n-2} A_k (b_k - b_{k+1}) + a_n b_n = \sum_{k=1}^{n-1} A_k (b_k - b_{k+1}) + A_{n-1} b_n + a_n b_n \\ &= A_n b_n + \sum_{k=1}^{n-1} A_k (b_k - b_{k+1}).\end{aligned}$$

□

Corollary 9.12. *Let $a_1, a_2, \ldots \in \mathbb{C}$ such that the partial sums $A_n := \sum_{k=1}^{n} a_k$ are bounded. Let $b_1, b_2, \ldots \in \mathbb{R}$ be a monotonically decreasing sequence converging to zero. Then $\sum_{n=1}^{\infty} a_n b_n$ converges.*

Proof. Let $|A_n| \leq C$ for all $n \in \mathbb{N}$. For $n \leq m$, it holds that

$$\Big|\sum_{k=n}^{m} a_k b_k\Big| \overset{(9.5)}{\leq} |A_m - A_{n-1}| b_m + \sum_{k=n}^{m-1} |A_k - A_{n-1}| \underbrace{(b_k - b_{k+1})}_{\geq 0} \leq 2C b_n.$$

Because of $\lim_{n\to\infty} b_n = 0$, the partial sums $\sum_{k=1}^{n} a_k b_k$ form a Cauchy sequence. □

Definition 9.13. Continuity and differentiability of complex functions $f\colon \mathbb{C} \to \mathbb{C}$ are defined as in the real case:

- We say f *converges* at the point $z \in \mathbb{C}$ to $a \in \mathbb{C}$, if

  $$\forall \epsilon > 0\, \exists \delta > 0\, \forall w \in \mathbb{C} \setminus \{z\} : |z - w| < \delta \Longrightarrow |f(z) - a| < \epsilon.$$

  If applicable, we write $\lim_{w\to z} f(w) = a$.

- f is called *continuous* at the point $z \in \mathbb{C}$, if $\lim_{w\to z} f(w) = f(z)$ holds. If f is continuous at every point of the domain, then f is called *continuous*.

- f is called *differentiable* (or *holomorphic*) at the point $z \in \mathbb{C}$, if

  $$f'(z) := \lim_{w\to z} \frac{f(z) - f(w)}{z - w}$$

  exists. If applicable, $f'(z)$ is called the *derivative* of f at z. If f is differentiable at every point of the domain, then f is called *differentiable* (or *holomorphic*).

Remark 9.14. If f is differentiable at z, then f is also continuous at z. The usual differentiation rules hold for complex functions just as in the real case. In particular, $(fg)' = f'g + fg'$ (product rule) and $(f \circ g)' = (f' \circ g)g'$ (chain rule) for differentiable functions $f, g\colon \mathbb{C} \to \mathbb{C}$.

Example 9.15. As is well known, the *exponential function*

$$\exp\colon \mathbb{C} \to \mathbb{C}^\times, \qquad z \mapsto \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

is differentiable with $\exp' = \exp$. For $z \in \mathbb{C}$, $\exp(z) = e^z$ holds, where $e := \exp(1) \approx 2{,}718$ is *Euler's number*. The restriction $\exp\colon \mathbb{R} \to \mathbb{R}_{>0}$ is surjective and strictly monotonically increasing. It possesses a differentiable inverse function, the *natural logarithm* $\ln\colon \mathbb{R}_{>0} \to \mathbb{R}$.

Remark 9.16. From the Cauchy product of absolutely convergent series, it follows that

$$\exp(z + w) = \exp(z)\exp(w)$$

for $z, w \in \mathbb{C}$. By induction, one obtains $\exp(z_1 + \ldots + z_n) = \exp(z_1) \ldots \exp(z_n)$ for $z_1, \ldots, z_n \in \mathbb{C}$. From the continuity of exp, it follows that

$$\exp\Big(\sum_{k=1}^{\infty} z_k\Big) = \prod_{k=1}^{\infty} \exp(z_k) \tag{9.6}$$

for every convergent series $\sum_{k=1}^{\infty} z_k$.

Theorem 9.17. *Let $\chi \in \Psi_d \setminus \{\chi_0\}$. Then $L(s, \chi)$ is continuous on $[1, \infty)$ with $L(1, \chi) \neq 0$.*

Proof (Monsky). For $n \in \mathbb{N}$ and $s \geq 1$ let $a_n := \chi(n)$ and $b_n := \frac{1}{n^s}$. According to the first orthogonality relation (Theorem 9.5), it holds that

$$A_d := \sum_{n=1}^{d} a_n = \sum_{n=1}^{d} \chi(n)\chi_0(n) = 0$$

and it follows that

$$|A_k| \leq \sum_{n=d\lfloor k/d \rfloor + 1}^{k} |\chi(n)| \leq d$$

for all $k \in \mathbb{N}$. The proof of Corollary 9.12 shows

$$\Big|L(s, \chi) - \sum_{n=1}^{N-1} \frac{\chi(n)}{n^s}\Big| \leq \Big|\sum_{n=N}^{\infty} a_n b_n\Big| \leq \frac{2d}{N^s} \leq \frac{2d}{N}.$$

Therefore, the partial sums of $L(s, \chi)$ converge uniformly towards $L(s, \chi)$ for $s \geq 1$. In particular, $L(s, \chi)$ is continuous on $[0, \infty)$.

Now let us assume $L(1, \chi) = 0$.

Case 1: $\overline{\chi} \neq \chi$.
For $f\colon \mathbb{R}_{\geq 1} \to \mathbb{R}$, $x \mapsto x^{-1} - x^{-s}$ it holds that

$$f'(x) \leq 0 \iff sx^{-s-1} - x^{-2} \leq 0 \iff x \geq s^{\frac{1}{s-1}} =: t,$$

where $t = 1$ for $s = 1$. Therefore, f is monotonically decreasing for $x \geq t$.[14] In particular, $b_n := f(n) = \frac{1}{n} - \frac{1}{n^s}$ is a monotonically decreasing null sequence for $n \geq t$. According to the mean value theorem, applied to $g\colon \mathbb{R} \to \mathbb{R}$, $s \mapsto n^{-s}$, there exists $1 \leq \xi_n \leq s$ with

$$b_n = g(1) - g(s) = g'(\xi_n)(1-s) = \frac{\ln(n)}{n^{\xi_n}}(s-1).$$

With b_n, $\frac{\ln(n)}{n^{\xi_n}}$ is also a monotonically decreasing null sequence for $n \geq t$. According to Corollary 9.12,

$$\gamma(s) := \sum_{n=1}^{\infty} a_n \frac{\ln(n)}{n^{\xi_n}}$$

converges for all $s \geq 1$ (the finitely many summands $n \leq t$ have no influence on the convergence). The proof of Corollary 9.12 shows (as for $L(s,\chi)$) that the partial sums converge uniformly and thus $\gamma(s)$ is continuous on $[0,\infty)$. In total,

$$L(s,\chi) = L(s,\chi) - L(1,\chi) = -\sum_{n=1}^{\infty} a_n b_n = (1-s)\gamma(s) \tag{9.7}$$

for $s \geq 1$.

By assumption, $L(1,\overline{\chi}) = \overline{L(1,\chi)} = 0$ holds. The product $P(s) := \prod_{\psi \in \Psi_d} L(s,\psi)$ from (9.4) can be split into $P(s) = L(s,\chi_0)L(s,\chi)L(s,\overline{\chi})Q(s)$. The continuity of $L(s,\psi)$ for all $\psi \neq \chi_0$ shows $\lim_{s\to 1} Q(s) < \infty$. According to (9.7) and (9.3), on the other hand,

$$\lim_{s\to 1} L(s,\chi_0)L(s,\chi)L(s,\overline{\chi}) = \lim_{s\to 1} L(s,\chi_0)(1-s) \lim_{s\to 1}(1-s)\gamma(s)\overline{\gamma(s)} = 0.$$

Thus, $\lim_{s\to 1} P(s) = 0$ also holds, in contradiction to (9.4).

Case 2: $\overline{\chi} = \chi$.
For $0 \leq x < 1$ and $n \in \mathbb{N}$, $\frac{x^n}{1-x^n} \leq \frac{x^n}{1-x}$ holds. Therefore,

$$f(x) := \sum_{n=1}^{\infty} \chi(n) \frac{x^n}{1-x^n}$$

converges absolutely for $0 \leq x < 1$. It holds that

$$-f(x) = \frac{1}{1-x} L(1,\chi) - f(x) = \sum_{n=1}^{\infty} a_n \underbrace{\left(\frac{1}{n(1-x)} - \frac{x^n}{1-x^n}\right)}_{=:b_n}$$

with

$$\begin{aligned}(1-x)(b_n - b_{n+1}) &= \frac{1}{n} - \frac{1}{n+1} - \frac{x^n}{1+x+\ldots+x^{n-1}} + \frac{x^{n+1}}{1+x+\ldots+x^n} \\ &= \frac{1}{n(n+1)} - \frac{x^n}{(1+x+\ldots+x^{n-1})(1+x+\ldots+x^n)}.\end{aligned}$$

From the inequality between arithmetic and geometric means, it follows that

$$\frac{1-x^n}{1-x} = 1 + x + \ldots + x^{n-1} \geq n x^{\frac{1}{n}\binom{n}{2}} = n x^{\frac{n-1}{2}} \geq n x^{n/2} \geq n x^n.$$

[14] it holds that $t = (1+(s-1))^{\frac{1}{s-1}} \leq e$

This yields $b_n \geq 0$ and

$$(1-x)(b_n - b_{n+1}) \geq \frac{1}{n(n+1)} - \frac{x^n}{n(n+1)x^n} = 0,$$

i. e. $1 = b_1 \geq b_2 \geq \ldots \geq 0$. Abel summation yields

$$\Big|\sum_{k=1}^{n} a_k b_k\Big| \leq db_n + d\sum_{k=1}^{n-1}(b_k - b_{k+1}) = db_1 = d.$$

In particular, $f(x)$ is bounded on $[0,1)$. Because of $\frac{x^n}{1-x^n} = \sum_{k=1}^{\infty} x^{kn}$, it holds that

$$\begin{aligned}\Big|\sum_{n=1}^{N}\chi(n)\frac{x^n}{1-x^n} - \sum_{n=1}^{N}\Big(\sum_{k|n}\chi(k)\Big)x^n\Big| &= \Big|\sum_{n=1}^{N}\chi(n)\sum_{k=\lfloor N/n\rfloor+1}^{\infty} x^{kn}\Big| \leq \sum_{n=1}^{N}\frac{x^{n\lfloor N/n\rfloor+n}}{1-x^n} \\ &\leq \frac{1}{1-x}\sum_{n=1}^{N} x^N = \frac{Nx^N}{1-x} \xrightarrow{N\to\infty} 0.\end{aligned}$$

This shows

$$f(x) = \sum_{n=1}^{\infty}\underbrace{\Big(\sum_{k|n}\chi(k)\Big)}_{=:c_n}x^n.$$

Since χ is real, $\chi(k) \in \{0, \pm 1\}$ holds for all $k \in \mathbb{N}$. For every prime number p, it follows that $c_{p^r} = 1 + \chi(p) + \ldots + \chi(p)^r \geq 0$. With the prime factorization $n = p_1^{r_1}\ldots p_t^{r_t}$, we obtain

$$c_n = c_{p_1^{r_1}}\ldots c_{p_t^{r_t}} \geq 0.$$

Because $d \geq 2$, d has a prime divisor p. Then $c_{p^r} = 1$ holds and $f(x) \geq \sum_{r=1}^{\infty} x^{p^r}$. Consequently, $\lim_{x\to 1} f(x) = \infty$, in contradiction to the boundedness of $f(x)$. □

Example 9.18. Using elementary analysis, it holds that

$$\begin{aligned}L(2,\chi_0) &= 1 + \frac{1}{9} + \frac{1}{25} + \ldots = \zeta(2) - \frac{1}{4}\zeta(2) = \frac{\pi^2}{8} \qquad (\chi_0 \in \Psi_2), \\ L(1,\chi) &= 1 - \frac{1}{3} + \frac{1}{5} \mp \ldots = \frac{\pi}{4} \qquad (\chi \in \Psi_4 \setminus \{\chi_0\}), \\ L(3,\chi) &= 1 - \frac{1}{27} + \frac{1}{125} \mp \ldots = \frac{\pi^3}{32} \qquad (\chi \in \Psi_4 \setminus \{\chi_0\}).\end{aligned}$$

From the partial fraction decomposition of the cotangent with $x = \frac{1}{3}$ or $x = \frac{1}{6}$, it also follows that

$$\begin{aligned}L(1,\chi) &= 1 + \sum_{n=1}^{\infty}\Big(\frac{1}{3n+1} - \frac{1}{3n-1}\Big) = \frac{1}{3}\pi\cot(\pi/3) = \frac{\pi}{3\sqrt{3}} \qquad (\chi \in \Psi_3 \setminus \{\chi_0\}), \\ L(1,\chi) &= 1 + \sum_{n=1}^{\infty}\Big(\frac{1}{6n+1} - \frac{1}{6n-1}\Big) = \frac{1}{6}\pi\cot(\pi/6) = \frac{\pi}{2\sqrt{3}} \qquad (\chi \in \Psi_6 \setminus \{\chi_0\}).\end{aligned}$$

Definition 9.19. A non-empty subset $Z \subseteq \mathbb{C}$ is called *convex*, if for all $x, y \in Z$ the connecting line segment $\{\lambda x + (1-\lambda)y : 0 \leq \lambda \leq 1\}$ between x and y lies in Z.

Lemma 9.20. *Let $Z \subseteq \mathbb{C}$ be convex and $f\colon Z \to \mathbb{C}$ be differentiable with $f'(z) = 0$ for all $z \in Z$. Then f is constant.*

Proof. Let $x, y \in Z$. The real function

$$g\colon [0,1] \to \mathbb{R}, \qquad \lambda \mapsto f\big(\lambda x + (1-\lambda)y\big) + \overline{f\big(\lambda x + (1-\lambda)y\big)} = 2\Re\big(f(\lambda x + (1-\lambda)y)\big)$$

is well-defined (since Z is convex) and satisfies

$$g'(\lambda) = (x-y)f'\big(\lambda x + (1-\lambda)y\big) + \overline{(x-y)f'\big(\lambda x + (1-\lambda)y\big)} = 0$$

for all $0 \le \lambda \le 1$ by the chain rule. From the mean value theorem, it follows that g is constant. In particular, $\Re(f(x)) = \frac{1}{2}g(1) = \frac{1}{2}g(0) = \Re(f(y))$. Analogously, one shows for the imaginary part that $\Im(f(x)) = \Im(f(y))$. Thus f is constant on Z. □

Remark 9.21. According to analysis, every $z \in \mathbb{C}^\times$ can be uniquely written in *polar coordinates*

$$z = re^{\mathrm{i}\varphi} = r(\cos\varphi + \mathrm{i}\sin\varphi)$$

with $r = |z| > 0$ and $-\pi < \varphi \le \pi$. Therefore, the restriction

$$\exp\colon \{z \in \mathbb{C} : -\pi < \Im(z) \le \pi\} \to \mathbb{C}^\times$$

is bijective.

Definition 9.22. The *principal branch* of the complex *logarithm* is defined by

$$\log\colon \mathbb{C}^\times \to \mathbb{C}, \qquad re^{\mathrm{i}\varphi} \mapsto \ln(r) + \mathrm{i}\varphi \qquad (r > 0,\ -\pi < \varphi \le \pi).$$

Remark 9.23. For $z = re^{\mathrm{i}\varphi} \in \mathbb{C}$ it holds that

$$\exp(\log(z)) = \exp(\ln(r) + \mathrm{i}\varphi) = re^{\mathrm{i}\varphi} = z. \tag{9.8}$$

On the other hand, $\log(\exp(2\pi\mathrm{i})) = \log(1) = \ln(1) = 0 \neq 2\pi\mathrm{i}$.

Lemma 9.24.

(i) The complex logarithm is differentiable on $D := \mathbb{C} \setminus \mathbb{R}_{\le 0}$ with $\log'(z) = \frac{1}{z}$ for $z \in D$.

(ii) For $z \in \mathbb{C}^\times$ with $|z| < 1$, it holds that $\log(1-z) = -\sum_{n=1}^{\infty} \frac{z^n}{n}$.

Proof.

(i) According to Analysis, $\ln\colon \mathbb{R}_{>0} \to \mathbb{R}$ is differentiable with $\ln'(x) = 1/x$ for $x > 0$. Let $z = re^{\mathrm{i}\varphi} \in D$ with $r > 0$ and $-\pi < \varphi < \pi$. Let $z_k := r_k e^{\mathrm{i}\varphi_k} \in D$ be a sequence with $\lim_{k\to\infty} z_k = z$ and $-\pi < \varphi_k < \pi$ for $k \in \mathbb{N}$. Then there exists an $\epsilon > 0$ with $|\varphi - \varphi_k| < 2\pi - \epsilon$ for all $k \in \mathbb{N}$. Because of

$$|r - r_k| = \big||z| - |z_k|\big| \le |z - z_k| \xrightarrow{k\to\infty} 0$$

it holds that $\lim_{k\to\infty} r_k = r$. From

$$\cos(\varphi - \varphi_k) + \mathrm{i}\sin(\varphi - \varphi_k) = e^{\mathrm{i}(\varphi - \varphi_k)} = \frac{r_k}{r}\frac{z}{z_k} \xrightarrow{k\to\infty} 1$$

and $|\varphi - \varphi_k| < 2\pi - \epsilon$ follows $\lim_{k\to\infty} \varphi_k = \varphi$ (arccos is continuous). This shows

$$\lim_{k\to\infty} \log(z_k) = \lim_{k\to\infty} (\ln(r_k) + \mathrm{i}\varphi_k) = \ln(r) + \mathrm{i}\varphi = z,$$

i. e. log is continuous on D. Now assume $z_k \neq z$ for $k \in \mathbb{N}$. As the inverse function of the restricted exponential function, log is injective. In particular, $\log(z_k) \neq \log(z)$ holds. This shows

$$\lim_{k\to\infty} \frac{\log(z) - \log(z_k)}{z - z_k} \overset{(9.8)}{=} \frac{1}{\lim\limits_{k\to\infty} \frac{\exp(\log(z)) - \exp(\log(z_k))}{\log(z) - \log(z_k)}} = \frac{1}{\exp'(\log(z))} = \frac{1}{\exp(\log(z))} = \frac{1}{z}$$

for all $z \in D$.

(ii) According to (i), the function $f(z) := \log(1 - z)$ is differentiable on the convex set $Z := \{z \in \mathbb{C} : |z| < 1\}$ with $f'(z) = -\log'(1 - z) = -\frac{1}{1-z}$ for $z \in Z$. Because of

$$\sum_{n=1}^{\infty} \frac{|z|^n}{n} \leq \sum_{n=1}^{\infty} |z|^n = \frac{|z|}{1 - |z|} < \infty$$

the series $g(z) := -\sum_{n=1}^{\infty} \frac{z^n}{n}$ converges absolutely for $z \in Z$. According to Analysis, it holds that

$$g'(z) = -\sum_{n=1}^{\infty} z^{n-1} = -\frac{1}{1 - z} = f'(z).$$

According to Lemma 9.20, there exists a constant C with $f(z) = g(z) + C$ and $C = f(0) - g(0) = 0$. □

Remark 9.25. From Lemma 9.24 follows

$$\log\Big(\frac{1}{1 - z}\Big) = \log\Big(\frac{1 - z}{1 - z}\Big) - \log(1 - z) = \log(1) - \log(1 - z) = \sum_{n=1}^{\infty} \frac{z^n}{n} \tag{9.9}$$

for $|z| < 1$.

Theorem 9.26 (Dirichlet's Prime Number Theorem)**.** *For all coprime numbers $a, d \in \mathbb{N}$, it holds that*

$$\sum_{\substack{p\in\mathbb{P} \\ p\equiv a \pmod d}} \frac{1}{p} = \infty.$$

In particular, there exist infinitely many prime numbers $p \equiv a \pmod d$.

Proof. Wlog. let $d \geq 2$. According to Theorem 9.17, there exists a $t > 1$ with $L(s, \chi) \neq 0$ for all $\chi \in \Psi_d$ and $1 < s < t$ (note $L(s, \chi_0) \geq 1$ for all $s > 1$). In the following, let always $1 < s < t$. For $\chi \in \Psi_d$ we have

$$\sum_{p\in\mathbb{P}} \sum_{k=2}^{\infty} \frac{|\chi(p^k)|}{kp^{ks}} \leq \sum_{p\in\mathbb{P}} \sum_{k=2}^{\infty} (p^{-s})^k = \sum_{p\in\mathbb{P}} \frac{p^{-2s}}{1 - p^{-s}} = \sum_{p\in\mathbb{P}} \frac{1}{p^s(p^s - 1)} \leq \sum_{n=2}^{\infty} \Big(\frac{1}{n-1} - \frac{1}{n}\Big) = 1.$$

According to the second orthogonality relation (Theorem 9.5), we have

$$\sum_{\psi\in\Psi_d} \overline{\chi(a)}\chi(p) = \begin{cases} |\Psi_d| = \varphi(d) & \text{if } p \equiv a \pmod d, \\ 0 & \text{otherwise.} \end{cases}$$

This shows

$$f(s) := \sum_{\chi\in\Psi_d} \overline{\chi(a)} \sum_{p\in\mathbb{P}} \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}} = \sum_{p\in\mathbb{P}} \sum_{\chi\in\Psi_d} \overline{\chi(a)} \Big(\frac{\chi(p)}{p^s} + \sum_{k=2}^{\infty} \frac{\chi(p^k)}{kp^{ks}} \Big) \leq \varphi(d) \sum_{p\equiv a \pmod d} \frac{1}{p^s} + C$$

for a constant C (since Ψ_d is closed under complex conjugation according to Theorem 9.5, $f(s) \in \mathbb{R}$). It therefore suffices to show $\lim_{s\to 1} f(s) = \infty$. Because of $|\chi(p)p^{-s}| < 1$, we have

$$\exp\Big(\sum_{p\in\mathbb{P}} \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}} \Big) \overset{(9.6)+(9.9)}{=} \prod_{p\in\mathbb{P}} \exp\Big(\log\Big(\frac{1}{1-\chi(p)p^{-s}} \Big) \Big) \overset{(9.8)}{=} \prod_{p\in\mathbb{P}} \frac{1}{1-\chi(p)p^{-s}} \overset{(9.2)}{=} L(s,\chi).$$

For $\chi \neq \chi_0$, the limit $\lim_{s\to 1} \sum_{p\in\mathbb{P}} \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}}$ is therefore bounded. On the other hand, because of $\gcd(a,d) = 1$, we have $\chi_0(a) = 1$ and $\lim_{s\to 1} \sum_{p\in\mathbb{P}} \sum_{k=1}^{\infty} \frac{\chi_0(p^k)}{kp^{ks}} = \infty$ according to Example 9.9. This shows $\lim_{s\to 1} f(s) = \infty$. □

Remark 9.27.

(i) Let $a, d \in \mathbb{N}$ be coprime. One can show that the prime numbers are distributed "uniformly" among the prime residue classes, i. e.

$$\lim_{n\to\infty} \frac{|\{p \in \mathbb{P}_n : p \equiv a \pmod d\}|}{\pi(n)} = \frac{1}{\varphi(d)}.$$

(ii) In complex analysis, one extends the Riemann ζ-function to a holomorphic function on $\mathbb{C} \setminus \{1\}$. It then possesses the so-called trivial zeros $-2k$ for $k \in \mathbb{N}$. The Gaussian Prime Number Theorem

$$\lim_{n\to\infty} \frac{\pi(n)\ln(n)}{n} = 1$$

is equivalent to $\zeta(s) \neq 0$ for $\Re(s) = 1$ and can therefore be proven using complex analysis. Here, too, there are "elementary" proofs by Erdős, Selberg, and others.

(iii) The *Riemann Hypothesis* states that all non-trivial zeros of ζ have real part $\frac{1}{2}$. This is one of the greatest unsolved problems in mathematics. It is known that there are infinitely many such zeros. The zero with the smallest positive imaginary part is $\approx \frac{1}{2} + 14{,}347\,\mathrm{i}$. A proof of the Riemann Hypothesis would imply the following improvement of the Gaussian Prime Number Theorem:

$$\Big| n - \sum_{p\in\mathbb{P}_n} \log(p) \Big| < \frac{\sqrt{n}\ln(n/\ln(n))^2}{8\pi} \qquad (n \geq e^{78}).$$

(iv) The Green-Tao Theorem from the year 2004 states that there are arbitrarily long sequences of prime numbers with constant difference. That is, for all $k \in \mathbb{N}$ there exist $a, d \in \mathbb{N}$ with $a + di \in \mathbb{P}$ for $i = 1, \ldots, k$. Currently, such sequences are known for $k \leq 27$. In the year 2019, the sequence

$$224.584.605.939.537.911 + 18.135.696.597.948.930i \in \mathbb{P} \qquad (i = 0, \ldots, 26)$$

was discovered.

10 Cryptology

Remark 10.1.

(i) For a long time, number theory was considered pure play. The first important applications outside of mathematics emerged in cryptology and coding theory with the beginning of the computer age in the 1970s. *Cryptology* deals with the encryption (*cryptography*) and decryption (*cryptanalysis*) of confidential messages. Coding theory deals with error detection and correction during the transmission of digital data over a noise-prone channel.[15]

(ii) Messages of any form (text, sound, images, ...) can, as is well known, be digitized in the form of decimal or binary numbers. Since messages can be divided into blocks, we can assume that such numbers are bounded.

(iii) *Kerckhoffs's principle* states that the security of an encryption method should not depend on the secrecy of the algorithm, but only on the secrecy of the key. Therefore, common methods are freely available (without patent) and well-studied.

(iv) A fundamental tool of cryptography is a *one-way function*. This is an injective function that is algorithmically easy to compute, but whose inverse mapping is very difficult to compute. The following algorithm shows that the power mapping in a group is efficiently computable.

Theorem 10.2 (Binary exponentiation)**.** *Let G be a group, $g \in G$ and $n \in \mathbb{N}$. The following algorithm computes $g^n \in G$:*

Initialization: $h := g$, $x := g$ and $m := n$.
As long as $m > 0$, repeat:
If $m \equiv 1 \pmod 2$, compute $h := hx$.
Compute $x := x^2$.
Compute $m := \lfloor m/2 \rfloor$.
Output: $h = g^n$.

Proof. Let $n = \sum_{i=0}^{k} b_i 2^i$ be the binary representation of n, where $b_k = 1$. The loop is executed $(k+1)$ times with the following values:

m	n	$\sum_{i=1}^{k} b_i 2^{i-1}$	$\sum_{i=2}^{k} b_i 2^{i-2}$	$\cdots$	$b_k = 1$	0
h	1	g^{b_0}	$g^{2b_1+b_0}$	$\cdots$	$g^{2^{k-1}b_{k-1}+\ldots+b_0}$	g^n
x	g	g^2	g^4	$\cdots$	g^{2^k}	$g^{2^{k+1}}$

□

Remark 10.3. The naive algorithm for computing g^n requires $n-1$ multiplications ($g \to g^2 \to g^3 \to \ldots \to g^n$), while binary exponentiation requires at most $2k = 2\lfloor \log_2(n) \rfloor$ multiplications (for $h = 1$ the computation of $h := 1x$ is trivial, while in the last iteration the computation of $x := x^2$ is redundant).

Example 10.4.

(i) In arithmetic in residue class rings modulo a number n, it is sensible to reduce modulo n after each operation. For example,

$$2^{27} = 2^{16+8+2+1} = 4^{8+4+1}2 \equiv (-1)^{4+2}4 \cdot 2 \equiv 8 \pmod{17}.$$

[15] See Algebra notes

(ii) Binary exponentiation is not in every case the most efficient method for exponentiation. For example, the binary exponentiation of $g^{15} = gg^2g^4g^8$ requires six multiplications, although it is also possible with five:

$$g \to g^2 \to g^3 = gg^2 \to g^5 = g^2g^3 \to g^{10} = (g^5)^2 \to g^{15} = g^{10}g^5.$$

The construction of such so-called *addition chains* is, however, costly and rarely worthwhile in practice.

Definition 10.5. Let $G = \langle g \rangle$ be a cyclic group of order n. The *discrete logarithm* is the inverse function of exponentiation $\log\colon G \to \mathbb{Z}/n\mathbb{Z}$, $g^k \mapsto k + n\mathbb{Z}$.

Remark 10.6. The calculation of the discrete logarithm depends on the given representation of the group G. In $G = (\mathbb{Z}/n\mathbb{Z}, +) = \langle g + n\mathbb{Z} \rangle$, the logarithm of $h + n\mathbb{Z}$ can be easily calculated by multiplying by $g^{-1} + n\mathbb{Z}$ ($g^{-1} + n\mathbb{Z}$ can be efficiently calculated with the extended Euclidean algorithm). In general, the calculation of log is difficult, i.e., exponentiation is a one-way function. Instead of calculating all n powers of g, the following algorithm manages with $2\sqrt{n}$ multiplications (which is still a lot in practice).

Theorem 10.7 (Baby-step giant-step algorithm)**.** *Let $G = \langle g \rangle$ be a group of order n and $h \in G$. The following algorithm calculates $k + n\mathbb{Z}$ with $g^k = h$:*

Initialization: $m := \lceil \sqrt{n} \rceil$.
Calculate and store: $P := \{1 = g^0, g^1, g^2, \ldots, g^m\}$ (*Baby steps*).
For $i = 0, \ldots, m$*:*
    Calculate $x := hg^{-mi}$ (*Giant steps*).
    If $x = g^j \in P$ *holds, then stop.*
Output: $k + n\mathbb{Z} = mi + j + n\mathbb{Z}$.

Proof. Obviously there exist $0 \leq i, j \leq m$ with $k = mi + j$. The algorithm terminates when $hg^{-mi} = x = g^j$ holds, i.e., $h = g^{mi+j} = g^k$. □

Example 10.8. Let $G = \langle 3 + 101\mathbb{Z} \rangle = (\mathbb{Z}/101\mathbb{Z})^\times$ and $h = 4 + 101\mathbb{Z}$. Then $m = \lceil \sqrt{101} \rceil = 11$. We calculate the baby steps (all values modulo 101):

i	0	1	2	3	4	5	6	7	8	9	10	11
g^i	1	3	9	27	−20	41	22	−35	−4	−12	−36	−7

Because of $7 \cdot 29 = 203 \equiv 1 \pmod{101}$, $g^{-11} \equiv -7^{-1} \equiv -29 \pmod{101}$. With this we calculate the giant steps:

i	0	1	2	3	4	5
hg^{-mi}	4	−15	31	10	13	27

Because of $27 \equiv g^3 \pmod{101}$, we obtain $k = 5 \cdot 11 + 3 = 58$ with $g^k = h$. In total we required 15 multiplications, while the naive approach would have required 57 multiplications.

Remark 10.9. In the Baby-step Giant-step algorithm, one trades a time advantage for increased memory requirements to store the set P (*Time-Memory Tradeoff*). The following algorithm reduces the calculation of the discrete logarithm to the case where n is a prime number. Thus, if $|G|$ is a product of "small" prime numbers, one has a chance to calculate $\log(h)$.

Theorem 10.10 (POHLIG-HELLMAN-Algorithm)**.** *Let $G = \langle g \rangle$ be a group of order $n = p_1^{a_1} \dots p_s^{a_s}$ (prime factorization). Let $h \in G$. The following algorithm calculates $k + n\mathbb{Z}$ with $g^k = h$:*

For $i = 1, \dots, s$:
Set $x := g^{n/p_i}$, $y := g^{n/p_i^{a_i}}$, $z := h^{n/p_i^{a_i}}$ and $l_0 := 0$.
For $j = 0, \dots, a_i - 1$:
Calculate $w := (y^{-l_j} z)^{p_i^{a_i - 1 - j}}$.
Determine $0 \leq r_j < p_i$ with $x^{r_j} = w$ (e. g. with Theorem 10.7).
Calculate $l_{j+1} := l_j + p_i^j r_j$.
Set $k_i := l_{a_i}$.
Determine k with $k \equiv k_i \pmod{p_i^{a_i}}$ for $i = 1, \dots, s$ (Chinese Remainder Theorem).
Output: $k + n\mathbb{Z}$.

Proof. We consider the i-th iteration and set $p^a := p_i^{a_i}$ for better clarity. By construction, x has order p. For $j = 0$, $w = z^{p^{a-1}} \in \langle x \rangle$. Therefore, there exists exactly one r_0 with $0 \leq r_0 < p$ and $y^{p^{a-1} r_0} = x^{r_0} = w = z^{p^{a-1}}$, i. e. $(y^{-r_0} z)^{p^{a-1}} = 1$. One then sets $l_1 := r_0$. For $j = 1$, again $w = (y^{-r_0} z)^{p^{a-2}} \in \langle x \rangle$. Let us now assume inductively that in the j-th step there exists an r_j with $0 \leq r_j < p$ and $y^{p^{a-1} r_j} = x^{r_j} = w = (x^{-l_j} z)^{p^{a-1-j}}$. Then

$$(y^{-l_{j+1}} z)^{p^{a-1-j}} = (y^{-(l_j + p^j r_j)} z)^{p^{a-1-j}} = 1.$$

This guarantees that r_{j+1} exists. For $j = a - 1$, finally $y^{p^{a-1} r_j} = x^{r_j} = w = y^{-l_j} z$ holds. With $k_i := l_a = l_j + p^{a-1} r_j$, then $y^{k_i} = z$. We set $y_i := y$ and $z_i := z$.

Since $p_1^{a_1}, \dots, p_s^{a_s}$ are pairwise coprime, k can be calculated using the Chinese Remainder Theorem. Let $q_i := n / p_i^{a_i}$ for $i = 1, \dots, s$. According to the Euclidean algorithm, there exist $b_1, \dots, b_s \in \mathbb{Z}$ with $b_1 q_1 + \dots + b_s q_s = 1$. Then

$$g^k = g^{k b_1 q_1 + \dots + k b_s q_s} = y_1^{b_1 k_1} \dots y_s^{b_1 k_s} = z_1^{b_1} \dots z_s^{b_s} = h^{b_1 q_1 + \dots + b_s q_s} = h. \qquad \square$$

Example 10.11. Let $G := \langle 2 + 101\mathbb{Z} \rangle = (\mathbb{Z}/101\mathbb{Z})^\times$ and $h := 57 + 101\mathbb{Z}$. It holds that $|G| = \varphi(101) = 100 = 2^2 5^2$. With the notation from the above proof, $x_1 = g^{50} = -1 + 101\mathbb{Z}$, because this is the only element of order 2 in G. Due to $10^2 \equiv -1 \pmod{101}$, $y_1 = 10 + 101\mathbb{Z}$. Furthermore,

$$z_1 = 57^{25} \equiv (-44)^{16+8+1} \equiv 17^{8+4}(-44) \equiv \dots \equiv 10 \pmod{101}.$$

We can immediately read off $k_1 = 1$ without running through the inner loop.

For $p_2 = 5$, one obtains $y_2 = g^4 = 16 + 101\mathbb{Z}$ and

$$\begin{aligned} x_2 &= y_2^5 = 16^4 16 \equiv (-13)16 \equiv -6 \pmod{101}, \\ z_2 &= 57^4 \equiv 17^2 \equiv -14 \pmod{101}, \\ w &= z_2^5 \equiv (-6)^2(-14) \equiv \dots \equiv 1 \pmod{101}. \end{aligned}$$

Thus $l_1 = r_0 = 0$ holds. In the next step ($j = 1$), $w = z_2$. Because of $(-6)^3 \equiv -14 \pmod{101}$, $k_2 = l_2 = 5 \cdot 3 = 15$ holds. For $k = 65$, finally $k \equiv 1 \pmod 4$ and $k \equiv 15 \pmod{25}$ holds. Thus $2^{65} \equiv 57 \pmod{101}$.

Theorem 10.12 (Index Calculus Method)**.** *Let $G = \langle g \rangle$ be a group of order n and $h \in G$. The following algorithm computes $k + n\mathbb{Z}$ with $g^k = h$:*

Choose $g_1, \dots, g_s \in G$ and $e_1, \dots, e_s, f \in \mathbb{Z}$ with $hg^f = g_1^{e_1} \dots g_s^{e_s}$.
Initialize a matrix A and a column vector v.
For $a = 1, 2, \dots$:
    If one finds $a_1, \dots, a_s \in \mathbb{Z}$ with $g^a = g_1^{a_1} \dots g_s^{a_s}$:
        Append the column $(a_1, \dots, a_s)^{\mathrm{t}}$ to A.
        Append a to v.
    If there exists an integer vector x with $Ax \equiv (e_1, \dots, e_s)^{\mathrm{t}} \pmod{n}$, then terminate.
Output: $k + n\mathbb{Z} = v^{\mathrm{t}}x - f + n\mathbb{Z}$.

Proof. Let $v = (v_1, \dots, v_t)^{\mathrm{t}}$ and $A = (a_{ij})_{i,j} \in \mathbb{Z}^{s \times t}$ with $g^{v_i} = g_1^{a_{1i}} \dots g_s^{a_{si}}$. For $x = (x_1, \dots, x_t)^{\mathrm{t}}$, it holds that

$$g^{v^{\mathrm{t}}x} = \prod_{i=1}^{t} (g^{v_i})^{x_i} = \prod_{i=1}^{t} \prod_{j=1}^{s} g_j^{a_{ji}x_i} = \prod_{j=1}^{s} g_j^{\sum_{i=1}^{t} a_{ji}x_i} = \prod_{j=1}^{s} g_j^{e_j} = hg^f,$$

i. e. $g^{v^{\mathrm{t}}x - f} = h$. The algorithm terminates at the latest when $g^a = hg^f$ and one finds the solution $g^a = g_1^{e_1} \dots g_s^{e_s}$. □

Remark 10.13. The success of the Index Calculus Method depends significantly on the choice of the parameters $g_1, \dots, g_s$ and f. The choice $s = 1$, $f = 0$ and $g_1 = h$ obviously offers no benefit. If $G \leq (\mathbb{Z}/m\mathbb{Z})^\times$, then one can choose prime numbers for $g_1, \dots, g_s$. One chooses f such that the prime divisors of hg^f lie in $\{g_1, \dots, g_s\}$. The e_i result from the prime factorization of hg^f. In the loop, one searches for g^a whose prime factors also lie in $\{g_1, \dots, g_s\}$, i. e. one solves the equation in $\mathbb{Z}$ instead of in G.

Example 10.14. Let $G = \langle 31 + 127\mathbb{Z} \rangle \leq (\mathbb{Z}/127\mathbb{Z})^\times$ and $h = 19 + 127\mathbb{Z}$ (it is not yet clear whether $h \in G$). We have $n := |G| = 63$. We set $f := 1$. Then $hg = 19 \cdot 31 \equiv 3^4 \pmod{127}$. Furthermore,

$$31^2 = 2^3 \cdot 3^2, \qquad 31^5 \equiv 2^4 \cdot 11, \qquad 31^7 \equiv 3^2 \cdot 11, \qquad 31^9 \equiv 2^4 \pmod{127}.$$

We can therefore choose $(g_1, g_2, g_3) := (2, 3, 11)$ and $e := (0, 4, 0)$. Then $v = (2, 5, 7, 9)^{\mathrm{t}}$ and

$$A = \begin{pmatrix} 3 & 4 & 0 & 4 \\ 2 & 0 & 2 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

One calculates $x = (0, -2, 2, 2)^{\mathrm{t}}$.[16] Thus $k + n\mathbb{Z} = v^{\mathrm{t}}x - 1 + n\mathbb{Z} = 21 + n\mathbb{Z}$.

Remark 10.15.

(i) A *hash function* is an easily computable function $h\colon A \to B$, such that preimages $f^{-1}(b)$ for $b \in B$ are very difficult to compute. In practice, $|B| < |A|$, so that h, in contrast to one-way functions, cannot be injective. Nevertheless, one wants that *collisions* $f(a) = f(a')$ with $a \neq a'$ do not occur in practice. Due to the *birthday paradox*, collisions occur surprisingly frequently (the probability that out of 23 people two have their birthday on the same day is greater than 50%).

(ii) Hash functions are used, for example, for the comparison of passwords during logins. Instead of storing a password a in plain text, one only stores the hash value (fingerprint) $h(a)$ in a database. If a password a' is entered during login, one checks $h(a') = h(a)$. An attacker can do nothing with the hash values from the database. To prevent the trying out of frequently used passwords

[16] The first three columns of A are indeed linearly independent over $\mathbb{Z}$, but they do not generate the vector e modulo n.

(dictionary attack), one can extend the passwords with a *salt*, i.e., a random character string, before "hashing".

(iii) In everyday life, we often use hash functions unconsciously, for example when comparing telephone numbers (a look at the last digits is sufficient). The cryptographically insecure algorithm (collisions are known) *MD5* (Message-digest) is used to check files for errors (for instance after a download). It converts an input of arbitrary length into a sequence of 16 bytes (so there are $2^{128} \approx 10^{38}$ possible hash values). The algorithm *SHA-2* is currently considered collision-resistant and cryptographically secure.

(iv) In *symmetric* cryptosystems, the same key is used for encryption and decryption (the algorithm may, however, differ). The question arises how both parties agree on a secret key before the message transmission. A solution to this seemingly simple problem was only developed in the 70s by Diffie, Hellman, and Merkle. It uses the discrete logarithm as a one-way function.

Theorem 10.16 (DHM key exchange)**.** *Euler and Gauss publicly choose a group $G = \langle g \rangle$. Euler secretly chooses $a \in \mathbb{N}$ and sends g^a to Gauss. Gauss secretly chooses $b \in \mathbb{N}$ and sends g^b to Euler. Both can now use $(g^a)^b = g^{ab} = (g^b)^a$ as a secret key.*

Proof. Trivial. □

Remark 10.17.

(i) According to the Pohlig-Hellman algorithm, the security of the DHM key exchange depends on the prime factorization of $|G|$. In practice, one chooses a Germain prime $p > 10^{100}$, i. e. $n := 2p+1$ is also a prime (one then calls n a *safe* prime). For $G = (\mathbb{Z}/n\mathbb{Z})^\times$, $|G| = \varphi(n) = 2p$ holds, so that Theorem 10.10 still requires the calculation of the discrete logarithm modulo p.

(ii) The DHM key exchange does not protect against so-called *Man-in-the-Middle attacks*, in which an attacker, say Fermat, can manipulate the data exchange of the parties. Fermat receives g^a from Euler and g^b from Gauss, but sends g^c to both. Euler calculates the key g^{ac}, while Gauss calculates g^{bc} as the key. Fermat possesses both keys and can therefore decrypt the further communication. We will return to this in Remark 10.28.

(iii) The DHM key exchange assumes that one can randomly generate large (safe) primes. For this purpose, one uses random number generators and efficient primality tests. True random numbers cannot be generated deterministically. In practice, however, so-called *pseudorandom numbers* are sufficient.

(iv) (Linear congruential generator) Given natural numbers $a, b < n$, where n is as large as possible. One generates a starting value (*seed*) $x_0 \in \mathbb{N}$ (for example from the system time or from noise of analog devices). The recursive sequence

$$x_{i+1} := ax_i + b \pmod{n}$$

with $i \in \mathbb{N}$ provides pseudorandom numbers. The command `rand()` in the programming languages C and C++ is based on this algorithm. For serious cryptographic applications, however, the generated numbers are not random enough. One can vary the algorithm in many ways, for example, by using non-linear functions in more than two parameters. Depending on the chosen parameters, the sequence will in any case repeat sooner or later.

Example 10.18. Let $n = 1000$, $x_0 := 387$ and $x_{i+1} := 19x_i + 397 \pmod{n}$. This yields the sequence:

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
x_i	387	750	647	690	507	30	967	770	27	910	687	687	450	947	390	807

The sequence repeats for the first time after 100 terms, i. e. $x_{100} = x_0$.

Remark 10.19. Let $n \in \mathbb{N}$ be a randomly generated number with 100 decimal digits. By a suitable choice of the last decimal digit, we can assume $\gcd(n, 30) = 1$ (Exercise 21). There are $\frac{\varphi(30)}{30}(10^{101} - 10^{100}) = \frac{6}{5}10^{100}$ such numbers. According to the Gaussian Prime Number Theorem, there are

$$\pi(10^{101}) - \pi(10^{100}) \approx \frac{10^{101}}{101\ln(10)} - \frac{10^{100}}{100\ln(10)}$$

prime numbers with 100 decimal digits. The probability that n is a prime number is therefore approx.

$$\frac{25}{3 \cdot 101\ln(10)} - \frac{1}{6 \cdot 20\ln(100)} \approx 0{,}016.$$

This can be checked with the Miller-Rabin test. Once a large prime number p has been found, one can verify whether $2p + 1$ is a safe prime number using the following test.

Theorem 10.20 (Pocklington test)**.** *Let $p \in \mathbb{P}$ and $n = 2p+1$. $n \in \mathbb{P}$ if and only if there exists an $a \in \mathbb{N}$ with $a^{2p} \equiv 1 \pmod{n}$ and $a^2 \not\equiv 1 \pmod{n}$.*

Proof. If $n \in \mathbb{P}$, then every primitive root a satisfies the specified conditions. Conversely, let us assume that the conditions for a hold. Then $p \mid \operatorname{ord}_n(a) \mid \varphi(n)$. If n is not a prime number, then $\varphi(n)$ is a product of numbers $\leq \frac{1}{3}n < p$. □

Example 10.21. We describe some symmetric crypto-systems:

(i) (Caesar cipher) Given is a message text t consisting of Latin letters (A, $B, \ldots, Z$) and possibly spaces. The key is a number $1 \leq s \leq 25$. To encrypt, each letter in t is shifted by s in the alphabet, modulo 26 (spaces can be ignored). The choice $s = \frac{26}{2} = 13$ is particularly practical because here encryption and decryption are identical (*ROT13*). Since there are only 25 possible keys, the method is extremely insecure. In practice, it suffices to consider the first letters of the encrypted message to exclude keys.

(ii) (Substitution cipher) Again, a message text t with letters of an alphabet A is given (A could include uppercase and lowercase letters, umlauts, punctuation marks, or special characters). The key is a permutation $\pi\colon A \to A$. During encryption, each letter $a \in A$ in t is replaced by $\pi(a)$. Although there is a large number of possible keys here (namely $|A|! \geq 26! \approx 4 \cdot 10^{26}$), encrypted messages can be decrypted by a frequency analysis. In German texts, for example, the letter e occurs more frequently than other letters. One can therefore draw conclusions about which positions in the plaintext an e could be located.

(iii) (One-Time Pad) Given is a message in binary format $t = (t_1, \ldots, t_n)$ with $t_1, \ldots, t_n \in \{0, 1\}$. The key also has binary format $s = (s_1, \ldots, s_n)$ with $s_1, \ldots, s_n \in \{0, 1\}$. Encryption is performed by addition in $\mathbb{F}_2$:[17]

$$\tilde{t} := t + s = (t_1 + s_1, \ldots, t_n + s_n).$$

[17] In computer science, one speaks of the XOR operator, which performs an "exclusive or".

Because of $\tilde{t} + s = t + (s + s) = t$, encryption and decryption are identical procedures. Because of $t_i + s_i = 0 \Leftrightarrow t_i = s_i$, one cannot draw any conclusions about t_i from $t_i + s_i$ ($t_i = 0$ and $t_i = 1$ are equally probable). Therefore, the method is absolutely secure, but impractical, as the key requires as much storage as the message. If s is used to encrypt another message $\tilde{r} = r + s$ (contrary to the name), an attacker can calculate $\tilde{t} + \tilde{r} = t + r$. With frequency analyses, one can draw conclusions about t and r.

(iv) (Advanced Encryption Standard, AES) A message in binary format is divided into blocks $A_1, A_2, \ldots$ of 16 bytes each (if necessary, the last block must be filled with a *padding*). The key s is also a block of 16 bytes. Each byte consists of eight bits and can therefore be represented as an element of the field $\mathbb{F}_{2^8}$. Each block is interpreted as a matrix in $\mathbb{F}_{2^8}^{4\times 4}$. The algorithm uses a fixed bijection $f\colon \mathbb{F}_{2^8} \to \mathbb{F}_{2^8}$ with

$$f(x) = \begin{cases} ax^{-1} + b & \text{if } x \neq 0, \\ b & \text{if } x = 0 \end{cases}$$

for certain $a, b \in \mathbb{F}_{2^8}^\times$. Since f takes only 256 values, these are explicitly stored to speed up the application of f. Furthermore, a fixed matrix $M \in \mathrm{GL}(4, 2^8)$ is given.

Set $s_1 := s$.
For $i = 1, 2, \ldots$
Set $\tilde{A}_i := (\tilde{a}_{uv}) := A_i$.
Set $t_1 := s_i$.
For $r = 1, \ldots, 10$

$$\tilde{A}_i := M \begin{pmatrix} f(\tilde{a}_{11}) & f(\tilde{a}_{12}) & f(\tilde{a}_{13}) & f(\tilde{a}_{14}) \\ f(\tilde{a}_{22}) & f(\tilde{a}_{23}) & f(\tilde{a}_{24}) & f(\tilde{a}_{21}) \\ f(\tilde{a}_{33}) & f(\tilde{a}_{34}) & f(\tilde{a}_{31}) & f(\tilde{a}_{32}) \\ f(\tilde{a}_{44}) & f(\tilde{a}_{41}) & f(\tilde{a}_{42}) & f(\tilde{a}_{43}) \end{pmatrix} \oplus t_r.$$

Generate t_{r+1} from t_r using complicated bit arithmetic.
Generate s_{i+1} from s_i and $\tilde{A}_i$ depending on the chosen mode.

Here, $\oplus\, t_r$ describes the element-wise bit addition of the corresponding matrix entries. In the simplest and most insecure mode (Electronic Code Book, ECB), $s_i = s$ for all i. We will not go into detail about the other modes (mathematically uninteresting). During decryption, the procedure is performed in reverse.

The algorithm fulfills the criteria introduced by Shannon *diffusion* (even small changes in the input should cause larger changes in the output) and *confusion* (there should be no simple, e. g. linear, relationship between input, key, and output).

AES is a widespread crypto-standard that is even implemented at the hardware level.[18] The algorithm is used, for example, for WLAN communication (WPA2).

Remark 10.22. We now come to *asymmetric* crypto-systems, in which different keys are used for encryption and decryption. This allows parties unknown to each other to communicate without having previously exchanged a key. The first method is again based on the discrete logarithm.

Theorem 10.23 (ElGamal method)**.** *Let $G = \langle g \rangle$ be a group of order n. Euler secretly chooses a* private *key $d \in \mathbb{N}$ and announces the* public *key $h := g^d$. Gauss wants to send a message $t \in G$ to*

[18] Among others in most Intel i3, i5, and i7 processors

Euler. To do this, he chooses a random number $k \in \mathbb{N}$ and sends the pair $(g^k, h^k t)$. Euler decrypts the message with $t = (g^k)^{-d} h^k t$.

Proof. The claim follows from $(g^k)^d = (g^d)^k = h^k$. □

Theorem 10.24 (RSA method[19])**.** *Euler secretly chooses two distinct prime numbers p, q and sets $n := pq$. Euler's public key consists of n and a number e coprime to $\varphi(n)$. Euler's private key is $d \in \mathbb{N}$ with $de \equiv 1 \pmod{\varphi(n)}$. Gauss wants to send a message $t < n$ to Euler. He encrypts his message as $\tilde{t} := t^e \pmod{n}$. Euler can decrypt by $t \equiv \tilde{t}^d \pmod{n}$.*

Proof. Let $a \in \mathbb{Z}$ with $de = 1 + a\varphi(n)$. By Euler-Fermat, $\tilde{t}^d \equiv t^{de} \equiv t(t^{\varphi(n)})^a \equiv t \pmod{n}$ holds. Since $t < n$, t is uniquely determined by the residue class $\tilde{t}^d + n\mathbb{Z}$. □

Remark 10.25. The RSA method is used in many places for communication on the Internet (HTTPS, SSH, PGP, VPN etc.). In practice, the Fermat prime $2^{2^4} + 1 = 65537$ is often chosen for e. The calculation of t^e with binary exponentiation then requires only 17 multiplications. The security is based on the difficulty of the prime factorization of n when p and q are sufficiently large. Without knowledge of p and q, one can calculate neither $\varphi(n)$ nor d from n and e. Furthermore, no fast algorithm is known for calculating the (discrete) e-th root of $\tilde{t}$. If one knows $\varphi(n) = (p-1)(q-1) = n - p - q + 1$, then p and q can be determined as the solution to the quadratic equation $X^2 + (\varphi(n) - n - 1)X + n = 0$.

Example 10.26. The website `https://www.uni-hannover.de` uses the public 2048-bit key:[20]

$$
\begin{aligned}
n = {} & 804097290201759584167565762096369971072309542045307454962599587655044502378231794656163232952275496527104657485385134967337408436345009977728129645706706450743956176563384533851106410986353692839865946702914876875636580409962216287798998276658446889745392651943244880126242522381234194848629445663810711453658929787191572604961292146741585966201150509440311412937052891049456604830839988190246528266697286741413900129860255294665119080802030528133808354115327889235773371455487445518599483440674914025590826151538167056809571492274006761275819786169647162569533777267897462385372484956915007304108660822548590964505288625611712001822119264741011605033755571165375097731952989542102157180321716440117385673147891283233890977430427886675860458638260295546230771596012210666782671354230415171677940042475436058920119123094640701413617878371875233422012068502448658645179645781833083898365472234891716647496250801882470415987624658991379703365228665719509557328047000773180606025748353225535560480318561314039201970840076092982104138482358214323420989803163780079035136015343037147103973004922061808258551535868759935738718164609306021972433318394035956161479465720626055354947315137055607140703046593366182217705364354130429515352611379 \\
e = {} & 65537
\end{aligned}
$$

Theorem 10.27. *In the RSA procedure, p and q can be efficiently calculated from n, e, and d.*

[19] Named after Rivest, Shamir and Adleman
[20] Time: 2024

Proof. We follow the proof of Theorem 4.27. Wlog. let p and q be odd. Let $a \in \{2, \dots, n-1\}$ be chosen randomly and uniformly distributed. In the case $\gcd(a,n) \neq 1$, we have $\gcd(a,n) \in \{p,q\}$ and one can calculate p (or q) with the Euclidean algorithm. So let $\gcd(a,n) = 1$. Then $\operatorname{ord}_n(a) \mid \varphi(n) = (p-1)(q-1)$ holds. The probability that $\operatorname{ord}_n(a)$ is odd is at most $\frac{1}{4}$. By choosing sufficiently many random numbers, we can assume $2 \mid \operatorname{ord}_n(a)$. By construction, $b := de - 1 \equiv 0 \pmod{\varphi(n)}$ and $a^b \equiv 1 \pmod{n}$ hold. Let $b = 2^k m$ with $2 \nmid m$. Because $2 \mid \operatorname{ord}_n(a)$, there exists an $l < k$ with $a^{2^l m} \not\equiv 1 \pmod{n}$ and $a^{2^{l+1} m} \equiv 1 \pmod{n}$. As in the proof of Theorem 4.27, one shows that $a^{2^l m} \not\equiv -1 \pmod{n}$ holds with probability $\geq \frac{3}{4}$. We can assume this. Now it holds that

$$n \mid a^{2^{l+1} m} - 1 = (a^{2^l m} - 1)(a^{2^l m} + 1).$$

Since n can divide neither $a^{2^l m} - 1$ nor $a^{2^l m} + 1$, it follows that $\gcd(a^{2^l m} - 1, n) \in \{p,q\}$. The claim follows with the Euclidean algorithm. □

Remark 10.28.

(i) If Euler uses binary exponentiation to calculate $\tilde{t}^d$, a *side-channel* attacker can determine the binary representation of d from a timing measurement (for every 1 in the binary representation, an additional multiplication is required). To prevent this, one uses algorithms for exponentiation that do not depend on the binary representation of the exponent (Exercise 51).

(ii) In the RSA procedure, a man-in-the-middle attacker cannot read the encrypted messages, but can manipulate them at will, because he only needs the public key for this. So-called *signatures* provide a remedy. Let (n', e') be the public key of Gauss and d' the private key. First, Gauss calculates an integer hash value $h(t)$ of his secret message t. Subsequently, he transmits the signature $s(t) := h(t)^{d'} \pmod{n'}$ in addition to the encrypted message $\tilde{t} = t^e \pmod{n}$. Euler can calculate both t and $h(t) = s(t)^{e'} \pmod{n'}$ and compare them (the hash function h is assumed to be publicly known). An attacker can neither determine t from $h(t)$, nor calculate $s(t')$ for a manipulated message t'. In this way, Euler can verify that the message truly originates from Gauss. Due to the difficulty of the discrete logarithm, Gauss does not reveal his private key with $s(t)$.

(iii) An attacker could try to impersonate Euler using their own public key. To ensure that public RSA keys are assigned to the correct persons or websites, one uses *certificates*. For this, Euler must personally present his ID at a certification authority such as the LUH[21]. By issuing the certificate, the LUH guarantees that the public key is correctly assigned. Gauss can only verify Euler's certificate if he trusts the LUH. This is provided by a network of connected certification authorities. For example, the certificate of the LUH is issued by the higher authority *GEANT OV RSA CA 4*. This in turn receives its certificate from the *root certificate USERTrust RSA Certification Authority*, which all common operating systems trust.

(iv) Similar to the DHM key exchange, one must also ensure in the RSA procedure that $p-1$ and $q-1$ do not factor into "too small" prime numbers. This is illustrated by the following algorithm.

Theorem 10.29 (Pollards $p-1$-Method)**.** *The following algorithm finds divisors of a number $n \in \mathbb{N}$.*

Choose a bound $S \in \mathbb{N}$.
Calculate the product q of all prime power factors smaller than S.
Choose $a \in \{2, \dots, n-1\}$ randomly.
Calculate $d := \gcd(a^q - 1, n)$.

[21] LUH user certificates

If $1 < d < n$ holds, then a non-trivial divisor of n has been found.
Otherwise, choose a new a or adjust S.

Proof. There is actually nothing to prove, but we justify the motivation of the algorithm. Suppose n has a prime divisor p such that $p-1$ is a product of prime power factors $< S$. Then $a^q \equiv 1 \pmod{p}$ holds for all $a < p$ according to Euler-Fermat. If even $a^q \equiv 1 \pmod{n}$ (i.e., $d = n$), then $\operatorname{ord}_n(a)$ is "too small" or n decomposes into nothing but prime divisors p such that $p-1$ is a product of prime power factors $< S$. This situation can be changed by adjusting a or S. □

Theorem 10.30 (Pollards ρ-Method)**.** *Let $n \in \mathbb{N}$ and $x_0 = y_0 \in \mathbb{N}$ be an arbitrary starting value. Let $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be a function that is as random as possible.*

For $i \in \mathbb{N}$:
Calculate $x_i := f(x_{i-1}) \pmod{n}$ and $y_i := f(f(y_{i-1}))$.
If $1 < \gcd(x_i - y_i, n) < n$ holds, then a divisor of n is known.

Proof. The sequence (x_i) must repeat after finitely many steps. Thus there exist $i < j$ with $x_i \equiv x_j \pmod{n}$. For every (prime) divisor $p \nmid n$, $x_i \equiv x_j \pmod{p}$ also holds. The idea of the algorithm is that the sequence $(x_i \pmod{p})_i$ might repeat even earlier, so that $x_i \equiv x_j \pmod{p}$ and $x_i \not\equiv x_j \pmod{n}$ holds. In this case, $\gcd(x_i - x_j, n)$ yields a non-trivial divisor of n. We consider that one does not have to examine all differences $x_i - x_j$. For this, let $\delta := j - i$. Then $x_i \equiv x_{i+\delta} \pmod{p}$ and $x_k \equiv x_{k+\delta} \pmod{p}$ for all $k \geq i$. For $k := m\delta \geq i$, it now holds that $x_k \equiv x_{2k} \equiv y_k \pmod{p}$. □

Example 10.31.

(i) Let $n := 9701$, $x_0 = y_0 = 2$ and $f(x) := x^2 + 3 \pmod{n}$. Then

i	0	1	2	3
x_i	2	7	52	2707
y_i	2	52	3597	7424

and $\gcd(7424 - 2707, n) = 89$.

(ii) Using Pollard's ρ-method, the smallest prime divisor of the 8th Fermat number

$$F_8 = 2^{2^8} + 1 \equiv 0 \pmod{1238926361552897}.$$

was found.

Theorem 10.32 (Quadratic Sieve)**.** *Let $n \in \mathbb{N}$ and $p_1, \ldots, p_r$ be "small" prime numbers. Choose numbers $x_1, \ldots, x_m$ with the property $x_i^2 \equiv \prod_{j=1}^{r} p_j^{a_{ij}} \pmod{n}$ for $i = 1, \ldots, m$ and certain $a_{ij} \in \mathbb{N}_0$. Let $A := (a_{ji} + 2\mathbb{Z})_{ij} \in \mathbb{F}_2^{r \times m}$. Assume there exists a $v = (v_i) \in \mathbb{F}_2^m \setminus \{0\}$ with $Av = 0$. Let*

$$x := x_1^{v_i} \ldots x_m^{v_m} \pmod{n},$$
$$y := \prod_{i=1}^{r} p_i^{\frac{1}{2}(a_{i1}v_1 + \ldots + a_{im}v_m)} \pmod{n}.$$

Then $\gcd(x - y, n) \neq 1$ or $\gcd(x + y, n) \neq 1$ holds.

Proof. By assumption, $\sum_{j=1}^{m} a_{ij}v_j = (Av)_i \equiv 0 \pmod 2$ for $i = 1, \ldots, r$. Therefore $y \in \mathbb{N}$. Furthermore,

$$x^2 \equiv x_1^{2v_1} \ldots x_m^{2v_m} \equiv \prod_{i=1}^{m}\prod_{j=1}^{r} p_j^{a_{ij}v_i} = \prod_{j=1}^{r} p_j^{\sum_{i=1}^{m} a_{ij}v_i} \equiv y^2 \pmod n.$$

It follows that $(x+y)(x-y) = x^2 - y^2 \equiv 0 \pmod n$. □

Remark 10.33. Using Heron's method, one can calculate $\sqrt{n}$ (in particular, one can check whether n is a perfect square, cf. Exercise 48). It is advisable to choose the x_i above $\sqrt{n}$, because then $x_i^2 - n$ is "small" and can be easily factored. If r is small enough, trial divisions suffice (if this fails, then $x_i^2 - n$ does not have the desired form). For $m > r$, $Av = 0$ can always be solved (using the Gaussian algorithm), i.e., the algorithm is successful as long as one finds enough x_i. For "large" numbers n up to approx. 100 decimal digits, the quadratic sieve is the fastest known factorization method. For even larger numbers, the *number field sieve* is used. This is a similar algorithm in the ring of integers of a number field.

Example 10.34.

(i) Let $n = 101069$ and $\{p_1, p_2, p_3\} = \{2, 5, 11\}$. With $\lceil \sqrt{n} \rceil = 318$ we find the following decompositions:

$$\begin{aligned} 318^2 - n &= 5 \cdot 11, \\ 320^2 - n &= 11^3, \\ 337^2 - n &= 2^2 \cdot 5^5. \end{aligned}$$

Thus

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

with the solution $v = (1, 1, 1)$. We set $x = 318 \cdot 320 \cdot 337 \equiv 30729 \pmod n$ and $y = 2 \cdot 5^3 \cdot 11^2 = 30250$. This yields $\gcd(x + y, n) = 211$ and $\gcd(x - y, n) = 479$.

(ii) In 1994, a 129-digit number known as RSA-129 was factored into the following prime numbers using the quadratic sieve:

$$\begin{aligned} &3490529510847650949147849619903898133417764638493387843990820577 \\ &3276913299326670954996198819083446141317764296799294253979828853 3 \end{aligned}$$

Remark 10.35. If the prime numbers p and q in the RSA procedure are close to each other, it can happen that one encounters $x = x_i = \frac{p+q}{2}$ in the quadratic sieve. With $y := \frac{|p-q|}{2}$, then $x^2 - y^2 = pq = n$ and $\{x + y, x - y\} = \{p, q\}$ holds. However, there is a better "attack" for this.

Theorem 10.36. *If $|p - q| < 2\sqrt[4]{n}$ holds in the RSA procedure, then $p + q = \lceil 2\sqrt{n} \rceil$. In particular, p and q can be calculated from n.*

Proof. From

$$(p + q - 2\sqrt{n})(p + q + 2\sqrt{n}) = (p + q)^2 - 4n = (p - q)^2 \geq 0$$

it follows that

$$0 \le p+q-2\sqrt{n} = \frac{|p-q|^2}{p+q+2\sqrt{n}} < \frac{4\sqrt{n}}{4\sqrt{n}} = 1.$$

This shows $p+q = \lceil 2\sqrt{n} \rceil$. Thus $p+q$ can be calculated from n. Now p and q are the solutions of the quadratic equation $X^2 - (p+q)X + n$. □

Definition 10.37. Let K be a field and $a_1, \ldots, a_5 \in K$. One calls

$$\mathcal{E}(a_1, \ldots, a_5) := \left\{(x,y) \in K^2 : y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5\right\}$$

an *elliptic curve*.[22]

Lemma 10.38. *In the case* $\operatorname{Char} K \notin \{2,3\}$*, every elliptic curve can be transformed by an affine transformation into the* Weierstrass normal form

$$\mathcal{E}(a,b) := \left\{(x,y) \in K^2 : y^2 = x^3 + ax + b\right\}$$

with $a, b \in K$.

Proof. For $y \in K$ let $\widetilde{y} := y + \frac{1}{2}a_1x + \frac{1}{2}a_2$ (well-defined because $\operatorname{Char} K \neq 2$). Then

$$(x,y) \in \mathcal{E}(a_1, \ldots, a_5) \iff \widetilde{y}^2 = y^2 + a_1xy + a_2y + \frac{1}{4}a_1^2x^2 + \frac{1}{4}a_2^2 + \frac{1}{2}a_1a_2x = x^3 + a'x^2 + b'x + c'$$

holds with certain $a', b', c' \in K$. With the affine transformation $\widetilde{x} := x + \frac{1}{3}a'$ one obtains $\widetilde{y}^2 = \widetilde{x}^3 + a\widetilde{x} + b$ with certain $a, b \in K$. □

Remark 10.39. In the following, we exclusively consider elliptic curves in Weierstrass normal form.

Definition 10.40. Let $\mathcal{E} = \mathcal{E}(a,b)$ be an elliptic curve. Let $O = (\infty, \infty)$ be a new symbol and $\mathcal{E}^+ := \mathcal{E} \cup \{O\}$. For $P \in \mathcal{E}^+$ let $P + O := P =: O + P$. For $P = (x_1, y_2) \in \mathcal{E}$, $Q = (x_2, y_2) \in \mathcal{E}$ let $P + Q = (x_3, y_3) = \big(d^2 - x_1 - x_2,\ d(x_1 - x_3) - y_1\big)$ with

$$d := \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P \neq Q, \\ \frac{3x_1^2 + a}{2y_1} & \text{if } P = Q. \end{cases}$$

Lemma 10.41. *Let* $\mathcal{E}$ *be an elliptic curve. Then* $P + Q \in \mathcal{E}^+$ *for all* $P, Q \in \mathcal{E}^+$.

Proof. Wlog. let $P = (x_1, y_1) \neq O$ and $Q = (x_2, y_2) \neq O$. First, let $x_1 \neq x_2$ and $d = \frac{y_2 - y_1}{x_2 - x_1} \in K$. We consider the monic polynomial

$$\alpha := X^3 + aX + b - \big(d(X - x_1) + y_1\big)^2 \in K[X].$$

Clearly, $\alpha(x_1) = \alpha(x_2) = 0$ holds. Polynomial division yields an $x_3 \in K$ with $\alpha = (X - x_1)(X - x_2)(X - x_3)$. A comparison of the coefficients of X^2 shows $d^2 = x_1 + x_2 + x_3$, i. e. $x_3 = d^2 - x_1 - x_2$. For $y_3 := d(x_1 - x_3) - y_1$, it holds that

$$y_3^2 = \big(d(x_3 - x_1) + y_1\big)^2 = x_3^3 + ax_3 + b - \alpha(x_3) = x_3^3 + ax_3 + b.$$

[22] The equation itself does not describe an ellipse, but equations of this form occur in line integrals of ellipses.

This shows $P + Q = (x_3, y_3) \in \mathcal{E}^+$.

Now let $x_1 = x_2$. Then $y_1^2 = y_2^2$ holds, i. e. $y_1 = \pm y_2$. If $y_1 = -y_2$, then the definition yields $P + Q = O$ by interpreting $\frac{1}{0} = \infty$. Finally, let $P = Q$ and $y_1 \neq 0$. Then $d = \frac{3x_1^2 + a}{2y_1} \in K$. The (formal) derivative of α (as above) is

$$\alpha' = 3X^2 + a - 2d\big(d(X - x_1)^2 + y_1\big).$$

Because of $\alpha'(x_1) = 3x_1^2 + a - 2y_1 d = 0$, x_1 is a double root of α. Therefore, there exists an $x_3 \in K$ with $\alpha = (X - x_1)^2(X - x_3)$. A comparison of the coefficients of X^2 shows $x_3 = d^2 - 2x_1$. For $y_3 := d(x_1 - x_3) - y_1$, it holds as before that $y_3^2 = x_3^3 + ax_3 + b$. Thus, in this case as well, $P + Q = (x_3, y_3) \in \mathcal{E}^+$. □

Remark 10.42. It is natural to suspect that $\mathcal{E}^+$ is an abelian group. Obviously, O is an identity element and $(x, -y)$ is inverse to $(x, y) \in \mathcal{E}$. Furthermore, one easily sees that $P + Q = Q + P$ holds for all $P, Q \in \mathcal{E}^+$. Associativity, on the other hand, is by no means clear and only holds under an additional assumption. For example, $(0, 0), (1, 1) \in \mathcal{E}(0, 0)$ and $(0, 0) + (1, 1) = (0, 0)$ in contradiction to $(1, 1) \neq O$.

Definition 10.43. An elliptic curve $\mathcal{E}(a, b)$ is called *singular*, if $4a^3 + 27b^2 = 0$.

Remark 10.44.

(i) One can show that an elliptic curve $\mathcal{E}(a, b)$ is singular if and only if the polynomial $X^3 + aX + b \in K[X]$ has a multiple root.[23] If $\mathcal{E}$ is non-singular, then $\mathcal{E}^+$ is indeed an abelian group. The proof of associativity can be carried out either with a lengthy calculation[24] or with algebraic geometry.

(ii) For each $x \in K$, there exists at most one $y \in K$ with $(x, y), (x, -y) \in \mathcal{E}$. For finite fields K, it therefore holds that $|\mathcal{E}^+| = |\mathcal{E}| + 1 \leq 2|K| + 1$. Hasse proved the stronger estimate

$$|K| - 2\sqrt{|K|} + 1 \leq |\mathcal{E}^+| \leq |K| + 2\sqrt{|K|} + 1.$$

An element of order 2 in $\mathcal{E}^+$ has the form $(x, 0)$, where x is a root of $X^3 + aX + b$. There can therefore be at most three such elements. One can show that $\mathcal{E}^+$ is a direct product of at most two cyclic groups. Often $\mathcal{E}^+$ itself is cyclic.

(iii) One can formulate the DHM key exchange or the Elgamal procedure with the discrete logarithm in $\mathcal{E}^+$. Through the parameters K, a and b, one has significantly more possibilities than in the residue class ring $\mathbb{Z}/n\mathbb{Z}$. Heuristically, a good security level can thereby be achieved with a shorter key length. Bitcoin[25] uses, for example, $\mathcal{E}(0, 7) = \{(x, y) : y^2 = x^3 + 7\}$ over $K = \mathbb{F}_p$ with

$$\begin{aligned} p &= 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1 \\ &= 115792089237316195423570985008687907853269984665640564039457584007908834671663 \in \mathbb{P}. \end{aligned}$$

Here $\mathcal{E}^+$ is cyclic with prime order

$$\begin{aligned} |\mathcal{E}^+| &= 115792089237316195423570985008687907852837564279074904382605163141518161494337 \\ &= p - 432420386565659656852420866390673177326. \end{aligned}$$

One may compare the parameter order of magnitude with Example 10.26.

[23] see discriminant in Algebra notes
[24] see [Zwegers, *An Elementary Approach to the Group Law on Elliptic Curves*, 2024, arXiv:2401.02346v2]
[25] see `https://en.bitcoin.it/wiki/Secp256k1`

(iv) Shor has developed efficient algorithms for the discrete logarithm and for the factorization of numbers on quantum computers. The idea for factorizing a number n consists of choosing $1 < a < n$ randomly and calculating the powers $\{(a + n\mathbb{Z})^k : k = 1, \ldots, n-1\}$ *simultaneously*. In this way, one obtains $\mathrm{ord}_n(a)$ and can argue as in the proof of Theorem 10.27. Should powerful quantum computers become available in the future, common asymmetric encryption methods will become insecure (symmetric methods like AES are not affected by this so far). In *post-quantum cryptography*, alternatives are therefore being developed. They are based, for example, on lattices, linear codes or decision problems in finitely generated (non-abelian) groups.

Example 10.45. Let $\mathcal{E} = \mathcal{E}(1,2)$ over $K = \mathbb{F}_{11}$. Because of $4 + 27 \cdot 2^2 \equiv 2 \pmod{11}$, $\mathcal{E}$ is non-singular. One calculates

$$\mathcal{E} = \big\{(1, \pm 2), (2, \pm 1), (4, \pm 2), (5, 0), (6, \pm 2), (7, 0), (8, \pm 4), (9, \pm 5), (10, 0)\big\}$$

and $|\mathcal{E}^+| = 16$. Since there are three elements of order 2, $\mathcal{E}^+$ is not cyclic. Because of

$$2(4,2) = \big(d^2 + 3, d(4 - x_3) - 2\big) = (8,4) \qquad \Big(d = \frac{3 \cdot 5 + 1}{4} = 4\Big)$$

$\mathcal{E}^+$ possesses an element of order 8 with $(4,2)$. Therefore $\mathcal{E}^+ \cong \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ holds.

Exercises

Exercise 1 (2 points)**.** Construct the 11-adic expansion of 123456789.

Exercise 2 (2 + 2 points)**.** We consider the Nim game from Example 1.6.

(a) Let three piles with 45, 33, 24 coins each be given. Check which of the players can force a win and provide a corresponding sequence of moves.

(b) Who can win with the starting position $(m_1, m_2, m_3) = (1, 2k, 2k+1)$ or $(1, 2k, 2k-1)$?

Exercise 3 (2 + 2 + 2 + 2 + 3 points)**.** The *Fibonacci numbers* are recursively defined by $f_1 := 1$, $f_2 := 1$ and $f_{n+2} := f_{n+1} + f_n$ for $n \in \mathbb{N}$.

(a) Show $f_1 + f_3 + \ldots + f_{2n+1} = f_{2n+2}$ for $n \geq 0$.

(b) Show $1 + f_1 + f_2 + \ldots + f_n = f_{n+2}$ for $n \geq 1$.

(c) For which n is f_n divisible by 3?

(d) For which n is f_n divisible by 4?

(e) Prove

$$f_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

for $n \in \mathbb{N}$.

Exercise 4 (3 points)**.** Calculate $\gcd(813, 1329)$ and find $a, b \in \mathbb{Z}$ with

$$813a + 1329b = \gcd(813, 1329).$$

Exercise 5 (3 points)**.** (Lamé) How large must $a, b \in \mathbb{N}$ at least be, so that the Euclidean algorithm for calculating $\gcd(a, b)$ runs through exactly $k \in \mathbb{N}$ iterations?
Note: The solution leads to a well-known sequence of numbers.

Exercise 6 (Coin problem)**.** Suppose you possess arbitrarily many coins with values a and b Euro, where $a, b \in \mathbb{N}$ are coprime. Show:

(a) You cannot pay the amount $ab - a - b$ Euro exactly (i. e. without change).

(b) You can pay every integer Euro amount greater than $ab - a - b$.

Exercise 7 (2 points)**.** Show that there are infinitely many prime numbers of the form $6n - 1$.

Exercise 8 ($2 + 2 + 2$ points)**.** For $n \in \mathbb{N}_0$ let $F_n := 2^{2^n} + 1$ be the n-th Fermat number. Show that:

(a) $\prod_{k=0}^{n-1} F_k = F_n - 2$ for $n \in \mathbb{N}_0$.

(b) $\gcd(F_n, F_m) = 1$ for $n \neq m$.

(c) Using (b), give a new proof for $|\mathbb{P}| = \infty$.

Exercise 9 (2 points)**.** Let $b \in \mathbb{N}$ such that at least one prime divisor of b occurs with multiplicity 1. Let $a \in \mathbb{N}$ be no power of b. Show that $\log_b(a)$ is irrational.

Exercise 10 ($2 + 3$ points)**.**

(a) Calculate $\operatorname{lcm}(10.403, 10.807)$.

(b) Show $\gcd(a^n - 1, a^m - 1) = a^{\gcd(n,m)} - 1$ for $a, n, m \in \mathbb{N}$.

Exercise 11 (3 points)**.** Determine the prime factorization of 42!. How many zeros are at the end of the decimal expansion of 42!?

Exercise 12 (3 points)**.** Suppose there are 8-euro bills and you possess arbitrarily many 5- and 8-euro bills. Show that you can pay every sufficiently large natural euro amount.

Exercise 13 ($2 + 2 + 2$ points)**.** Prove:

(a) $\pi(n^2) \geq n$ for $n \in \mathbb{N} \setminus \{1\}$.

(b) If p_n is the n-th prime (i.e., $p_1 = 2$, $p_2 = 3$, etc.), then $p_n \leq n^2$ for $n \geq 2$.

(c) If $n! = m^k \geq 2$ for $n, m, k \in \mathbb{N}$, then $k = 1$.

Exercise 14 (2 points)**.** Let $n \in \mathbb{N}$ be divisible by all numbers from $1, \ldots, 200$ except for two consecutive numbers $d, d + 1$. Determine d.

Exercise 15 (3 points)**.** Determine the smallest natural number n with the property

$$\forall p \in \mathbb{P} : p \mid n \iff (p-1) \mid n.$$

Exercise 16 (2 + 2 points)**.** Let $p, q \in \mathbb{P} \setminus \{3, 5\}$. Show:

(a) $p^2 \equiv q^2 \pmod{24}$.

(b) $p^4 \equiv 1 \pmod{240}$.

Exercise 17 (2 + 2 + 2 points)**.**

(a) Solve the equation $47x \equiv 27 \pmod{89}$ in $\mathbb{Z}$.

(b) Solve the system

$$\begin{aligned} x &\equiv 11 \pmod{37}, \\ 2x &\equiv 13 \pmod{41}. \end{aligned}$$

Exercise 18 (3 points)**.** Five pirates and a monkey are stranded on a desert island. On the first day they collect n coconuts. In the following night, one pirate wakes up to secure his share. He divides the pile of coconuts into five equal parts, with one coconut remaining, which he gives to the monkey. Then he brings one of the five parts to a secret hiding place and goes back to sleep. A short time later, the second pirate also wakes up to perform the same procedure (again one nut remains for the monkey). In the further course of the night, the remaining three pirates also perform this procedure. The next morning, the remaining pile is distributed in equal parts to the five pirates, whereby this time no nut remains. How large was n at least?

Exercise 19 (3 points)**.** Show that there are 48 consecutive natural numbers that all have a square divisor.
Hint: Chinese Remainder Theorem.

Exercise 20 (2 points)**.** Check whether the ISBN 123456789X is valid.

Exercise 21 (2 + 2 + 2 + 2 + 2 points)**.** Let $n \in \mathbb{N}$. Show:

(a) n is divisible by 2^k (resp. 5^k) if and only if the number formed by the last k decimal digits is divisible by 2^k (resp. 5^k).

(b) n is divisible by 3 (resp. 9) if and only if the *digit sum* of n is divisible by 3 (resp. 9). (The digit sum is the sum of the decimal digits.)

(c) n is divisible by 11 if and only if the alternating sum of the decimal digits of n is divisible by 11. It does not matter whether one starts the sum from the left or right. Example: $n = 253 \to 2-5+3 = 0 \implies 7 \mid 253$.

(d) Let $n = 10a+b$. n is divisible by 7 if and only if $a-2b$ is divisible by 7. Example: $1452 \to 145-4 = 141 \to 14-2 = 12 \not\equiv 0 \pmod{7}$.

(e) Find a divisibility rule for 13.

Exercise 22 (3 points). (Wilson) Let $2 \leq n \in \mathbb{N}$. Show that n is a prime number if and only if

$$(n-1)! \equiv -1 \pmod{n}$$

holds.

Exercise 23 (2 + 2 points).

(a) Determine all $n \in \mathbb{N}$ with $\varphi(n) = 14$.

(b) Determine the prime factorization of 626.257.
Hint: $\varphi(626.257) = 624.640$.

Exercise 24 (3 + 3 points). Let p and $q = 2p - 1$ be prime numbers and $n := pq$. Let $a \in \mathbb{N}$ be a quadratic residue, but not a fourth power modulo q. Let a not be a quadratic residue modulo p.

(a) Show that the Miller-Rabin test with base a does not detect that n is not a prime number.

(b) Construct a p such that the specified properties are satisfied for $a = 2$.

Exercise 25 (3 + 1 points). Let $n \in \mathbb{N}$ and $a_1 + n\mathbb{Z}, \ldots, a_r + n\mathbb{Z}$ be a generating set for $(\mathbb{Z}/n\mathbb{Z})^\times$. Show:

(a) The Miller-Rabin test with $a_1, \ldots, a_r$ provides a deterministic answer (no probability).

(b) It suffices to perform the Miller-Rabin test with prime numbers $a_1, \ldots, a_r$.

Exercise 26 (2 points). Let $n \geq 2$ and $R := \mathbb{Z}/n\mathbb{Z}$. Show that n is a prime number if and only if $(X+1)^n = X^n + 1$ holds in the polynomial ring $R[X]$.
Remark: This is the basis of the AKS algorithm.

Exercise 27 (2 points). Let $(G, \cdot)$ be an abelian group and $f, F \colon \mathbb{N} \to G$. Show that the following statements are equivalent:

(a) $F(n) = \prod_{d|n} f(d)$ for all $n \in \mathbb{N}$.

(b) $f(n) = \prod_{d|n} F(n/d)^{\mu(d)}$ for all $n \in \mathbb{N}$.

Exercise 28 (2 points). Let $s > 1$ be real. Show that

$$\Big(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\Big)^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Remark: Both series converge absolutely.

Exercise 29 (2 + 2 + 3 points).

(a) Calculate $(45 + 101\mathbb{Z})^{-1}$ in $(\mathbb{Z}/101\mathbb{Z})^\times$.

(b) Determine all generators of $(\mathbb{Z}/22\mathbb{Z})^\times$.

(c) Determine the number of elements in $(\mathbb{Z}/2200\mathbb{Z})^\times$ with order 5.

Exercise 30 (3 points)**.** Check with Fermat's Little Theorem whether 341 is a prime number.

Exercise 31 (2 points)**.**

(a) Show that 7 is the smallest primitive root modulo 71.

(b) Show that 4 is not a primitive root for any prime number.

Exercise 32 (2 + 2 + 2 points)**.** Show:

(a) For $n \geq 3$, $5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}$ holds.

(b) For $n \geq 2$, $\mathrm{ord}_{2^n}(5) = 2^{n-2}$ holds.

(c) For $n \in \mathbb{N}$, $(\mathbb{Z}/2^n\mathbb{Z})^\times = \{\pm 5^k + 2^n\mathbb{Z} : k = 1, \ldots, 2^{n-2}\}$ holds.

Exercise 33 (3 points)**.** Let $p > 2$ be a prime number and $a \in \mathbb{Z}$ with $\mathrm{ord}_{p^2}(a) = \varphi(p^2)$. Show that $\mathrm{ord}_{p^m}(a) = \varphi(p^m)$ for all $m \in \mathbb{N}$.

Exercise 34 (2 + 3 points)**.**

(a) Determine the period of the decimal expansion of $\frac{1}{43}$.

(b) Determine the period length of $\frac{3}{814}$.

Exercise 35 (2 points)**.** Determine the (infinite) 3-adic expansion of $\frac{3}{5}$ according to Theorem 5.2. *Hint:* Recall the method of long division from school.

Exercise 36 (3 points)**.** Determine a convergent $\frac{a}{b}$ for $\sqrt[3]{2}$ with $b \leq 1000$ and $|\sqrt[3]{2} - a/b| < \frac{1}{1001b}$.

Exercise 37 (2 + 2 + 2 points)**.**

(a) Determine the continued fraction of $\frac{1+\sqrt{7}}{2}$.

(b) Write the continued fraction $[2, 1, \overline{2, 3}]$ as a solution of a quadratic equation.

(c) Determine the solutions of the Pell equation $x^2 - 7y^2 = 1$.

Exercise 38 (3 points)**.** (Battle of Hastings) Harold's men stood, according to old custom, crowded together in 13 squares of equal size, and woe to the Norman who dared to try to break into such a phalanx. (...) But when Harold himself appeared on the battlefield, the Saxons formed a single massive square with their king at the head. How large is the army of Harold II supposed to have been?

Exercise 39 (2 points)**.** Let $k \in \mathbb{N}$ and $q := \lfloor 3^k/2^k \rfloor$. Show that $2^k q - 1$ cannot be written as a sum of $q + 2^k - 3$ non-negative k-th powers.

Exercise 40 (2 points)**.** Let $\omega := \frac{1+\sqrt{-3}}{2} \in \mathbb{Z}_{-3}$. Check whether $3 + 7\omega$ is a prime element in $\mathbb{Z}_{-3}$.

Exercise 41 (2 points)**.** Let $x \in \mathbb{C}$ be transcendental. Show that

$$\mathbb{Z}[x] := \Big\{ \sum_{i=0}^{n} a_i x^i : n \in \mathbb{N}, a_0, \ldots, a_n \in \mathbb{Z} \Big\} \subseteq \mathbb{C}$$

is a Euclidean ring.
Hint: Consider the smallest n with $a_n \neq 0$.

Exercise 42 (2 points)**.** Show that $\mathbb{Z}_{10}$ is not factorial.

Exercise 43 (2 points)**.** Write 941 as a sum of two squares.

Exercise 44 (2 points)**.** Let $n = 4^a(8b + 7) \in \mathbb{N}$ with $a, b \in \mathbb{N}_0$. Show that n is not the sum of three squares.

Exercise 45 (2 + 2 points)**.** Let $a, b \in \mathbb{Z}$ and $p \in \mathbb{P} \setminus \{2\}$. Describe using the Legendre symbol when the quadratic equation

$$x^2 + ax + c \equiv 0 \pmod{p}$$

has a solution $x \in \mathbb{Z}$. Use this to investigate whether $x^2 + x + 10 \equiv 0 \pmod{101}$ has a solution.

Exercise 46 (3 points)**.** Calculate the Jacobi symbols $\left(\frac{444}{97}\right)$, $\left(\frac{201}{91}\right)$ and $\left(\frac{551}{437}\right)$.

Exercise 47 (3 points)**.** For which prime numbers p is 3 a quadratic residue modulo p?

Exercise 48 (2 + 2 + 2 points)**.**

(a) To verify whether $n \in \mathbb{N}$ is a square, one can check whether n is a quadratic residue modulo given numbers $p_1, \ldots, p_r$ (this can be done efficiently using the Jacobi symbol). Investigate with what probability this algorithm provides a correct answer.

(b) We now want to check whether n is a k-th power of a natural number ($k \in \mathbb{N}$). Show that one has to test at most $\lceil \log_2(n) \rceil$ numbers a for $a^k = n$.
Hint: "Divide and conquer".

(c) Construct an algorithm with polynomial runtime in $\log(n)$ that checks whether n is a perfect power of a natural number ($a^k = n$ with $k \geq 2$).

Exercise 49 (2 points)**.** (HASTAD attack) We want to use the RSA procedure to send a mass email $m \in \mathbb{N}$ to $k \geq e$ many recipients with the public keys $(e, n_1), \ldots, (e, n_k)$ ($m < n_1, \ldots, n_k$). Is this a good idea?
Hint: Chinese Remainder Theorem.

Exercise 50 (2 + 2 points)**.**

(a) Encrypt the message $t = 14$ with the RSA procedure with respect to the public key $(n, e) = (209, 13)$, i. e. calculate $\tilde{t}$ with the notation from Theorem 10.24.

(b) Decrypt the message $\tilde{t} = 100$ with the help of the private key $d = 11$.

Exercise 51 (3 points)**.** (MONTGOMERY ladder) Let $G = \langle g \rangle$ be a group and $n = \sum_{i=0}^{k} b_i 2^i \in \mathbb{N}$ (binary representation) with $b_k = 1$. Show that the following algorithm calculates g^n with $2k$ multiplications:

Initialization: $x := g$, $y := g^2$.
For $i = k-1, k-2, \ldots, 0$:
    If $b_i \equiv 0 \pmod 2$, calculate $y := xy$ and $x := x^2$.
    If $b_i \equiv 1 \pmod 2$, calculate $x := xy$ and $y := y^2$.
Output: $x = g^n$.

A Appendix

Supplementary results

Definition A.1. A function $f\colon \mathbb{N} \to \mathbb{R}$ is called *multiplicative*, if $f(ab) = f(a)f(b)$ holds for all coprime $a, b \in \mathbb{N}$.

Example A.2. The Euler φ-function (Theorem 3.16) and the Möbius function μ (Definition 3.19) are multiplicative. Furthermore, the restriction of a Dirichlet character to $\mathbb{N}$ is multiplicative. For all $r \in \mathbb{R}$, $f\colon \mathbb{N} \to \mathbb{R}$, $n \mapsto n^r$ is multiplicative.

Theorem A.3 (Erdős)**.** *Let $f\colon \mathbb{N} \to \mathbb{R}$ be monotonically increasing, multiplicative and not constantly 0. Then there exists an $r \in \mathbb{R}$ with $f(n) = n^r$ for all $n \in \mathbb{N}$.*

Proof (Moser-Lambek). In the case $f(1) = 0$, it would follow that $f(n) = f(n)f(1) = 0$ for all $n \in \mathbb{N}$. Thus $f(1) \neq 0$. From $f(1) = f(1)^2$ it follows that $f(1) = 1$. Since f is monotonically increasing, $f(n) \geq 1$ holds for all $n \in \mathbb{N}$. For $a, t \in \mathbb{N}$ with $a \geq 3$ we consider

$$\begin{aligned} \sigma(t) &:= a^t + a^{t-1} + \ldots + 1 \in \mathbb{N}, \\ \tau(t) &:= a^t - a^{t-1} - \ldots - 1 \in \mathbb{N}. \end{aligned}$$

Because of $\sigma(t) \equiv 1 \equiv -\tau(t) \pmod{a}$, we have $\gcd(a, \sigma(t)) = \gcd(a, \tau(t)) = 1$. From the monotonicity of f it follows that

$$\begin{aligned} f(\sigma(t)) \geq f(\sigma(t) - 1) = f(a\sigma(t-1)) = f(a)f(\sigma(t-1)) \geq \ldots \geq f(a)^t, \\ f(\tau(t)) \leq f(\tau(t) + 1) = f(a\tau(t-1)) = f(a)f(\tau(t-1)) \leq \ldots \leq f(a)^t. \end{aligned} \tag{A.1}$$

For $n \geq 4$ let $k \in \mathbb{N}$ be the largest number with $a^k < n$. Then $k < \log_a(n) \leq k + 1$ holds. By the definition of σ and τ, we have $\sigma(k-1) \leq a^k < n$ and $\tau(k+2) \geq a^{k+2} - 2a^{k+1} \geq a^{k+1} \geq n$. From (A.1) it follows that

$$\begin{aligned} f(n) \geq f(\sigma(k-1)) \geq f(a)^{k-1} \geq f(a)^{\log_a(n)-2}, \\ f(n) \leq f(\tau(k+2)) \leq f(a)^{k+2} \leq f(a)^{\log_a(n)+2}. \end{aligned}$$

For arbitrary $a, b \geq 3$ one obtains $f(a)^{\log_a(n)-2} \leq f(n) \leq f(b)^{\log_b(n)+2}$. We exponentiate with $\ln(n)^{-1}$. Because of $\frac{\ln(n)}{\ln(a)} = \log_a(n)$ one obtains

$$f(a)^{\ln(a)^{-1} - 2\ln(n)^{-1}} \leq f(n)^{\ln(n)^{-1}} \leq f(b)^{\ln(b)^{-1} + 2\ln(n)^{-1}}.$$

With $n \to \infty$ it follows that $f(a)^{\ln(a)^{-1}} \leq f(b)^{\ln(b)^{-1}}$. After swapping a and b, $c := f(a)^{\ln(a)^{-1}} \geq 1$ is constant for all $a \geq 3$. For $r := \ln(c)$ we have

$$f(a) = c^{\ln(a)} = e^{r\ln(a)} = a^r \qquad (a \geq 3).$$

For $a = 1$ we have $f(1) = 1 = 1^r$. Because of $6^r = f(6) = f(2)f(3) = f(2)3^r$, we also have $f(2) = 2^r$. □

Definition A.4.

- For $a, b \in \mathbb{N}$ let $[a, b] := \{a, a+1, \ldots, b\}$ be the closed interval between a and b in $\mathbb{N}$ (in the case $a > b$ let $[a, b] = \varnothing$).

- For a set M and $k \in \mathbb{N}$ let $\binom{M}{k}$ be the set of all k-element subsets of M.

Theorem A.5 (Schur)**.** *For all $n \in \mathbb{N}$ there exists an $S(n) \in \mathbb{N}$ with the following property: For every mapping $f\colon \mathbb{N} \to [1,n]$ there exist $x, y \in \mathbb{N}$ with $x + y \leq S(n)$ and $f(x) = f(y) = f(x+y)$.*

Proof. Let first $S \in \mathbb{N}$ be arbitrary and $f\colon \mathbb{N} \to [1,n]$. For $i \in [1,n]$ let

$$\mathcal{M}_i := \Big\{\{a,b\} \in \binom{[1,S]}{2} : f(|a-b|) = i\Big\}.$$

Then $\binom{[1,S]}{2} = \mathcal{M}_1 \,\dot\cup \ldots \dot\cup\, \mathcal{M}_n$. According to Ramsey's Theorem[26] there exist $1 \leq a < b < c \leq S$ with $\{a,b\}, \{a,c\}, \{b,c\} \in \mathcal{M}_i$, i. e. $f(b-a) = f(c-b) = f(c-a)$, provided S is large enough (depending on n). The assertion then holds with $x := b-a$ and $y := c-b$ (the case $x = y$ is allowed). □

Remark A.6. We show that Fermat's Last Theorem over finite fields is false.

Theorem A.7 (Dickson)**.** *For all $n \in \mathbb{N}$ there exists a $D(n) \in \mathbb{N}$ with the following property: For every prime $p \geq D(n)$ there exist $x, y, z \in \mathbb{F}_p^\times$ with $x^n + y^n = z^n$.*

Proof. Let $D := S + 1$ with $S := S(n)$ from Theorem A.5 and $p \geq D$. Let $\zeta \in \mathbb{F}_p$ be a generator of $G := \mathbb{F}_p^\times$ (Theorem 4.18) and $H := \langle \zeta^n \rangle \leq G$. Because of $S < D \leq p$, the map

$$f\colon [1,S] \to G/H, \qquad a \mapsto (a + p\mathbb{Z})H$$

is well-defined. According to Lemma 4.13, $|G : H| = \gcd(p-1, n) \leq n$. According to Schur, there exist $a, b \in \mathbb{N}$ with $a + b \leq S$ and $(a + p\mathbb{Z})H = (b + p\mathbb{Z})H = (a + b + p\mathbb{Z})H$. For $\bar a := a + p\mathbb{Z} \in G$ and $\bar b := b + p\mathbb{Z} \in G$, it therefore holds that $\bar a^{-1}\bar b, 1 + \bar a^{-1}\bar b \in H$. Thus there exist $s, t \in \mathbb{Z}$ with $\bar a^{-1}\bar b = \zeta^{sn}$ and $1 + \bar a^{-1}\bar b = \zeta^{tn}$. For $x := 1$, $y := \zeta^s$ and $z := \zeta^t$, it now holds that

$$x^n + y^n = 1 + \zeta^{sn} = 1 + \bar a^{-1}\bar b = z^n.$$ □

Example A.8. According to Fermat's Little Theorem, the equation $x^{p-1} + y^{p-1} = z^{p-1}$ can have no solutions in $\mathbb{F}_p^\times$ (otherwise $0 = 1$ would hold). Thus $D(n) \geq n + 2$. Obviously $1 + 1 = 2$ is a solution for $n = 1$ and $p \geq 3$. One can therefore set $D(1) = 3$. For $(n,p) = (2,5)$ there is no solution, because $x^2 \equiv \pm 1 \pmod 5$ for all $x \in \mathbb{F}_5^\times$. For $p \geq 7$, on the other hand, the Pythagorean triple $3^2 + 4^2 = 5^2$ is a solution. One obtains $D(2) = 6$. In the case $\gcd(n, p-1) = 1$, $\mathbb{F}_p^\times = \{x^n : x \in \mathbb{F}_p^\times\}$ holds and the equation always has a solution.

Exercise 52. Determine $D(3)$.

Definition A.9. In the following, let a map $f\colon \mathbb{N} \to [1,r]$ be given.

- We use the shorthand notation $[a;k] := [a, a+k-1]$ for intervals of length k. Two intervals $[a;k]$ and $[b;k]$ are called *congruent* with respect to f if $f(a+i) = f(b+i)$ for $i = 0, \ldots, k-1$. If applicable, we write $[a;k] \equiv [b;k]$.

[26] See notes on logic and set theory

- An interval $[a;k]$ is called (d,s)-*shiftable* in $[b;n]$ if $b \le a \le a+sd+k \le b+n$ and $[a;k] \equiv [a+id;k]$ for $i = 1,\dots,s-1$. The intervals $[a+id;k]$ shifted by multiples of d are thus congruent and lie in $[b;n]$. The last interval $[a+sd;k]$ still lies in $[b;n]$, but does not have to be congruent to $[a;k]$.

Remark A.10.

(i) The congruence of intervals is an equivalence relation on the set of all intervals of length k of $\mathbb{N}$. The number of equivalence classes is at most k^r for a given $f\colon \mathbb{N} \to [1,r]$.

(ii) If $[a;k]$ is (d,s)-shiftable in $[b;n]$, then every subinterval $[a';k'] \subseteq [a;k]$ is also (d,s)-shiftable in $[b;n]$ (note $k' \le k$).

Lemma A.11 (Mills). *For all $r,s,t \in \mathbb{N}$ there exists an $N \in \mathbb{N}$ with the following property: For all $b \in \mathbb{N}$ and $f\colon \mathbb{N} \to [1,r]$ there exist $a,d \in \mathbb{N}$, such that $[a;t]$ is (d,s)-shiftable in $[b;N]$.*

Proof. If the assertion holds for N, then it also holds for $N+1$. Let therefore $W_s(t)$ be the smallest number N for which the assertion holds (depending on s,t with fixed r). For $s=1$, $[a;t]$ is already $(d,1)$-shiftable if $b \le a \le a+d+t \le b+n$ holds. With $a=b$ and $d=1$ one obtains $W_1(t) = t+1$. Let us assume inductively that $W_s(t)$ exists for some $s \ge 1$ and all t. Let $u := r^t$, $t_0 := t$ and $t_i := W_s(t_{i-1})$ for $i = 1,\dots,u$. It suffices to show $W_{s+1}(t) \le 2t_u$.

Let $I_u := [b;t_u]$. For $i = u-1, u-2, \dots, 0$ there exists by induction a (d_i,s)-shiftable interval $I_i := [a_i;t_i]$ in I_{i+1}. Let

$$b_i := a_0 + s(d_0 + \dots + d_{i-1})$$

for $i = 0,\dots,u$. Among the $u+1$ intervals $[b_i;t]$, at least two must be congruent by the pigeonhole principle and Remark A.10. So let $0 \le p < q \le u$ with $[b_p;t] \equiv [b_q;t]$ and

$$d := d_p + d_{p+1} + \dots + d_q.$$

It suffices to show that $[b_p;t]$ is $(d,s+1)$-shiftable in $[b;2t_u]$.

By assumption $I_0 = [a_0,t_0] = [b_0;t]$ is (d_0,s)-shiftable in I_1. In particular, $[b_1;t] = [b_0+sd_0;t] \subseteq I_1$ holds. By Remark A.10, $[b_1;t]$ is (d_1,s)-shiftable in I_2. It follows $[b_2;t] = [b_1+sd_1;t] \subseteq I_2$. Iteratively one obtains $[b_p;t] \subseteq I_p$. Let $0 \le i < s$. By the same argument $[b_p+id_p;t] \subseteq I_{p+1}$, $[b_p+i(d_p+d_{p+1});t] \subseteq I_{p+2}$ etc. Finally $[b_p+id;t] \subseteq I_q \subseteq I_u \subseteq [b;2t_u]$. Furthermore

$$[b_p;t] \equiv [b_p+id_p;t] \equiv \dots \equiv [b_p+id;t]$$

holds. For $i=s$ one obtains $[b_p+sd;t] = [b_q;t] \equiv [b_p;t]$ by the choice of p and q. From $[b_q;t] \subseteq [b;t_u]$ it follows $b_q + t \le b + t_u$. Because of

$$b + d \le b_p + sd + t = b_q + t \le b + t_u$$

it follows $d \le t_u$. Thus $b_p + (s+1)d + t \le b + 2t_u$. This shows that $[b_p;t]$ is $(d,s+1)$-shiftable in $[b;2t_u]$. □

Theorem A.12 (van der Waerden). *For all $r,n \in \mathbb{N}$ there exists an $N(r,n) \in \mathbb{N}$ with the following property: For every mapping $f\colon \mathbb{N} \to [1,r]$ there exist $a,d \in \mathbb{N}$, such that f is constant on the* arithmetic progression

$$\{a+id : i = 0,\dots,n\} \subseteq [1,N(r,n)].$$

Proof. We choose $N \in \mathbb{N}$ as in Mills Lemma with $t = 1$ and $s = n + 1$. For $b = 1$ there exist $a, d \in \mathbb{N}$, such that $[a; 1] = \{a\}$ is (d, s)-shiftable in $[1; N] = [1, N]$. This means that $f(a) = f(a + id)$ holds for $i = 1, \ldots, s - 1 = n$ as claimed. □

Example A.13.

(i) If one lines up enough people in a row, one can choose arbitrarily many people of the same gender at equal intervals (this is the case $r = 2$).

(ii) Let $W(r, n)$ be the smallest number N for which Theorem A.12 holds. The above proof provides a conceivably poor upper bound for $W(r, n)$. Obviously $W(1, n) = n + 1$ (choose $a = d = 1$). According to the pigeonhole principle, f must take the same value twice on $[1, r + 1]$. Therefore $W(r, 1) = r + 1$. Beyond that, only a few values of $W(r, n)$ are known:

$$W(2,3) = 9, \qquad W(3,3) = 27, \qquad W(4,3) = 76, \qquad W(2,4) = 35$$
$$W(3,4) = 293, \qquad W(2,5) = 178, \qquad W(2,6) = 1132.$$

Tables

Prime numbers ≤ 1000:

2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569	571	577	587	593
599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743
751	757	761	769	773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881	883	887	907	911
919	929	937	941	947	953	967	971	977	983	991	997

Smallest primitive root modulo p:

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
	1	2	2	3	2	2	3	2	5	2	3	2	6	3	5	2	2
p	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137	139
	2	2	7	5	3	2	3	5	2	5	2	6	3	3	2	3	2

Primitive Pythagorean triples:

a	b	c	a	b	c	a	b	c
3	4	5	5	12	13	6	8	10
7	24	25	8	15	17	9	40	41
10	24	26	11	60	61	12	35	37
13	84	85	14	48	50	15	112	113
16	30	34	16	63	65	17	144	145
18	80	82	19	180	181	20	21	29
20	99	101	21	220	221	22	120	122
23	264	265	24	70	74	24	143	145
25	312	313	26	168	170	27	364	365
28	45	53	28	195	197	29	420	421
30	224	226	31	480	481	32	126	130
32	255	257	33	56	65	33	544	545
34	288	290	35	612	613	36	77	85
36	323	325	37	684	685	38	360	362
39	80	89	39	760	761	40	42	58
40	198	202	40	399	401	44	117	125
48	55	73	48	286	290	51	140	149
52	165	173	56	90	106	56	390	394
57	176	185	60	91	109	60	221	229
64	510	514	65	72	97	66	112	130
68	285	293	69	260	269	72	154	170
72	646	650	75	308	317	76	357	365
78	160	178	84	187	205	85	132	157
87	416	425	88	105	137	88	234	250
93	476	485	95	168	193	96	110	146
96	247	265	102	280	298	104	153	185

Jacobi symbol $\left(\frac{p}{q}\right)$ for $p, q \leq 20$ (p indexes the rows):

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	0	−	0	−	0	+	0	+	0	−	0	−	0	+	0	+	0	−	0
3	−	0	+	−	0	−	−	0	+	+	0	+	+	0	+	−	0	−	−
4	0	+	0	+	0	+	0	+	0	+	0	+	0	+	0	+	0	+	0
5	−	−	+	0	+	−	−	+	0	+	−	−	+	0	+	−	−	+	0
6	0	0	0	+	0	−	0	0	0	−	0	−	0	0	0	−	0	+	0
7	+	+	+	−	+	0	+	+	−	−	+	−	0	−	+	−	+	+	−
8	0	−	0	−	0	+	0	+	0	−	0	−	0	+	0	+	0	−	0
9	+	0	+	+	0	+	+	0	+	+	0	+	+	0	+	+	0	+	+
10	0	+	0	0	0	−	0	+	0	−	0	+	0	0	0	−	0	−	0
11	−	−	+	+	+	+	−	+	−	0	−	−	−	−	+	−	−	+	+
12	0	0	0	−	0	−	0	0	0	+	0	+	0	0	0	−	0	−	0
13	−	+	+	−	−	−	−	+	+	−	+	0	+	−	+	+	−	−	−
14	0	−	0	+	0	0	0	+	0	+	0	+	0	−	0	−	0	−	0
15	+	0	+	0	0	+	+	0	0	+	0	−	+	0	+	+	0	−	0
16	0	+	0	+	0	+	0	+	0	+	0	+	0	+	0	+	0	+	0
17	+	−	+	−	−	−	+	+	−	−	−	+	−	+	+	0	+	+	−
18	0	0	0	−	0	+	0	0	0	−	0	−	0	0	0	+	0	−	0
19	−	+	+	+	−	−	−	+	−	−	+	−	+	+	+	+	−	0	+
20	0	−	0	0	0	−	0	+	0	+	0	−	0	0	0	−	0	+	0

Smallest solution of the Pell equation $p^2 - nq^2 = 1$.

n	p	q	n	p	q	n	p	q
2	3	2	3	2	1	5	9	4
6	5	2	7	8	3	8	3	1
10	19	6	11	10	3	12	7	2
13	649	180	14	15	4	15	4	1
17	33	8	18	17	4	19	170	39
20	9	2	21	55	12	22	197	42
23	24	5	24	5	1	26	51	10
27	26	5	28	127	24	29	9801	1820
30	11	2	31	1520	273	32	17	3
33	23	4	34	35	6	35	6	1
37	73	12	38	37	6	39	25	4
40	19	3	41	2049	320	42	13	2
43	3482	531	44	199	30	45	161	24
46	24335	3588	47	48	7	48	7	1
50	99	14	51	50	7	52	649	90
53	66249	9100	54	485	66	55	89	12
56	15	2	57	151	20	58	19603	2574
59	530	69	60	31	4	61	1766319049	226153980
62	63	8	63	8	1	65	129	16
66	65	8	67	48842	5967	68	33	4
69	7775	936	70	251	30	71	3480	413
72	17	2	73	2281249	267000	74	3699	430
75	26	3	76	57799	6630	77	351	40
78	53	6	79	80	9	80	9	1
82	163	18	83	82	9	84	55	6
85	285769	30996	86	10405	1122	87	28	3
88	197	21	89	500001	53000	90	19	2
91	1574	165	92	1151	120	93	12151	1260
94	2143295	221064	95	39	4	96	49	5
97	62809633	6377352	98	99	10	99	10	1

Index