CIT413038 Winter 24/25

Elementary Number Theory

Lecturer: Prof. Dr. Violetta Weger

These lecture notes will be consistently updated before the lectures. If you find any typos, please send them to me via email.

Overview Number Theory is one of the oldest, most famous and most elegant branches of mathematics. It deals with the relationship between particular types of numbers.

Of great interest will be the integers and prime numbers. This particular interest is due to one of the most fundamental theorems of mathematics: *the fundamental theorem of arithmetic*, saying that any positive integer (larger than 1) has a unique prime factorization.

We will meet many famous mathematicians along the lecture, including Euler, Fermat and Gauss.

This lecture is called *elementary* number theory, as it is not based on any advanced or abstract mathematics and to distinguish it from analytical and algebraic number theory. At the end of the lecture, we will have a quick glance at algebraic number theory, i.e., the study of algebraic number fields.

You will learn how to deal with congruences, how to test for primality, how to find integer solutions of equations, how to approximate irrational numbers with rational numbers, and how to apply this beautiful branch of mathematics to cryptography.

Die Mathematik ist die Königin der Wissenschaften
und die Zahlentheorie ist die Königin der Mathematik.
Carl Friedrich Gauss

Administrative Information

The lectures will be held

- Tuesdays, 16:15-17:45 in MI 03.06.011
- Fridays, 10:15-11:45 in MI 02.08.011

Exercises: I will upload exercise sheets on Moodle, which are voluntary to solve, but upon 70% of correct completion, I will provide a grade bonus of $+0.3$. The tutorials will take place instead of every third lecture.

More precisely: we mark lectures in black and tutorials in blue.

Tuesday	Friday
15.10	18.10
22.10	25.10
29.10	
05.11	08.11
12.11	15.11
19.11	22.11
26.11	29.11
03.12	06.12
10.12	13.12
17.12	20.12
07.01	10.01
14.01	17.01
21.01	24.01
28.01	31.01
04.02	07.02

On 29.11, 10.01 there will be guest lectures by Prof. Panny. On 07.01, the tutorial will be skipped. In the last lecture we have an exam preparation.

Exam: The exam is on 11.2 and will either be in written (60 min) or oral (20 min) form, depending on the number of students.

Prerequisites:

- MA0004 Linear Algebra 1,
- MA0005 Linear Algebra 2 and Discrete Structures

Material: Most of the content of these lecture notes is based on

- the book *Elementary Number Theory* by G.A. Jones and J.M. Jones [1] and
- the wonderful book *Elementary Number Theory,* by K.H. Rosen [2] which is available online `https://tinyurl.com/3dwkn85h`

Let us have a quick glance at the highlights of this lecture.

Theorem 0.1 (Fundamental Theorem of Arithmetics)**.** *Every integer greater than 1 has a unique prime factorization.*

Theorem 0.2. *There exist infinitely many primes.*

And of course, the famous prime number theorem, proven in 1896 by Hadamard and de la Vallée-Poussin.

Theorem 0.3. *The number of primes behaves asymptotically as*

$$\lim_{x\to\infty} \frac{|\{p\,\textit{prime} \ \mid p \leq x\}|\ln(x)}{x} = 1.$$

Theorem 0.4 (Fermat)**.** *Every odd prime is the sum of two squares, i.e., there exists* $(x, y) \in \mathbb{Z}^2$ *with* $p = x^2 + y^2$ *if and only if* $p \equiv 1 \mod 4$*, i.e.,* $p = 4n + 1$ *for some positive integer* n*.*

We can then extend this to *Pythagorean triples*: $(a, b, c) \in \mathbb{N}^3$ with $a^2 + b^2 = c^2$. We will see a method in this lecture on how to find such triples.

However, we cannot extend this result to other powers:

Theorem 0.5 (Fermat's Last Theorem)**.** $a^n + b^n = c^n$ *has no non-trivial positive integer solutions, for* $n \geq 3$*.*

Note that Fermat only provided a proof for $n = 4$ in 1640 and Euler proved that

Theorem 0.6 (Euler)**.** $a^3 + b^3 = c^3$ *has no non-trivial positive integer solutions.*

Fermat's last Theorem has been an open conjecture for a long time, until it was finally proven by Wiles in 1994.

Theorem 0.7 (Catalan's Conjecture)**.** *8 and 9 are the only perfect powers (powers with exponents larger than 1) which are consecutive.*

This conjecture from 1844 was proven only in 2002 by Mihailescu.

One of the most famous conjectures in elementary number theory is the twin prime conjecture.

Open Question 0.8. *There exist infinitely many twin primes, i.e., prime number pairs* $(p, p + 2)$*.*

The generalization of this conjecture has recently (2013) been proven.

Theorem 0.9 (Zhang)**.** *There exist infinitely many prime pairs* $(p, p + k)$ *for at least one* $2 \leq k \leq 70000000$.

Another famous conjecture which is still wide open since 1742 is the following:

Open Question 0.10 (Goldbach's Conjecture)**.** *Every even integer greater than 2 is the sum of two primes.*

Although we will not solve these conjectures in the lecture, if such questions are interesting to you, then you might enjoy this course.

Contents

Notation

Since we cannot include everything, we will assume a certain background. For example, we assume that the integers, rationals, the pigeonhole principle, proof by induction or proof by contradiction are known concepts.

Throughout these lecture notes, we will make use of the following notation

- $\mathbb{N}$, to denote the positive integers,
- $\mathbb{N}_0$, to denote the non-negative integers,
- $\mathbb{Z}$, to denote the integers,
- $\mathbb{Q}$, to denote the rationals,
- $\mathbb{R}$, to denote the reals,
- For integers a, b we write $a \mid b$, to denote a divides b.
- For integers a, b we write $[a, b]$, respectively $[a, b)$, to denote the set of integers x with $a \leq x \leq b$, respectively with $a \leq x < b$.
- For a real number a we write $|a|$ to denote the absolute value of a.
- For a real number a we write $\lfloor a \rfloor$, respectively $\lceil a \rceil$, to denote the largest integer smaller than a, respectively the smallest integer larger than a.
- For a set S we denote by $|S|$ its cardinality.

This list might get updated as we progress in the course.

1 Divisibility

This section serves as a gentle start, as all of the covered topics should already be familiar to you from the lecture ”Discrete Structures”. In order to have self-contained lecture notes, we quickly cover it anyways.

1.1 Greatest Common Divisor

Definition 1.1. The *greatest common divisor* between two nonzero integers a, b, denoted by $\gcd(a, b)$, is defined as the largest positive integer c, which divides both a and b, i.e.,

$$\gcd(a, b) = \max\{c \in \mathbb{N} \mid c \mid a \text{ and } c \mid b\}.$$

Definition 1.2. The *least common multiple* between a, b, denoted by $\operatorname{lcm}(a, b)$, is defined as the smallest positive integer c, which is divisible by both a and b, i.e.,

$$\operatorname{lcm}(a, b) = \min\{c \in \mathbb{N} \mid a \mid c \text{ and } b \mid c\}.$$

If $\gcd(a, b) = 1$, we say that a and b are *relatively prime* or *coprime*.

Proposition 1.3. *Let a, b be integers with gcd$(a, b) = d$. Then,*

$$gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

Proof. Let a, b be positive integers with $\gcd(a, b) = d$ and assume that e is a positive integer with $e \mid \frac{a}{d}$ and $e \mid \frac{b}{d}$. Then, there exist integers k, ℓ with $\frac{a}{d} = ke$ and $\frac{b}{d} = \ell e$. Thus, $a = dek$ and $b = de\ell$, which makes de a common divisor of a and b. Since d is the greatest common divisor, this implies $e = 1$. □

1.2 Euclidean Division Algorithm

One way to compute the greatest common divisor between two integers is given by the *Euclidean division algorithm.*

The algorithm is given as input two integers $0 < b \leq a$ and outputs $\gcd(a, b)$. It works successively, updating variables r_i for the remainder of the division and q_i for the largest multiple. It starts by setting $r_0 = a, r_1 = b$ and in each step i finds r_{i+1}, q_i with $0 \leq r_{i+1} < r_i$, such that

$$r_{i-1} = r_i q_i + r_{i+1}.$$

That is in the first step it finds q_1 and $0 \leq r_2 < b$ such that

$$a = r_0 = q_1 b + r_2 = q_1 r_1 + r_2.$$

It proceeds with finding $0 \leq r_3 < r_2$ and q_2 such that

$$b = r_1 = q_2 r_2 + r_3.$$

The algorithm ends, as soon as $r_{n+1} = 0$, in which case $\gcd(a, b) = r_n$, the last nonzero remainder.

Thus the penultimate equation is

$$r_{n-2} = q_{n-1} r_{n-1} + r_n$$

and the last equation is

$$r_{n-1} = q_n r_n + 0.$$

Example 1.4. *Let $a = 1492, b = 1066$, then the Euclidean division algorithm proceeds as*

$$\begin{aligned}
1492 &= 1 \cdot 1066 + 426 \\
1066 &= 2 \cdot 426 + 214 \\
426 &= 1 \cdot 214 + 212 \\
214 &= 1 \cdot 212 + 2 \\
212 &= 106 \cdot 2 + 0,
\end{aligned}$$

hence we have found gcd$(1492, 1066) = 2$. We will see later (In Section 1.5 Representation of Integers) that the other remainders, r_i, also play an important role.

1.3 Bézout's Identity

The following result uses the Euclidean division algorithm to give a simple expression of $\gcd(a, b)$ in terms of a and b.

Theorem 1.5 (Bézout's Identity)**.** *Let a, b be nonzero integers, then there exist integers u, v such that*

$$gcd(a, b) = au + bv.$$

Proof. We use the equations which arise during the Euclidean division to compute $d = \gcd(a, b)$ as the last nonzero remainder. The penultimate equation is of the form

$$r_n = d = r_{n-2} - q_{n-1} r_{n-1}.$$

We use the previous equation of the form

$$r_{n-1} = r_{n-3} - q_{n-2} r_{n-2}$$

to eliminate r_{n-1} and express d instead as multiple of r_{n-3} plus a multiple of r_{n-2}. That is

$$d = r_{n-2} - q_{n-1}(r_{n-3} - q_{n-2}4r_{n-2}) = r_{n-2}(1 + q_{n-1}q_{n-2}) - r_{n-3}q_{n_1}.$$

We gradually work backwards until we have expressed d as multiple of a plus a multiple of b, that is

$$au + bv = d.$$

□

We also call this procedure the *extended Euclidean algorithm.*

Example 1.6. *Let us consider again* $a = 1492, b = 1066$. *In the penultimate equation we have*

$$2 = 214 - 1 \cdot 212.$$

We insert here the previous equation, which was

$$212 = 426 - 1 \cdot 214,$$

giving

$$2 = 214 - 1 \cdot (426 - 1 \cdot 214) = -1 \cdot 426 + 2 \cdot 214.$$

We continue in the same way, getting

$$\begin{aligned} d &= 2 \\ &= 214 - 1 \cdot 212 \\ &= 214 - 1 \cdot (426 - 1 \cdot 214) \\ &= -1 \cdot 426 + 2 \cdot 214 \\ &= -1 \cdot 426 + 2 \cdot (1066 - 2 \cdot 426) \\ &= 2 \cdot 1066 - 5 \cdot 426 \\ &= 2 \cdot 1066 - 5 \cdot (1492 - 1 \cdot 1066) \\ &= -5 \cdot 1492 + 7 \cdot 1066, \end{aligned}$$

which gives us $u = -5, v = 7$.

1.4 Diophantine Equations

Consider the following problem: you would like to buy 510 € worth of chocolate. The shop is only selling chocolate bars for either 20 € or 50 €. How many of each chocolate bar should you buy?

In other words we are looking for non-negative integer solutions (x, y) to the equation

$$50x + 20y = 510.$$

Whenever we deal with equations that require integer solution, we have a *Diophantine equation.*

Theorem 1.7. *Let a, b, c be integers and $d = gcd(a, b)$. The equation $ax + by = c$ has no integer solutions if $d \nmid c$. For $d \mid c$, we have infinitely many integer solutions.*

In particular, if one integer solution is given by (x_0, y_0), then all solutions are given by

$$\left(x_0 + \frac{bn}{d}, y_0 - \frac{an}{d}\right),$$

where n is an integer.

Proof. Assume that x, y are integers with $ax + by = c$. Since $d \mid a$ and $d \mid b$, we must also have $d \mid c$.

By Bézout's identity, we know that there exist integers s and t with $\gcd(a, b) = d = as + bt$. Since $d \mid c$, there exists an integer e with $c = de = (as + bt)e = a(se) + b(te)$. Thus, one solution for the equation is given by $x_0 = se, y_0 = te$.

Let us now consider $x = x_0 + \frac{bn}{d}, y = y_0 - \frac{an}{d}$, where n is an integer. We see that (x, y) is a solution as

$$ax + by = ax_0 + a\frac{bn}{d} + by_0 - b\frac{an}{d} = ax_0 + by_0 = c.$$

In fact, every solution must be of this form: assume x, y are integers with $ax + by = c$. Since $ax_0 + by_0 = c$, we can subtract the two equations to get

$$a(x - x_0) + b(y - y_0) = 0.$$

Thus, we can reformulate this to $a(x - x_0) = b(y_0 - y)$ and dividing both sides with d, we get

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y).$$

By Proposition 1.3, we have that gcd $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, and thus, we must have $\frac{a}{d} \mid (y_0 - y)$.

Hence, there is an integer n such that $n\frac{a}{d} = y_0 - y$, or equivalently $y = y_0 - \frac{an}{d}$. We can insert this value into the equation $a(x - x_0) = b(y_0 - y)$ to get $x = x_0 + \frac{bn}{d}$.

□

The proof also shows a technique to construct all integer solutions to linear Diophantine equations of the form

$$ax + by = c.$$

1. Compute $d = \gcd(a, b)$ using the Euclidean division algorithm.
2. Check if $d \mid c$. If it does not, there are no solutions. If $d \mid c$, then write $c = de$.
3. Using the extended Euclidean algorithm find the integers u, v such that $d = au + bv$. Set $x_0 = ue, y_0 = ve$.

4. Every integer solution is of the form $x = x_0 + \frac{bn}{d}, y = y_0 - \frac{an}{d}$, for integers n.

Example 1.8. *We can now solve our initial question: find* $(x, y) \in \mathbb{N}^2$ *such that* $50x + 20y = 510$. *Using the Euclidean algorithm we get*

$$\begin{aligned} 50 &= 2 \cdot 20 + 10, \\ 20 &= 2 \cdot 10 + 0 \end{aligned}$$

and hence gcd$(50, 20) = 10 = d$. *As* $10 \mid 510$ *we have solutions and find* $e = 51$. *Using the extended Euclidean algorithm, we get*

$$10 = 1 \cdot 50 - 2 \cdot 20,$$

which gives $u = 1, v = (-2)$. *We thus set* $x_0 = 51$ *and* $y_0 = -102$. *Hence, all solutions are given by*

$$(51 + 2n, -102 - 5n).$$

To get positive integers, we set $n \leq -21$ *and find the smallest positive solution given by* $x = 9, y = 3$.

1.5 Representation of Integers

Have you ever wondered why we write integers the way we do? When we write the number 529 we mean

$$5 \cdot 10^2 + 2 \cdot 10^1 + 9 \cdot 10^0.$$

This *representation* is called the *decimal system* and is most likely due to the fact that (most) humans have 10 fingers.

If we, however, would have 6 fingers, we would most likely be using the *heximal system* right now. That is, instead of 529 we would write 2241, as

$$2 \cdot 6^3 + 2 \cdot 6^2 + 4 \cdot 6^1 + 1 \cdot 6^0 = 529.$$

In order not to confuse the different systems, we rather write $(2, 2, 4, 1)_6$.

There are many different ways to represent integers. In fact, any positive integer b can be chosen as a basis, and for any positive integer n there exists a unique representation of n in the base of b. We use the notation $(a_k, \ldots, a_0)_b$ to denote

$$\sum_{i=0}^{k} a_i b^i.$$

Theorem 1.9. *Let b be a positive integer. Then, every positive integer n can be written uniquely in the form*

$$n = \sum_{i=0}^{k} a_i b^i,$$

with $a_k \neq 0$ *and* $0 \leq a_i < b$ *for all* $i \in \{0, \ldots, k\}$.

Proof. If $b > n$, then we easily see that $n = b^0 a_0$, with $0 \leq a_0 = n < b$, i.e., $n = (n)_b$. If $b \leq n$, we can apply the Euclidean division algorithm successively, starting with inputs $r_0 = n, r_1 = b$, thus writing $n = bn_0 + a_0$ with $0 \leq a_0 < b$ and continuing with $n_0 = bn_1 + a_1$ with $0 \leq a_1 < b$. We repeat this process until we find $n_{k-1} = b \cdot 0 + a_k$.

Thus, reinserting the equations to the previous ones, we get

$$n = bn_0 + a_0 = b(bn_1 + a_1) + a_0 = \cdots = \sum_{i=0}^{k} a_i b^i.$$

In order to show the uniqueness, let us assume that we have two different representations:

$$n = \sum_{i=0}^{k} a_i b^i = \sum_{i=0}^{k} c_i b^i.$$

As they are distinct, there must be a smallest j, for which $a_j \neq c_j$. We thus get that

$$b^j \left(\sum_{i=j}^{k} (a_i - c_i) b^{i-j} \right) = 0,$$

and hence

$$\sum_{i=j}^{k} (a_i - c_i) b^{i-j} = 0.$$

As we can write

$$-(a_j - c_j) = b(\sum_{i=j+1}^{k} (a_i - c_i) b^{i-j-1})$$

we get that $b \mid (a_j - c_j)$. However, due to the fact that $0 \leq a_j, c_j < b$ we see that $-b < a_j - c_j < b$, leaving us only with $a_j - c_j = 0$, contradicting our assumption. □

The proof also tells us how to find the representation in base b: using the Euclidean division algorithm.

Example 1.10. *Let us write* 529 *in base* 7*:*

$$\begin{aligned} 529 &= 7 \cdot 75 + 4 \\ 75 &= 7 \cdot 10 + 5 \\ 10 &= 7 \cdot 1 + 3 \\ 1 &= 7 \cdot 0 + 1. \end{aligned}$$

The remainders $4, 5, 3, 1$ *are in fact the sought representation in basis* 7*. (You can also check this by reinserting). Hence, we get* $(5, 2, 9)_{10} = (1, 3, 5, 4)_7$.

2 Diophantine Approximation

A large branch in elementary number theory is dedicated to approximating real numbers with rational numbers. This branch is called *Diophantine approximation*.

2.1 Irrational numbers

Any rational number $r \in \mathbb{Q}$ can be written as $r = p/q$, for some $p, q \in \mathbb{Z}, q \neq 0$. Any number which is not rational, is called *irrational.*

Theorem 2.1. $\sqrt{2}$ *is irrational.*

Proof. Assume by contradiction, that $\sqrt{2} = p/q$ is rational with p, q being the smallest positive integers to write $\sqrt{2}$ as fraction. Thus, $2 = p^2/q^2$.

Note that $2q^2 = p^2$, forces p^2 to be even, and thus also p, i.e., there exists an integer k with $p = 2k$. As then $q^2 = 2k^2$ is also even, both p and q must be divisible by 2.

This contradicts the assumption that p, q have been chosen as the smallest positive integers to write $\sqrt{2}$ as fraction. □

There exists a more general result to show that a number is irrational.

Theorem 2.2. *Let α be a root of the polynomial $f(x) = \sum_{i=0}^{n-1} c_i x^i + x_n$, with $c_i \in \mathbb{Z}$. Then α is either an integer or an irrational number.*

Proof. Assume that $\alpha = a/b$ is a rational number, with $a, b \in \mathbb{Z}, b \neq 0$ and $\gcd(a, b) = 1$. Since α is a root of f, we have that $\sum_{i=0}^{n-1} c_i \left(\frac{a}{b}\right)^i + \frac{a^n}{b^n} = 0$. Multiplying with b^n, we get

$$\sum_{i=0}^{n-1} c_i a^i b^{n-i} + a^n = 0,$$

and thus

$$a^n = -b \sum_{i=0}^{n-1} c_i a^i b^{n-i-1}.$$

Hence, $b \mid a^n$.

If $b \neq \pm 1$, then b has a prime divisor p with $p \mid a^n$, and thus $p \mid a$. This contradicts the assumption that $\gcd(a, b) = 1$.

Thus, we must have that $b = \pm 1$. Consequently, if α is rational, then $\alpha = \pm a \in \mathbb{Z}$. □

Example 2.3. *Let a be a positive integer, which is not the mth power of an integer. Then $a^{1/m}$ is irrational, since it is the root of the polynomial $x^m - a$. For $a = m = 2$ we have a different proof for $\sqrt{2}$ being irrational.*

2.2 Dirichlet's Approximation Theorem

Note that any real number x has distance at most $1/2$ from some closest integer. However, one might ask; can we find a multiple jx within the first n multiples which is closer to the integers?

For this we quickly introduce the notion of *fractional part.* The fractional part of $x \in \mathbb{R}$ denoted by $[x]$, is given by

$$[x] = x - \lfloor x \rfloor.$$

Note that $0 \leq [x] < 1$.

Theorem 2.4 (Dirichlet's Approximation Theorem). *If $x \in \mathbb{R}$ and $n \in \mathbb{N}$, then there exist $a, b \in \mathbb{Z}$, with $1 \leq a \leq n$, such that*

$$\mid ax - b \mid < 1/n.$$

Proof. Consider the fractional parts of the first $n+1$ multiples of x, i.e.,

$$[0], [x], [2x], \ldots, [nx]$$

and note that each fractional part lives in one of the disjoint intervals

$$[0, 1/n), [1/n, 2/n), \ldots, [(n-1)/n, 1).$$

Since there are $n+1$ fractional parts but only n intervals, two fractional parts, say $[ix], [jx]$ with $i < j$, must live in the same interval and hence have distance at most $1/n$, i.e.,

$$|[jx] - [ix]| < 1/n.$$

Let $a = j - i$ and $b = \lfloor jx \rfloor - \lfloor ix \rfloor$, then

$$|ax - b| = |(j-i)x - \lfloor jx \rfloor + \lfloor ix \rfloor| = |[jx] - [ix]| < 1/n.$$

□

Example 2.5. *Observe that*

$$\sqrt{2} \sim 1.414,\ 2\sqrt{2} \sim 2.828,\ 3\sqrt{2} \sim 4.243,\ 4\sqrt{2} \sim 5.657,\ 5\sqrt{2} \sim 7.071,\ 6\sqrt{2} \sim 8.484.$$

With this we found the following approximation

$$|5\sqrt{2} - 7| < 1/6.$$

Later in this lecture we will see a stronger result:

Theorem 2.6. *For any irrational number α there exist infinitely many rational numbers p/q such that*

$$|\alpha - p/q| < 1/q^2.$$

3 Primes

Clearly, 1 is a divisor of any positive integer and any positive integer different from 1 has at least two positive divisors: 1 and itself.

Definition 3.1. Positive integers with exactly two positive divisors are called *primes*. We denote the set of prime numbers by $\mathcal{P}$. Positive integers greater than 1, which are not prime are called *composite numbers.*

One important tool, is Euclid's Lemma:

Theorem 3.2 (Euclid's Lemma)**.** *Let $a, b \in \mathbb{Z}$ and $p \in \mathcal{P}$. If $p \mid (a \cdot b)$, then $p \mid a$ or $p \mid b$.*

Proof. Assume that $\gcd(a, p) = 1$, then by Bézout's identity there exist $s, t \in \mathbb{Z}$, such that $1 = ps + at$. Since $p \mid ab$, there also exists $c \in \mathbb{Z}$ such that $pc = ab$. Hence

$$b = (ps + at)b = psb + atb = psb + pct = p(sb + ct),$$

and thus $p \mid b$. □

Exercise 3.3. *Is Euclid's Lemma also true for non-primes?*

3.1 The Fundamental Theorem of Arithmetic

Theorem 3.4 (The Fundamental Theorem of Arithmetic)**.** *Any positive integer greater than 1 has a unique prime factorization. That is, for any positive integer n there exists a unique representation (apart from permutation of the factors)*

$$n = \prod_{i=1}^{k} p_i^{e_i},$$

where $p_i \in \mathcal{P}$, are distinct primes and $e_i \in \mathbb{N}$ for all $i \in \{1, \ldots, k\}$.

Proof. Let us start with the existence. For this we rely on strong induction. For $p = 2$ the factorization is clear. Assume that for any $m < n$ there exists a unique factorization of m into prime powers.

If n is prime, then there exists a unique $p_1 \in \mathcal{P}$, with $n = p_1$. If n is composite, then there exist $1 < a \leq b < n$, such that $a \cdot b = n$. By the induction hypothesis, a and b have unique prime factorizations, and by substituting these factorizations in $n = ab$ and collecting together powers of the same primes, we get the prime factorization of n.

For the uniqueness, assume that there exist two distinct factorizations

$$n = \prod_{i=1}^{k} p_i^{e_i} = \prod_{i=1}^{\ell} q_i^{f_i},$$

where $p_i \in \mathcal{P}$, respectively $q_j \in \mathcal{P}$, are distinct primes and $e_i, f_j \in \mathbb{N}$ for all $i \in \{1, \dots, k\}, j \in \{1, \dots, \ell\}$.

Since p_1 divides $\prod_{i=1}^{\ell} q_i^{f_i}$, due to Euclid's Lemma, p_1 divides some q_i. Assume w.l.o.g. that $p_1 \mid q_1$. However, as q_1 is prime, we have that $p_1 = q_1$.

Thus,

$$p_1^{e_1-1} \prod_{i=2}^{k} p_i^{e_i} = q_1^{f_i-1} \prod_{i=2}^{\ell} q_i^{f_i}.$$

Clearly, by continuing in this manner, we get that $p_i = q_i$ for all i. □

Knowing the prime factorizations of a and b, we can immediately compute their greatest common divisor and their least common multiple.

Exercise 3.5. *Show that for $a, b > 1$ two positive integers with prime factorization $a = \prod_{i=1}^{k} p_i^{e_i}$, $b = \prod_{i=1}^{k} p_i^{f_i}$, where we allow $e_i, f_i \in \mathbb{N}_0$, to have common prime divisors, then,*

$$\textit{gcd}(a, b) = \prod_{i=1}^{k} p_i^{\min\{e_i, f_i\}},$$
$$\textit{lcm}(a, b) = \prod_{i=1}^{k} p_i^{\max\{e_i, f_i\}}.$$

Exercise 3.6. *For a, b positive integers, show that lcm(a, b)gcd$(a, b) = ab$.*

Exercise 3.7. *Prove Proposition 1.3 differently, using the Exercise 3.5.*

Proposition 3.8. *Let m, n be positive integers and a an integer. Then, gcd$(a, mn) = 1$ if and only if gcd$(a, n) = 1$ and gcd$(a, m) = 1$.*

Proof. For one direction, we assume that $\gcd(a, mn) = 1$. Thus, if $\gcd(a, m) = d$, then $d \mid a$ and as $d \mid m$, we also have $d \mid mn$. Since 1 as the largest common divisor of a and mn, we must have $d = 1$. Same argument holds for $d' = \gcd(a, n)$.

For the other direction, we assume that $\gcd(a, n) = \gcd(a, m) = 1$. If $\gcd(a, mn) = d$, then $d \mid mn$. If $d \neq 1$ there exists some prime $p \mid d$, with $p \mid m$ or $p \mid n$. Since $p \mid d$, then also $p \mid a$, but as 1 was the largest common divisor between a and n, this gives a contradiction.

□

3.2 Primality Testing

Theorem 3.9 (Euclid)**.** *There are infinitely many primes.*

Proof. Assume that we only have finitely many primes $p_1, \dots, p_n$. Consider $q = \prod_{i=1}^{n} p_i + 1$. Due to the fundamental theorem of arithmetics, we know that q has at least one prime divisor, say p_i. However, as p_i then divides both q and $q - 1$, we get that p_i divides their difference, i.e., 1, which is a contradiction. □

The proof is non-constructive, and so important questions remain: how to construct primes, and how to detect if an integer is prime?

A simple test would be to go through all smaller integers and check if they divide the number in question, n. Due to commutativity, for such a division test, we only have to go up to $\sqrt{n}$.

One way to find all primes up to n was provided by Eratosthenes: cancel all multiples of the primes up to $\sqrt{n}$. However, this sieving method is quite inefficient. Later in this lecture, we will cover some primality tests like the Miller-Rabin test, used in practice.

The following technique for factorization is due to Fermat.

Lemma 3.10. *If n is an odd positive integer, then there is a one-to-one correspondence between factorizations of n into two positive integers and differences of two squares that equal n.*

Proof. Let n be an odd positive integer and let $n = ab$ be a factorization of n into two positive odd integers. Then n can be written as the difference of two squares, as

$$n = ab = s^2 - r^2,$$

where $r = (a-b)/2$ and $s = (a+b)/2$. On the other hand, if n is the difference of two squares $n = s^2 - r^2$, then we can factor $n = (s-r)(s+r)$. □

To carry out Fermat's factorization, we look for solutions of the equation

$$n = x^2 - y^2$$

by searching squares of the form $x^2 - n$. That is, to find factorizations of n we search among the sequence

$$t^2 - n, (t+1)^2 - n, \dots,$$

where $t = \lceil \sqrt{n} \rceil$. This procedure is guaranteed to terminate, as $n = 1 \cdot n$ leads to

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

Example 3.11. *We can factor 6077 using Fermat's technique. First, we identify $t = 78$ and construct the sequence*

$$\begin{aligned} 78^2 - 6077 &= 7, \\ 79^2 - 6077 &= 164, \\ 80^2 - 6077 &= 323, \\ 81^2 - 6077 &= 22^2. \end{aligned}$$

Now, that we have found a square, we can stop as

$$6077 = 81^2 - 22^2$$

and hence

$$6077 = (81-22)(81+22) = 59 \cdot 103.$$

It has been a long standing open question, whether one can in fact check if any integer is prime in polynomial time. In 2002, (very recent for number theory), the breakthrough was finally managed, with the paper "PRIMES is in P".

3.3 Special Primes

Several other mathematicians have tried to construct primes, famous examples include Fermat and Mersenne.

Lemma 3.12. *If* $2^m + 1$ *is prime, then* $m = 2^n$ *for some non-negative integer* n.

Proof. Assume $m \neq 2^n$, then we can write $m = 2^n q$, for some $q > 1$ odd. Let us consider the polynomial $f(x) = x^q + 1$. Clearly, -1 is a root, hence $(x + 1) \mid f(x)$. Thus, we can set $x = 2^{2^n}$ to get

$$(2^{2^n} + 1) \mid f(2^{2^n}) = 2^{2^n q} + 1 = 2^m + 1,$$

which is a contradiction to the assumption that $2^m + 1$ is prime. □

Definition 3.13. A number of the form $F(n) = 2^{2^n} + 1$, with n a non-negative integer, is called a *Fermat number*. If $F(n)$ is prime, we call it a *Fermat prime.*

Fermat famously conjectured, that every Fermat number is prime. For $n \in \{0, \ldots, 4\}$ this is indeed the case. However, in 1732 Euler showed that for $n = 5$ the Fermat number is composite. The Fermat primes have been extensively studied, but no further Fermat primes have been found.

Lemma 3.14. *If* $m > 1$ *is a positive integer and* $a^m - 1$ *is prime, then* $a = 2$ *and* $m \in \mathcal{P}$.

Proof. If $a = 1$, then $a^m - 1 = 0 \notin \mathcal{P}$. If $a > 1$ is odd, then $a^m - 1$ is an even number larger than 2, and hence not prime.

If $a > 2$, then

$$a^m - 1 = (a - 1)(a^{m-1} + a^{m-2} + \cdots + a + 1),$$

and hence $a^m - 1 \notin \mathcal{P}$.

Thus, we must have $a = 2$. Assume m is not a prime, then we can write $m = bc$, for some integers $b, c > 1$. Let us consider the polynomial $f(x) = x^b - 1$. Clearly, 1 is a root, hence $(x - 1) \mid f(x)$. Thus, we can set $x = 2^c$ to get

$$(2^c - 1) \mid f(2^c) = 2^{bc} - 1 = 2^m - 1,$$

which is a contradiction to the assumption that $2^m - 1$ is prime. □

Definition 3.15. Integers of the form $M(p) = 2^p - 1$, for $p \in \mathcal{P}$, are called *Mersenne numbers.* If $M(p)$ is prime, we call it a *Mersenne prime.*

Again, for $p \in \{2, 3, 5, 7\}$ these numbers are indeed prime. However, for $p = 11$ the Mersenne number is composite.

In fact,

$$2^{11} - 1 = 2047 = 23 \cdot 89.$$

While there exists a simple test, to check whether a integer of this form really is prime, we do not know how many exist.

For both, Mersenne and Fermat primes it is conjectured that there exist infinitely many.

Using Fermat numbers, we can give a different proof for the fact that there are infinitely many primes.

Lemma 3.16. *Let $F(k) = 2^{2^k} + 1$ denote the kth Fermat number, for some non-negative integer k. Then, for all positive integers n we have*

$$\prod_{i=0}^{n-1} F(i) = F(n) - 2.$$

Proof. We prove the lemma using induction. For $n = 1$ the identity becomes $F(0) = 3 = F(1) - 2 = 5 - 2$, which is true. Assume the identity holds for n, that is

$$\prod_{i=0}^{n-1} F(i) = F(n) - 2.$$

We now show that the identity also holds for $n + 1$. In fact,

$$\begin{aligned}\prod_{i=0}^{n} F(i) &= \prod_{i=0}^{n-1} F(i)F(n) \\ &= (F(n) - 2)F(n) = \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) \\ &= \left(2^{2^n}\right)^2 - 1 = 2^{2^{n+1}} - 1 = F(n + 1) - 2.\end{aligned}$$

□

Theorem 3.17. *Let n, m be distinct non-negative integers. Then,*

$$gcd(F(n), F(m)) = 1.$$

Proof. Let us assume that $m < n$. Assume that d is a common divisor of $F(m)$ and $F(n)$. Then,

$$d \mid (F(n) - \prod_{i=0}^{n-1} F(i)).$$

By Lemma 3.16, this implies that $d \mid 2$, hence $d = 1$ or $d = 2$. Since $F(m), F(n)$ are both odd, this leaves us with $d = 1$. □

Theorem 3.18. *There are infinitely many primes.*

Proof. Any Fermat number $F(n) > 1$ has a prime divisor p_n. Since $\gcd(F(m), F(n)) = 1$, we must have $p_m \neq p_n$ for $m \neq n$. As there are infinitely many Fermat numbers $F(m)$, there are infinitely many primes. □

3.4 Distribution of Primes

Definition 3.19. For a positive integer x, let $\pi(x)$ denote the number of primes less than or equal to x, i.e.,

$$\pi(x) = |\{p \in \mathcal{P} \mid p \leq x\}|.$$

This brings us to another famous result in number theory: the prime number theorem.

Theorem 3.20. *The number of primes behaves asymptotically as*

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

We usually write this as $\pi(x) \sim \frac{x}{\ln(x)}$. Unfortunately, there is no elementary proof, which could fit in this lecture.

However, we can sketch the lower and upper bounds. For this, let us first prove the following:

Lemma 3.21. *Let $p \in \mathcal{P}$ and $n \in \mathbb{N}_0$. Then the multiplicity of p in the prime factorization of $n!$ is*

$$\sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Proof. We prove this result by induction on n. The base case $n = 0$ is clear. For the inductive step, we have, for $d \in \mathbb{N}$ that

$$\left\lfloor \frac{n}{d} \right\rfloor - \left\lfloor \frac{n-1}{d} \right\rfloor = \begin{cases} 1 & \text{if } d \mid n, \\ 0 & \text{else.} \end{cases} \tag{1}$$

Since $n! = n(n-1)!$ the multiplicity of p in $n!$ is the sum of the multiplicity in $(n-1)!$ and in n, thus applying (1) to powers of p gives the result.

□

Theorem 3.22. *There exist constants $0 < C_1 < 1 < C_2$ such that*

$$C_1 \frac{x}{\log(x)} \leq \pi(x) \leq C_2 \frac{x}{\log(x)},$$

for sufficiently large x.

Proof. Let us start with the easier one: the lower bound.

Let m be a positive integer, $p \leq m$ a prime. With Lemma 3.21, we get that the largest power e, such that $p^e \mid m!$ is given by

$$e = \left\lfloor \frac{m}{p} \right\rfloor + \left\lfloor \frac{m}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{m}{p^k} \right\rfloor,$$

where k is such that $p^k \leq m < p^{k+1}$.

For the binomial coefficient $\binom{2n}{n}$, we get that the largest e such that $p^e \mid \binom{2n}{n}$, is

$$e = \sum_{i=1}^{k_p} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor \right),$$

where k_p is such that $p^{k_p} \leq 2n < p^{k_p+1}$. Note that $\lfloor 2x \rfloor - 2\lfloor x \rfloor \leq 1$, thus $e \leq k_p$.

Let us write the prime factorization of $\binom{2n}{n}$ as

$$\prod_{p \leq 2n} p^{e_p(n)}.$$

We get that

$$2^n \leq \binom{2n}{n} = \prod_{p \leq 2n} p^{e_p(n)} \leq \prod_{p \leq 2n} p^{k_p} \leq \prod_{p \leq 2n} 2n \leq (2n)^{\pi(2n)}.$$

Hence,

$$\pi(2n) \geq \frac{n \log(2)}{\log(2n)},$$

and setting $n = \left\lceil \frac{x}{2} \right\rceil$, we get

$$\pi(x) \geq \frac{x}{\log(x)} \log(2) - 2.$$

Thus, there exists some C_1 with $C_1 \frac{x}{\log(x)} \leq \pi(x)$.

For the upper bound, we can use similar tricks. We again write

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{e_p(n)}.$$

Note that for $n < p \leq 2n$ we get $e_p(n) \leq 1$. In fact, if $p^2 \leq 2n$ then $p > n$.

Thus,

$$\prod_{n < p \leq 2n} p \leq \binom{2n}{n} \leq \sum_{k=0}^{2n} \binom{2n}{k} = 4^n.$$

For $n = \lfloor \frac{x}{2} \rfloor$, we get

$$\prod_{\frac{x}{2} < p \leq 2\lfloor \frac{x}{2} \rfloor} p \leq 4^{\lfloor \frac{x}{2} \rfloor} \leq 2^x.$$

Note that there exists at most one prime between $2\lfloor \frac{x}{2} \rfloor$ and x, thus

$$\prod_{\frac{x}{2} < p \leq x} p \leq x 2^x \leq C_2^x,$$

for some constant C_2. Since the number of primes between $\frac{x}{2}$ and x is $\pi(x) - \pi\left(\frac{x}{2}\right)$, we get

$$C_2^x \geq \prod_{\frac{x}{2} < p \leq x} p \geq \prod_{\frac{x}{2} < p \leq p} \frac{x}{2} \geq \left(\frac{x}{2}\right)^{\pi(x) - \pi\left(\frac{x}{2}\right)}.$$

Hence,

$$\pi(x) \leq \pi\left(\frac{x}{2}\right) + \frac{x \log(C_2)}{\log\left(\frac{x}{2}\right)}.$$

As this also holds for $\pi\left(\frac{x}{2}\right)$, we get

$$\pi(x) \leq \pi\left(\frac{x}{4}\right) + \frac{x \log(C_2)}{\log\left(\frac{x}{2}\right)} + \frac{\frac{x}{2} \log(C_2)}{\log\left(\frac{x}{4}\right)}.$$

We may continue in this way, until

$$\pi(x) \leq \pi\left(\frac{x}{2^m}\right) + 2x \log(C_2) \sum_{i=1}^{m} \frac{2^{-i}}{\log\left(\frac{x}{2^i}\right)}.$$

Let m be such that $2^m \leq \sqrt{x}$, hence $\pi\left(\frac{x}{2^m}\right) \leq \frac{x}{2^m} \leq 2\sqrt{x}$. We also note that for all $i \leq m$ we have that $\log\left(\frac{x}{2^i}\right) \geq \log(\sqrt{x}) = \frac{1}{2}\log(x)$. Thus,

$$\pi(x) \leq 2\sqrt{x} + \frac{2x \log(C_2)}{\frac{1}{2}\log(x)} \sum_{i=1}^{m} \frac{1}{2^i} = 2\sqrt{x} + \frac{2x \log(C_2)}{\frac{1}{2}\log(x)} \left(1 - 2^{-m}\right).$$

This is in $\mathcal{O}\left(\frac{x}{\log(x)}\right)$, giving the upper bound. □

Corollary 3.23. *Let us denote by p_n the n-th prime, for n a positive integer. Then $p_n \sim n \ln(n)$.*

Thus, if we were to sample at random a positive integer, the likeliness of this number being a prime is going to zero. Note that we avoid words such as "uniform at random" or "probability". In fact, in the case of integers, we do not have such tools. Instead, number theorists have come up with *natural densities*.

For $d \in \mathbb{N}$, the natural density of a set $T \subset \mathbb{Z}^d$ is defined by restricting to a d-dimensional cube of height H, thus we can count how many elements in the cube are in T, and then dividing by the size of the cube, and finally letting H go to infinity.

Definition 3.24. Let $d \in \mathbb{N}$. The natural density of a set $T \subset \mathbb{Z}^d$ is defined to be

$$\rho(T) = \lim_{H \to \infty} \frac{|T \cap [-H, H)^d|}{(2H)^d},$$

if the limit exists.

If you are interested in natural densities, a student friendly introduction is given here [3].

Theorem 3.25. *The natural density of $\mathcal{P}$ is*

$$\rho(\mathcal{P}) = 0.$$

Proof. By the prime number theorem, we know that $\pi(x) \sim \frac{x}{\ln(x)}$. Hence, we have that

$$\begin{aligned} \rho(\mathcal{P}) &= \lim_{H \to \infty} \frac{|\mathcal{P} \cap [-H, H)|}{2H} = \lim_{H \to \infty} \frac{\pi(H)}{2H} \\ &= \lim_{H \to \infty} \frac{H}{2H \ln(H)} = 0. \end{aligned}$$

□

3.5 Gaps

We also know about gaps in the distribution of primes. In fact, there are arbitrarily long runs of integers containing no primes.

A *geometric progression* is a sequence of the form $a, ar, ar^2, \ldots$, where a (the initial term) and r (the common ratio) are real numbers.

An *arithmetic progression* is a sequence of the form $a, a + r, a + 2r, \ldots$, with $a, r \in \mathbb{R}$.

Theorem 3.26. *For any positive integer n, there are at least n consecutive composite positive integers.*

Proof. Consider the n consecutive positive integers

$$(n + 1)! + 2, (n + 1)! + 3, \ldots, (n + 1)! + n + 1.$$

When $2 \leq j \leq n + 1$, we know that $j \mid (n + 1)!$. Thus, it follows that $j \mid (n + 1)! + j$ and thus these n consecutive integers are not prime. □

Every odd integer is either of the form $4n + 1$ or $4n + 3$, but are there infinitely many primes in both of these forms? What about other arithmetic progressions, such as $3n + 1$, etc. ?

This leads us to Dirichlet.

Theorem 3.27 (Dirichlet's Theorem on Primes in Arithmetic Progression)**.** *Let a, b be positive integers, not divisible by the same prime. Then, the arithmetic progression $an+b$ contains infinitely many primes.*

Unfortunately, there is no elementary proof known, and thus, we will skip it. We can prove though a special version.

Theorem 3.28. *There are infinitely many primes of the form $4n + 3$, where n is a positive integer.*

Proof. First, we note that if a, b are positive integers of the form $4n + 1$, then ab is as well. In fact, we can write

$$ab = (4r + 1)(4s + 1) = 16rs + 4r + 4s + 1 = 4(4rs + r + s) + 1,$$

for some positive integers r, s. Now, let us assume that there are only finitely many prime numbers of the form $4n + 3$, namely $p_0 = 3, p_1, \dots, p_r$. Let

$$q = 4\prod_{i=1}^{r} p_i + 3.$$

Then there is at least one prime in the factorization of q of the form $4n + 3$. In fact, otherwise all of the primes would be of the form $4n + 1$ and thus also q would be of the form $4n + 1$, which is a contradiction. However, none of the primes $p_0, \dots, p_r$ divides q. Indeed, assume $3 \mid q$, then $3 \mid (q-3) = 4\prod_{i=1}^{r} p_i$, which is a contradiction. Likewise, if any $p_i \mid q$, then $p_i \mid (q - 4\prod_{i=1}^{r} p_i) = 3$, which is also a contradiction. Thus, there are infinitely many primes of the form $4n + 3$. □

Exercise 3.29. *Show that there is no odd prime of the form $n^3 + 1$, for n a positive integer.*

In fact, in 2004, Green and Tao proved that there are arbitrary long arithmetic progressions of primes.

Theorem 3.30 (Green-Tao)**.** *Let $A \subset \mathcal{P}$ such that*

$$\limsup_{n\to\infty} \frac{|A \cap [1, n)|}{\pi(n)} > 0,$$

then for all positive integers k, the set A contains infinitely many arithmetic progressions of length k.

Again, there is no elementary proof of this.

3.6 Open Questions

The fundamental theorem of arithmetic can be used to prove the following result, which relates the Riemann-zeta function with prime numbers.

Definition 3.31. The *Riemann-zeta function* is given by

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

for $s > 1$ a real number.

Theorem 3.32 (Euler Product)**.** *If s is a real number greater than 1, then*

$$\zeta(s) = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

While we will note prove this theorem (needs heavy analysis), a key point is that the term $\frac{1}{n^s}$ appears exactly once when the product is expanded. This is due to the fact that

$$\frac{1}{1 - p^{-s}} = \sum_{k \geq 0} \frac{1}{p^{k_s}}.$$

This shows the connection of primes, even to one of the greatest mysteries in mathematics, the Riemann hypothesis.

Even if this was a short excursion into the realm of prime numbers, studied since the dawn of mathematics, we do still have many open questions. In fact, there is a tremendous amount of conjectures on prime numbers, several of which have been proven but many remain wide open. Although we do not encourage students to try to prove century old conjectures, we provide a small list here.

Luckily, the next conjecture from 1845 has been proven by Chebyshev in 1852, which is why it is now called a postulate.

Theorem 3.33 (Bertrand's Postulate)**.** *For every positive integer $n > 1$, there exists a prime p, such that $n < p < 2n$*

The most famous one, is probably about twin primes.

Definition 3.34. Let $p \leq q \in \mathcal{P}$. We say that p and q are twin primes, if $q - p = 2$.

Open Question 3.35. *Are there infinitely many twin primes?*

Another famous conjecture, is that of Goldbach (written in a letter to Euler in 1742).

Open Question 3.36. *Every even integer greater than two is the sum of two primes.*

A weaker version of Goldbach's conjecture is the following:

Open Question 3.37. *Every odd integer greater than seven is the sum of three primes.*

And lastly, the $n^2 + 1$ conjecture.

Open Question 3.38. *There are infinitely many primes of the form $n^2 + 1$, where n is a positive integer.*

4 Modular Arithmetics

The language of congruences was invented by Gauss and allows us to work with division relationships like we work with equations. Here we simplify number-theoretic problems by replacing integers with their remainder when divided by a fixed positive integer. This has the effect of replacing the infinite set $\mathbb{Z}$ with the finite set $\mathbb{Z}/m\mathbb{Z}$. We will find that we can add, subtract and multiply in this new rings, but we have to be careful with division. The *integer residue ring* $\mathbb{Z}/m\mathbb{Z}$ inherits many properties of $\mathbb{Z}$, but due to its finiteness is easier to deal with.

We will see how to solve linear congruence equations and state the main result, the *Chinese Remainder Theorem.*

4.1 Congruences

Definition 4.1. Let m be a positive integer and a, b be integers. We say that a is *congruent* to b mod m if $m \mid (a-b)$, and write $a \equiv b \mod m$. The positive integer m is called the *modulus*. If a and b are not congruent, they are called *incongruent* and we write $a \not\equiv b \mod m$.

Example 4.2. $22 = 4 \mod 9$ *since* $9 \mid (22-4)$. *However,* 13 *and* 5 *are incongruent modulo* 9*, as* $9 \nmid (13-5)$.

Congruences arise in our every-day life, for example when telling the time. Saying that the lecture is at 4, we actually mean at 16:00 o'clock. Thus, for hours of the day we use the modulus 12.

Theorem 4.3. *Let m be a positive integer and a, b be integers. Then $a \equiv b \mod m$ if and only if there exists an integer k such that $a = b + km$.*

Proof. If $a \equiv b \mod m$, then by definition we have $m \mid (a-b)$, thus there exists an integer k, such that $mk = a - b$. □

The congruence relation "$\equiv$" has similar properties as the equality relation "$=$".

Theorem 4.4. *Let m be a positive integer. The congruence relation is an equivalence relation.*

Proof. In order to prove this statement, we need to show that the congruence relation is reflexive, symmetric and transitive.

- Reflexive property: we have to show that if a is an integer then $a \equiv a \mod m$. This easily follows from the definition as $m \mid (a-a)$.

- Symmetric property: if a, b are integers with $a \equiv b \mod m$, then also $b \equiv a \mod m$. This also easily follows as $m \mid (a-b)$, implies that there exists an integer k such that $mk = a - b$ and hence also $(-k)m = b - a$, which implies $m \mid (b-a)$.

- Transitivity property: if a, b, c are integers with $a \equiv b \mod m$ and $b \equiv c \mod m$, then also $a \equiv c \mod m$.

  In fact, if $m \mid (a-b)$ and $m \mid (b-c)$, then there exist integers k, ℓ with $km = a-b$ and $\ell m = b-c$. Thus,

  $$a - c = (a-b) + (b-c) = km + \ell m = (k+\ell)m,$$

  and hence $m \mid (a-c)$.

□

As the congruence relation "$\equiv$" defines an equivalence relation, we can consider the corresponding equivalence classes. The congruence relation divides the integers $\mathbb{Z}$ into m distinct sets, called *congruence classes* modulo m:

$$[i]_m = \{x \in \mathbb{Z} \mid x \equiv i \mod m\} = i + m\mathbb{Z}.$$

Definition 4.5. The *integer residue ring* $\mathbb{Z}/m\mathbb{Z}$, or integers modulo m, is the set of all congruence classes modulo m, that is

$$\mathbb{Z}/m\mathbb{Z} = \{[a]_m \mid a \in \mathbb{Z}\} = \{[0]_m, \dots, [m-1]_m\}.$$

Clearly, each congruence class consists of infinitely many elements, however, we will be mostly interested in the representative between 0 and $m-1$, called *least positive residue.* This representative is easily found with the usual division algorithm.

For m a positive integer and an integer a, we know by the division algorithm that we can write $a = qm + r$, where $0 \leq r < m$. Since each class $[i]_m$ has a unique representative, we thus often consider the set of least positive residues, $\{0, 1, \dots, m-1\}$. By abuse of notation, we might sometimes write $\mathbb{Z}/m\mathbb{Z} = \{0, 1, \dots, m-1\}$.

The integers modulo m form indeed a ring. An easy proof of this, is to know that $m\mathbb{Z}$ is an ideal, and noting that $\mathbb{Z}/m\mathbb{Z}$ is a quotient ring, where we define $(a+m\mathbb{Z})+(b+m\mathbb{Z}) = (a+b)+m\mathbb{Z}$ and $(a+m\mathbb{Z})(b+m\mathbb{Z}) = (ab)+m\mathbb{Z}$. As we do not assume any algebraic background, we prove it without such notions.

Theorem 4.6. $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ *is a ring, where the operations are defined as*

- $[a]_m + [b]_m = [a+b]_m$,
- $[a]_m \cdot [b]_m = [ab]_m$.

Exercise 4.7. *Prove Theorem 4.6.*

We can also do arithmetics with congruences.

Theorem 4.8. *Let m be a positive integer and a, b, c be integers such that $a \equiv b \mod m$. Then,*

- $a + c \equiv b + c \mod m$,
- $a - c \equiv b - c \mod m$,
- $ac \equiv bc \mod m$.

Proof.

- Since $m \mid (a - b)$ and $(a + c) - (b + c) = a - b$, we also have $m \mid (a + c) - (b + c)$.
- Similarly, we can rewrite $a - b = (a - c) - (b - c)$, from which follows $a - c \equiv b - c \mod m$.
- Since $m \mid (a - b)$, we also have that $m \mid (a - b)c = ac - bc$.

□

Example 4.9. *Note that* $7 \equiv 2 \mod 5$ *and hence*

$$\begin{aligned} 11 = 7 + 4 &\equiv 2 + 4 = 6 \mod 5, \\ 3 = 7 - 4 &\equiv 2 - 4 = -2 \mod 5, \\ 28 = 7 \cdot 4 &\equiv 2 \cdot 4 = 8 \mod 5. \end{aligned}$$

Exercise 4.10. *Is it true that* $\frac{a}{c} \equiv \frac{b}{c} \mod m$ *if* $a \equiv b \mod m$*?*

Lemma 4.11. *Let* a, b, c, m *be positive integers. If gcd*$(m, c) = d$ *and* $ac \equiv bc \mod m$*, then* $a \equiv b \mod m/d$*.*

Proof. Since $ac \equiv bc \mod m$, we have that $m \mid (ac - bc)$ and thus $m \mid c(a - b)$. That is, there exists an integer k with $mk = c(a - b)$.

As gcd$(m, c) = d$, we may divide both sides by d to get

$$k\frac{m}{d} = \frac{c}{d}(a - b),$$

and thus $\frac{m}{d} \mid (a - b)$. □

Corollary 4.12. *Let* m *be a positive integer and* a, b, c *integers with gcd*$(m, c) = 1$ *and* $ac \equiv bc \mod m$*, then* $a \equiv b \mod m$*.*

We can generalize this even further.

Theorem 4.13. *Let* m *be a positive integer and* a, b, c, d *be integers such that* $a \equiv b \mod m$ *and* $c \equiv d \mod m$*. Then,*

- $a + c \equiv b + d \mod m$,
- $a - c \equiv b - d \mod m$,
- $ac \equiv bd \mod m$.

Proof.

- We note that $(a+c)-(b+d) = (a-b)+(c-d)$ and m divides both, thus $a+c \equiv b+d \mod m$.
- We note that $(a-c)-(b-d) = (a-b)-(c-d)$ and m divides both, thus $a-c \equiv b-d \mod m$.
- We note that $ac-bd = (ad-bd)+(ac-ad) = d(a-b)+a(c-d)$ and m divides both, thus $ac \equiv bd \mod m$.

□

What happens if we have different moduli?

Theorem 4.14. *Let $m_1, \dots, m_k$ be positive integers and a, b integers such that $a \equiv b \mod m_i$ for all $i \in \{1, \dots, k\}$. Then $a \equiv b \mod lcm(m_1, \dots, m_k)$.*

Proof. Since $m_i \mid (a-b)$ for all $i \in \{1, \dots, k\}$, we know that $\text{lcm}(m_1, \dots, m_k) \mid (a-b)$. □

Corollary 4.15. *Let $m_1, \dots, m_k$ be relatively coprime, positive integers and a, b integers such that $a \equiv b \mod m_i$ for all $i \in \{1, \dots, k\}$. Then $a \equiv b \mod \prod_{i=1}^k m_i$.*

In fact, also the contrary is true (the proof will be postponed however).

Theorem 4.16. *Let $m = \prod_{i=1}^k p_i^{e_i}$ for distinct primes p_i and let a, b be integers. Then $a \equiv b \mod m$ if and only if $a \equiv b \mod p_i^{e_i}$ for all $i \in \{1, \dots, k\}$.*

4.2 Linear Congruences

Let us consider a positive integer m and integers a, b such that $ax \equiv b \mod m$ for an unknown integer x. Such an equation is called *linear congruence*. First, note that if x_0 is a solution to the equation, then any $x_1 \equiv x_0 \mod m$ is also a solution. In fact, if $m \mid (ax_0 - b)$ and $m \mid (x_1 - x_0)$ then there exist integers k, ℓ such that $km = ax_0 - b$ and $\ell m = x_1 - x_0$. With this we can write

$$ax_1 - b = a(x_1 - x_0) + (ax_0 - b) = a\ell m + km,$$

hence $m \mid (ax_1 - b)$.

Thus, if one element of a congruence class is a solution to a linear congruence, then all elements are. The question hence becomes, how many of the congruence classes are solutions, or equivalently how many incongruent solutions are there?

Theorem 4.17. *Let m be a positive integer, a, b be integers and $d = gcd(a, m)$. If $d \nmid b$, then $ax \equiv b \mod m$ has no solution and if $d \mid b$, then $ax \equiv b \mod m$ has d incongruent solutions.*

Proof. Note that $ax \equiv b \mod m$ is equivalent to $m \mid (ax - b)$, hence there exists some integer y with $my = ax - b$. Thus, $ax \equiv b \mod m$ is equivalent to the linear Diophantine equation

$$ax - my = b,$$

with the unknown integer solutions (x, y).

Using Theorem 1.7, we know that $ax \equiv b \mod m$ has no integer solution x if $d \nmid b$. If $d \mid b$, the linear congruence has infinitely many solutions of the form

$$(x_0 + \frac{m}{d}n, y_0 + \frac{a}{d}n),$$

where (x_0, y_0) is a solution to $ax \equiv b \mod m$ and n is an integer. Consider two solutions $x_1 = x_0 + \frac{m}{d}n_1$ and $x_2 = x_0 + \frac{m}{d}n_2$. If they are congruent modulo m, i.e.,

$$x_0 + \frac{m}{d}n_1 \equiv x_0 + \frac{m}{d}n_2 \mod m,$$

then we can subtract x_0 to get $\frac{m}{d}n_1 \equiv \frac{m}{d}n_2 \mod m$. Note that $\gcd(m, m/d) = m/d$ and hence by Lemma 4.11, we get $n_1 \equiv n_2 \mod d = m/(m/d)$. Thus, we get d incongruent solutions. □

Corollary 4.18. *Let m be a positive integer and a, b integers with gcd$(a, m) = 1$. Then, $ax \equiv b \mod m$ has a unique (incongruent) solution.*

Example 4.19. *To find all solutions to $9x \equiv 12 \mod 15$, we first compute that gcd$(9, 15) = 3$ and since $3 \mid 12$, we have 3 incongruent solutions. To find a particular solution, we solve the Diophantine equation*

$$9x - 15y = 12$$

using the Euclidean division algorithm:

$$\begin{aligned} 15 &= 9 \cdot 1 + 6 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= 3 \cdot 2 + 0. \end{aligned}$$

Thus,

$$3 = 9 - 6 \cdot 1 = 9 - (15 - 9 \cdot 1) = 9 \cdot 2 - 15.$$

Hence multiplying by $12/3 = 4$ we get $9 \cdot 8 - 15 \cdot 4 = 12$ and the particular solution $(8, 4)$. Hence, all solutions are of the form

$$x = 8 + \frac{15}{3}n = 8 + 5n$$

and the incongruent ones are

$$\begin{aligned} x &\equiv 8 + 5 \cdot 0 \equiv 8 \mod 15 \\ x &\equiv 8 + 5 \cdot 1 \equiv 13 \mod 15 \\ x &\equiv 8 + 5 \cdot 2 \equiv 3 \mod 15. \end{aligned}$$

4.3 Units of Integer Residue Rings

If we want to solve the equation $ax \equiv 1 \mod m$, we are actually looking for the multiplicative inverse of a modulo m, that is $[a]_m^{-1}$.

Using Theorem 4.17, we get

Corollary 4.20. *Let m be a positive integer and a an integer. Then there exists an integer b such that $ab \equiv 1 \mod m$ if and only if gcd$(a, m) = 1$.*

This element b is called the *multiplicative inverse* of a modulo m and is denoted by a^{-1}.

Example 4.21. *We want to find the inverse of 2 modulo 7. For this we write*

$$\frac{1}{2} \equiv \frac{1+7}{2} \equiv 4 \mod 7.$$

Exercise 4.22. *What is the inverse of 2 modulo 10 and what is the inverse of 3 modulo 10?*

Lemma 4.23. *Let $p \in \mathcal{P}$ and a a positive integer. Show that $a \equiv a^{-1} \mod p$, if and only if $a \equiv \pm 1 \mod p$.*

Proof. Since $a^2 \equiv 1 \mod p$, we get that $p \mid (a^2 - 1) = (a-1)(a+1)$. Thus, we either have $p \mid (a-1)$ or $p \mid (a+1)$, that is $a \equiv 1 \mod p$ or $a \equiv -1 \mod p$. □

We denote the elements in $\mathbb{Z}/m\mathbb{Z}$ which have a multiplicative inverse by $\mathbb{Z}/m\mathbb{Z}^\times$, called the *group of units* or the *multiplicative group*.

Exercise 4.24. *Show that $(\mathbb{Z}/m\mathbb{Z}^\times, \cdot)$ is a group. Note that it is enough to show that it is closed under multiplication.*

Due to Corollary 4.20, we know that

$$\mathbb{Z}/m\mathbb{Z}^\times = \{a \in \mathbb{Z}/m\mathbb{Z} \mid \text{gcd}(a, m) = 1\}.$$

How large is such a group of units?

Example 4.25. $\mathbb{Z}/6\mathbb{Z}^\times = \{1, 5\}$, *while* $\mathbb{Z}/7\mathbb{Z}^\times = \mathbb{Z}/7\mathbb{Z} \setminus \{0\}$.

The cardinality of the group of units is thus given by

$$|\mathbb{Z}/m\mathbb{Z}^\times| = |\{a \in \{1, \dots, m\} \mid \text{gcd}(a, m) = 1\}|.$$

Definition 4.26 (Euler Totient Function)**.** Define $\varphi(1) = 1$ and for any integer m with $m > 1$, the Euler totient function is defined as

$$\varphi(m) = |\mathbb{Z}/m\mathbb{Z}^\times|.$$

Theorem 4.27. *Let $m > 1$ be an integer with prime factorization $m = \prod_{i=1}^{k} p_i^{e_i}$. Then*

$$\varphi(m) = \prod_{i=1}^{k} p_i^{e_i-1}(p_i - 1).$$

Exercise 4.28. *We may prove this theorem in 3 steps.*

- *For $p \in \mathcal{P}$ show that $\varphi(p) = p - 1$.*
- *For $p \in \mathcal{P}$ show that $\varphi(p^e) = p^{e-1}(p - 1)$.*
- *Show that if gcd$(a, b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$. For this use Proposition 3.8.*

Note that this formula is equivalent to writing

$$\varphi(m) = m \prod_{p \in \mathcal{P}:p|m} \left(1 - \frac{1}{p}\right).$$

We will later (in the section on arithmetic functions) see more properties of the Euler totient function.

Exercise 4.29. *For which values of m is $\varphi(m)$ odd?*

Note that the expression $\varphi(m) = \prod_{p \in \mathcal{P}:p|m} \left(1 - \frac{1}{p}\right)$ has a probabilistic interpretation. If we choose a randomly, the probability that it is coprime to p is $\left(1 - \frac{1}{p}\right)$. For distinct primes, these events are independent and thus for a to be coprime to m, we get the probability $\prod_{p \in \mathcal{P}:p|m} \left(1 - \frac{1}{p}\right)$. This must be equal to the proportion of equivalence classes which are units, that is $\varphi(m)/m$.

4.4 Chinese Remainder Theorem

What if we are given a system of linear congruences? This question arose in ancient Chinese puzzles, such as *" Find a number that leaves as a remainder 1 when divided by 3, a remainder 2 when divided by 5 and a remainder 3 when divided by 7"*

That is, we are given the system of linear congruences

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 2 \mod 5 \\ x &\equiv 3 \mod 7. \end{aligned}$$

A general method to solve these kind of puzzles was only discovered in 1247 by Ch'in Chin-Shao.

Theorem 4.30 (Chinese Remainder Theorem)**.** *Let $m_1, \dots, m_k$ be pairwise coprime positive integers and $a_1, \dots, a_k$ be integers. Then $x \equiv a_i \mod m_i$ for all $i \in \{1, \dots, k\}$ has a unique solution modulo $M = \prod_{i=1}^{k} m_i$.*

Note that *unique* here refers to a unique congruence class of solutions, or only one incongruent solution.

Proof. We first construct a simultaneous solution. For this consider $M_i = \frac{M}{m_i}$, which is such that $\gcd(M_i, m_i) = 1$. Thus, we can find the inverse of M_i modulo m_i, denoted by y_i. Doing so for all $i \in \{1, \dots, k\}$, we define

$$x = \sum_{i=1}^{k} a_i M_i y_i.$$

As a next step we show that x is a solution to the system of linear congruences. In fact, since $m_i \mid M_j$ for any $i \neq j$, we have that $M_j \equiv 0 \mod m_i$ and thus

$$x \equiv a_i M_i y_i \equiv a_i \mod m_i.$$

We continue by showing that any two solutions are congruent modulo M. Consider x_0, x_1 two solutions of the system of linear congruences. That is, for any $i \in \{1, \dots, k\}$ we have $x_0 \equiv x_1 \equiv a_i \mod m_i$ and hence $m_i \mid (x_0 - x_1)$, from which follows $M \mid (x_0 - x_1)$.

□

Note that the proof also provides a formula for a particular solution x_0 and for all solutions (which are of the form $x = x_0 + Mn$).

Example 4.31. *Let us solve the initial puzzle.*

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 2 \mod 5 \\ x &\equiv 3 \mod 7. \end{aligned}$$

Thus we compute $M = 3 \cdot 5 \cdot 7 = 105, M_1 = 35, M_2 = 21$ and $M_3 = 15$. We now compute the inverses; y_1 is such that $35y_1 \equiv 2y_1 \equiv 1 \mod 3$, hence $y_1 \equiv \frac{1}{2} \equiv \frac{4}{2} \equiv 2 \mod 3$. Similarly, y_2 is such that $21y_2 \equiv y_2 \equiv 1 \mod 5$ and y_3 is such that $15y_3 \equiv y_3 \equiv 1 \mod 7$. Thus we write

$$x \equiv 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \equiv 52 \mod 105.$$

Theorem 4.16 follows from the Chinese Remainder Theorem, by setting $m_i = p_i^{e_i}$ and $M = \prod_{i=1}^{k} m_i$.

The Chinese Remainder Theorem has also been extended to the case where the moduli are not coprime.

Theorem 4.32. *Let $m_1, \dots, m_k$ be positive integers and $a_1, \dots, a_k$ be integers. The system of linear congruences $x \equiv a_i \mod m_i$ for all $i \in \{1, \dots, k\}$ has a solution if and only if gcd$(m_i, m_j) \mid (a_i - a_j)$ for all $i \neq j$.*

Proof. If a solution x exists, then $m_i \mid (x - a_i)$ for all $i \in \{1, \dots, k\}$. Let us denote $d_{i,j} = \gcd(m_i, m_j)$ for $i \neq j$. Since $d_{i,j} \mid m_i$ and $d_{i,j} \mid m_j$ we also have $d_{i,j} \mid (x - a_i)$ and $d_{i,j} \mid (x - a_j)$. Hence $d_{i,j} \mid (x - a_j) - (x - a_i) = a_i - a_j$.

Let x_0 be a solution, then x_1 is a solution if and only if $x_1 \equiv x_0 \mod m_i$ for all $i \in \{1, \dots, k\}$. Hence $m_i \mid (x_1 - x_0)$ and in turn lcm$(m_1, \dots, m_k) \mid (x_1 - x_0)$.

This implies that all solutions belong to the same congruence class $[x_0]_m$.

In the other direction, we assume $d_{i,j} \mid (a_i - a_j)$ for all $i \neq j$.

We apply Theorem 4.16 to replace each congruence $x \equiv a_i \mod m_i$ with the equivalent system $x \equiv a_i \mod p^e$, for all p^e in the prime factorization of m_i. The new system has now only prime powers as moduli, however, they might not be coprime (for example if m_i and m_j have the same prime divisor). For a fixed p we choose i such that m_i is divisible by the highest power of p, say p^e.

Thus, if $p^f \mid m_j$ and $f \leq e$, then we note that $p^f \mid d_{i,j}$ and hence $p^f \mid (a_i - a_j)$. Thus if $x \equiv a_i \mod p^e$ then $x \equiv a_i \mod p^f$ as well. This step allows us to discard all linear congruences $x \equiv a_i \mod p^f$ for $f \leq e$. Doing so for each prime in the prime factorization of $m_1, \dots, m_k$ leaves us with a system of linear congruences of coprime prime powers, and we can apply the Chinese Remainder Theorem.

□

We usually state the Chinese Remainder Theorem more algebraically. Namely,

Theorem 4.33 (Chinese Remainder Theorem). *Let $m = \prod_{i=1}^{k} p_i^{e_i}$ for distinct primes p_i. Then, there exists a ring isomorphism $\psi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}$.*

4.5 System of Linear Congruences in Several Variables

What if we have a system in more than one unknown?

Example 4.34. *We are looking for the solution $(x, y) \in \mathbb{Z}^2$, to the system of equation*

$$3x + 4y \equiv 5 \mod 13 \tag{2}$$

$$2x + 5y \equiv 7 \mod 13. \tag{3}$$

We can erase one of the variables e.g., y by considering (2) $\cdot 5 -$ (3) $\cdot 4$, *that is*

$$7x \equiv -3 \mod 13.$$

Since $\frac{1}{7} \equiv \frac{14}{7} \equiv 2 \mod 13$, we can multiply both sides with 2, to get

$$x \equiv -6 \equiv 7 \mod 13.$$

We are left with inserting x into one of the equations, e.g. (2) *to get*

$$3 \cdot 7 + 4y \equiv 5 \mod 13,$$

which is equivalent to $4y \equiv -3 \mod 13$ *and since* $\frac{1}{4} \equiv \frac{14}{4} \equiv \frac{7}{2} \equiv \frac{20}{2} \equiv 10 \equiv -3$, *by multiplying with* -3 *on both sides, we get*

$$y \equiv 9 \mod 13.$$

Thus a solution to this system is given by $(7, 9)$.

As you can already guess, we need to make use of matrices and matrix inversion over $\mathbb{Z}/m\mathbb{Z}$. This works exactly the same as over $\mathbb{Z}$, with the only difference, that a matrix $A \in \mathbb{Z}/m\mathbb{Z}^{k\times k}$ is invertible if $\det(A) \in \mathbb{Z}/m\mathbb{Z}^{\times}$.

Theorem 4.35. *Let m be a positive integer and $a_{i,j}, b_i$ be integers for all $i, j \in \{1, \ldots, k\}$. Let $A \in \mathbb{Z}/m\mathbb{Z}^{k\times k}$ denote the matrix with entries $a_{i,j}$. If* $\det(A) \in \mathbb{Z}/m\mathbb{Z}^{\times}$*, then the system*

$$A \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} \mod m$$

has a unique solution, given by $A^{-1} \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix}$.

The proof is straightforward and omitted.

Example 4.36. *In the previous example, we had*

$$A = \begin{pmatrix} 3 & 4 \\ 2 & 5 \end{pmatrix}, b = \begin{pmatrix} 5 \\ 7 \end{pmatrix}.$$

Since $\det(A) \equiv 3 \cdot 5 - 2 \cdot 4 \equiv 7 \mod 13$*, A is invertible and*

$$A^{-1} \equiv \frac{1}{7} \begin{pmatrix} 5 & 9 \\ 11 & 3 \end{pmatrix} \equiv \begin{pmatrix} 10 & 5 \\ 9 & 6 \end{pmatrix} \mod 13.$$

Thus, the solution is given by

$$\begin{pmatrix} x \\ y \end{pmatrix} \equiv A^{-1}b \equiv \begin{pmatrix} 7 \\ 9 \end{pmatrix} \mod 13.$$

The Special Case of $\mathbb{Z}/p\mathbb{Z}$ One important case of integer residue rings, is when the modulo is a prime, i.e., $\mathbb{Z}/p\mathbb{Z}$. In this case, we do not only have a ring, but even a field.

In fact, the only difference between our finite rings $\mathbb{Z}/m\mathbb{Z}$ and a finite field, is the condition

- any non-zero element has a multiplicative inverse.

While this is not satisfied for a composite $m,$ this is true for prime moduli.

Indeed, as we have seen in Section 4.3,

$$\varphi(p) = |\mathbb{Z}/p\mathbb{Z}^\times| = p - 1.$$

Do note that these are not the only finite fields. They are called *prime fields* and can be extended to any finite field of prime power (these are however not integer residue rings anymore).

This additional field structure will provide many more beautiful results, as we will see in the next section, Section 5.

5 Famous Theorems

In this section, we will see three famous theorems, by Fermat, Euler and Wilson, which have a large impact and find many applications, for example in primality testing.

Let us start with a different one, called *Freshman's dream.* This result is called like this as Freshman's (new students) often make the mistake of writing $(a+b)^n = a^n + b^n$. Over $\mathbb{Z}/p\mathbb{Z}$, this is, however, possible.

Theorem 5.1 (Freshman's Dream)**.** *Let a, b be integers and p a prime. Then,*

$$(a+b)^p \equiv a^p + b^p \mod p.$$

Proof. Using the binomial theorem, we can write

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

Note that $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ always has a factor p and is thus zero modulo p, except for $i = 0$ and $i = p$. In these cases we get $\binom{p}{0} = \binom{p}{p} = 1$. Thus,

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

□

This result actually holds for any integer residue ring $\mathbb{Z}/m\mathbb{Z}$, for the same reason. The result is also true for any finite field with characteristic p.

5.1 Fermat's Little Theorem

The following result is called Fermat's Little Theorem (not to be confused with Fermat's Last Theorem). Fermat mentioned this result in a letter in 1640, but it was only proven by Euler in 1736.

Theorem 5.2 (Fermat's Little Theorem)**.** *Let $p \in \mathcal{P}$ and a be an integer such that $a \not\equiv 0 \mod p$. Then $a^{p-1} \equiv 1 \mod p$.*

Proof. Consider $a \in \{1, \dots, p-1\}$. Since $\gcd(a, p) = 1$ we have that $xa \equiv ya \mod p$ implies $x \equiv y$. Thus, $a, 2a, \dots, (p-1)a$ are congruent to $1, 2, \dots, p-1$ in some order. The product of these two sets must thus lie in the same congruence class, that is

$$\prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} ai \mod p.$$

This is equivalent to $(p-1)! \equiv (p-1)!a^{p-1} \mod p$. Since $(p-1)!$ is coprime to p, we can divide by $(p-1)!$ to get the claim. □

Knowing some group theory, we can give a much quicker proof.

For this we need Lagrange's Theorem.

Theorem 5.3 (Lagrange's Theorem)**.** *Let G be a finite group and $S < G$ a subgroup. Then*

$$|S| \mid |G|.$$

An important implication of this theorem is as follows.

Corollary 5.4. *Let G be a finite group of order d. Then any element of $g \in G$ has multiplicative order ord$(g) \mid d$.*

Exercise 5.5. *Proof Corollary 5.4.*

Corollary 5.6. *Let G be a finite group of order d. Then, for any element $g \in G$, we have $g^d = e$, where e denotes the neutral element.*

Exercise 5.7. *Prove Fermat's Little Theorem using the fact that $a \in \mathbb{Z}/p\mathbb{Z}^\times$ and using Lagrange's Theorem.*

This result implies that all congruence classes in $\mathbb{Z}/p\mathbb{Z}$, except for $[0]_p$, are roots of the polynomial $x^{p-1} - 1$. If we want to find a polynomial which has all congruence classes in $\mathbb{Z}/p\mathbb{Z}$ as roots, we can simply multiply by x. Getting

Corollary 5.8. *Let $p \in \mathcal{P}$. For every integer a, we have $a^p \equiv a \mod p$.*

Exercise 5.9. *Prove the corollary using Freshman's Dream and induction (instead of using Fermat's Little Theorem).*

5.2 Euler's Theorem

This result presents a generalization of Fermat's Little Theorem, which tells us how to deal with congruences modulo p. What happens if the modulo is not a prime? It is not true that

$$a^{m-1} \equiv 1 \mod m,$$

as we can easily check for $m = 4, a = 3$. We can thus ask: which exponent $e(m)$ do we need to get

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

for any a coprime to m?

Theorem 5.10 (Euler's Theorem)**.** *Let m be a positive integer and a an integer with gcd$(a, m) = 1$. Then, $a^{\varphi(m)} \equiv 1 \mod m$.*

Proof. Note that by definition $|\mathbb{Z}/m\mathbb{Z}^\times| = \varphi(m)$. Consider the set of least positive residues of the units modulo m, say $\{r_1, \ldots, r_{\varphi(m)}\}$. If $\gcd(a, m) = 1$, then the elements $ar_1, \ldots, ar_{\varphi(m)}$ must be congruent to $r_1, \ldots, r_{\varphi(m)}$ in some order. Thus, their product is in the same congruence class, meaning

$$\prod_{i=1}^{\varphi(m)} r_i \equiv \prod_{i=1}^{\varphi(m)} ar_i \mod m.$$

Since all r_i are units, we can divide by them, which leads to $1 \equiv a^{\varphi(m)} \mod m$. □

Exercise 5.11. *Prove Euler's Theorem using $a \in \mathbb{Z}/m\mathbb{Z}^\times$ and Lagrange's Theorem.*

5.3 Wilson's theorem

Wilson was a student at the time of his discovery, and although a first proof was published only by Lagrange in 1770, the result is called after him.

Theorem 5.12 (Wilson's Theorem)**.** *An integer n is prime if and only if $(n-1)! \equiv -1 \mod n$.*

Proof. For the first direction, assume that n is a prime p. If $p = 2$, then $(p-1)! \equiv 1 \equiv -1 \mod 2$, as required. Thus, we may assume that p is odd. We define the polynomial

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

which has integer coefficients and degree $d < p-1$ (in fact the two terms with exponent $p-1$ cancel). For $a \in \{1, \ldots, p-1\}$ then $f(a) \equiv 0 \mod p$, as f has a factor $(a-x)$ and due to Fermat's Little Theorem we have $1 - a^{p-1} \equiv 0 \mod p$.

Thus, $f(x)$ has more than d roots modulo p, meaning that it must be $f \equiv 0 \mod p$, that is each coefficient of f is divisible by p. In particular, p divides the constant term $(p-1)! + 1$, and hence $(p-1)! \equiv -1 \mod p$.

For the other direction, assume that $(n-1)! \equiv -1 \mod n$. Thus, also for any factor m of n we have that $(n-1)! \equiv -1 \mod m$. However, if $m < n$, then m appears as factor of $(n-1)!$, that is $(n-1)! \equiv 0 \mod m$ and this leads to $-1 \equiv 0 \mod m$ and this in turn gives $m = 1$. □

We can also give an alternative proof.

Proof. If $n \in \mathcal{P}$, then we recall from Lemma 4.23, that the only x with $x^2 \equiv 1 \mod n$ are $x \equiv \pm 1 \mod n$. In $(n-1)!$ we can see all non-zero elements in $\mathbb{Z}/n\mathbb{Z}$ and for each $a \in \mathbb{Z}/n\mathbb{Z}$, with $a \neq 0, \pm 1,$, there exists a $b \in \mathbb{Z}/n\mathbb{Z}$ with $b \neq 0, \pm 1, a$ and $ab \equiv 1 \mod n$. Thus,

$$(n-1)! \equiv 1 \cdot 2 \cdots a \cdots b \cdots (n-2) \cdot (n-1) \equiv 1 \cdot (n-1) \equiv -1 \mod n,$$

as all other elements cancel with their inverse.

For the other direction, we assume that

$$1 \cdot 2 \cdots (n-2) \cdot (n-1) \equiv -1 \mod n,$$

by multiplying with (-1) we get

$$1 \cdot 2 \cdots (n-2) \equiv 1 \mod n.$$

Now we can group this product to get

$$a \cdot \prod_{1 \leq i \leq (n-2), i \neq a} i \equiv 1 \mod n,$$

implying that any $a \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ has a multiplicative inverse. Thus, gcd$(a, n) = 1$ for all $a < n$, and hence $n \in \mathcal{P}$. □

6 Primality Tests

In this section, we will see how to apply these theorems to check if integers are prime.

6.1 Pollard's $p-1$ Method

Fermat's Little Theorem builds the basis for a factorization method invented in 1974 by Pollard.

The method is known as Pollard $p-1$ method, as there also exist some generalizations. The method finds a non-trivial factor of n (that is not 1 or n), if n has a prime factor p, such that all $q \in \mathcal{P}$ with $q \mid (p-1)$ are small. Such primes p are called *smooth*.

The opposite of smooth primes, so called *strong primes* or Sophie Germain primes, are of the form $p = 2q+1$ for some prime q.

For Pollard's $p-1$ method, assume that $p \in \mathcal{P}$ and $p \mid n$. If we can find some integer k such that $(p-1) \mid k!$, then we can apply Fermat's Little Theorem. In fact, there exists some integer ℓ such that $(p-1)\ell = k!$ and hence,

$$2^{k!} = 2^{(p-1)\ell} = \left(2^{p-1}\right)^{\ell} \equiv 1^{\ell} \equiv 1 \mod p.$$

Thus, $p \mid (2^{k!} - 1)$.

Consider $M \equiv 2^{k!} - 1 \mod n$ the smallest positive residue, then $p \mid M$ and $p \mid n$. We now want to detect such prime by computing $d = \gcd(M, n)$ using the Euclidean algorithm, as then $p \mid d$.

As we do not know k, we simply go through all $k \geq 1$ until

$$\gcd(2^{k!} - 1, n) \neq 1.$$

How can we quickly compute $2^{k!} \mod n$?

$$\begin{aligned}
k &= 1, \quad r_1 = 2^1 \mod n \\
k &= 2, \quad r_2 = 2^{1 \cdot 2} = r_1^2 \mod n \\
k &= 3, \quad r_3 = 2^{1 \cdot 2 \cdot 3} = r_2^3 \mod n \\
&\vdots
\end{aligned}$$

That is, at any step i we compute $r_i = r_{i-1}^i \mod n$.

Example 6.1. *Let us factor 713.*

$$\begin{aligned}
&r_1 = 2 \mod 713 \quad \mathit{gcd}(2-1, 713) = 1\\
&r_2 = r_1^2 = 4 \mod 713 \quad \mathit{gcd}(4-1, 713) = 1\\
&r_3 = 2_2^3 = 64 \mod 713 \quad \mathit{gcd}(64-1, 713) = 1\\
&r_4 = r_3^4 = 326 \mod 713 \quad \mathit{gcd}(326-1, 713) = 1\\
&r_5 = r_4^5 = 311 \mod 713 \quad \mathit{gcd}(311-1, 713) = 31
\end{aligned}$$

Thus, we have found that

$$\mathit{gcd}(2^{5!}-1, 713) = 31$$

and 31 is a prime factor of 713.

Note that Pollard's $p-1$ method does not always work. In fact, if $n = pq$, with $p, q \in \mathcal{P}$, it is possible that $p \mid (2^{k!}-1)$ and $q \mid (2^{k!}-1)$, which leads to $n \mid (2^{k!}-1)$ and hence $\gcd(2^{k!}-1, n) = n$.

6.2 Pseudoprimes

In theory, Wilson's Theorem solves the primality testing problem. However, the factorial makes this test very inefficient.

Fermat's Theorem provides a better test, that is:

Given n a positive integer, check if there exists an integer a such that $a^n \not\equiv a \mod n$.
If this is the case, then n is composite.

Note that we prefer powers over factorials, as we can compute powers quite efficiently using *consecutive squaring:*

To compute $a^k \mod n$, we first note that if $\gcd(a, n) = 1$, then due to Euler's Theorem we can reduce the exponent to

$$k' \equiv k \mod \varphi(n)$$

the smallest positive residue.

Then we write k' in its binary representation, i.e., $k' = (k_N, \ldots, k_0)_2$, so that

$$a^k \equiv a^{k'} \equiv a^{2^N k_N} \cdots a^{2^0 k_0} = \prod_{i \in \{1,\ldots,N\}: k_i = 1} a^{2^i} \mod n.$$

We can hence compute all the a^{2^i} powers up to $i = N$ and then compute their product

$$a^k \equiv \prod_{i \in \{1,\ldots,N\}: k_i = 1} a^{2^i} \mod n.$$

Example 6.2. *If we want to compute* $3^{23} \mod 7$*, we first reduce* $23 \equiv 5 \mod 6$ *and then write* $5 = (1,0,1)_2$*. We then compute*

$$\begin{aligned} 3^{2^0} &\equiv 3 \mod 7, \\ 3^{2^1} &\equiv 9 \equiv 2 \mod 7, \\ 3^{2^2} &\equiv 4 \mod 7. \end{aligned}$$

Thus,

$$3^{23} \equiv 3^5 \equiv 3^4 \cdot 3^1 \equiv 4 \cdot 3 \equiv 5 \mod 7.$$

Exercise 6.3. *Perform the primality test of Wilson on* $n = 5$.

Exercise 6.4. *Perform the primality test of Fermat on* $n = 63$.

With Fermat's primality test, we can quickly show that a number is composite. However, Fermat's primality test does not imply anything on n which passes the test and it would be much more useful, if we could show that a number is a prime.

Side remark: the Chinese, by mistake of translation, believed that if $2^n \equiv 2 \mod n$, then n is a prime. Only in 1819 a counterexample to this test was given.

Exercise 6.5. *Using consecutive squaring, show that* $n = 341 = 11 \cdot 31$ *passes the Chinese test, i.e.,* $2^n \equiv 2 \mod n$.

Definition 6.6. Numbers which pass Fermat's test, i.e., $b^n \equiv b \mod n$, but are not prime are called *pseudoprimes to the base* b.

While pseudoprimes are rare, there are still infinitely many of them.

Theorem 6.7. *There exist infinitely many pseudoprimes to the base* 2.

Proof. We start by showing that if n_i is a pseudoprime to the base 2, then so is $n_{i+1} = 2^{n_i} - 1$. Then, since $n_{i+1} = 2^{n_i} - 1 > n_i$ we can iterate this starting at the smallest pseudoprime to the base 2, which is $n_0 = 341$.

From Lemma 3.14, recall that if n_i is composite, then $n_{i+1} = 2^{n_i} - 1$ is composite as well.

Now we need to prove that $2^{n_{i+1}} = 2^{2^{n_i}-1} \equiv 2 \mod 2^{n_i} - 1$, that is n_{i+1} passes the test $2^{n_{i+1}} \equiv 2 \mod n_{i+1}$.

Since $2^{n_i} \equiv 2 \mod n_i$, there exists an integer k, such that $2^{n_i} = 2 + n_i k$. Further,

$$\left(2^{n_i}\right)^k - 1 = \left(2^{n_i} - 1\right)\left(2^{n_i(k-1)} + \cdots + 1\right),$$

hence $\left(2^{n_i} - 1\right) \mid \left(2^{n_i k} - 1\right)$. This implies that

$$2^{n_i k} \equiv 1 \mod 2^{n_i} - 1,$$

and hence

$$2^{2^{n_i}-1} = 2^{2+n_i k-1} = 2^{n_i k+1} = 2 \cdot 2^{n_i k} \equiv 2 \mod 2^{n_i} - 1.$$

□

Lemma 6.8. *The Fermat numbers $F(k) = 2^{2^k} + 1$, pass Fermat's test for base 2.*

Proof. We want to show that $2^{F(k)} \equiv 2 \mod F(k)$. For this we first note that $F(k) \equiv 2^{2^k} + 1 \equiv 0 \mod F(k)$, hence $2^{2^k} \equiv -1 \mod F(k)$. We may raise both sides to the power $2^{2^k - k}$, getting

$$2^{2^k(2^{2^k-k})} \equiv 2^{2^{2^k}} \equiv (-1)^{2^{2^k-k}} \equiv 1 \mod F(k).$$

By multiplying with 2 on both sides, we get

$$2^{2^{2^k}+1} \equiv 2^{F(k)} \equiv 2 \mod F(k).$$

□

Exercise 6.9. *Show that the Mersenne numbers $M(p) = 2^p - 1$, for a prime p, pass Fermat's test for the base 2.*

6.3 Carmichael Numbers

Note that there exist composite integers, which pass the primality test by Fermat for any base b.

Definition 6.10. A *Carmichael number* is a composite integer n, such that $a^n \equiv a \mod n$ for all $a \in \mathbb{Z}$.

The smallest example of a Carmichael number is $n = 561 = 3 \cdot 11 \cdot 17$.

Theorem 6.11. *$n = 561$ is a Carmichael number.*

Proof. In order to show that $a^{561} \equiv a \mod 561$, we can equivalently (due to the Chinese Remainder Theorem), show that

$$\begin{aligned} a^{561} &\equiv a \mod 3, \\ a^{561} &\equiv a \mod 11, \\ a^{561} &\equiv a \mod 17. \end{aligned}$$

These equations can be reduced using Fermat's Little Theorem to

$$\begin{aligned} a^{561 \mod 2} &\equiv a \mod 3, \\ a^{561 \mod 10} &\equiv a \mod 11, \\ a^{561 \mod 16} &\equiv a \mod 17, \end{aligned}$$

which are obviously true as $561 \equiv 1$ modulo 2, 10 or 16.

□

Exercise 6.12. *Show that $n = 1729$ is a Carmichael number.*

In 1912 Carmichael conjectured that there exist infinitely many Carmichael numbers. A first proof was given in 1992 by Alford, Granville and Pomerance.

Theorem 6.13. *If $n = p_1 \cdots p_k$ with $p_i \in \mathcal{P}$ distinct and $k > 2$ such that $(p_i - 1) \mid (n - 1)$ for all $i \in \{1, \dots, k\}$, then n is a Carmichael number.*

Proof. Let b be a positive integer with $\gcd(b, n) = 1$. Then, $\gcd(b, p_i) = 1$ for all $i \in \{1, \dots, k\}$ and due to Fermat's Little Theorem, we have

$$b^{p_i - 1} \equiv 1 \mod p_i.$$

Since $(p_i - 1) \mid (n - 1)$, there exists an integer k_i with

$$k_i(p_i - 1) = n - 1$$

for all $i \in \{1, \dots, k\}$ and hence

$$b^{n-1} \equiv b^{k_i(p_i - 1)} \equiv \left(b^{p_i - 1}\right)^{k_i} \equiv 1^{k_i} \equiv 1 \mod p_i,$$

and as this holds for all p_i, with the Chinese Remainder Theorem, we also have $b^{n-1} \equiv 1 \mod n$. □

Actually, the other direction is also true, this is called the Korselt's criterion.
We will later see some more properties on Carmichael numbers and their use in RSA.

6.4 Miller's Test

If $b^{n-1} \equiv 1 \mod n$ is verified, another approach to check for primality is to consider $b^{(n-1)/2} \mod n$.

For $x = b^{(n-1)/2}$, we know that $x^2 = b^{n-1} \equiv 1 \mod n$. Due to Exercise 4.23, if n was prime, then $x \equiv \pm 1 \mod n$.

Thus, if $b^{(n-1)/2} \not\equiv \pm 1 \mod n$, then n must be a composite number.

Exercise 6.14. *Let $n = 561$ (the smallest Carmichael number). Check for $b = 5$ if $b^{(n-1)/2} \equiv \pm 1 \mod n$.*

Definition 6.15. Let $n > 2$ be a positive integer, $n - 1 = 2^s t$, for a non-negative integer s and an odd positive integer t. We say that *n passes Miller's test* for the base b, if

$$\text{either} \quad b^t \equiv 1 \mod n \quad \text{or} \quad b^{2^j t} \equiv -1 \mod n,$$

for some $j \in \{0, \dots, s - 1\}$.

Example 6.16. *Let $n = 2047 = 23 \cdot 89$. Then,*

$$2^{2046} = \left(2^{11}\right)^{186} = (2048)^{186} \equiv 1 \mod 2047.$$

Hence, 2047 is a pseudoprime for the base 2. Since

$$2^{2046/2} = 2^{1023} = \left(2^{11}\right)^{93} = (2048)^{93} \equiv 1 \mod 2047,$$

n also passes Miller's test for the base 2.

Theorem 6.17. *If $p \in \mathcal{P}$ and b a positive integer with $p \nmid b$, then p passes Miller's test for the base b.*

Proof. Let $p - 1 = 2^s t$, for a non-negative s and an odd positive integer t. Let $x_k = b^{(p-1)/2^k} = b^{2^{s-k}t}$ for $k \in \{0, \dots, s\}$. Fermat's Little Theorem then states that $x_0 = b^{p-1} \equiv 1 \mod p$ and $x_1^2 = x_0 \equiv 1 \mod p$, implies that $x_1 \equiv \pm 1 \mod p$.

If $x_1 \equiv 1 \mod p$, then we can continue in the same way, that is $x_2^2 = x_1 \equiv 1 \mod p$ implies that $x_2 \equiv \pm 1 \mod p$. Thus, we either end up with $x_0 \equiv \cdots \equiv x_s \equiv 1 \mod p$, and the first condition of Miller's test is satisfied, or for some $k \in \{1, \dots, s\}$ we have that $x_k \equiv -1 \mod p$, and thus the second condition of Miller's test is satisfied. □

Definition 6.18. If n is composite and passes Miller's test to the base b, n is called *strong pseudoprime* to the base b.

Example 6.19. *2047 is a strong pseudoprime to the base 2.*

Theorem 6.20. *There exist infinitely many strong pseudoprimes to the base 2.*

Proof. We show that if n is a pseudoprime to the base 2, then $N = 2^n - 1$ is a strong pseudoprime to the base 2. The result then follows from Theorem 6.7.

Hence, we assume that n is an odd composite number and $2^{n-1} \equiv 1 \mod n$. Then, there exists an odd integer k such that $kn = 2^{n-1} - 1$.

We have the following factorization of $N - 1$:

$$N - 1 = 2^n - 2 = 2\left(2^{n-1} - 1\right) = 2nk.$$

Since $2^n = N + 1 \equiv 1 \mod N$, we get

$$2^{(N-1)/2} = 2^{nk} = (2^n)^k \equiv 1^k \equiv 1 \mod N$$

and hence N passes Miller's test.

From Exercise 3.14, we know that if n is composite (as we assumed), then also $N = 2^n - 1$ is composite. Thus, N is a strong pseudoprime to the base 2. □

A natural question is: does there exist an analogue to the Carmichael numbers for Miller's test? That is a number which is composite and passes Miller's test for any base?

The answer to this question is no, due to the following theorem.

Theorem 6.21. *If n is an odd composite positive integer, then n passes Miller's test for at most $(n-1)/4$ bases $b \in \{1, \ldots, n-1\}$.*

Thus, if n passes Miller's test for more than $(n-1)/4$ bases $b < n$, then n must be a prime. While checking all bases is again inefficient, it gives us a quick way to check if a number is "probably prime".

In fact, take any positive integer $b < n$, if n is composite, the probability that n passes Miller's test to the base b is less than $1/4$. Thus, if we were to take k different bases and perform the test on each of them, we reduce the probability to $1/4^k$.

Theorem 6.22 (Rabin's Probabilistic Primality Test)**.** *Let n be a positive integer. Pick k different positive integers less than n and perform Miller's test on n for each of the k bases. If n is composite, the probability for n to pass each test is less than $1/4^k$.*

7 Arithmetic Functions

An *arithmetic function* is simply a function that is defined over the set of the positive integers $\mathbb{N}$.

Definition 7.1. An arithmetic function f is called *multiplicative*, if $f(1) = 1$ and $f(ab) = f(a)f(b)$ for $\gcd(a, b) = 1$.

Additionally, we say that f is *completely multiplicative*, if we can drop the coprime condition.

This means, that a multiplicative function evaluated at an integer n, gives the the product of the evaluations of each prime power in the prime factorization of n.

Theorem 7.2. *If f is a multiplicative function and $n = \prod_{i=1}^{k} p_i^{e_i}$ is the prime factorization of a positive integer n, then*

$$f(n) = \prod_{i=1}^{k} f(p_i^{e_i}).$$

Proof. We prove this theorem using induction on k. For $k = 1$, we consider $n = p^e$ and the result trivially follows.

Assume the theorem is true for any n with k distinct prime divisors. Now we may consider m with $k + 1$ distinct prime divisors, say $m = \prod_{i=1}^{k+1} p_i^{e_i}$. Since f is multiplicative, we get that

$$f(m) = f(m/p_{k+1}^{e_{k+1}})f(p_{k+1}^{e_{k+1}}).$$

As the theorem is true for $n = m/p_{k+1}^{e_{k+1}}$, which has k different prime divisors, we get the claim as

$$f(m) = \prod_{i=1}^{k} f(p_i^{e_i})f(p_{k+1}^{e_{k+1}}).$$

□

We will use this fact, to obtain a closed formula for the evaluation of these functions based on the prime factorizations.

Definition 7.3. Let f be an arithmetic function. The *summatory function* of f is given by

$$\begin{aligned} F : \mathbb{N} &\to \mathbb{Z}, \\ n &\mapsto \sum_{d \in \mathbb{N}: d \mid n} f(d). \end{aligned}$$

The summatory function is again an arithmetic function and can provide information on the function itself.

Lemma 7.4. *If f is a multiplicative function, then F is a multiplicative function.*

Proof. Let us consider the prime factorizations $m = \prod_{i=1}^{\ell} p_i^{e_i}, n = \prod_{i=1}^{r} q_i^{f_i}$. We first show that

$$\begin{aligned} \varphi : \{d \mid mn \mid \text{gcd}(m,n) = 1\} &\to \{(a,b) \mid \text{gcd}(a,b) = 1, a \mid m, b \mid n\} \\ d &\mapsto (\text{gcd}(d,m), \text{gcd}(d,n)\} \end{aligned}$$

is a bijection. In fact, for $d, d' \mid mn$, if $\varphi(d) = \varphi(d')$ then gcd$(m,d) =$ gcd$(m,d') = \prod_{i\in S} p_i^{e_i'}$ for some set $S \subseteq \{1,\dots,\ell\}$ and gcd$(n,d) =$ gcd$(n,d') = \prod_{i\in T} q_i^{f_i'}$, for some set $T \subseteq \{1,\dots,r\}$ with $e_i', f_i' > 0$, then $d = \prod_{i\in S} p_i^{e_i'} \prod_{i\in T} q_i^{f_i'} = d'$. And for any (a,b) with $a \mid m$, i.e., $a = \prod_{i\in S} p_i^{e_i'}$ and $b \mid n$, thus $b = \prod_{i\in T} p_i^{f_i'}$ with gcd$(a,b) = 1$ we have $d = ab$ such that $\varphi(d) = (a,b)$. Thus, we can change the summation over $\{d \mid mn\}$ with $\{a \mid m\}$ and $\{b \mid n\}$:

$$F(mn) = \sum_{d\in\mathbb{N}:d|mn} f(d) = \sum_{a\in\mathbb{N}:a|m} \sum_{b\in\mathbb{N}:b|n} f(ab).$$

Since f is multiplicative and gcd$(a,b) = 1$, we get

$$F(mn) = \sum_{a\in\mathbb{N}:a|m} f(a) \sum_{b\in\mathbb{N}:b|n} f(b) = F(m)F(n).$$

□

We have already seen a multiplicative function, namely the Euler totient function.

7.1 Euler Totient Function

Definition 7.5. The Euler totient function is defined as $\varphi(1) = 1$ and for $n > 1$:

$$\begin{aligned} \varphi : \mathbb{N} &\to \mathbb{Z}, \\ n &\mapsto |\mathbb{Z}/n\mathbb{Z}^\times|. \end{aligned}$$

Theorem 7.6. *The Euler totient function is a multiplicative function.*

Proof. The proof basically follows from the Chinese Remainder Theorem, as

$$\mathbb{Z}/(ab)\mathbb{Z}^\times \cong \mathbb{Z}/a\mathbb{Z}^\times \times \mathbb{Z}b\mathbb{Z}^\times.$$

Equivalently, the proof follows from Proposition 3.8. □

Theorem 7.7 (Gauss Theorem). *Let n be a positive integer, then*

$$\sum_{d\in\mathbb{N}:d|n} \varphi(d) = n.$$

Proof. Let $S = \{1, \dots, n\}$ and for every $d \mid n$ we denote by $S_d = \{a \in S \mid \gcd(a, n) = n/d\}$. The sets S_d partition S into disjoint subsets. Thus,

$$|\bigcup_{d \in \mathbb{N}: d|n} S_d| = \sum_{d \in \mathbb{N}: d|n} |S_d| = |S| = n.$$

We are left with showing that $|S_d| = \varphi(d)$.

Again, we show that

$$\varphi : \{a \in \{1, \dots, n\} \mid \gcd(a, n) = 1\} \to \{x \in \{1, \dots, d\} \mid \gcd(x, d) = 1\}$$
$$a \mapsto a\frac{d}{n}$$

is a bijection. Indeed, $\gcd(a\frac{d}{n}, d) = 1$ due to Proposition 1.3. If $\varphi(a) = \varphi(a')$ then $a\frac{d}{n} = a'\frac{d}{n}$, and hence $a = a'$. And for each $x \in \{1, \dots, d\}$ with $\gcd(x, d) = 1$ there exists $a = x\frac{n}{d}$ with $\gcd(x\frac{n}{d}, n) = \gcd(x\frac{n}{d}, d\frac{n}{d}) = 1$ as $\gcd(x, d) = 1$.

Thus,

$$|S_d| = |\{a \in \{1, \dots, n\} \mid \gcd(a, n) = \frac{n}{d}\}| = |\{x \in \{1, \dots, d\} \mid \gcd(x, d) = 1\}| = \varphi(d).$$

□

Note that in terms of summatory function, we have just proven that the summatory function of the Euler totient function, i.e., $F(n) = \sum_{d \in \mathbb{N}: d|n} \varphi(d) = n$, is an identity function $N(n) = n$.

7.2 More Multiplicative Functions

Let us consider two trivial multiplicative functions:

$$u(n) = 1,$$
$$N(n) = n,$$

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

Although these functions seem trivial, they help us to define many more multiplicative functions.

Definition 7.8. The number of divisors function is defined as

$$\tau : \mathbb{N} \to \mathbb{Z},$$
$$n \mapsto |\{d \in \mathbb{N} \mid d \mid n\}|.$$

Theorem 7.9. *The number of divisors function τ is multiplicative.*

Proof. We have that $\tau(n) = \sum_{d \in \mathbb{N}: d|n} 1 = \sum_{d \in \mathbb{N}: d|n} u(d)$. Since u is a multiplicative function, we can apply Lemma 7.4. □

Definition 7.10. The sum of the divisors function is defined as

$$\begin{aligned} \sigma : \mathbb{N} &\to \mathbb{Z}, \\ n &\mapsto \sum_{d \in \mathbb{N} : d \mid n} d. \end{aligned}$$

Theorem 7.11. *The sum of the divisors function is multiplicative.*

Proof. We have that $\sigma(n) = \sum_{d \in \mathbb{N}:d|n} d = \sum_{d \in \mathbb{N}:d|n} N(d)$. Since N is a multiplicative function, we can apply Lemma 7.4. □

The functions τ and σ are called *divisor functions*, and are special cases of the function

$$\sigma_k(n) = \sum_{d \in \mathbb{N}:d|n} d^k.$$

In fact, $\sigma_0 = \tau$ and $\sigma_1 = \sigma$.

Exercise 7.12. *Show that σ_k is multiplicative for any positive integer k.*

Theorem 7.13. *Let n be a positive integer with prime factorization $n = \prod_{i=1}^k p_i^{e_i}$. Then,*

$$\begin{aligned} \tau(n) &= \prod_{i=1}^k (e_i + 1), \\ \sigma(n) &= \prod_{i=1}^k \frac{p_i^{e_i+1} - 1}{p_i - 1}. \end{aligned}$$

Proof. Since both τ and σ are multiplicative function, with Theorem 7.2 it is enough to compute $\tau(p^e)$, respectively $\sigma(p^e)$ for some $p \in \mathcal{P}$ and positive integer e.

We note that the only divisors of p^e are of the form p^j for some $j \leq e$, that is

$$\tau(p^e) = |\{d \in \{1, \ldots, p^e\} \mid d \mid p^e\}| = \{p^j \mid j \in \{0, \ldots, e\}| = e + 1.$$

Hence, if $n = \prod_{i=1}^k p_i^{e_i}$, Theorem 7.2 implies

$$\tau(n) = \prod_{i=1}^k (e_i + 1).$$

Similarly, for $\sigma(p^e)$:

$$\sigma(p^e) = \sum_{d \in \mathbb{N}:d|p^e} d = \sum_{j=0}^e p^j = \frac{p^{e+1} - 1}{p - 1}.$$

Hence, if $n = \prod_{i=1}^k p_i^{e_i}$, Theorem 7.2 implies

$$\sigma(n) = \prod_{i=1}^k \frac{p_i^{e_i+1} - 1}{p_i - 1}.$$

□

Exercise 7.14. *For which n is $\tau(n)$ odd?*

7.3 Perfect Numbers

Definition 7.15. A positive integer n is called *perfect*, if n is the sum of its proper divisors (i.e., not n), that is $n = \sum_{d\in\mathbb{N}:d|n,d\neq n} d$.

Since $\sigma(n)$ is the sum of all divisors, we can write this condition as $n = \sigma(n) - n$, or equivalently, $\sigma(n) = 2n$.

Example 7.16. *6 and 28 are the first two perfect numbers as*

$$\begin{aligned} 6 &= 1 + 2 + 3, \\ 28 &= 1 + 2 + 4 + 7 + 14. \end{aligned}$$

Even perfect numbers have a one-to-one correspondence with Mersenne primes.

Theorem 7.17. *Let n be an even positive integer. Then n is perfect if and only if $n = (2^p - 1)2^{p-1}$, for $p \in \mathcal{P}, M(p) = 2^p - 1 \in \mathcal{P}$.*

Proof. Let us start with the first direction: if $n = (2^p - 1)2^{p-1}$ with $p \in \mathcal{P}$ and $2^p - 1 \in \mathcal{P}$. Note that $\sigma(q) = \sum_{d\in\mathbb{N}:d|q} = 1 + q$ for $q \in \mathcal{P}$. We also note that 2^{p-1} only has divisors of the form 2^j, while $2^p - 1$ is odd, thus the two factors are coprime. As σ is multiplicative, we get

$$\sigma(n) = \sigma(2^p - 1)\sigma(2^{p-1}).$$

Due to Theorem 7.13, we know that $\sigma(2^{p-1}) = 2^p - 1$ and $\sigma(2^p - 1) = 2^p$, since $2^p - 1 \in \mathcal{P}$. Thus,

$$\sigma(n) = 2^p(2^p - 1) = 2(2^{p-1}(2^p - 1)) = 2n.$$

For the other direction, since n is even, there exists some positive integer $p \geq 2$ and odd integer q, such that $n = 2^{p-1}q$. Again, we have that $\gcd(2^{p-1}, q) = 1$ and can use that σ is multiplicative, to get

$$\sigma(n) = \sigma(2^{p-1})\sigma(q) = (2^p - 1)\sigma(q).$$

Since n is perfect, we have $\sigma(n) = 2n = 2^p q$ and hence

$$(2^p - 1)\sigma(q) = 2^p q.$$

Since $\gcd(2^p - 1, 2^p) = 1$, we must have $2^p \mid \sigma(q)$. Thus, there exists an integer r, such that

$$2^p r = \sigma(q).$$

Hence $\sigma(n) = 2n$ becomes

$$(2^p - 1)\sigma(q) = (2^p - 1)2^p r = 2^p q,$$

and hence $(2^p - 1)r = q$. This means that $r \mid q$ and $r \neq q$, as $p \geq 2$.

Let us add r on both sides to get

$$(2^p - 1)r + r = 2^p r = \sigma(q) = q + r.$$

Since $\sigma(q)$ is the sum of all divisors and q, r are divisors, we must have that they are the only divisors. Thus, q is prime and $r = 1$. Since $q = 2^p - 1$ is prime, it follows from Lemma 3.14, that $p \in \mathcal{P}$.

□

Hence even perfect numbers are generated by Mersenne primes.

What about odd perfect numbers though? In fact, it is not known whether odd perfect numbers exist. But we do know how they should behave or look like:

Exercise 7.18. *Show that if n is an odd perfect number, then $n = p^a m^2$, where p is an odd prime, $p \equiv a \equiv 1 \mod 4$ and m is an integer.*

Exercise 7.19. *Show that if n is an odd perfect number, then $n \equiv 1 \mod 4$.*

Exercise 7.20. *Show that if n is an odd perfect number, then n has at least three different prime divisors.*

7.4 Möbius Inversion Formula

The multiplicative property is very useful to provide identities between such functions.

Lemma 7.21. *Let f, g be multiplicative functions with $f(p^e) = g(p^e)$ for all $p \in \mathcal{P}$ and non-negative integers e. Then $f = g$.*

Proof. Let n be a positive integer with prime factorization $n = \prod_{i=1}^{k} p_i^{e_i}$, then

$$f(n) = \prod_{i=}^{k} f(p_i^{e_i}) = \prod_{i=1}^{k} g(p_i^{e_i}) = g(n).$$

□

Exercise 7.22. *Give another proof of Theorem 7.7, showing that the summatory function $F = \sum_{d \in \mathbb{N}: d|n} \varphi(n)$ and N agree on all prime powers.*

We have already seen some summatory identities, i.e., of the form $F(n) = \sum_{d \in \mathbb{N}: d|n} f(d)$. For example

- in Theorem 7.7 $F = N$, $f = \varphi$,
- in Theorem 7.11 $F = \sigma$, $f = N$,
- in Theorem 7.9 $F = \tau, f = u$.

We will later generalize this notion to the Dirichlet product and revisit these identities.

In this situation it is often useful if we are able to invert the roles of f and F. This is done by the *Möbius Inversion Formula.*

In order to introduce the Möbius Inversion Formula, we need the following function.

Definition 7.23. The *identity function* is given by $\varepsilon(1) = 1, \varepsilon(n) = 0$ for all $n \neq 1$.

ε is clearly multiplicative. In fact, for any a, b we have

$$\varepsilon(ab) = \begin{cases} 1 & \text{if } ab = 1, \\ 0 & \text{else} \end{cases} = \begin{cases} 1 & \text{if } a = b = 1, \\ 0 \text{ else} \end{cases} = \varepsilon(a)\varepsilon(b).$$

A useful alternative formulation of the identity is

$$\varepsilon(n) = \left\lfloor \frac{1}{n} \right\rfloor .$$

We first define the *Möbius function* via the formula

$$\sum_{d \in \mathbb{N}: d|n} \mu(d) = \varepsilon(n),$$

i.e., as the function having ε as summatory function.

While this gives a recursive definition, we will later see an explicit definition as well. In fact, if $n = 1$, then

$$\varepsilon(1) = \sum_{d \in \mathbb{N}: d|1} \mu(d) = \mu(1) = 1$$

and for $n > 1$ we have

$$\sum_{d \in \mathbb{N}: d|n} \mu(d) = 0 = \varepsilon(n),$$

thus

$$\mu(n) = - \sum_{d \in \mathbb{N}: d|n, d<n} \mu(d).$$

Proposition 7.24. *Let $p, q \in \mathcal{P}$ be distinct, then*

- $\mu(p) = -1,$
- $\mu(pq) = 1,$
- $\mu(p^e) = 0,$ *for any* $e \geq 2.$

Proof.
- If $p \in \mathcal{P}$, then $\mu(p) = -\sum_{d \in \mathbb{N}: d<p, d|p} \mu(d) = -\mu(1) = -1.$

- If $p \neq q$, we get $\mu(pq) = -\sum_{d\in\mathbb{N}:d<pq,d|pq} \mu(d) = -(\mu(1)+\mu(p)+\mu(q)) = -(1-1-1) = 1.$
- We may proceed by induction. For $e = 2$, we get $\mu(p^2) = -\sum_{d\in\mathbb{N}:d<p^2,d|p^2} \mu(d) = -(\mu(1)+\mu(p))) = -(1-1) = 0$. Assume the claim holds for all $e' < e$. For any $e \geq 2$, we have

  $$\mu(p^e) = -\sum_{d\in\mathbb{N}:d<p^e,d|p^e} \mu(d) = -(\mu(1)+\mu(p)+\mu(p^2)+\cdots+\mu(p^{e-1})) = -(1-1+0) = 0,$$

  by the induction hypothesis.

□

The Möbius function derives its importance from the following major result, called *Möbius Inversion Formula.*

Theorem 7.25. *Let f be an arithmetic function and consider the summatory function $F(n) = \sum_{d\in\mathbb{N}:d|n} f(d)$ for all $n \in \mathbb{N}$, then*

$$f(n) = \sum_{d\in\mathbb{N}:d|n} F(d)\mu\left(\frac{n}{d}\right) = \sum_{d\in\mathbb{N}:d|n} \mu(d)F\left(\frac{n}{d}\right),$$

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

Proof. Let $e = n/d$, then due to the commutativity of $ed = de = n$, we get

$$\sum_{d\in\mathbb{N}:d|n} F(d)\mu\left(\frac{n}{d}\right) = \sum_{d,e\in\mathbb{N}:de=n} F(d)\mu(e) = \sum_{e,d\in\mathbb{N}:ed=n} \mu(d)F(e) = \sum_{d\in\mathbb{N}:d|n} \mu(d)F\left(\frac{n}{d}\right).$$

Thus, we are left with showing that these expressions are equal to $f(n)$.

Since $F(n) = \sum_{d\in\mathbb{N}:d|n} f(d)$, we can also evaluate at n/d :

$$F\left(\frac{n}{d}\right) = \sum_{t\in\mathbb{N}:t|\frac{n}{d}} f(t).$$

Thus, we can insert this formula in $\sum_{d\in\mathbb{N}:d|n} \mu(d)F\left(\frac{n}{d}\right)$, to get

$$\sum_{d\in\mathbb{N}:d|n} \mu(d)F\left(\frac{n}{d}\right) = \sum_{d\in\mathbb{N}:d|n} \left(\mu(d) \sum_{t\in\mathbb{N}:t|\frac{n}{d}} f(t)\right) = \sum_{d\in\mathbb{N}:d|n} \left(\sum_{t\in\mathbb{N}:t|\frac{n}{d}} \mu(d)f(t)\right).$$

We note that $\{(d,t) \mid d \mid n, t \mid \frac{n}{d}\}$ is the same as $\{(t,d) \mid t \mid n, d \mid \frac{n}{t}\}$. In fact, if (d,t) is such that $t \mid \frac{n}{d}$, there exists a $\ell \in \mathbb{N}$ such that $t\ell = \frac{n}{d}$, thus $t(\ell d) = n$ and $t \mid n$ and $d\ell = \frac{n}{t}$, hence $d \mid \frac{n}{t}$. The other direction follows in the same way. Thus, we can exchange the sums, instead of running over (d,t) with $d \mid n$ and $t \mid \frac{n}{d}$ to run over (t,d) with $t \mid n$ and $d \mid \frac{n}{t}$.

Hence,

$$\sum_{d\in\mathbb{N}:d|n}\left(\sum_{t\in\mathbb{N}:t|\frac{n}{d}}\mu(d)f(t)\right)=\sum_{t\in\mathbb{N}:t|n}\left(\sum_{d\in\mathbb{N}:d|\frac{n}{t}}f(t)\mu(d)\right)=\sum_{t\in\mathbb{N}:t|n}\left(f(t)\sum_{d\in\mathbb{N}:d|\frac{n}{t}}\mu(d)\right).$$

Recall by the definition of μ we have

$$\sum_{d\in\mathbb{N}:d|\frac{n}{t}}\mu(d)=\begin{cases}1 & \text{if } \frac{n}{t}=1,\\ 0 & \text{if } \frac{n}{t}>1.\end{cases}$$

Hence, the only non-zero coefficients of $f(t)$ is when $n=t$, that is

$$\sum_{t\in\mathbb{N}:t|n}\left(f(t)\sum_{d\in\mathbb{N}:d|\frac{n}{t}}\mu(d)\right)=f(n)\cdot 1=f(n).$$

□

This shows that if F is the summatory function of f, then we can also write f in a similar way.

Corollary 7.26. *Let n be a positive integer. Then,*

$$\varphi(n)=\sum_{d\in\mathbb{N}:d|n}d\mu\left(\frac{n}{d}\right)=\sum_{d\in\mathbb{N}:d|n}\mu(d)\frac{n}{d}.$$

Exercise 7.27. *Prove Corollary 7.26 using Theorem 7.25 with $F=N$ and $f=\varphi$.*

We can now give a more explicit definition of the Möbius function.

Theorem 7.28. *Let n be a positive integer with prime factorization $n=\prod_{i=1}^{k}p_i^{e_i}$. Then,*

$$\mu(n)=\begin{cases}0 & \textit{if some } e_i>1,\\ (-1)^k & \textit{else,}\end{cases}$$

and $\mu(1)=1$.

Proof. Let us consider the function defined in the statement μ', that is $\mu'(1)=1$ and if n is a product of k distinct primes, then $\mu'(n)=(-1)^k$ and $\mu'(n)=0$ else.

We prove that $\mu'=\mu$ from the recursive definition by induction on n.

Clearly $\mu(1)=\mu'(1)=1$. Thus, let us assume that for all $d<n$ we have $\mu(d)=\mu'(d)$.

Let $n>1$ with prime factorization $n=\prod_{i=1}^{k}p_i^{e_i}$. We first show that $\sum_{d\in\mathbb{N}:d|n}\mu'(d)=\sum_{d\in\mathbb{N}:d|n}\mu(d)=\varepsilon(n)=0$.

Note that the non-zero terms in $\sum_{d\in\mathbb{N}:d|n} \mu'(d)$ are such that d is a product of $0 \leq r \leq k$ distinct primes, that is $d = p_{i_1} \cdots p_{i_r}$, in which case $\mu'(d) = (-1)^r$.

For each r, we have $\binom{k}{r}$ possibilities to form such product, which are divisors d of n. Summing over all r, we get

$$\sum_{d\in\mathbb{N}:d|n} \mu'(d) = \sum_{r=0}^{k} \binom{k}{r} (-1)^r = (1 + (-1))^k = 0,$$

by the Binomial Theorem.

Since $\sum_{d\in\mathbb{N}:d|n} \mu'(d) = 0$, we can write

$$\mu'(n) = - \sum_{d\in\mathbb{N}:d|n,d<n} \mu'(d),$$

and by induction hypothesis $\mu'(d) = \mu(d)$ for all $d < n$ we get

$$\mu'(n) = - \sum_{d\in\mathbb{N}:d|n,d<n} \mu(d) = \mu(n).$$

□

Exercise 7.29. *Find a simple formula for*

$$\sum_{d\in\mathbb{N}:d|n} |\mu(d)|.$$

Definition 7.30. We say that a positive integer n is *square-free*, if there exists not $p \in \mathcal{P}$ with $p^2 \mid n$.

All square-free integers are of the form $n = \prod_{i=1}^{k} p_i$.

Note that from Theorem 7.28, it follows that $\mu(n) \neq 0$ if and only if n is square-free.

Exercise 7.31. *Use Theorem 7.28 to show*

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

Corollary 7.32. *The Möbius function μ is multiplicative.*

Exercise 7.33. *Prove Corollary 7.32, distinguishing between square-free a, b and a, b being a product of k, respectively r, distinct primes.*

7.5 Convolution

Let us recall the summatory function of f, i.e.,

$$F(n) = \sum_{d\in\mathbb{N}:d|n} f(d)$$

and the identities we have seen

- Theorem 7.9:
$$F(n) = \tau(n) = \sum_{d\in\mathbb{N}:d|n} 1 = \sum_{d\in\mathbb{N}:d|n} u(d),$$
- Theorem 7.7:
$$F(n) = N(n) = \sum_{d\in\mathbb{N}:d|n} \varphi(d),$$
- Theorem 7.11:
$$F(n) = \sigma(n) = \sum_{d\in\mathbb{N}:d|n} d = \sum_{d\in\mathbb{N}:d|n} N(d),$$
- by definition
$$F(n) = \varepsilon(n) = \sum_{d\in\mathbb{N}:d|n} \mu(d).$$

And we have seen the Möbius Inversion Formula, stating that if F is the summatory function of f, then we can write

$$f(n) = \sum_{d\in\mathbb{N}:d|n} \mu(d)F(n/d).$$

We will now use this expression to give an operation between arithmetic functions, and then rewrite the identities.

Definition 7.34. Let f, g be arithmetic functions. The *Dirichlet product* or *convolution* $\star$ is defined as

$$f \star g(n) = \sum_{d\in\mathbb{N}:d|n} f(d)g\left(\frac{n}{d}\right).$$

Proposition 7.35. *The Dirichlet product of two multiplicative functions is again multiplicative.*

Proof. As we have seen in the proof of Lemma 7.4 Let a, b be two positive coprime integers. Then

$$\begin{aligned}\varphi : \{d \in \mathbb{N} \mid d \mid ab, \text{gcd}(a,b) = 1\} &\to \{(c,e) \mid \text{gcd}(c,d) = 1, c \mid a, e \mid b\},\\ d &\mapsto (\text{gcd}(a,d), \text{gcd}(b,d)),\end{aligned}$$

is a bijection between the positive integers dividing ab and the positive integers dividing a and b. We also note that $c = \text{gcd}(a,d), e = \text{gcd}(b,d)$ are coprime and $d = ce$.

Thus,

$$\begin{aligned} f\star g(ab) &= \sum_{d\in\mathbb{N}:d|ab} f(d)g\left(\frac{ab}{d}\right) = \sum_{c\in\mathbb{N}:c|a}\sum_{e\in\mathbb{N}:e|b} f(ce)g\left(\frac{a}{c}\frac{b}{e}\right) \\ &= \sum_{c\in\mathbb{N}:c|a}\sum_{e\in\mathbb{N}:e|b} f(c)f(e)g\left(\frac{a}{c}\right)g\left(\frac{b}{e}\right) = \sum_{c\in\mathbb{N}:c|a} f(c)g\left(\frac{a}{c}\right)\sum_{e\in\mathbb{N}:e|b} f(e)g\left(\frac{b}{e}\right) \\ &= (f\star g(a))(f\star g(b)). \end{aligned}$$

□

Using this new notation, we can write the summatory function as

$$F = u\star f.$$

Thus, the Möbius Inversion Formula states: if $F = u\star f$, then $f = \mu\star F$.

With this we can rewrite our previous summatory identities, and their Möbius inversion.

- Theorem 7.9: $\tau = u\star u$ and its inversion: $u = \tau\star\mu$,
- Theorem 7.7: $N = u\star\varphi$ and its inversion $\varphi = N\star\mu$,
- Theorem 7.11: $\sigma = u\star N$ and its inversion $N = \sigma\star\mu$,
- by definition $\varepsilon = u\star\mu$ and its inversion $\mu = \varepsilon\star\mu$.

The Dirichlet product also has a lot of algebraic properties.

Lemma 7.36. *The Dirichlet product is commutative, associative and ε is the neutral element.*

Proof. Let f, g, h be arithmetic functions.

- For the commutativity, we see that

$$(f\star g)(n) = \sum_{e,d\in\mathbb{N}:ed=n} f(d)g(e) = \sum_{e,d\in\mathbb{N}:ed=n} g(d)f(e) = (g\star f)(n).$$

- For the associativity, we check that

$$\begin{aligned} ((f\star g)\star h)(n) &= \sum_{c,d\in\mathbb{N}:cd=n} (f\star g)(d)h(c) \\ &= \sum_{c,d\in\mathbb{N}:cd=n}\left(\sum_{a,b\in\mathbb{N}:ab=d} f(a)g(b)\right)h(c) = \sum_{a,b,c\in\mathbb{N}:abc=n} f(a)g(b)h(c) \end{aligned}$$

and similarly

$$\begin{aligned} (f\star(g\star h))(n) &= \sum_{a,e\in\mathbb{N}:ae=n} f(a)(g\star h)(e) \\ &= \sum_{a,e\in\mathbb{N}:ae=n} f(a)\sum_{b,c\in\mathbb{N}:bc=e} g(b)h(c) = \sum_{a,b,c\in\mathbb{N}:abc=n} f(a)g(b)h(c). \end{aligned}$$

- For the neutral element, we observe that

  $$(f \star \varepsilon)(n) = \sum_{e,d \in \mathbb{N}: ed = n} f(d)\varepsilon(e) = f(n),$$

  since $\varepsilon(e) = 1$ only for $e = 1$.

□

Having a neutral element for the Dirichlet product, we may ask: which arithmetic functions have inverse functions?

Lemma 7.37. *If f is an arithmetic function with $f(1) \neq 0$, then there exists an arithmetic function g such that $f \star g = \varepsilon$, and is given by $g(1) = f(1)^{-1}$ and*

$$g(n) = -f(1)^{-1} \sum_{d \in \mathbb{N}: d|n, d<n} g(d) f\left(\frac{n}{d}\right),$$

for all $n > 1$.

Proof. For $n = 1$, the claim trivially follows:

$$f \star g(1) = f(1)g(1) = f(1)f(1)^{-1} = 1 = \varepsilon(1).$$

For $n > 1$, we have

$$\begin{aligned}(g \star f)(n) &= g(n)f(1) + \sum_{d \in \mathbb{N}: d|n, d<n} g(d) f\left(\frac{n}{d}\right) \\ &= -\sum_{d \in \mathbb{N}: d|n, d<n} g(d) f\left(\frac{n}{d}\right) + \sum_{d \in \mathbb{N}: d|n, d<n} g(d) f\left(\frac{n}{d}\right) = 0.\end{aligned}$$

□

Thus, for multiplicative functions, we get

Corollary 7.38. *Let f be a multiplicative function, then there exists a multiplicative function g with $f \star g = \varepsilon$, given by*

$$g(n) = -\sum_{d \in \ltimes: d|n, d<n} g(d) f\left(\frac{n}{d}\right),$$

for all $n \geq 1$.

Let us now show a stronger version of the Möbius Inversion Formula:

Theorem 7.39. *Let f be an arithmetic function. Then, $F = u \star f$ if and only if $f = \mu \star F$.*

Proof. We can easily recover the Möbius Inversion Formula as follows: if $F = u \star f$, then

$$F \star \mu = (f \star u) \star \mu = f \star (u \star \mu) = f \star \varepsilon = f.$$

We also have the other direction: if $f = F \star \mu$, then

$$F = F \star \varepsilon = F \star (\mu \star u) = (F \star \mu) \star u = f \star u.$$

□

Exercise 7.40. *Prove Proposition 7.35 using a similar argument as in Lemma 7.4 with the equation*

$$f(mn) = \sum_{d \in \mathbb{N}: d | mn} g(d) h\left(\frac{mn}{d}\right).$$

8 Applications in Cryptography

We will now see one of the main applications of elementary number theory: cryptography.

> *Thank God that number theory is unsullied by any application.*
> Leonard Dickson

Let us start with explaining the objective of cryptography.

Cryptography is the art of *secure* communication. That is, there are the two parties, called *Alice* and *Bob*, who want to communicate in a secure way, that means, such that an eavesdropper (usually called *Eve*) is not able to read the messages.

In cryptography we differ between two main branches, called symmetric cryptography and asymmetric cryptography.

In *symmetric cryptography*, Alice and Bob have exchanged some key prior to communication, that will enable them a secure communication. Such secret key exchange might be performed using protocols such as the Diffie-Hellman key exchange, which itself lies in the realm of asymmetric cryptography.

More mathematically involved is the branch of *asymmetric cryptography* or *public-key cryptography*, where the two parties do not share the same key.

The main public-key cryptosystems are: *Public-Key Encryption* (PKE) schemes, Key Encapsulation Mechanisms (KEM) and signature schemes.

8.1 PKE

A PKE consists of three steps:

1. key generation,
2. encryption,
3. decryption.

The main idea is that one party, Alice, constructs a *secret key* S and a connected *public key* P. The public key, as the name suggests, is made publicly known, while the secret key is kept private.

This allows an other party, Bob, to use the public key to encrypt a *message* m by applying the public key, gaining the so called *ciphertext* c.

The ciphertext is now sent through the insecure channel to Alice, who can use her secret key S to decrypt the ciphertext and recover the message m.

An adversary, Eve, can only see the ciphertext c and the public key P. In order for a public-key encryption scheme to be considered secure, it should be infeasible for Eve to recover from c and P the message m. This also implies that the public key should not reveal the secret key.

What exactly does infeasible mean, however? This is the topic of *security*. For a cryptographic scheme, we define its *security level* to be the average number of binary operations needed for an adversary to break the cryptosystem, that means either to recover the message (called *message recovery*) or the secret key (called *key recovery*).

Usual security levels are $2^{80}, 2^{128}, 2^{256}$ or even 2^{512}, meaning for example that an adversary is expected to need at least 2^{80} binary operations in order to reveal the message. These are referred to as 80 bit, 128 bit, 256 bit, or 512 bit security levels.

Apart from the security of a PKE, one is also interested in the performance, including how fast the PKE can be executed and how much storage the keys require. Important parameters of a PKE are

- the public key size,
- the secret key size,
- the ciphertext size,
- the decryption time.

With ’size’ we intend the bits that have to be sent or stored for this key, respectively for the ciphertext. Clearly, one prefers small sizes and a fast decryption.

8.2 RSA

One of the most used PKE schemes is called RSA. This stands for its inventors Rivest, Shamir and Adleman. Although RSA was published by the three in 1977, the system was already invented before by the British secret agent Ellis, who, unfortunately, was not allowed to publish his idea.

RSA is widely used for internet communication protocols, email encryption, EC payments, online banking and many more applications.

The tools we require to understand RSA are: Euclidean’s algorithm, the Chinese Remainder Theorem, the Euler totient function and Euler’s theorem.

Let us quickly give the three steps, and then explain why it works and how secure it is.

1. Key Generation: Alice chooses two distinct primes p, q and computes $n = pq$ and $\varphi(n) = (p-1)(q-1)$. She chooses a positive integer $e < \varphi(n)$, which is coprime to $\varphi(n)$. The public key is $P = (n, e)$ and the secret key is $S = (p, q)$.
2. Encryption: Bob chooses a message m and encrypts it by computing

$$c = m^e \mod n.$$

3. Decryption: Alice can decrypt the ciphertext by first computing d and b such that

$$de + b\varphi(n) = 1.$$

She can then recover the message as $c^d \equiv m \mod n$.

Why does this scheme work? Or equivalently, why is Alice able to recover the message correctly?

Proposition 8.1. *RSA is correct, i.e., Alice can recover the message.*

Proof. If $\gcd(m, n) = 1$, then this follows by Euler's Theorem:

$$c^d \equiv (m^e)^d \equiv m^{1-b\varphi(n)} \equiv m \left(m^{\varphi(n)}\right)^{-b} \equiv m1^{-b} \equiv m \mod n.$$

If $t = \gcd(m, n) \neq 1$, we note that $t \in \{p, q, n\}$. We assume that $t \neq n$ as else Bob sent $c = 0$. Assume $t = p$ and hence $m = kp$ for some integer k. Now, we argue using the Chinese Remainder Theorem and Fermat's Little Theorem.

In order to solve $x \equiv c^d \mod n$ we can equivalently solve

$$x \equiv c^d \mod p,$$
$$x \equiv c^d \mod q.$$

Since $m = kp$, $c \equiv m^e \mod n$ is also a multiple of p and thus the first equation is simply $x \equiv 0 \mod p$. Recall that d was chosen such that

$$ed + b(p - 1)(q - 1) = 1.$$

Thus, for $b' = b(p - 1)$, we have

$$ed + b'\varphi(q) = 1.$$

Hence,

$$c^d \equiv m^{1-b'(q-1))} \equiv m \left(m^{q-1}\right)^{-b'} \equiv m \equiv m' \mod q.$$

Now we can recover m using

$$x \equiv 0 \mod p,$$
$$x \equiv m' \mod q$$

and the Chinese Remainder Theorem, getting $x \equiv m \mod n$. □

How secure is the scheme? Eve is able to see n, e and the ciphertext c. In order for Eve to recover m, she needs to compute $d \equiv e^{-1} \mod \varphi(n)$. However, Eve does not know $\varphi(n)$.

Thus, RSA is based on the hardness of integer factorization.

Proposition 8.2. *Let p, q be distinct primes and $n = pq$. Then, knowing p, q is equivalent to knowing $n, \varphi(n)$.*

Proof. The first direction is easy, as p, q reveals $n = pq$ and $\varphi(n) = (p-1)(q-1)$.

On the other hand, knowing n and $\varphi(n)$, one can use the two equations

$$p + q = n - \varphi(n) + 1,$$
$$|p - q| = \sqrt{(p+q)^2 - 4n}$$

to recover p, q.

□

While we do not know any algorithm that solves integer factorization in polynomial time, there is still the threat coming from capable quantum computers: Shor's algorithm is able to factor integers in polynomial time using a quantum algorithm.

While the scheme still works for messages m which are not coprime to the public n, such choices should be avoided. In fact, if gcd$(m, n) = p$, then gcd$(c, n) = p$ as well and an attacker can compute this quickly using the Euclidean algorithm.

Example 8.3. *Alice chooses $p = 7, q = 13$ and compute $n = 91$ and $\varphi(n) = 72$.*

She then chooses $e < 72$, which is coprime to 72, for example $e = 5$. Alice then publishes $P = (91, 5)$ and keeps $S = (7, 13)$ a secret.

Bob has a message, say $m = 3$, and computes the ciphertext as $m^e \equiv 3^5 \mod 91$. Bob can do so efficiently using consecutive squaring:

$$c = 3^5 = (3^2)^2 \cdot 3 \equiv 61 \mod 91.$$

Alice can now apply the Euclidean algorithm to find integers d, b such that

$$de + b\varphi(n) = d \cdot 5 + b \cdot 91 = 1.$$

Doing so, Alice finds that

$$72 = 14 \cdot 5 + 2,$$
$$5 = 2 \cdot 2 + 1.$$

And by inserting these equations backwards, she gets that

$$1 = 5 - 2 \cdot 2 = 5 - 2(72 - 14 \cdot 5) = (-2) \cdot 72 + 29 \cdot 5.$$

Alice, thus, found the decryption exponent $d = 29$ and she can compute (again using consecutive squaring)

$$c^d \equiv 61^{29} \equiv m \equiv 3 \mod 91.$$

Exercise 8.4. *Use $p = 7, q = 13$ to encrypt the message $m = 21$.*

Exercise 8.5. *What happens if we choose $q = p$?*

8.3 Digital Signature Schemes

Digital signature schemes aim at giving a guarantee of the legitimate origin of an object, such as a digital message, exactly as signing a letter to prove that the sender of this letter is really you.

In this process we speak of *authentication*, meaning that a receiver of the message can (with some probability) be sure that the sender is legit, and of *integrity*, meaning that the message has not been altered.

A digital signature scheme again consists of three steps:

1. key generation,
2. signing,
3. verification.

In digital signature schemes we consider two parties: the *signer*, who has to prove their identity to the second party, called *verifier*, who in turn, verifies the identity of the signer.

As a first step, the signer constructs a secret key S, which is kept private and a public key P, which is made public. The signer then chooses a message m, and creates a signature s using his secret key S and the message m, getting a signed message (m, s).

The verifier can easily read the message m, but wants to be sure that the sender is legit. Thus, the verifier uses the public key P and the knowledge of the message m on the signature s to get authentication.

The security of a digital signature scheme introduces a new adversary, the *impersonator*. An impersonator, tries to cheat the verifier and acts as a signer, however without the knowledge of the secret key S.

An impersonator wins if a verifier has verified a forged signature. This comes with a certain probability, called *cheating probability* or *soundness error*. In order to ensure integrity a digital signature should always involve a secret key as well as the message itself.

Clearly, the secret key should still be infeasible to recover from the publicly known key, thus one still has the usual adversary, called Eve, and a security level, as in a public-key encryption scheme.

The performance of a digital signature scheme consists of

- the *signature size*,
- the public key size,
- the secret key size,
- the verification time.

8.4 RSA Signature Scheme

We can turn the RSA public-key encryption protocol into a signature scheme.

1. Key Generation: the signer chooses two distinct primes p, q and computes $n = pq$ and $\varphi(n) = (p-1)(q-1)$. The signer chooses a natural number $e < \varphi(n)$, which is coprime to $\varphi(n)$ and computes d and b such that
$$de + b\varphi(n) = 1.$$
The public key is $P = (n, e)$ and the secret key is $S = (p, q, d)$.
2. Signing: the signer chooses a message m and signs it by computing
$$s = m^d \mod n.$$
The signer then sends m, s to the verifier.
3. Verification: the verifier can verify the signature s by checking if
$$s^e = m \mod n.$$

Proposition 8.6. *The signature scheme RSA is correct, i.e., the verifier will accept a honest signer.*

Proof. The proof is similar to Proposition 8.1. If gcd$(m, n) = 1$ we can apply Euler's Theorem to get
$$s^e \equiv m^{de} \equiv m^{1-b\varphi(n)} \equiv m \left(m^{\varphi(n)}\right)^{-b} \equiv m \mod n.$$
If gcd$(m, n) = t \neq 1$, we can only have $t \in \{p, q, n\}$. We can exclude $t = n$, as else $m \equiv 0 \mod n$, and so is c. Thus, let us assume that $t = p$. Instead of solving $s^e \mod n$ we equivalently compute $s^e \mod p$ and $s^e \mod q$.

Again, as m is a multiple of p, so is s and thus $s^e \equiv 0 \mod p$. We can rewrite $ed + b\varphi(n) = 1$ as $ed + b'(q-1) = 1$ for $b' = b(p-1)$ and thus
$$s^e \equiv m^{de} \equiv m \left(m^{q-1}\right)^{-b'} \equiv m \equiv m' \mod q.$$
Using the Chinese Remainder Theorem for $s^e \equiv 0 \mod p$ and $s^e \equiv m' \mod q$ we recover $s^e \equiv m \mod n$. □

Example 8.7. *The signer chooses $p = 7, q = 13$ and compute $n = 91$ and $\varphi(n) = 72$.*

The signer then chooses $e < 72$, which is coprime to 72, for example $e = 5$.

The signer computes
$$1 = 5 - 2 \cdot 2 = 5 - 2(72 - 14 \cdot 5) = (-2) \cdot 72 + 29 \cdot 5.$$
Thus, $d = 29$. The public key is given by $P = (91, 5)$ and the secret key by $S = (7, 13, 29)$ a secret.

In order to sign a message, say $m = 3$, the signer computes $s = m^d \equiv 3^{29} \equiv 61 \mod 91$. The signer then sends $(m, s) = (3, 61)$ to the verifier. The verifier can check the signature as
$$s^e \equiv 61^5 \equiv m \equiv 3 \mod 91.$$

The signature scheme (in the presented form) is unfortunately not secure.

In fact, after seeing two message and signature pairs (m_1, s_1) and (m_2, s_2) an impersonator can construct another valid pair:

$$(m \equiv m_1 m_2 \mod n, s \equiv s_1 s_2 \mod n),$$

since

$$s^e \equiv (s_1 s_2)^e \equiv s_1^e s_2^e \equiv m_1 m_2 \equiv m \mod n.$$

We call this a homomorphic property.

Exercise 8.8. *How would an impersonator forge a signature provided that the impersonator does not care about the content of the message m?*

In order to prevent such attacks, we first compute the hash of the message and then sign this.

A *hash function* is a function that compresses the input value to a fixed length. In addition, we want that it is computationally hard to reverse a hash function and also to find a different input giving the same hash value. We denote the publicly known hash function by Hash.

Thus, we can update the RSA signature scheme with

1. Key Generation: the signer chooses two distinct primes p, q and computes $n = pq$ and $\varphi(n) = (p-1)(q-1)$. The signer chooses a natural number $e < \varphi(n)$, which is coprime to $\varphi(n)$ and computes d and b such that

   $$de + b\varphi(n) = 1.$$

   The public key is $P = (n, e)$ and the secret key is $S = (p, q, d)$.

2. Signing: the signer chooses a message m and computes $\mathsf{Hash}(m)$. The signer computes

   $$s = \mathsf{Hash}(m)^d \mod n$$

   and sends m, s to the verifier.

3. Verification: the verifier can verify the signature s by checking if

   $$s^e = \mathsf{Hash}(m) \mod n.$$

8.5 Discrete Logarithm

Another public-key encryption scheme is based on the hardness of the discrete logarithm problem in $\mathbb{Z}/p\mathbb{Z}$, for $p \in \mathcal{P}$.

Definition 8.9. Let $p \in \mathcal{P}$ and $\alpha \in \mathbb{Z}/p\mathbb{Z}$ of order $p-1$. Let $A = \alpha^i \in \mathbb{Z}/p\mathbb{Z}^\times$, for some $i \in \{0, \dots, p-2\}$. Then i is called the *discrete logarithm* of A in the base α modulo p.

Similar to factoring integers, we do not know any algorithm that finds discrete logarithms in polynomial time. However, Shor's algorithm is able to do so on a capable quantum computer.

We start this section with the famous Diffie-Hellmann key exchange protocol, as it revolutionized cryptography, opening the door to public-key cryptosystems.

8.5.1 Diffie-Hellmann Key Exchange

This protocol is a key encapsulation mechanism, also called key agreement or key exchange protocol. In fact, its purpose is to securely exchange a key in order to enable symmetric cryptosystems.

1. Alice and Bob agree on a public key $P = (p, \alpha)$, where $p \in \mathcal{P}$ and $\alpha \in \mathbb{Z}/p\mathbb{Z}$ of order $p-1$.
2. Alice chooses $a \in \{2, \dots, p-2\}$ and computes $A = \alpha^a \mod p$ and sends A to Bob.
3. Bob chooses $b \in \{2, \dots, p-2\}$ and computes $B = \alpha^b \mod p$ and sends B to Alice.
4. Both can now compute the shared secret key $\alpha^{ab} \equiv A^b \equiv B^a \mod p$.

Clearly, the values $1, p-1$ are avoided for the secret a, b as sending $\alpha^1 = \alpha$ reveals $k = 1$ and $\alpha p - 1 \equiv 1 \mod p$ reveals $k = p - 1$.

Example 8.10. *Alice and Bob agree on* $p = 11$ *and* $\alpha = 2$.
Alice then chooses $a = 4$ *and computes* $A \equiv 2^4 \equiv 5 \mod 11$. *She sends* $A = 5$ *to Bob.*
Bob chooses $b = 8$ *and computes* $B \equiv 2^8 \equiv 3 \mod 11$ *and sends this to Alice.*
Both can now compute

$$2^{ab} = 2^{4\cdot 8 \mod p-1} \equiv 2^2 \equiv 4 \mod p.$$

8.5.2 ElGamal cryptosystem

This idea also gives raise to the ElGamal public-key encryption scheme.

1. Key generation: Alice chooses $p \in \mathcal{P}$ and $\alpha \in \mathbb{Z}/p\mathbb{Z}$ of order $p-1$, $a \in \{2, \dots, p-2\}$ and computes $A \equiv \alpha^a \mod p$. The secret key is given by $S = a$ and the public key is $P = (p, \alpha, A)$.
2. Encryption: Bob chooses $b \in \{2, \dots, p-2\}$ and computes $B \equiv \alpha^b \mod p$. For a message m, Bob computes $c \equiv A^b m \mod p$ and sends the ciphertext (c, B).
3. Decryption: Alice can compute

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

Why does this work?

Proposition 8.11. *The ElGamal cryptosystem is correct, i.e., Alice can recover the message.*

Proof. Note that

$$B^{p-1-a} c \equiv \alpha^{b(p-1-a)} A^b m \equiv \alpha^{b(p-1-a)} \alpha^{ab} m \equiv \alpha^{ab-ab} m \equiv m \mod p.$$

□

Let us consider the same example again.

Example 8.12. *Alice chooses* $p = 11, \alpha = 2$ *and* $a = 4$, *and computes* $A \equiv 2^4 \equiv 5 \mod 11$. *The public key is* $P = (11, 2, 5)$ *and the secret key is* $S = 4$.

Bob chooses $b = 8$ *and computes* $B \equiv 2^8 \equiv 3 \mod 11$. *For a message* $m = 6$, *Bob computes* $c \equiv A^b m \equiv 5^8 \cdot 6 \equiv 4 \cdot 6 \equiv 2 \mod 11$ *and sends* $(2, 3)$ *to Alice.*

Alice can decrypt as

$$B^{p-1-a} c \equiv 3^6 \cdot 2 \equiv 3 \cdot 2 \equiv 6 \equiv m \mod 11.$$

Unfortunately, there are several problems with the ElGamal cryptosystem:

- Given two ciphertexts, one can construct a new ciphertext: let (c, B) be the ciphertext for m and (c', B') be the ciphertext of m'. Then $(cc', BB') = (A^{b+b'}, A^{b+b'} mm')$ is a ciphertext for mm'.

- Given a ciphertext of a message m, one can construct several ciphertexts for the same message m: Let (c, B) be the ciphertext of m and choose b'. Then, $(cA^{b'} = A^{b+b'} m, B\alpha^{b'} = \alpha^{b+b'})$ is again a ciphertext of m.

- In fact, the secret b is ephemeral, meaning that for each encryption of a new message we have to choose a new b. Else, Eve would see $c = A^b m, c' = A^b m'$ and can recover m/m'.

ElGamal Signature Scheme Finally, we can also turn the idea to a signature scheme (which is was later adapted to the DSA signature scheme).

1. Key generation: the signer chooses $p \in \mathcal{P}, \alpha \in \mathbb{Z}/p\mathbb{Z}$ of order $p - 1$ and computes $A \equiv \alpha^a \mod p$. The secret key is given by $S = a$ and the public key is $P = (p, \alpha, A)$.

2. Signing: given a message m, the signer can compute $b \in \{2, \ldots, p-2\}$ with $\gcd(b, p-1) = 1$ and computes $B \equiv \alpha^b \mod p$ and $s = (m - aB)b^{-1} \mod p - 1$. The signature is given by (B, s).

3. Verification: the verifier can check that

$$\alpha^m \equiv A^B B^s \mod p.$$

Why does this work?

Proposition 8.13. *The ElGamal signature scheme is correct, that is a verifier accepts an honest signer.*

Proof. We note that $m \equiv aB + sb \mod p - 1$, thus

$$\alpha^m \equiv \alpha^{aB+sb} \equiv (\alpha^a)^B \left(\alpha^b\right)^s \equiv A^B B^s \mod p.$$

□

Example 8.14. *The signer chooses* $p = 11, \alpha = 2$ *and* $a = 4$, *and computes* $A \equiv 2^4 \equiv 5 \mod 11$. *The public key is* $P = (11, 2, 5)$ *and the secret key is* $S = 4$. *The signer chooses* $b = 3$ *and computes* $B \equiv 2^3 \equiv 8 \mod 11$. *For a message* $m = 6$*, the signer computes* $s \equiv (m - aB)b^{-1} \equiv (6 - 4 \cdot 8)3^{-1} \equiv 8 \mod 10$ *and sends* $m = 6$ *and the signature* $(8, 8)$ *to the verifier.*

The verifier can check that

$$\alpha^m \equiv 2^6 \equiv 9 \equiv A^B B^s \equiv 5^8 8^8 \equiv 4 \cdot 5 \equiv 9 \mod 11.$$

Actually, the version of RSA we have presented here is the original proposal, but is not the one that is used. For this we first need to introduce the *Carmichael totient function* and need to make a quick excursion to the group of units in $\mathbb{Z}/n\mathbb{Z}$.

8.6 Excursion to Group of Units

Recall that we wanted to find an exponent $e(n)$ such that

$$a^{e(n)} \equiv 1 \mod n.$$

We have seen that $\varphi(n)$ is a simple solution, however, it is not necessarily the smallest one.

For this, we need to ask: how does the group of units $\mathbb{Z}/n\mathbb{Z}^\times$ look like?

Clearly, it is an abelian group, but is it *cyclic*, i.e., generated by a single element?

Example 8.15. $\mathbb{Z}/5\mathbb{Z}^\times = \{1, 2, 3, 4\}$ *is cyclic as* $2^0 \equiv 1, 2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 3 \mod 5$.

As it often happens, the prime factor $2 \mid n$ will play a special role. In fact, while $\mathbb{Z}/p^e\mathbb{Z}^\times$ is cyclic for odd p, any $\mathbb{Z}/2^e\mathbb{Z}^\times$ with $e \geq 3$ is not.

Definition 8.16. If $\mathbb{Z}/n\mathbb{Z}^\times$ is cyclic, then any generator g is called a *primitive root* modulo n.

In particular, a primitive root modulo n has order $\varphi(n)$, thus, for n with cyclic $\mathbb{Z}/n\mathbb{Z}^\times$, the exponent $\varphi(n)$ is the smallest one.

The question now becomes: when is $\mathbb{Z}/n\mathbb{Z}^\times$ cyclic?

Theorem 8.17. *Let* $p \in \mathcal{P}$ *and* $d \mid (p - 1)$. *Then, there exist* $\varphi(d)$ *elements in* $\mathbb{Z}/p\mathbb{Z}$ *of order* d.

Proof. For each $d \mid (p - 1)$, define $S_d = \{a \in \mathbb{Z}/p\mathbb{Z}^\times \mid \text{ord}(a) = d\}$ of size $s(d)$. We want to prove $s(d) = \varphi(d)$.

First, we show that $s(d) \leq \varphi(d)$: This is trivial if $s(d) = 0$. Otherwise, there exists some $a \in S_d$. Then, by definition of the order of a, the elements $a^1, a^2, ..., a^d$ are all distinct and satisfy $(a^i)^d = (a^d)^i = 1^i = 1$. Hence, they are all distinct roots of $f(x) = x^d - 1$ over $\mathbb{Z}/p\mathbb{Z}$. Since d is also the degree of f, there cannot be any other roots. Thus, we have shown $S_d \subseteq \{a^1, a^2, ..., a^d\}$.

Still fixing some $a \in S_d$, we now show that any element $b \in S_d$ is of the form a^i for some $i \in \{1, ..., d\}$ with $\gcd(i, d) = 1$. Since $S_d \subseteq \{a^1, a^2, ..., a^d\}$, only $\gcd(i, d)$ remains to be shown. Let $j = \gcd(i, d)$; then

$$b^{d/j} = a^{id/j} = \left(a^d\right)^{i/j} = 1 \in \mathbb{Z}/p\mathbb{Z}.$$

Since $\operatorname{ord}(b) = d$, we get that $d = \operatorname{ord}(b) \mid (d/j)$, hence $j = 1$.

In summary, this proves $s(d) \leq \varphi(d)$.

Now, by Lagrange's Theorem, we know that $\operatorname{ord}(a) \mid (p-1)$ for all $a \in \mathbb{Z}/p\mathbb{Z}^\times$, thus the sets S_d partition $\mathbb{Z}/p\mathbb{Z}^\times$ and

$$\sum_{d\in\mathbb{N}\colon\, d\mid(p-1)} s(d) = p - 1.$$

On the other hand, from the Gauss Theorem (Theorem 7.7), we get

$$\sum_{d\in\mathbb{N}\colon\, d\mid(p-1)} \varphi(d) = p - 1,$$

hence

$$\sum_{d\in\mathbb{N}\colon\, d\mid(p-1)} (\varphi(d) - s(d)) = 0.$$

Thus, since we've shown that every summand is nonnegative, if $s(d) < \varphi(d)$ for any $d \mid (p-1)$, then this sum would have to be strictly positive. Therefore $s(d) = \varphi(d)$ for all summands. □

We can immediately deduce (setting $d = p - 1$) that $\mathbb{Z}/p\mathbb{Z}^\times$ is cyclic.

Corollary 8.18. *If $p \in \mathcal{P}$, then $\mathbb{Z}/p\mathbb{Z}^\times$ is cyclic.*

Theorem 8.19. *Let $p \in \mathcal{P}$ be odd and let e be a positive integer. Then, $\mathbb{Z}/p^e\mathbb{Z}^\times$ is cyclic.*

Proof. We already know this for $e = 1$ from Corollary 8.18. The proof for $e \geq 2$ uses induction. Base case ($e = 2$): Since $\mathbb{Z}/p\mathbb{Z}$ is cyclic, there exists an integer $g \in \mathbb{Z}$, not divisible by p, such that g has order $\varphi(p) = p - 1$ modulo p. By Lagrange's Theorem, the order $\operatorname{ord}(g)$ of g modulo p^2 is a divisor of $\varphi(p^2) = p(p-1)$. On the other hand, since $g^k \equiv 1 \mod p^2$ implies $g^k \equiv 1 \mod p$, we have $p - 1 = \varphi(p) \mid \operatorname{ord}(g)$, hence there are only the two possibilities $\operatorname{ord}(g) = p - 1$ and $\operatorname{ord}(g) = p(p-1)$. In the latter case, g is a primitive root modulo p^2, so we are done; hence, assume $\operatorname{ord}(g) = p - 1$. Let $h := g + p$. Since $h \equiv g \mod p$, the order $\operatorname{ord}(h)$ of h modulo p^2 again satisfies $(p-1) \mid \operatorname{ord}(h) \mid p(p-1)$. With the Binomial Theorem we get

$$\begin{aligned}
h^{p-1} &= (g+p)^{p-1} \\
&= \sum_{i=0}^{p-1} \binom{p-1}{i} g^{p-1-i} p^i \\
&\equiv \binom{p-1}{0} g^{p-1-0} + \binom{p-1}{1} g^{p-1-1} p \mod p^2 \\
&= g^{p-1} + (p-1) g^{p-2} p \\
&= g^{p-1} + g^{p-2} p^2 - g^{p-2} p \\
&\equiv 1 - g^{p-2} p \mod p^2 .
\end{aligned}$$

Since $p \nmid g$, we have $g^{p-2}p \not\equiv 0 \mod p^2$ and thus $\mathrm{ord}(h) \neq p-1$, which means that only $\mathrm{ord}(h) = p(p-1)$ is possible. But then h is a primitive root modulo p^2.

Induction step ($(e-1, e) \to e+1$): Suppose $\mathbb{Z}/p^e\mathbb{Z}$ is cyclic. Hence, there exists an integer $g \in \mathbb{Z}$ such that $\gcd(g, p^e) = 1$, so that g is a unit in $\mathbb{Z}/p^e\mathbb{Z}$, and such that the order of g modulo p^{e+1} is equal to $n := \varphi(p^e) = p^{e-1}(p-1)$. From $\gcd(g, p^e) = 1$ it directly follows that $\gcd(g, p^{e+1}) = 1$, hence g is also a unit in $\mathbb{Z}/p^{e+1}\mathbb{Z}$.

Using Lagrange's Theorem as before, the order $\mathrm{ord}(g)$ of g modulo p^{e+1} must be a divisor of $\varphi(p^{e+1}) = np$. On the other hand, since $g^k \equiv 1 \mod p^{e+1}$ implies $g^k \equiv 1 \mod p^e$ and the order of g modulo p^e is $\varphi(p^e) = n$, we have $n \mid \mathrm{ord}(g)$. So the only two possibilities are $\mathrm{ord}(g) = n$ and $\mathrm{ord}(g) = np$. In the latter case, g is a primitive root modulo p^{e+1}, so we are done. Thus, suppose now that $\mathrm{ord}(g) = n$.

Since g has order n modulo p^e, we have $g^{n/p} \not\equiv 1 \mod p^e$. However, since $n/p = \varphi(p^{e-1})$, Euler's Theorem implies $g^{n/p} \equiv 1 \mod p^{e-1}$. Combining these two, there exists some integer k, not divisible by p, such that $g^{n/p} = 1 + kp^{e-1}$.

Using the Binomial Theorem we get

$$g^n = (1 + kp^{e-1})^p = \sum_{i=0}^{p} \binom{p}{i} (kp^{e-1})^i.$$

Since $e \geq 2$ and thus $p^{i(e-1)} \equiv 0 \mod p^{e+1}$ unless $i \in \{0, 1, 2\}$, we are left with

$$g^n \equiv 1 + p \cdot kp^{e-1} + \tfrac{p(p-1)}{2} \cdot k^2 p^{2e-2} \mod p^{e+1}.$$

Since $e \geq 2$ and p is odd, we have $\frac{p(p-1)}{2} \cdot p^{2e-2} \equiv 0 \mod p^{e+1}$. Hence,

$$g^n \equiv 1 + kp^e \not\equiv 1 \mod p^{e+1},$$

since p does not divide k. □

Note that we really required p to be odd, else $\frac{p(p-1)}{2} \cdot p^{2e-1} \equiv 2^{2e-2} \not\equiv 0 \mod 2^{e+1}$, for $e = 2$. Thus, we need to pay special attention to the case $p = 2$:

Theorem 8.20. *Let e be a positive integer. Then, $\mathbb{Z}/2^e\mathbb{Z}$ is cyclic if and only if $e \leq 2$.*

Proof. One can easily check that $\mathbb{Z}/2\mathbb{Z}^\times$ and $\mathbb{Z}/4\mathbb{Z}^\times$ are cyclic.

We show that for $e \geq 3$ the group $\mathbb{Z}/2^e\mathbb{Z}^\times$ has no elements of order $\varphi(2^e) = 2^{e-1}$ by proving

$$a^{2^{e-2}} \equiv 1 \mod 2^e$$

for all integers a with $2 \nmid a$. We again use induction on e.

Base case ($e = 3$): We prove that $a^2 \equiv 1 \mod 8$ for all odd a: Writing $a = 2b + 1$, we get

$$a^2 = 4b^2 + 4b + 1 = 4b(b+1) + 1 \equiv 1 \mod 8.$$

Induction step ($e \to e{+}1$): Let us assume

$$a^{2^{e-2}} \equiv 1 \mod 2^e,$$

for all odd a. Thus, there exists an integer k such that $a^{2^{e-2}} = 1 + 2^e k$. But then

$$a^{2^{(e+1)-2}} = (1 + 2^e k)^2 = 1 + 2^{e+1}k + 2^{2e}k^2 = 1 + 2^{e+1}(k + 2^{e-1}k^2) \equiv 1 \mod 2^{e+1}.$$

□

Within this proof we have also showed that

Corollary 8.21. *Let a be an odd integer and $e \geq 3$. Then,*

$$a^{\varphi(2^e)/2} \equiv 1 \mod 2^e.$$

Lemma 8.22. *Let r, s be two positive coprime integers $r, s \geq 3$. Then, $\mathbb{Z}/rs\mathbb{Z}^\times$ is not cyclic.*

Proof. Since $\gcd(r, s) = 1$, we get from Corollary 7.26 that $\varphi(rs) = \varphi(r)\varphi(s)$ and that $\varphi(r), \varphi(s)$ are both even (see Exercise 4.29).

Thus, $4 \mid \varphi(rs)$. Let $k = \varphi(rs)/2$, which is a multiple of both $\varphi(r)$ and $\varphi(s)$.

Let $a \in \mathbb{Z}$ be coprime to rs. Then $\gcd(a, r) = 1$ and $\gcd(a, s) = 1$, hence Euler's Theorem implies $a^{\varphi(r)} \equiv 1 \mod r$ and $a^{\varphi(s)} \equiv 1 \mod s$.

Now, since $\varphi(r), \varphi(s)$ both divide k, we also have $a^k \equiv 1 \mod r$ and $a^k \equiv 1 \mod s$ and therefore $a^k \equiv 1 \mod rs$ via the Chinese Remainder Theorem.

Thus, every element of $\mathbb{Z}/rs\mathbb{Z}^\times$ has order dividing $k < \varphi(rs)$ and there is no primitive root. □

Putting all these results together, we get the following theorem:

Theorem 8.23. *Let n be a positive integer. The group $\mathbb{Z}/n\mathbb{Z}^\times$ is cyclic if and only if n is of the form 1, 2, 4, p^e, or $2p^e$, where p is an odd prime and e is a positive integer.*

Proof. "$\Leftarrow$": The cases $n = 1, 2, 4$ are easily checked and Theorem 8.19 deals with $n = p^e$. For $n = 2p^e$, Corollary 7.26 gives $\varphi(n) = \varphi(2)\varphi(p^e) = \varphi(p^e)$. By Theorem 8.19, there exists a primitive root g modulo p^e. Then $g + p^e$ is also a primitive root modulo p^e. Since either g or $g + p^e$ is odd, one of these integers must be a primitive root h modulo p^e:

- Since h is coprime to 2 and p^e, it is a unit modulo $2p^e$.
- If $h^k \equiv 1 \mod 2p^e$, then $h^k \equiv 1 \mod p^e$ and thus $\varphi(p^e) \mid k$. But note $\varphi(2p^e) = \varphi(p^e)$. Moreover, from Lagrange's theorem the order of h modulo $2p^e$ satisfies $\operatorname{ord}(h) \mid \varphi(2p^e)$; hence, $\operatorname{ord}(h) = \varphi(2p^e)$ and it is thus a primitive root.

"⇒": For the "only if" part, we note that every $n \notin \{1, 2, 4, p^e, 2p^e\}$ falls into (at least) one of the following cases:

- $n = 2^e$ with $e \geq 3$. Here we know $\mathbb{Z}/n\mathbb{Z}^\times$ is not cyclic by Theorem 8.20.
- $n = 2^e p^f$ with $e \geq 2, f \geq 1$ and p an odd prime. This we can exclude using Lemma 8.22 and $r = 2^e, s = p^f$.
- $n = p^e q^f ms$ with p, q distinct odd primes and $p, q \nmid m$. This we can exclude using Lemma 8.22 with p^e dividing n and $s = q^f m$.

□

Recall that the Chinese Remainder Theorem gives a ring isomorphism

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{e_1} \times \cdots \times \mathbb{Z}/p_k^{e_k},$$

for n with prime factorization $n = \prod_{i=1}^k p_i^{e_i}$. This ring isomorphism yields the group isomorphism

$$\mathbb{Z}/n\mathbb{Z}^\times \cong \mathbb{Z}/p_1^{e_1}\mathbb{Z}^\times \times \cdots \times \mathbb{Z}/p_k^{e_k}\mathbb{Z}^\times.$$

Thus, we get a complete description of the group of units of any $\mathbb{Z}/n\mathbb{Z}$.

8.7 Carmichael Totient Function

In the previous section, we have seen that $\varphi(n)$ is not always the smallest exponent $e(n)$ for which

$$a^{e(n)} \equiv 1 \mod n \tag{4}$$

holds for all a coprime to n.

Thus, with the structure of $\mathbb{Z}/n\mathbb{Z}^\times$ in mind, we ask again: what *is* the smallest exponent $e(n)$?

Definition 8.24. Let n be a positive integer. The *Carmichael totient function* $\lambda(n)$ is defined as the smallest positive integer m such that

$$a^m \equiv 1 \mod n$$

holds for any a coprime to n.

How is this different from the Euler totient function? Let us consider an example.

Example. Let $n = 15 = 3 \cdot 5$. The Euler totient function is then $\varphi(15) = (3-1)(5-1) = 8$. However, we can show that for any integer a with $\gcd(a, 15) = 1$, we have

$$a^4 \equiv 1 \mod 15.$$

Lemma 8.25. *Let $e \geq 3$ be an integer. Then every $a \in \mathbb{Z}/2^e\mathbb{Z}^\times$ can be written in a unique way as $(-1)^i \cdot 5^j$ with $i \in \{0, 1\}$ and $j \in \{0, ..., 2^{e-2} - 1\}$.*

Proof. We first show that 5 has order 2^{e-2}: This is done by induction. The base cases $e=3$ and $e=4$ can be verified by inspection. For the induction step $(e-1,e) \to e+1$, suppose 5 has order 2^{e-2} modulo 2^e and order 2^{e-3} modulo 2^{e-1}. Thus $5^{2^{e-3}} = 1 + 2^{e-1}k$ for some odd $k \in \mathbb{Z}$. Hence

$$5^{2^{e-2}} = (1+2^{e-1}k)^2 = 1 + 2^e k + 2^{2e-2}k^2 \equiv 1 + 2^e k \pmod{2^{e+1}}.$$

Therefore 5 has order 2^{e-1} modulo 2^{e+1}, as claimed.

Finally, note that powers of 5 only cover the two residue classes 5 and $5^2 = 25 \equiv 1$ modulo 8. Negation defines a bijection to the residue classes $-5 \equiv 3$ and $-1 \equiv 7$ modulo 8. □

Theorem 8.26. *Let n be a positive integer with prime factorization $n = \prod_{i=1}^{k} p_i^{e_i}$. Then*

$$\lambda(n) = \begin{cases} \varphi(n) & \textit{if } n = 1,2,4,p^e \textit{ for } p \in \mathcal{P} \textit{ odd}, \\ \varphi(n)/2 & \textit{if } n = 2^e, e \geq 3, \\ \operatorname{lcm}(\lambda(p_1^{e_1}),\ldots,\lambda(p_k^{e_k})) & \textit{else.} \end{cases}$$

Proof. The proof follows from the excursion to the group of units: If $n = 1,2,4$ or an odd prime power, then Theorem 8.19 tells us that $\mathbb{Z}/n\mathbb{Z}^\times$ is cyclic and has a primitive root g, i.e., an element of order $\varphi(n)$. Thus, $\varphi(n)$ is the smallest exponent of Equation (4).

For the special case $n = 2^e$ and $e \geq 3$, Theorem 8.20 tells us that there actually exists a smaller exponent $\varphi(n)/2$. Indeed, by Lemma 8.25, we know that this is the smallest possible choice.

Finally, the Chinese Remainder Theorem tells us how to deal with a product of different primes: If $\lambda_i = \lambda(p_i^{e_i})$ is the smallest exponent to get

$$a^{\lambda_i} \equiv 1 \mod p_i^{e_i},$$

then also $a^{k\lambda_i} \equiv 1 \mod p_i^{e_i}$ for any positive integer k. Since we want an exponent that works modulo all prime powers $p_i^{e_i}$, we are looking for the least common multiple of all the λ_i. □

Exercise 8.27. *Let n be a positive integer. Then, $\lambda(n) \mid \varphi(n)$.*

Exercise 8.28. *Let a, b be two positive integers with $a \mid b$. Show that $\lambda(a) \mid \lambda(b)$.*

8.8 Revisiting RSA

Instead of using the Euler totient function for RSA, in practice one uses the Carmichael totient function.

1. Key Generation: Alice chooses two distinct primes p, q and computes $n = pq$ and $\lambda(n) = \operatorname{lcm}(p-1, q-1)$. She chooses a positive integer $e < \lambda(n)$, which is coprime to $\lambda(n)$. The public key is $P = (n, e)$ and the secret key is $S = (p, q)$.

2. Encryption: Bob chooses a message m and encrypts it by computing

$$c = m^e \mod n.$$

3. Decryption: Alice can decrypt the ciphertext by first computing d and b such that

$$de + b\lambda(n) = 1.$$

She can then recover the message as $c^d \equiv m \mod n$.

Note that any d which satisfied

$$d \cdot e \equiv 1 \mod \varphi(n)$$

also satisfies

$$d \cdot e \equiv 1 \mod \lambda(n).$$

Hence, the new decryption exponent d satisfies a weaker but sufficient condition.

However, $\lambda(n) = \text{lcm}(p-1, q-1)$ is much smaller than $\varphi(n) = (p-1)(q-1)$ and will thus lead to smaller decryption exponents, making the scheme ultimately more efficient.

Exercise 8.29. *Give an example of how RSA works using λ and $p = 3, q = 5$.*

9 Quatdratic Residues

In this chapter we consider the general question, whether an integer a has a square root modulo n and if so, how many and how to find them. We will later see applications of such squares in primality tests.

How many elements in $\mathbb{Z}/n\mathbb{Z}$ are squares? We could simply go through all $x \in \{0, \dots, n-1\}$ and collect all x^2. Clearly, we can do better, as $x^2 \equiv (n - x^2) \mod n$, i.e., we only need to go through all $x \in \{0, \dots, \lceil \frac{n-1}{2} \rceil\}$, but even in this case we can still have two distinct x, y with $x^2 \equiv y^2 \mod n$.

Example 9.1. *In $\mathbb{Z}/2\mathbb{Z}$ all elements are squares, as $0^2 \equiv 0 \mod 2$ and $1^2 \equiv 1 \mod 2$.*
The case $\mathbb{Z}/3\mathbb{Z}$ is already more interesting, as 2 is not a square.

Clearly, 0 is always a square. Even more, we are mostly interested in the squares of the group of units $\mathbb{Z}/n\mathbb{Z}^\times$.

Definition 9.2. Let $a \in \mathbb{Z}/n\mathbb{Z}^\times$. We say that a is a *quadratic residue* modulo n if the congruence $x^2 \equiv a \mod n$ has solutions, i.e., there exists a $s \in \mathbb{Z}/n\mathbb{Z}^\times$ such that $s^2 \equiv a \mod n$. If the congruence has no solutions, we call a a *quadratic non-residue* modulo n.

The set of all quadratic residues is denoted by Q_n, i.e.,

$$Q_n = \{s^2 \in \mathbb{Z}/n\mathbb{Z}^\times \mid s \in \mathbb{Z}/n\mathbb{Z}^\times\}.$$

Example 9.3. $Q_7 = \{1, 2, 4\}$, *while* $Q_6 = \{1\}$ *and* $Q_8 = \{1\}$.

How many s are there to write $a \equiv s^2 \mod n$?

Lemma 9.4. *Let n be a positive integer with prime factorization $n = \prod_{i=1}^k p_i^{e_i}$. Then, $a \in Q_n$ has*

$$N = \begin{cases} 2^{k+1} & \text{if } n \equiv 0 \mod 8, \\ 2^{k-1} & \text{if } n \equiv 2 \mod 4, \\ 2^k & \text{else} \end{cases}$$

many square roots.

Proof. If $a \in Q_n$, then there exists $s \in \mathbb{Z}/n\mathbb{Z}^\times$ with $s^2 \equiv a \mod n$. Any element $t \in \mathbb{Z}/n\mathbb{Z}^\times$ has the form $t = sx$ (indeed take $x = ts^{-1}$), for some unique $x \in \mathbb{Z}/n\mathbb{Z}^\times$.

We thus have $t^2 \equiv s^2x^2 \equiv a \mod n$ if and only if $x^2 \equiv 1 \mod n$. Thus, N is the number of solutions of $x^2 \equiv 1 \mod n$ for $x \in \mathbb{Z}/n\mathbb{Z}^\times$.

We count these by first considering different solutions modulo p^e, where $p \in \mathcal{P}$ and e is a positive integer.

If p is an odd prime, then $x^2 \equiv 1 \mod p^e$ implies $p^e \mid (x^2 - 1) = (x-1)(x+1)$. Thus, $p^e \mid (x-1)$ or $p^e \mid (x+1)$ and we only have two solutions $x \equiv \pm 1 \mod p^e$.

If $p^e = 2$ we only have one solution $x \equiv 1 \mod n$ and if $p^e = 4$, then we have the two solutions $x \equiv \pm 1 \mod 4$.

For $p^e = 2^e$, with $e \geq 3$, a similar argument shows that there are four solutions: $x \equiv \pm 1 \mod 2^e$ and $x \equiv 2^{e-1} \pm 1 \mod 2^e$, which are distinct from $\pm 1 \mod 2^e$.

In fact, for any solution x, we get $2^e \mid (x-1)(x+1)$ and either $x - 1 \equiv 2 \mod 4$ and $x+1 \equiv 0 \mod 2^{e-1}$ or vice versa.

For $n = \prod_{i=1}^k p_i^{e_i}$ we can apply the Chinese Remainder Theorem and for each p_i odd, we get two solutions, while for $p_i = 2$, we either get $1, 2$ or 4 solutions depending on e_i. □

There are several properties that we can state for general Q_n. For this we will first introduce the index.

Definition 9.5. Let n be a positive integer, such that there exists a primitive root α modulo n, that is $\text{ord}(\alpha) = \varphi(n)$. Then any $b \in \mathbb{Z}/n\mathbb{Z}^\times$ can be written as $b = \alpha^k$ for a unique $k \in \{0, \dots, \varphi(n)-1\}$. We say k is the *index* of b to the base α modulo n, (or also discrete logarithm) and write $\text{ind}_\alpha(b) = k$.

Recall from Theorem 8.23, that this implies $n \in \{2, 4, p^e, 2p^e\}$.

Example 9.6. *Let us consider $p = 7, \alpha = 3$. Then,*

$$\textit{ind}_3(1) = 0, \textit{ind}_3(2) = 2, \textit{ind}_3(3) = 1, \textit{ind}_3(4) = 4, \textit{ind}_3(5) = 5, \textit{ind}_3(6) = 3.$$

We note that ind_α introduces a function similar to the logarithm, where

$$\begin{aligned} \text{ind}_\alpha : \mathbb{Z}/n\mathbb{Z}^\times &\to \mathbb{Z}/\varphi(n)\mathbb{Z}, \\ \alpha^i &\mapsto i. \end{aligned}$$

We also have similar properties to the logarithm function:

Proposition 9.7. *Let n be a positive integer, such that there exists a primitive root α modulo n. If $a, b \in \mathbb{Z}/n\mathbb{Z}^\times$, then*

- *$\textit{ind}_\alpha(1) \equiv 0 \mod \varphi(n)$,*
- *$\textit{ind}_\alpha(ab) \equiv \textit{ind}_\alpha(a) + \textit{ind}_\alpha(b) \mod \varphi(n)$,*
- *$\textit{ind}_\alpha(a^k) \equiv k \cdot \textit{ind}_\alpha(a) \mod \varphi(n)$.*

Proof.

- From Euler's Theorem, we know that $\alpha^{\varphi(n)} \equiv 1 \mod n$. Since α is a primitive root modulo n, there is no smaller positive integer r such that $\alpha^r \equiv 1 \mod n$. Thus, $\text{ind}_\alpha(1) \equiv \varphi(n) \equiv 0 \mod \varphi(n)$.
- We note that by the definition of index, $ab \equiv \alpha^{\text{ind}_\alpha(a)}\alpha^{\text{ind}_\alpha(b)} \equiv \alpha^{\text{ind}_\alpha(a)+\text{ind}_\alpha(b)} \mod n$. Thus, $\alpha^{\text{ind}_\alpha(ab)} \equiv \alpha^{\text{ind}_\alpha(a)+\text{ind}_\alpha(b)} \mod n$ and since α has order $\varphi(n)$, we get $\text{ind}_\alpha(ab) \equiv \text{ind}_\alpha(a) + \text{ind}_\alpha(b) \mod \varphi(n)$. In fact, for any positive integers $\ell \leq k$ with $\alpha^\ell \equiv \alpha^k \mod n$, we also get $\alpha^{k-\ell} \equiv 1 \mod n$, thus $\varphi(n) \mid (k - \ell)$.

- By definition, we have that

$$\alpha^{\mathrm{ind}_\alpha(a^k)} \equiv a^k \equiv \left(\alpha^{\mathrm{ind}_\alpha(a)}\right)^k \equiv \alpha^{k\mathrm{ind}_\alpha(a)} \mod n,$$

and we can again follow that $\mathrm{ind}_\alpha(a^k) \equiv k\mathrm{ind}_\alpha(a) \mod \varphi(n)$.

□

Example 9.8. *Let* $p = 7, \alpha = 3$ *then* $5^2 \equiv 4 \mod 7$ *and*

$$ind_3(5^2) \equiv ind_3(4) \equiv 4 \equiv 2 \cdot ind_3(5) \equiv 2 \cdot 5 \mod 6.$$

9.1 Group of Quadratic Residues

Lemma 9.9. *Let* $n > 2$ *be a positive integer, such that there exists a primitive root* α *modulo* n *and* $a \in \mathbb{Z}/n\mathbb{Z}^\times$. *Then* a *is a quadratic residue modulo* n *if and only if* $ind_\alpha(a)$ *is even.*

Proof. For the first direction, we assume that $\mathrm{ind}_\alpha(a) = 2k$, for some positive integer k. That means $\alpha^{2k} \equiv a \mod n$ and hence $\left(\alpha^k\right)^2 \equiv a \mod n$, i.e., α^k is a square root of a modulo n.

For the other direction, suppose that a is a quadratic residue modulo n, thus there exists some $b \in \mathbb{Z}/n\mathbb{Z}^\times$ with $b^2 \equiv a \mod n$, thus $\mathrm{ind}_\alpha(b^2) \equiv \mathrm{ind}_\alpha(a) \mod \varphi(n)$ and due to Proposition 9.7, we also have $\mathrm{ind}_\alpha(b^2) \equiv 2\mathrm{ind}_\alpha(b) \equiv \mathrm{ind}_\alpha(a) \mod \varphi(n)$. □

Thus

$$|Q_n| = |\{a \in \mathbb{Z}/n\mathbb{Z}^\times \mid \mathrm{ind}_\alpha(a) \text{ is even }\}| = |\{\alpha^{2k} \mid k \in \{1, \dots, \varphi(n)/2\}\}| = \frac{\varphi(n)}{2}.$$

Theorem 9.10. *Let* $n > 2$ *be a positive integer such that there exists a primitive root* α *modulo* n. *Then,* Q_n *is a cyclic subgroup of* $\mathbb{Z}/n\mathbb{Z}^\times$ *of order* $\varphi(n)/2$, *generated by* α^2.

Proof. In Lemma 9.9, we have seen that $Q_n = \{\alpha^{2k} \mid k \in \{1, \dots, \varphi(n)/2\}\}$, thus we only have to show that Q_n contains the neutral element, is closed under the product and inverses. Clearly $1 \in Q_n$ since $1^2 \equiv 1 \mod n$. If $a, b \in Q_n$, then there exist $s, t \in \mathbb{Z}/n\mathbb{Z}^\times$ with $a \equiv s^2 \mod n$ and $b \equiv t^2 \mod n$. Thus $ab \equiv (st)^2 \mod n$ is also in Q_n as $st \in \mathbb{Z}/n\mathbb{Z}^\times$. Similarly, for $a^{-1} \equiv (s^{-1})^2 \mod n$, and since $s^{-1} \in \mathbb{Z}/n\mathbb{Z}^\times$, also $a^{-1} \in Q_n$. □

Example 9.11. *Let* $p = 7, \alpha = 3$, *then* $Q_7 = \{1, 2, 4\} = \{3^0, 3^2, 3^4\}$.

Next, we want to determine whether a given a is a quadratic residue or not.

For this, we will mostly focus on prime moduli, as we can always reduce quadratic residues in $\mathbb{Z}/p^e\mathbb{Z}$ to the case $\mathbb{Z}/p\mathbb{Z}$.

Theorem 9.12. *Let* $p \in \mathcal{P}$ *be odd and* $e \geq 1$ *be a positive integer. Then,* $a \in Q_{p^e}$ *if and only if* $a \in Q_p$.

Proof. Let us start with the first direction: if $a \in Q_{p^e}$, then there exists $s \in \mathbb{Z}/p^e\mathbb{Z}^\times$ (that is $\gcd(p,s) = 1$) such that $s^2 \equiv a \mod p^e$. Thus, $s^2 = a + kp^e$, for some $k \in \mathbb{Z}$ and hence $s^2 \equiv a \mod p$. Since s is coprime to p, $s \in \mathbb{Z}/p\mathbb{Z}^\times$ and thus $a \in Q_p$.

For the other direction, we assume that $a \in Q_p$. That is: there exists $s \in \mathbb{Z}/p\mathbb{Z}^\times$, with $s^2 \equiv a \mod p$.

We will lift this equation step by step to $\mathbb{Z}/p^e\mathbb{Z}$.

In each step we do the following: let $s \in \mathbb{Z}/p^{k-1}\mathbb{Z}^\times$ (thus $\gcd(p,s) = 1$) with $s^2 \equiv a \mod p^{k-1}$. We can hence write $s^2 = a + \ell p^{k-1}$, for some $\ell \in \mathbb{Z}$. Since p is odd, we now it is coprime to 2, and thus also $2s \in \mathbb{Z}/p^{k-1}\mathbb{Z}^\times$. Let us define $t = s - \ell(2s)^{-1}p^{k-1}$, then

$$t^2 \equiv s^2 - 2s\ell(2s)^{-1}p^{k-1} + \ell^2(2s)^{-2}p^{2k-2} \equiv s^2 - \ell p^{k-1} \equiv a + \ell p^{k-1} - \ell p^{k-1} \equiv a \mod p^k.$$

Since

$$(s-\ell(2s)^{-1}p^{k-1})\cdot(s^{-1}+\ell(2s^3)^{-1}p^{k-1}) \equiv s\cdot s^{-1}+s\ell(2s^3)^{-1}p^{k-1}-s^{-1}\ell(2s)^{-1}p^{k-1} \equiv 1 \mod p^k,$$

we also get that $t \in \mathbb{Z}/p^k\mathbb{Z}^\times$, thus $a \in Q_{p^k}$.

□

As a next step we cover the case $p = 2$.

Exercise 9.13. *For all positive integers n, show that $2^{n+2} \mid (5^{2^n} - 1)$, and $2^{n+3} \nmid (5^{2^n} - 1)$.*

Theorem 9.14. *Let a be an odd integer. Then,*

- $a \in Q_2$,
- $a \in Q_4$ *if and only if* $a \equiv 1 \mod 4$,
- *for* $e \geq 3$, $a \in Q_{2^e}$ *if and only if* $a \equiv 1 \mod 8$.

Proof.

- Clearly, $Q_2 = \{1\} = \mathbb{Z}/2\mathbb{Z}^\times$ and
- $Q_4 = \{1\}$.
- For this we first show that

$$\mathbb{Z}/2^e\mathbb{Z}^\times = \{\pm 5^i \mid i \in \{0, \dots, 2^{e-2} - 1\}\}.$$

By Euler's Theorem, we have that $\operatorname{ord}(5) \mid \varphi(2^e) = 2^{e-1}$, thus $\operatorname{ord}(5) = 2^k$ for some $k \in \{0, \dots, e-1\}$. Theorem 8.20 implies that there are no elements of order $\varphi(2^e)$, thus $k \in \{0, \dots, e-2\}$.

From Exercise 9.13 using $n = e - 3$ we get that $2^{e-1} \mid (5^{2^{e-3}} - 1)$ but $2^e \nmid (5^{2^{e-3}} - 1)$, thus $5^{2^{e-3}} \not\equiv 1 \mod 2^e$ and hence $k > e - 3$. This leaves us with $k = e - 2$, i.e., $\operatorname{ord}(5) = 2^{e-2}$.

Thus, 5^i for $i \in \{0, \dots, 2^{e-2} - 1\}$ are all distinct and in $\mathbb{Z}/2^e\mathbb{Z}^\times$. Since $5 \equiv 1 \mod 4$, all $5^i \equiv 1 \mod 4$. Note that $\mathbb{Z}/2^e\mathbb{Z}^\times$, has half the elements being congruent to 1 modulo 4 and the other half being congruent to 3 modulo 4. Thus,

$$\mathbb{Z}/2^e\mathbb{Z}^\times = \{\pm 5^i \mid i \in \{0, \dots, 2^{e-2} - 1\}\}.$$

Now, squaring our elements $\pm 5^i \in \mathbb{Z}/2^e\mathbb{Z}^\times$, we get that

$$Q_{2^e} = \{5^{2i} \mid i \in \{0, \dots, 2^{e-3} - 1\}\}$$

and all elements a in Q_{2^e} are such that $a \equiv 5^{2i} \equiv 1 \mod 8$.

Note that a quarter of the elements in $\mathbb{Z}/2^e\mathbb{Z}^\times$ are congruent to 1 modulo 8. Since $Q_{2^e} \subset \mathbb{Z}/2^e\mathbb{Z}^\times$ is also a quarter of $\mathbb{Z}/2^e\mathbb{Z}^\times$, these sets must be equal.

□

The following result allows us to combine our characterizations of Q_{p^e}.

Theorem 9.15. *Let n be a positive integer with prime factorization $n = \prod_{i=1}^k p_i^{e_i}$. Then $a \in Q_n$ if and only if $a \in Q_{p_i^{e_i}}$ for all $i \in \{1, \dots, k\}$.*

Proof. If $a \in Q_n$, then there exists a $s \in \mathbb{Z}/n\mathbb{Z}^\times$ with $s^2 \equiv a \mod n$. Thus, $a \equiv s^2 \mod p_i^{e_i}$ for all $i \in \{1, \dots, k\}$ and hence $a \in Q_{p_i^{e_i}}$.

Conversely, if $a \in Q_{p_i^{e_i}}$ for all $i \in \{1, \dots, k\}$, then there exist elements $s_i \in \mathbb{Z}/p_i^{e_i}\mathbb{Z}^\times$ with $s_i^2 \equiv a \mod p_i^{e_i}$.

By the Chinese Remainder Theorem, there also exists $s \in \mathbb{Z}/n\mathbb{Z}^\times$ with $s \equiv s_i \mod p_i^{e_i}$ for all $i \in \{1, \dots, k\}$ and hence

$$s^2 \equiv s_i^2 \equiv a \mod p_i^{e_i}$$

for all $i \in \{1, \dots, k\}$ and hence $s^2 \equiv a \mod n$. □

This result can be expressed more algebraically, as

$$Q_n \cong Q_{p_1^{e_1}} \times \cdots \times Q_{p_k^{e_k}}.$$

We can now answer whether $a \in Q_n$:

Theorem 9.16. *Let n be a positive integer and $a \in \mathbb{Z}/n\mathbb{Z}^\times$. Then, $a \in Q_n$ if and only if*

- *$a \in Q_p$ for all odd prime $p \mid n$ and*
- *$a \equiv 1 \mod 4$, if $4 \mid n$ but $8 \nmid n$*
- *$a \equiv 1 \mod 8$, if $8 \mid n$.*

Proof. By Theorem 9.15, we have that $a \in Q_n$ if and only if $a \in Q_{p^e}$ for all p^e in the factorization of n. For odd primes p, this is equivalent to $a \in Q_p$, by Theorem 9.12. For $p = 2$ we get the conditions from Theorem 9.14. □

9.2 Quadratic Residues for Prime Moduli

We have covered the cases $n = 2^e$ and seen that $a \in Q_{p^e}$ if and only if $a \in Q_p$. Thus, we now consider Q_p, for $p \in \mathcal{P}$ odd.

This first lemma is a special case of Lemma 9.4.

Lemma 9.17. *Let $p \in \mathcal{P}$ be odd and a be a positive integer, not divisible by p. Then a has either two square roots in $\mathbb{Z}/p\mathbb{Z}^\times$ or none.*

Here two or no solutions refers to incongruent solutions of $x^2 \equiv a \mod p$.

Proof. If x is a square root of a modulo p, then $p-x$ is also a square root modulo p as $x^2 \equiv (p-x)^2 \mod p$. Additionally, the two square roots are distinct, as $x \equiv p - x \mod p$ would imply $2x \equiv 0 \mod p$ and as p is odd, this would imply $p \mid x$, which is not possible as $x^2 \equiv a \mod p$ but $p \nmid a$.

On the other hand, if x, y are both square roots of a modulo p, then $x^2-y^2 \equiv (x-y)(x+y) \equiv 0 \mod p$, and hence $p \mid (x + y)$ or $p \mid (x - y)$. This only leaves the two choices $x \equiv -y \mod p$ or $x \equiv y \mod p$. □

Example 9.18. *In $\mathbb{Z}/7\mathbb{Z}$, for $a = 4$, we have the solutions 2 and 5, while for $a = 3$, there are no solutions.*

For odd primes, we have the same amount of quadratic residues as quadratic non-residues.

Theorem 9.19. *Let $p \in \mathcal{P}$ be odd. Then, there exist $(p-1)/2$ quadratic residues modulo p and $(p-1)/2$ quadratic non-residues modulo p.*

Proof. By Lemma 9.17, we know that the function

$$f : \mathbb{Z}/p\mathbb{Z}^\times \to Q_p, \quad x \mapsto x^2$$

is a 2-to-1 function, thus $|Q_p| = \frac{p-1}{2}$.

□

We can give an alternative proof due to Theorem 9.19, as

$$|Q_p| = |\{a \in \mathbb{Z}/p\mathbb{Z}^\times \mid \text{ind}_\alpha(a) \text{ is even }\}| = |\{\alpha^{2k} \mid k \in \{1, \ldots, (p-1)/2\}\}| = \frac{p-1}{2}.$$

We have seen how many quadratic residues there are, but how can we determine whether a is a quadratic residue?

9.3 Legendre Symbol

The following notation will be of great help to determine whether a given element is a quadratic residue.

Definition 9.20. Let $p \in \mathcal{P}$ be odd and $a \in \mathbb{Z}/p\mathbb{Z}^{\times}$. The *Legendre symbol* is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \in Q_p \\ -1 & \text{else.} \end{cases}$$

Example 9.21. *Let* $p = 11$ *and* $\left(\frac{3}{11}\right) = 1$, *while* $\left(\frac{2}{11}\right) = -1$.

Exercise 9.22. *Let* $p \in \mathcal{P}$ *be odd and* α *a primitive root modulo* p. *Then*

$$\left(\frac{\alpha^i}{p}\right) = (-1)^i.$$

While Exercise 9.22 is a method to decide whether $a \equiv \alpha^i \mod p$ is a quadratic residue, it is not easy to find i such that $a \equiv \alpha^i \mod p$, indeed this is the discrete logarithm problem over finite fields. A better criterion is the following.

Theorem 9.23 (Euler's Criterion). *Let* $p \in \mathcal{P}$ *be odd. Then,*

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

Proof. Let us first assume that $\left(\frac{a}{p}\right) = 1$, that is $x^2 \equiv a \mod p$ has a solution, say s. Using Fermat's Little Theorem, we have that

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

Hence if $\left(\frac{a}{p}\right) = 1$, then $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$.

If $\left(\frac{a}{p}\right) = -1$, then $x^2 \equiv a \mod p$ has no solution. For every integer k with $\gcd(k, p) = 1$, there exists an integer ℓ such that $k\ell \equiv a \mod p$ (indeed take $\ell = ak^{-1}$). Since $x^2 \equiv a \mod p$ has no solution, we also know that $\ell \not\equiv k \mod p$. Thus, we can group the integers $1, \ldots, p-1$ into $(p-1)/2$ pairs, each with product a.

By multiplying all the pairs together, we get

$$(p-1)! \equiv a^{(p-1)/2} \mod p.$$

Due to Wilson's Theorem, we know that $(p-1)! \equiv -1 \mod p$, thus $a^{(p-1)/2} \equiv -1 \mod p$. □

Example 9.24. *In order to determine whether 2 is a quadratic residue modulo 11, we compute* $2^{(11-1)/2} \equiv 2^5 \equiv -1 \mod 11$. *Thus,* $2 \notin Q_{11}$. *On the other hand* $3^5 \equiv 1 \mod 11$ *and* $3 \in Q_{11}$.

Theorem 9.25. *Let $p \in \mathcal{P}$ be odd. Then, for all a, b positive integers,*

- *If $a \equiv b \mod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$*
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
- $\left(\frac{a^2}{p}\right) = 1.$

In particular, we have that the Legendre symbol is a completely multiplicative function.

Proof.

- If $a \equiv b \mod p$, then $x^2 \equiv a \mod p$ has a solution if and only if $x^2 \equiv b \mod p$ has a solution.
- By Euler's criterion, we have that
$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$$
and
$$\left(\frac{b}{p}\right) \equiv b^{(p-1)/2} \mod p.$$
Hence
$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{(p-1)/2}b^{(p-1)/2} \equiv (ab)^{(p-1)/2} \equiv \left(\frac{ab}{p}\right) \mod p.$$
While this holds modulo p, we want them to be equal also over $\mathbb{Z}$. This follows, as $\left(\frac{a}{p}\right)$ can only have the values ± 1.
- Since $\left(\frac{a}{p}\right) = \pm 1$, using
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$
we get that
$$\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = 1.$$

□

An interesting property follows from this theorem:

- The product of a quadratic residue with a quadratic residue is a quadratic residue.
- The product of a quadratic non-residue with a quadratic non-residue is a quadratic residue.
- The product of a quadratic residue with a quadratic non-residue is a quadratic non-residue.

Theorem 9.26. *Let $p \in \mathcal{P}$ be odd. Then, $-1 \in Q_p$ if and only if $p \equiv 1 \mod 4$.*

Equivalently,

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

Proof. By Euler's criterion, we know that

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

If $p \equiv 1 \mod 4$, that is $p = 4k + 1$, for some integer k, then

$$(-1)^{(p-1)/2} = (-1)^{2k} = 1$$

and $\left(\frac{-1}{p}\right) = 1$.

If $p \equiv 3 \mod 4$, then $p = 4k + 3$, for some integer k, then

$$(-1)^{(p-1)/2} = (-1)^{2k+1} = -1,$$

so that $\left(\frac{-1}{p}\right) = -1$. □

Example 9.27. *For $p = 5, 13$ we have that $-1 \in Q_5, Q_{13}$, however, $-1 \notin Q_7$ or in Q_3.*

A first application of quadratic residues is the proof that there are infinitely many primes $p \equiv 1 \mod 4$. Recall that in Theorem 3.28, we already showed that there are infinitely many primes $p \equiv 3 \mod 4$.

Corollary 9.28. *There are infinitely many primes $p \equiv 1 \mod 4$.*

Proof. Let us assume there are finitely many primes $p_1, \ldots, p_k$ which are 1 modulo 4. Then, we define $q = 4\prod_{i=1}^{k} p_i^2 + 1$. Since q is odd, it must be divisible by some odd prime p. Thus, $4\prod_{i=1}^{k} p_i^2 \equiv -1 \mod p$, which means $(2\prod_{i=1}^{k} p_i)^2 \equiv -1 \mod p$ and thus $-1 \in Q_p$.

Due to Theorem 9.26, this means $p \equiv 1 \mod 4$. Since we assumed there are only $p_1, \ldots, p_k$, $p = p_i$ for some $i \in \{1, \ldots, k\}$. Thus, $p \mid (q - 4\prod_{i=1}^{k} p_i^2) = 1$, which is impossible. □

Theorem 9.29 (Gauss Lemma). *Let $p \in \mathcal{P}$ be odd and consider the two sets $P = \{1, \ldots, (p-1)/2\}$ and $N = \{-1, \ldots, -(p-1)/2\}$. Then,*

$$\left(\frac{a}{p}\right) = (-1)^{|aP \cap N|}.$$

Before we prove this theorem, let us give an example of N, P.

Example 9.30. *The sets N, P split $\mathbb{Z}/p\mathbb{Z}^\times$ into two halves, those closer to 0, and those closer to p.*

Let $p = 19$, so that $P = \{1, \dots, 9\}$ and $N = \{-1, \dots, -9\}$. We denote by

$$aP = \{ax \mid x \in P\} = \{a, 2a, \dots, a\frac{p-1}{2}\}.$$

For example $N = (-1)P$. For any $a \in \mathbb{Z}/p\mathbb{Z}$, the set aP may consist of elements from P or N. For example

$$11P = \{11, 3, 14, 6, 17, 9, 1, 12, 4\} = \{-8, 3, -5, 6, -2, 9, 1, -7, 4\}$$

contains four elements of N and 5 elements of P. Thus, the quantity $|aP \cap N| = 4$ and $\left(\frac{11}{19}\right) = (-1)^4 = 1$, that is $11 \in Q_{19}$.

Proof. If $x, y \in P$ are distinct, then $ax \not\equiv \pm ay \mod p$. In fact, if $ax \equiv \pm ay \mod p$, then $p \mid a(x \pm y)$. As $p \nmid a$, this implies $p \mid (x \pm y)$, which is a contradiction to $x, y \in P$ distinct.

Thus, all elements of aP live in distinct sets

$$\{\pm 1\},\ \{\pm 2\},\ \dots, \{\pm\frac{p-1}{2}\}.$$

There are $\frac{p-1}{2}$ many such sets and $\frac{p-1}{2}$ many elements in aP. Thus, each set contains exactly one element of aP :

$$aP = \{\sigma(x)x \mid x \in \{1, \dots, \frac{p-1}{2}\}\},$$

where $\sigma(x) \in \{\pm 1\}$, is such that $\sigma(x) = 1$ if $x \in aP$, and $\sigma(x) = -1$, if $x \notin aP$ (but $-x \in aP$). Thus, we have $|aP \cap N|$ many x with $\sigma(x) = -1$.

Thus, when multiplying over all elements in $aP = \{ax \mid x \in P\}$ we get $\prod_{i=1}^{(p-1)/2} ai \equiv a^{(p-1)/2}\left(\frac{p-1}{2}\right)! \mod p$, and as $aP = \{\sigma(x)x \mid x \in P\}$ this must be the same as

$$\prod_{i=1}^{(p-1)/2} \sigma(i)i \equiv (-1)^{|aP \cap N|}\left(\frac{p-1}{2}\right)! \mod p.$$

Thus,

$$a^{(p-1)/2}\left(\frac{p-1}{2}\right)! \equiv (-1)^{|aP \cap N|}\left(\frac{p-1}{2}\right)! \mod p,$$

and as $\left(\frac{p-1}{2}\right)! \in \mathbb{Z}/p\mathbb{Z}^\times$, we can divide by it and get:

$$a^{(p-1)/2} \equiv (-1)^{|aP \cap N|} \mod p.$$

Due to Euler's criterion, we get

$$\left(\frac{a}{p}\right) \equiv (-1)^{|aP \cap N|} \mod p,$$

and as both values can only attain ± 1, we finally get

$$\left(\frac{a}{p}\right) = (-1)^{|aP \cap N|}.$$

□

When is 2 a quadratic residue of p?

Example 9.31. *We can check that* $3^2 \equiv 2 \mod 7, 6^2 \equiv 2 \mod 17$, *but* $x^2 \equiv 2 \mod p$ *has no solution for* $p = 3, 5, 11$.

Theorem 9.32. *Let* $p \in \mathcal{P}$ *be odd. Then,* $2 \in Q_p$ *if and only if* $p \equiv \pm 1 \mod 8$.

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

Proof. We can apply Gauss' Lemma for $a = 2$, getting

$$2P = \{2, 4, \dots, p-1\}.$$

If $p \equiv 1 \mod 4$, that is there is some $k \in \mathbb{N}$ with $p = 4k+1$, then $(p-1)/2 = 2k$ is even and thus in $2P$. Similarly, $(p+3)/2 = 2k+2 \in 2P$. This is the exact point, where the elements in $2P$ become closer to p than to 0, as $(p-1)/2 < p - (p-1)/2 = (p+1)/2$ and $(p+3)/2 > p - (p+3)/2 = (p-3)/2$. Thus,

$$2P = \{\underbrace{2, 4, \dots, \frac{p-1}{2}}_{\in P}, \underbrace{\frac{p+3}{2}, \dots, p-1}_{\in N}\},$$

and we have $|2P \cap N| = \frac{p-1}{4}$, as $2P$ contains $(p-1)/2$ elements, and we discard $\{2x \mid x \in \{1, \dots, (p-1)/4\}$.

Gauss' Lemma then gives

$$\left(\frac{2}{p}\right) = (-1)^{(p-1)/4} = \left((-1)^{(p-1)/4}\right)^{(p+1)/2} = (-1)^{(p^2-1)/8},$$

where we have used the fact that $(p+1)/2 = 2k+1$ is odd and $(-1)^{2k+1} = (-1)$.

Now suppose that $p \equiv 3 \mod 4$, that is there exists some $k \in \mathbb{N}$ with $p = 4k+3$. Thus, $(p-3)/2 = 2k$ is even and thus in $2P$. Similarly, $(p+1)/2 = 2k+2 \in 2P$. This is the exact point, where the elements in $2P$ become closer to p than to 0, as $(p-3)/2 < p - (p-3)/2 = (p+3)/2$ and $(p+1)/2 > p - (p+1)/2 = (p-1)/2$. Thus,

$$2P = \{\underbrace{2, 4, \dots, \frac{p-3}{2}}_{\in P}, \underbrace{\frac{p+1}{2}, \dots, p-1}_{\in N}\},$$

and we have $|2P \cap N| = \frac{p+1}{4}$, as $2P$ contains $(p-1)/2$ elements, and we discard $\{2x \mid x \in \{1, \dots, (p-3)/4\}$.

Gauss' Lemma then gives

$$\left(\frac{2}{p}\right) = (-1)^{(p+1)/4} = \left((-1)^{(p+1)/4}\right)^{(p-1)/2} = (-1)^{(p^2-1)/8},$$

where we have used that $(p-1)/2 = 2k+1$ is odd and thus $(-1)^{2k+1} = -1$. □

Thus, 2 is a quadratic residue whenever $p \equiv \pm 1 \mod 8$, and a quadratic non-residue whenever $p \equiv \pm 3 \mod 8$.

Exercise 9.33. *For which p is $-2 \in Q_p$?*

Exercise 9.34. *Let $p \in \mathcal{P}$ be odd. Show*

$$\sum_{i=1}^{p-2} \left(\frac{i(i+1)}{p}\right) = -1$$

Exercise 9.35. *Let $p \in \mathcal{P}$ be odd and b a positive integer with $p \nmid b$. Show that*

$$\sum_{i=1}^{p-1} \left(\frac{ib}{p}\right) = 0.$$

9.4 Law of Quadratic Reciprocity

The law of quadratic reciprocity is one of the most celebrated results, relating the quadratic residues of different moduli.

The law of quadratic reciprocity was conjectured by Euler in 1783. Legendre tried several times, until finally in 1795, the 18-years old Gauss provided the first correct proof.

With this we can check whether $x^2 \equiv q \mod p$ has a solution knowing the solution to $x^2 \equiv p \mod q$.

Theorem 9.36 (Law of Quadratic Reciprocity)**.** *Let $p, q \in \mathcal{P}$ be odd and distinct. Then*

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

An equivalent formulation is:

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right),$$

except when $p \equiv q \equiv 3 \mod 4$, where

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

Or equivalently,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & p \equiv 1 \mod 4 \text{ or } q \equiv 1 \mod 4 \\ -1 & p \equiv q \equiv 3 \mod 4. \end{cases}$$

There exist many different proofs, the one presented here is the most elementary, but thus a bit longer.

Proof. We consider again $P = \{1, \dots, \frac{p-1}{2}\}$ and $N = (-1)P$, similarly, we denote by $Q = \{1, \dots, \frac{q-1}{2}\}$.

If we set $a = q$ in Gauss' Lemma, we get

$$\left(\frac{q}{p}\right) = (-1)^{|qP \cap N|},$$

where we note that $|qP \cap N|$ are all the $x \in P$ such that $qx \equiv n \mod p$, for some $n \in N$. This is equivalent to $qx - py \in N$ for some integer y, that is

$$-\frac{p}{2} < qx - py < 0.$$

We now look for the possible values of y.

Given $x \in P$, the values $qx - yp$ differ by multiples of p, thus $-\frac{p}{2} < qx - yp < 0$ for at most one integer y. If such integer y exists, then

$$0 < \frac{qx}{p} < y < \frac{qx}{p} + \frac{1}{2}.$$

Since $x \in P$, we have $x \leq \frac{p-1}{2}$, so

$$y < \frac{qx}{p} + \frac{1}{2} \leq \frac{q(p-1)}{2p} + \frac{1}{2} = \frac{q - q/p + 1}{2} < \frac{q+1}{2}.$$

Thus, $0 < y < \frac{q+1}{2}$ and hence $y \in Q$.

Thus,

$$w = |qP \cap N| = |\{(x, y) \in P \times Q \mid -\frac{p}{2} < qx - py < 0\}|.$$

We can now also consider Gauss' Lemma for q, setting $a = p$, that is

$$\left(\frac{p}{q}\right) = (-1)^v,$$

where

$$v = |\{(y, x) \in Q \times P \mid -\frac{q}{2} < py - qx < 0\}| = \{(x, y) \in P \times Q \mid 0 < qx - py < \frac{q}{2}\}|.$$

Putting both together, we get

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^w(-1)^v = (-1)^{v+w},$$

where

$$\begin{aligned} w + v &= |\{(x,y) \in P \times Q \mid -\frac{p}{2} < qx - py < 0 \text{ or } 0 < qx - py < \frac{q}{2}\}| \\ &= |\{(x,y) \in P \times Q \mid -\frac{p}{2} < qx - py < \frac{q}{2}\}|, \end{aligned}$$

as there are no x, y with $qx - py = 0$.

Note that the number of pairs $(x, y) \in P \times Q$ is

$$|P||Q| = \frac{p-1}{2}\frac{q-1}{2},$$

thus we may write

$$w + v = \frac{p-1}{2}\frac{q-1}{2} - (\alpha + \beta),$$

where $\alpha = |A| = |\{(x,y) \in P \times Q \mid -\frac{p}{2} \geq qx - py\}|$ and $\beta = |B| = |\{(x,y) \in P \times Q \mid qx - py \geq \frac{q}{2}\}|$.

If we can show that $\alpha = \beta$, then

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

In order to show that $\alpha = \beta$, we define the bijective function $\rho(x, y) = \left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right)$.

Since $-\frac{p}{2} \geq qx - py$ if and only if $q\left(\frac{p+1}{2} - x\right) - p\left(\frac{q+1}{2} - y\right) \geq \frac{q}{2}$, we have that $\rho(A) = B$ and $\rho(B) = A$ and hence $\alpha = \beta$.

□

Example 9.37. *The previous theorems provide very powerful tools to check whether $a \in Q_p$. For example $p = 103, a = 83$ two distinct odd primes. Then*

$$\begin{aligned}
\left(\frac{83}{103}\right) &= -\left(\frac{103}{83}\right) && \textit{Law of Quadratic Reciprocity}\\
&= -\left(\frac{20}{83}\right) && 103 \equiv 20 \mod 83\\
&= -\left(\frac{2}{83}\right)^2\left(\frac{5}{83}\right) && \textit{multiplicative}\\
&= -\left(\frac{5}{83}\right) && (\pm 1)^2 = 1\\
&= -\left(\frac{83}{5}\right) && \textit{Law of Quadratic Reciprocity}\\
&= -\left(\frac{3}{5}\right) && 83 \equiv 3 \mod 5\\
&= -\left(\frac{5}{3}\right) && \textit{Law of Quadratic Reciprocity}\\
&= -\left(\frac{2}{3}\right) && 5 \equiv 2 \mod 3\\
&= 1 && 2 \notin Q_3
\end{aligned}$$

and thus $83 \in Q_{103}$.

One application of the Law of Quadratic Reciprocity is a test by Pepin, to check whether a Fermat number is prime. Let us start with the following implication.

Corollary 9.38. *Let* $p \in \mathcal{P}$ *odd, then* $3 \in Q_p$ *if and only if* $p \equiv \pm 1 \mod 12$.

Proof. If $p \equiv 1 \mod 4$, then by the Law of Quadratic Reciprocity, we have that

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

which together with $p \equiv 1 \mod 4$ gives

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \mod 12, \\ -1 & \text{if } p \equiv 5 \mod 12. \end{cases}$$

If $p \equiv 3 \mod 4$, then

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

which together with $p \equiv 3 \mod 4$ gives,

$$\left(\frac{3}{p}\right) = \begin{cases} -1 & \text{if } p \equiv 7 \mod 12, \\ 1 & \text{if } p \equiv 11 \mod 12. \end{cases}$$

□

Theorem 9.39. *Let n be a positive integer. The Fermat number $F(n) = 2^{2^n} + 1$ is prime if and only if*

$$3^{(F(n)-1)/2} \equiv -1 \mod F(n).$$

Proof. For the first direction, we assume that $F(n) \in \mathcal{P}$.

We first note that $F(n) = 2^{2^n} + 1 \equiv 5 \mod 12$, since $2^{2^n} + 1 \equiv 2^{2^n \mod 2} + 1 \equiv 2 \mod 3$ and $2^{2^n} + 1 \equiv 1 \mod 4$.

Thus, $3 \notin Q_{F(n)}$ and by Euler's criterion, we get that

$$3^{(F(n)-1)/2} \equiv -1 \mod F(n).$$

For the converse, assume that $3^{(F(n)-1)/2} \equiv -1 \mod F(n)$. Squaring this congruence we get $3^{F(n)-1} \equiv 1 \mod F(n)$ and hence $3^{F(n)-1} \equiv 1 \mod p$ for any prime $p \mid F(n)$.

Thus, $3 \in \mathbb{Z}/p\mathbb{Z}^{\times}$ and ord(3) $\mid (F(n) - 1) = 2^{2^n}$. Thus, ord(3) $= 2^i$ for some $i \leq 2^n$.

However, since

$$3^{(F(n)-1)/2} \equiv 3^{2^{2^n-1}} \equiv -1 \not\equiv 1 \mod p$$

we must have $i = 2^n$, that is ord(3) $= 2^{2^n} = F(n) - 1$.

As we also require ord(3) $\leq p - 1$, we get that $F(n) \leq p$. Since we assumed $p \mid F(n)$, this implies $p = F(n)$, that is $F(n)$ is a prime. □

The proof further shows that 3 is a primitive root for any Fermat prime.

Example 9.40. *Let $n = 2$, so that $F(n) = 17$. Then,*

$$3^{(F(n)-1)/2} \equiv 3^8 \equiv -1 \mod 17,$$

confirming that 17 is a prime.

Let $n = 5$, then $F(n) = 4294967297$. Now it is harder to tell whether $F(n)$ is prime. Using Pepin's test we get that

$$3^{(F(n)-1)/2} \not\equiv -1,$$

and thus $F(5)$ is not prime.

Exercise 9.41. *Use Pepin's test to show that $F(3) = 257$ is prime.*

Exercise 9.42. *Let $p \in \mathcal{P}$ be odd. Show that*

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1 \mod 6, \\ -1 & \textit{if } p \equiv -1 \mod 6. \end{cases}$$

9.5 Jacobi Symbol

While we have seen characterizations of Q_n for arbitrary $n,$ we also want to ask whether there exists a generalization of the Legendre symbol.

Definition 9.43. Let n be an odd positive integer with prime factorization $n = \prod_{i=1}^{k} p_i^{e_i}$ and let a be a positive integer such that $\gcd(a, n) = 1$. The *Jacobi symbol* is defined as

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}.$$

While this generalized the Legendre symbol, in fact for $n \in \mathcal{P}$ they are the same, the Jacobi symbol does not tell us, whether a congruence $x^2 \equiv a \mod n$ has solutions.

We do know that if $x^2 \equiv a \mod n$ has solutions, then $\left(\frac{a}{n}\right) = 1$.

To see this, let $p \mid n$ be a prime. If $x^2 \equiv a \mod n$ has solutions then $x^2 \equiv a \mod p$ has solutions, i.e., $\left(\frac{a}{p}\right) = 1$.

Consequently, for $n = \prod_{i=1}^{k} p_i^{e_i}$, we get that

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i} = 1.$$

However, we could have $\left(\frac{a}{n}\right) = 1$, but $a \notin Q_n$.

Example 9.44. *Let $n = 15$ and $a = 2$. Then*

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

However, as there are no solutions of $x^2 \equiv 2 \mod 3$ and $\mod 5$, there is also no solution $\mod 15$.

On the positive side, the Jacobi symbol enjoys the same algebraic properties as the Legendre symbol.

Theorem 9.45. *Let n be an odd positive integer and a, b be positive integers with gcd$(a, n) =$ gcd$(b, n) = 1$. Then,*

- *if $a \equiv b \mod n$ then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.*
- $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.
- $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$
- $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$

Proof. Let us consider the prime factorization $n = \prod_{i=1}^{k} p_i^{e_i}$. Since n is odd, p_i is odd for all $i \in \{1, \dots, k\}$.

- For all p_i we have that $a \equiv b \mod n$ implies $a \equiv b \mod p_i$, thus we can apply Theorem 9.25 and get
$$\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right),$$
thus
$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i} = \prod_{i=1}^{k} \left(\frac{b}{p_i}\right)^{e_i} = \left(\frac{b}{n}\right).$$

- From Theorem 9.25, we know that
$$\left(\frac{ab}{p_i}\right) = \left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right).$$
Hence,
$$\begin{aligned}\left(\frac{ab}{n}\right) &= \prod_{i=1}^{k} \left(\frac{ab}{p_i}\right)^{e_i} = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i} \left(\frac{b}{p_i}\right)^{e_i} \\ &= \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).\end{aligned}$$

- From Theorem 9.26 we know that
$$\left(\frac{-1}{p_i}\right) = (-1)^{(p_i-1)/2}.$$
Thus,
$$\left(\frac{-1}{n}\right) = \prod_{i=1}^{k} \left(\frac{-1}{p_i}\right)^{e_i} = \prod_{i=1}^{k} (-1)^{e_i(p_i-1)/2} = (-1)^{\sum_{i=1}^{k} e_i \frac{p_i-1}{2}}.$$
Since
$$n = \prod_{i=1}^{k} (1 + (p_i - 1))^{e_i}$$
and $p_i - 1$ is even, we have that $(1 + (p_i - 1))^{e_i} \equiv 1 + e_i(p_i - 1) \mod 4$. Since
$$(1 + e_i(p_i - 1))(1 + e_j(p_j - 1)) \equiv 1 + e_i(p_i - 1) + e_j(p_j - 1) \mod 4$$
we get that
$$n \equiv 1 + \sum_{i=1}^{k} e_i(p_i - 1) \mod 4.$$

This further implies that

$$\frac{n-1}{2} \equiv \sum_{i=1}^{k} e_i \frac{p_i - 1}{2} \mod 2.$$

Thus, we can insert this and get

$$(-1)^{\sum_{i=1}^{k} e_i \frac{p_i-1}{2}} = (-1)^{\frac{n-1}{2}}.$$

- From Theorem 9.32 we know that

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

Hence,

$$\left(\frac{2}{n}\right) = \prod_{i=1}^{k} \left(\frac{2}{p_i}\right)^{e_i} = \prod_{i=1}^{k} (-1)^{(p_i^2-1)/8} = (-1)^{\sum_{i=1}^{k} \frac{p_i^2-1}{8}}.$$

As before, we note that

$$n^2 = \prod_{i=1}^{k} (1 + (p_i^2 - 1))^{e_i}.$$

We now show that $p_i^2 - 1 \equiv 0 \mod 8$. In fact, $(p_i^2 - 1) = (p_i + 1)(p_i - 1)$ and since p_i is odd, we have $p_i - 1 = 2\ell, p_i + 1 = 2\ell + 2$, for some $\ell \in \mathbb{N}$. Thus, $(p_i + 1)(p_i - 1) = 2\ell(2\ell + 2) = 4\ell(\ell + 1)$ and since either $2 \mid \ell$ or $2 \mid (\ell + 1)$, we get $8 \mid (p_i + 1)(p_i - 1) = (p_i^2 - 1)$.

Now,

$$(1 + (p_i^2 - 1))^{e_i} \equiv 1 + e_i(p_i^2 - 1) \mod 64.$$

Additionally,

$$(1 + e_i(p_i^2 - 1))(1 + e_j(p_j^2 - 1)) \equiv 1 + e_i(p_i^2 - 1) + e_j(p_j^2 - 1) \mod 64.$$

Hence,

$$n^2 = 1 + \sum_{i=1}^{k} e_i(p_i^2 - 1) \mod 64.$$

Which implies that

$$(n^2 - 1)/8 \equiv \sum_{i=1}^{k} e_i \frac{p_i^2 - 1}{8} \mod 8.$$

Thus, inserting this we get

$$(-1)^{\sum_{i=1}^{k} e_i (p_i^2-1)/8} = (-1)^{(n^2-1)/8}.$$

□

Additionally, we also have a reciprocity law.

Theorem 9.46 (Reciprocity Law). *Let n, m be two odd coprime positive integers. Then,*

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

Proof. Let us consider the prime factorizations of m and n, to be

$$m = \prod_{i=1}^{\ell} q_i^{f_i},$$
$$n = \prod_{i=1}^{k} p_i^{e_i}.$$

Then,

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{k}\left(\frac{m}{p_i}\right)^{e_i} = \prod_{i=1}^{k}\prod_{j=1}^{\ell}\left(\frac{q_j}{p_i}\right)^{e_i f_j},$$

where we have used that the Legendre symbol is multiplicative. Similarly,

$$\left(\frac{n}{m}\right) = \prod_{j=1}^{\ell}\left(\frac{n}{q_j}\right)^{f_j} = \prod_{j=1}^{\ell}\prod_{i=1}^{k}\left(\frac{p_i}{q_j}\right)^{e_i f_j},$$

and hence

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{k}\prod_{j=1}^{\ell}\left(\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\right)^{e_i f_j}.$$

We can apply the Law of Quadratic Reciprocity, i.e.,

$$\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}$$

to get

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{k}\prod_{j=1}^{\ell}(-1)^{e_i\frac{p_i-1}{2}f_j\frac{q_j-1}{2}} = (-1)^{\sum_{i=1}^{k}\sum_{j=1}^{\ell}e_i\frac{p_i-1}{2}f_j\frac{q_j-1}{2}}.$$

We note that

$$\sum_{i=1}^{k}\sum_{j=1}^{\ell}e_i\frac{p_i-1}{2}f_j\frac{q_j-1}{2} = \sum_{i=1}^{k}e_i\frac{p_i-1}{2}\sum_{j=1}^{\ell}f_j\frac{q_j-1}{2}.$$

Similar to before, we get that

$$\sum_{i=1}^{k}e_i\frac{p_i-1}{2} \equiv \frac{n-1}{2} \mod 2$$

and

$$\sum_{j=1}^{\ell} f_j \frac{q_j-1}{2} \equiv \frac{m-1}{2} \mod 2.$$

Thus,

$$\sum_{i=1}^{k} e_i \frac{p_i-1}{2} \sum_{j=1}^{\ell} f_j \frac{q_j-1}{2} \equiv \frac{n-1}{2}\frac{m-1}{2} \mod 2.$$

Thus, we get that

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

□

9.6 More Applications

We have already seen two applications of quadratic residues: that there are infinitely many primes $p \equiv 1 \mod 4$ and Pepin's primality test for Fermat's numbers.

In this section we give some more applications, namely the Euler-Jacobi Pseudoprimes, a Zero-Knowledge (ZK) protocol, a Private Information Retrieval (PIR) based on quadratic residues and the Lucas-Lehmer test for Mersenne numbers.

9.6.1 Euler-Jacobi pseudoprimes

Let p be an odd prime and b a positive integer not divisible by p. By Euler's criterion, we have that

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

Hence if we want to test whether a positive integer n is prime, we may take any integer b with $\gcd(b,n)=1$ and check is

$$b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \mod n,$$

using the Jacobi symbol. If the test fails, then n is composite.

Example 9.47. *Let $n = 341$ and $b = 2$. We compute*

$$2^{(341-1)/2} \equiv 2^{170} \equiv 1 \mod 341.$$

However,

$$\left(\frac{2}{341}\right) = -1,$$

as $341 \equiv 5 \mod 8$. Thus, 341 is not prime.

Definition 9.48. Let b be a positive integer and n be an odd positive and composite integer, with

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

Then n is called a *Euler-Jacobi pseudoprime* to the base b.

Theorem 9.49. *If n is an Euler-Jacobi pseudoprime to the base b, then n is also a pseudoprime to the base b.*

Proof. If n is an Euler-Jacobi pseudoprime to the base b, then

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

By squaring this congruence, we get

$$b^{n-1} \equiv \left(\frac{b}{n}\right)^2 \equiv 1 \mod n.$$

Since $b^{n-1} \equiv 1 \mod n$ it is a pseudoprime to the base b. □

However, the opposite direction is not true. For example 341 is not an Euler-Jacobi pseudoprime to the base 2, but it is a pseudoprime to the base 2.

Theorem 9.50. *If n is a strong pseudoprime to the base b, then n is a Euler-Jacobi pseudoprime to the base b.*

Proof. Let $n = \prod_{i=1}^{k} p_i^{e_i}$ be the prime factorization.

Let n be a strong pseudoprime to the base b. That is, if $n-1 = 2^s t$, where t is odd, then either $b^t \equiv 1 \mod n$, or $b^{2^j t} \equiv -1 \mod n$ for some $j \in \{0, \ldots, s-1\}$.

We first consider the case $b^t \equiv 1 \mod n$. Since $b^t \equiv 1 \mod p_i$, we have that $\text{ord}(b) \mid t$ modulo p_i. Since t is odd, $\text{ord}(b)$ must also be odd.

From Fermat's Little Theorem we also know that $\text{ord}(b) \mid (p_i - 1)$ and since it is odd also that $\text{ord}(b) \mid (p_i - 1)/2$. Thus,

$$b^{(p_i-1)/2} \equiv 1 \mod p_i.$$

Consequently, by Euler's criterion we have $\left(\frac{b}{p_i}\right) = 1$.

For the Jacobi symbol, recall

$$\left(\frac{b}{n}\right) = \prod_{i=1}^{k} \left(\frac{b}{p_i}\right)^{e_i}$$

and as $\left(\frac{b}{p_i}\right) = 1$ for all $i \in \{1, \ldots, k\}$ we get $\left(\frac{b}{n}\right) = 1$.

Since $b^t \equiv 1 \mod n$, we get that $b^{(n-1)/2} \equiv (b^t)^{2^{s-1}} \equiv 1 \mod n$ and hence it is a Euler-Jacobi pseudoprime as

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

Now we consider the case

$$b^{2^j t} \equiv -1 \mod n,$$

for some $j \in \{0, \ldots, s-1\}$. Thus also $b^{2^j t} \equiv -1 \mod p_i$ and squaring the congruence we get

$$b^{2^{j+1} t} \equiv 1 \mod p_i.$$

Thus, ord$(b) \mid 2^{j+1}t$, but ord$(b) \nmid 2^j t$. Thus, ord$(b) = 2^{j+1}c$, for some odd c.

From Fermat's Little Theorem we also have that ord$(b) \mid (p_i - 1)$, thus $2^{j+1} \mid (p_i - 1)$. We can write $p_i = 2^{j+1}d_i + 1$, for some integer d_i and $c \mid d_i$.

Since $b^{2^j t} \equiv -1 \mod p_i$, we have

$$\left(\frac{b}{p_i}\right) \equiv b^{(p_i-1)/2} \equiv b^{\frac{2^{j+1}c}{2} \cdot \frac{p_i - 1}{2^{j+1}c}} \equiv (-1)^{\frac{p_i-1}{2^{j+1}c}} \equiv (-1)^{\frac{2^{j+1}d_i}{2^{j+1}c}} \equiv (-1)^{\frac{d_i}{c}} \mod p_i.$$

Since c is odd, we have that d_i/c has the same parity as d, thus

$$\left(\frac{b}{p_i}\right) \equiv (-1)^{d_i} \mod p_i.$$

Since the Legendre symbol is only taking values is $\{\pm 1\}$, we get

$$\left(\frac{b}{p_i}\right) = (-1)^{d_i}.$$

Hence,

$$\left(\frac{b}{n}\right) = \prod_{i=1}^{k} \left(\frac{b}{p_i}\right)^{e_i} = \prod_{i=1}^{k} ((-1)^{d_i})^{e_i} = \prod_{i=1}^{k} (-1)^{e_i d_i} = (-1)^{\sum_{i=1}^{k} e_i d_i}.$$

We can now write again

$$n \equiv \prod_{i=1}^{k} p_i^{e_i} \equiv \prod_{i=1}^{k} (2^{j+1}d_i + 1)^{e_i} \equiv \prod_{i=1}^{k} (1 + 2^{j+1} d_i e_i) \equiv 1 + 2^{j+1} \sum_{i=1}^{k} e_i d_i \mod 2^{2(j+1)}.$$

Thus,

$$t 2^{s-1-j} \equiv \frac{n-1}{2^{j+1}} \equiv \sum_{i=1}^{k} e_i d_i \mod 2^{j+1}.$$

Hence,

$$b^{(n-1)/2} \equiv (b^{2^j t})^{2^{s-1-j}} \equiv (-1)^{2^{s-1-j}} \equiv (-1)^{2^{s-1-j}t} \equiv (-1)^{\sum_{i=1}^k e_i d_i} \mod n.$$

Thus, we get that

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

□

The opposite direction is again not true.

Example 9.51. *Let* $n = 1105$ *and* $b = 2$*. Then* $2^{552} \equiv 1 \mod 1105$ *and* $\left(\frac{2}{1105}\right) = 1$*, since* $1105 \equiv 1 \mod 8$*. Thus 1105 is an Euler-Jacobi pseudoprime to the base 2. However,*

$$2^{(1105-1)/2^2} \equiv 2^{276} \equiv 781 \not\equiv \pm 1 \mod 1105,$$

it is not a strong pseudoprime to the base 2.

With additional conditions, we can make the other direction work as well:

Theorem 9.52. *If* n *is an Euler-Jacobi pseudoprime to the base* b *and either*

- $n \equiv 3 \mod 4$ *or*
- $\left(\frac{b}{n}\right) = -1$,

then n *is a strong pseudoprime to the base* b*.*

Proof.

- If $n \equiv 3 \mod 4$, then $n = 3+4k$, for some integer k and hence $n-1 = 2(1+2k) = 2t$, where $t = 1+2k = (n-1)/2$ is odd. Since

$$b^t \equiv b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \equiv \pm 1 \mod n,$$

  n is also a strong pseudoprime to the base b.

- We write $n - 1 = 2^s t$, where t is odd and s is a positive integer. Since

$$b^{2^{s-1}t} \equiv b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \equiv -1 \mod n,$$

  we also have that n is a strong pseudoprime to the base b.

□

Note that the Euler's test is also basis for more primality tests, such as the Solovay-Strassen test.

Theorem 9.53. *Solovay Strassen Let* n *be an odd positive integer and choose* $b_1, \ldots, b_k$ *coprime to* n*. If* $\left(\frac{b_i}{n}\right) \equiv b_i^{(n-1)/2} \mod n$ *for all* $i \in \{1, \ldots, k\}$*, then the probability that* n *is composite is* $\leq 2^{-k}$*.*

9.6.2 Zero-Knowledge

The process and notation for ZK protocols are similar to that of signature schemes. We have two parties, a prover (instead of a signer) and a verifier.

A ZK protocol consists of two stages: key generation and verification.

A ZK protocol has three important attributes:

1. *Zero-knowledge:* this means that no information about the secret is revealed during the process.

2. *Completeness:* meaning that an honest prover will always get accepted.

3. *Soundness:* for this, we want that an impersonator has only a small cheating probability to get accepted.

In order to achieve an acceptable cheating probability, the protocols are often repeated several times (called *rounds*) and only if each round was accepted, will the prover be accepted.

One prominent ZK protocol from Feige, Fiat and Shamir is based on quadratic residues.

1. Key generation: The prover chooses two distinct primes p, q and computes $n = pq$ and some positive integer k. The prover chooses $s_1, \dots, s_k$ coprime to n. The prover now computes

$$v_i \equiv s_i^{-2} \mod n.$$

   The public key is given by $P = (n, v_1, \dots, v_k)$. The secret key is given by $S = (p, q, s_1, \dots, s_k)$.

2. Verification: The prover chooses a random integer c and a random sign $\sigma \in \{-1, 1\}$ and computes

$$x \equiv \sigma c^2 \mod n$$

   and sends this to the verifier. The verifier chooses the challenge $b = (b_1, \dots, b_k) \in \{0, 1\}^k$ and sends b to the prover. The prover then computes the response

$$r \equiv c \prod_{j:b_j=1} s_j \mod n$$

   and sends r to the verifier. The verifier can now check whether

$$x \equiv \pm r^2 \prod_{j:b_j=1} v_j \mod n.$$

Why does this work?

$$x \equiv \pm r^2 \prod_{j:b_j=1} v_j \equiv \pm c^2 \prod_{j:b_j=1} s_j^2 v_j \equiv \pm c^2 \equiv x \mod n$$

since $s_j^2 \equiv v_j^{-1} \mod n$.

Eve, the impersonator, can see the public v_i but she does not know the s_i. She can pick a random r and $b = (b_1, \dots, b_k) \in \{0,1\}^k$. She then computes

$$x \equiv r^2 \prod_{j:b_j=1} v_j \mod n$$

and sends x to the verifier. The verifier will then challenge her with his b', but Eve simply returns her r. If Eve has correctly chosen $b = b'$, she will be verified. Thus, the cheating probability is 2^{-k}.

The hardness of this protocol relies on integer factorization. Since Eve could easily compute s_i if she knew p, q.

Example 9.54.

- *Key generation: The prover chooses* $p = 7, q = 13$ *and computes* $n = 91$. *The prover further chooses* $s_1 = 4, s_2 = 5$ *coprime to 91. The prover then computes*

  $$v_1 \equiv 4^{-2} \mod 91, \quad v_2 \equiv 5^{-1} \mod 91,$$

  which is equivalent to computing $4^{-1} \equiv 2 \mod 7, 4^{-1} \equiv 10 \mod 13$*, thus*

  $$v_1 = 23^2 \equiv 74 \mod 91,$$

  and $5^{-1} \equiv 3 \mod 7, 5^{-1} \equiv 8 \mod 13$, *thus* $v_2 \equiv 73^2 \equiv 51 \mod 91$.

  Hence $P = (91, 74, 51)$ *and* $S = (7, 13, 4, 5)$.

- *Verification: The prover chooses* $c = 11, \sigma = 1$ *and computes* $x \equiv 11^2 \equiv 30 \mod 91$ *and sends* 30 *to the verifier.*

  The verifier chooses $b = (1, 0)$ *and sends this to the prover.*

  The prover computes the response

  $$r \equiv c \cdot s_1 \equiv 44 \mod 91$$

  and sends it to the verifier.

  The verifier now checks

  $$30 \equiv \pm 44^2 \cdot 74 \equiv 25 \cdot 74 \equiv 30 \mod 91.$$

9.6.3 Lucas-Lehmer Test

Recall that $M(p) = 2^p - 1$, for $p \in \mathcal{P}$ is a Mersenne number. The next theorem is able to test whether $M(p) \in \mathcal{P}$. For this we need to define the Lucas sequence.

Definition 9.55. The *Lucas sequence* is defined as: $s(0) = 4$ and for all positive integers n, we define

$$s(n) = s(n-1)^2 - 2.$$

Example 9.56. *Note that* $M(5) = 2^5 - 1 = 31$. *We compute* $s(1) = 14, s(2) = 194 \equiv 8 \mod 31$ *and* $s(3) \equiv 62 \equiv 0 \mod 31$. *Thus* $M(5) = 31 \in \mathcal{P}$ *as it is a divisor of* $s(3)$.

Theorem 9.57. *Let* p *be an odd prime, then* $M(p)$ *is prime if and only if* $M(p) \mid s(p-2)$.

Proof. First, we define $\omega = 2 + \sqrt{3}, \bar{\omega} = 2 - \sqrt{3}$. Note that $\omega\bar{\omega} = (2+\sqrt{3})(2-\sqrt{3}) = 4 - 3 = 1$.

Thus, $(\omega + \bar{\omega})^2 = \omega^2 + 2\omega\bar{\omega} + \bar{\omega}^2 = \omega^2 + \bar{\omega}^2 + 2$.

One can then show by induction that $s(n) = \omega^{2^n} + \bar{\omega}^{2^n}$, by observing that $\omega + \bar{\omega} = 4$, and $\omega^{2^{n+1}} + \bar{\omega}^{2^{n+1}} = \omega^{2^{n+1}} + \bar{\omega}^{2^{n+1}} + 2\omega^{2^n}\bar{\omega}^{2^n} - 2 = \left(\omega^{2^n} + \bar{\omega}^{2^n}\right)^2 - 2$.

For the first direction, let us assume that $M(p) = 2^p - 1 \in \mathcal{P}$. By Freshman's dream we know that

$$(1+\sqrt{3})^{M(p)} \equiv 1 + \sqrt{3}^{M(p)} \mod M(p).$$

Since $\sqrt{3} = 3^{1/2}$, we can also write

$$(1+\sqrt{3})^{M(p)} \equiv 1 + \sqrt{3}3^{(M(p)-1)/2} \mod M(p).$$

Euler's criterion tell us that

$$3^{(M(p)-1)/2} \equiv \left(\frac{3}{M(p)}\right) \mod M(p).$$

Since we assumed that $M(p)$ is an odd prime, we can apply the Law of Quadratic Reciprocity:

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

We can easily check that $M(p) \equiv 3 \mod 4$ and hence $\left(\frac{3}{M(p)}\right)\left(\frac{M(p)}{3}\right) = -1$, which is only possible if $M(p) \in Q_3$ but $3 \notin Q_{M(p)}$ or vice versa: $M(p) \notin Q_3$ and $3 \in Q_{M(p)}$.

Since $M(p) = 2^p - 1 \equiv (-1)^p - 1 \equiv -2 \equiv 1 \mod 3$, we get $M(p) \in Q_3$, thus $3 \notin Q_{M(p)}$. We again apply Euler's criterion, which tells us that

$$3^{(M(p)-1)/2} \equiv -1 \mod M(p).$$

Thus, we can insert this in

$$(1+\sqrt{3})^{M(p)} \equiv 1 + \sqrt{3}3^{(M(p)-1)/2} \equiv 1 - \sqrt{3} \mod M(p).$$

We can multiply both sides with $(1+\sqrt{3})$ to get

$$(1+\sqrt{3})^{M(p)+1} \equiv (1-\sqrt{3})(1+\sqrt{3}) \equiv 1 - 3 \equiv -2 \mod M(p).$$

Note that $(1+\sqrt{3})^2 = 1 + 2\sqrt{3} + 3 = 2\omega$, thus we can write

$$\left((1+\sqrt{3})^2\right)^{(M(p)+1)/2} \equiv (2\omega)^{(M(p)+1)/2} \equiv -2 \mod M(p).$$

Hence,

$$2^{(M(p)+1)/2}\omega^{(M(p)+1)/2} \equiv 2 \cdot 2^{(M(p)-1)/2}\omega^{(M(p)+1)/2} \equiv -2 \mod M(p).$$

Thus, we are interested in the value of $2^{(M(p)-1)/2}$, which by Euler's criterion is

$$\left(\frac{2}{M(p)}\right).$$

Recall from Theorem 9.32, that 2 is a quadratic residue for any prime congruent to ± 1 modulo 8.

$M(p) = 2^p - 1 \equiv 2^{p-3} \cdot 8 - 1 \equiv -1 \mod 8$, since $p > 2$. Thus, we get $2^{(M(p)-1)/2} \equiv 1 \mod M(p)$ and hence

$$2\omega^{(M(p)+1)/2} \equiv -2 \mod M(p),$$

or equivalently

$$\omega^{(M(p)+1)/2} \equiv -1 \mod M(p),$$

since $2 \nmid M(p)$. We may write this as

$$\omega^{2^{p-1}} \equiv \omega^{2^{p-2}}\omega^{2^{p-2}} \equiv -1 \mod M(p).$$

We can now multiply both sides with $\bar{\omega}^{2^{p-2}}$ to get

$$\omega^{2^{p-2}}\omega^{2^{p-2}}\bar{\omega}^{2^{p-2}} \equiv \omega^{2^{p-2}} \equiv -\bar{\omega}^{2^{p-2}} \mod M(p),$$

since $\omega\bar{\omega} = 1$.

Hence,

$$\omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}} \equiv 0 \mod M(p),$$

but since

$$s(p-2) = \omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}},$$

we get that $M(p) \mid s(p-2)$.

For the other direction, we assume that $(2^p - 1) \mid s(p-2)$, for some $p \in \mathcal{P}$.

Assume by contradiction that $2^p - 1 \notin \mathcal{P}$, thus there exists some $q \in \mathcal{P}$ with $q \mid (2^p - 1)$ with $q^2 \leq 2^p - 1$ and thus in turn $q \mid s(p-2)$.

Using $s(p-2) = \omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}}$, we get that there exists an integer k such that

$$qk = \omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}}.$$

We can multiply both sides with $\omega^{2^{p-2}}$ and use that $\omega\bar{\omega} = 1$, to get

$$qk\omega^{2^{p-2}} = \omega^{2^{p-1}} + 1$$

or equivalently

$$\omega^{2^{p-1}} = qk\omega^{2^{p-2}} - 1.$$

We can square both sides to get

$$\omega^{2^p} = \left(qk\omega^{2^{p-2}} - 1\right)^2.$$

We now want to consider this modulo q, however, we are unsure whether $3 \in Q_q$, which would allow us to consider $\sqrt{3} \in \mathbb{Z}/q\mathbb{Z}$.

Instead, we will consider $S = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}/q\mathbb{Z}\}$. In this new ring, we define addition and multiplication as

$$(a + b\sqrt{3}) + (c + d\sqrt{3}) = (a + c \mod q) + (b + d \mod q)\sqrt{3},$$
$$(a + b\sqrt{3}) \cdot (c + d\sqrt{3}) = (ac + 3bd \mod q) + (ad + bc \mod q)\sqrt{3}.$$

With number of units $|S^*| = q^2 - 1$.

Now, from $\omega^{2^p} = \left(qk\omega^{2^{p-2}} - 1\right)^2$ we get that

$$\omega^{2^p} \equiv (-1)^2 \equiv 1 \mod q,$$

hence in S we have $\text{ord}(\omega) \mid 2^p$, but since we also have

$$\omega^{2^{p-1}} \equiv -1 \mod q,$$

we get that $\text{ord}(\omega) = 2^p$.

Note that $\text{ord}(\omega) = 2^p \leq q^2 - 1$, which we assumed is such that $q^2 - 1 \leq 2^p - 2$, a contradiction.

□

This provides us with an efficient method (just involving computing two sequences defined via powers and integer division) to check whether a Mersenne number is prime.

9.6.4 PIR

Finally, we finish this section of applications with a Private Information Retrieval (PIR).

For this consider the scenario, where we have a database, containing files, managed by an untrusted server. We thus have two parties: a user and a server.

In order to get a file, the user sends a query to the server, the server will send back a response and from this the user should be able to retrieve the file we wanted. At the same time, we want that the query does not reveal any information on which file was requested.

Such a PIR protocol considers three steps:

- query generation,
- reply generation,
- file reconstruction.

In the easiest framework, we consider the files to be in $\{0, 1\}$ and assume the database has N many files $f_1, \ldots, f_N$.

- Query generation: the user chooses p, q large distinct primes and computes $n = pq$. Assume the user wants to retrieve file f_b. For each $i \in \{1, \dots, N\} \setminus \{b\}$ the user chooses $q_i \in Q_n$ and $q_b \notin Q_n$. The user sends $(q_1, \dots, q_N)$ as a query and n as public key.

- The server now computes
$$r \equiv \prod_{i : f_i = 1} q_i \mod n$$
and sends this as a response back to the user.

- File reconstruction: The user can now check if $r \in Q_n$ or not. If $r \in Q_n$ then all q_i in the product (i.e., all i with $f_i \neq 0$) must have been quadratic residues, thus $f_b = 0$. On the other hand, if $r \notin Q_n$ then $f_b \notin Q_n$ must have been in the product, i.e., $f_b = 1$.

We do not reveal any information to the server as we send N queries, one for each file. In order for the server to know which file we requested, the server needs to compute Q_n, which is only feasible when knowing p, q.

Example 9.58.

- *Query generation: The user chooses* $p = 7, q = 13$ *and computes* $n = 91$. *The user then chooses* $q_1 = 79 \equiv 25^2 \in Q_n, q_2 = 53 \equiv 12^2 \in Q_n$ *and* $q_3 = 5 \notin Q_n$. *The user then sends the query* $(79, 53, 5)$ *and the public key* 91.

- *The server is storing the files* $f_1 = 0, f_2 = 1, f_3 = 1$ *and computes the response*
$$r \equiv q_2 \cdot q_3 \equiv 83 \mod 91.$$

- *The user can now check whether* $83 \in Q_7$ *and* $83 \in Q_{13}$. *Note that as soon as one fails,* $83 \notin Q_n$. $\left(\frac{83}{7}\right) = \left(\frac{-1}{7}\right) = -1$, *thus the user recovers* $f_3 = 1$.

10 Continued Fractions

10.1 Representation of Reals

We recall that every integer $a \in \mathbb{Z}$ has a unique representation for any base $b > 1$ an integer, as

$$a = \sum_{i=0}^{N} a_i b^i,$$

denoted by $a = (a_N, \ldots, a_o)_b$.

We now show that this also holds for any real number $\alpha \in \mathbb{R}$.

For this recall that we denote the fractional part of α by

$$[\alpha] = \alpha - \lfloor \alpha \rfloor,$$

where $0 \leq [\alpha] < 1$. As $\lfloor \alpha \rfloor \in \mathbb{Z}$, it is enough to show that $[\alpha]$ has a unique representation to the base b.

Definition 10.1. Let $\gamma \in \mathbb{R}$ with $0 \leq \gamma < 1$ and $b > 1$ be an integer. The *representation* of γ to the base b is given by $\gamma = \sum_{i=1}^{\infty} c_i b^{-i}$, where $0 \leq c_i \leq b-1$ and for every $N \in \mathbb{N}$, there exists $n \geq N$ such that $c_n \neq b-1$. We denote this by

$$\gamma = (.c_1 c_2 \ldots)_b.$$

We further distinguish between representations which are finite and those which are periodic.

Definition 10.2. The representation of γ to the base b given by $(.c_1c_2...)_b$ is called *finite* if there exists an n such that $c_{n+1} = c_{n+2} = \ldots = 0$ and denote this by $\gamma = (.c_1 \ldots c_n)_b$.

Definition 10.3. The representation of γ to the base b given by $(.c_1c_2...)_b$ is called *periodic* if there exists N, k such that $c_n = c_{n+k}$ for all $n > N$ and denote this by $\gamma = (.c_1 \ldots c_N \overline{c_{N+1} \ldots c_{N+k}})_b$. We call $(.c_1 \ldots c_N)_b$ the *pre-period* of length N, and $(c_{N+1} \ldots c_{N+k})_b$ the *period* of length k.

Example 10.4. *For example* $1/3 = (.\overline{3})_{10}$.

Why did we require the condition that for all positive integer N there exists $n \geq N$ such that $c_n \neq b-1$?

Consider $(.\overline{9})_{10}$. This is the same as 1, as

$$\begin{aligned}(.\overline{9})_{10} &= \sum_{i\geq 1} 9 \cdot 10^{-i} = 9 \sum_{i \geq 1} 10^{-i} \\ &= 9 \cdot \frac{10^{-1}}{1-10^{-1}} = (10-1)\frac{10^{-1}}{1-10^{-1}} \\ &= 10(1-10^{-1})\frac{10^{-1}}{1-10^{-1}} = 1.\end{aligned}$$

This also works for any base b and the representation

$$(.c_1 \ldots c_n)_b = (.c_1 \ldots c_n \overline{(b-1)})_b$$

would not be unique.

Theorem 10.5. *Let $b > 1$ be a positive integer and $\gamma \in \mathbb{R}$ be such that $0 \le \gamma < 1$. Then γ has a unique representation to the base b.*

Proof. Let us denote by $c_1 = \lfloor b\gamma \rfloor$ which is such that $0 \le c_1 < b - 1$ (since $0 \le b\gamma < b$).

We can then define $\gamma_1 = b\gamma - c_1$ the fractional part of $b\gamma$ which is such that $0 \le \gamma_1 < 1$ and

$$\gamma = \frac{c_1}{b} + \frac{\gamma_1}{b}.$$

We can recursively define c_k and γ_k for all $k \ge 2$ as

$$c_k = \lfloor b\gamma_{k-1} \rfloor, \qquad \gamma_k = b\gamma_{k-1} - c_k,$$

which are such that $0 \le c_k \le b - 1$ and $0 \le \gamma_k < 1$.

Then, it follows that

$$\gamma = \sum_{i=1}^{n} c_i b^{-i} + \gamma_n b^{-n}. \tag{5}$$

Since $0 \le \gamma_n < 1$, we get that $0 \le \gamma_n b^{-n} < b^{-n}$ and hence $\lim_{n\to\infty} \gamma_n b^{-n} = 0$.

Thus

$$\gamma = \lim_{n\to\infty} \sum_{i=1}^{n} c_i b^{-i} = \sum_{i=1}^{\infty} c_i b^{-i}.$$

In order to show uniqueness, we assume that there exist two distinct representations

$$\gamma = \sum_{i=1}^{\infty} c_i b^{-i} = \sum_{i=1}^{\infty} d_i b^{-i},$$

with $0 \le c_i, d_i \le b - 1$ and for every positive integer N there exist n, m such that $c_n \ne b - 1$ and $d_m \ne b - 1$. Let k be the smallest index such that $c_k \ne d_k$. We may assume without loss of generality that $c_k > d_k$.

Then

$$0 = \sum_{i=1}^{\infty} (c_i - d_i) b^{-i} = (c_k - d_k) b^{-k} + \sum_{i=k+1}^{\infty} (c_i - d_i) b^{-i}.$$

Hence

$$(c_k - d_k) b^{-k} = \sum_{i=k+1}^{\infty} (d_i - c_i) b^{-i}$$

and as $c_k > d_k$ we have $(c_k - d_k) b^{-k} \ge b^{-k}$, whereas

$$\sum_{i=k+1}^{\infty} (d_i - c_i) b^{-i} \le \sum_{i=k+1}^{\infty} (b - 1) b^{-i} = (b - 1) \frac{b^{-k-1}}{1 - b^{-1}} = b^{-k}.$$

Thus

$$b^{-k} \le (c_k - d_k) b^{-k} \le \sum_{i=k+1}^{\infty} (d_i - c_i) b^{-i} \le b^{-k},$$

where we only have an equality for the last inequality, if $d_i - c_i = b - 1$ for all $i \geq k + 1$. Since $0 \leq c_i, d_i \leq b - 1$, this is only possible if $c_i = 0, d_i = b - 1$ for all $i \geq k + 1$, contradicting that $d_m \neq b - 1$. □

The proof of the theorem also gives us an algorithm how to compute the representation to the base b, namely

$$c_k = \lfloor b\gamma_{k-1} \rfloor, \qquad \gamma_k = b\gamma_{k-1} - \lfloor b\gamma_{k-1} \rfloor,$$

and $\gamma_0 = \gamma$.

Example 10.6. *We want to write* $1/6$ *in the base* 8.

$$\begin{aligned} c_1 &= \lfloor 8 \cdot 1/6 \rfloor = 1, & \gamma_1 &= 8 \cdot 1/6 - 1 = 1/3, \\ c_2 &= \lfloor 8 \cdot 1/3 \rfloor = 2, & \gamma_2 &= 8 \cdot 1/3 - 2 = 2/3, \\ c_3 &= \lfloor 8 \cdot 2/3 \rfloor = 5, & \gamma_3 &= 8 \cdot 2/3 - 5 = 1/3 \end{aligned}$$

thus it starts repeating, that is $c_4 = c_2$ *and* $\gamma_4 = \gamma_2$ *and so on. We get that*

$$1/6 = (.12525\ldots)_8 = (.1\overline{25})_8.$$

In fact, we can show that any rational number has a periodic or finite representation and vice versa.

Theorem 10.7. *Let* $b > 1$ *be a positive integer and* $\gamma \in \mathbb{R}$ *with* $0 < \gamma < 1$. *Then* γ *is a rational number if and only if it has either a finite representation or a periodic representation to the base* b.

Further, if $\gamma = \frac{r}{s}$ *with* $\gcd(r, s) = 1$ *and* $s = ut$ *with* $\gcd(b, u) = 1$ *and for every prime* $p \mid t$ *we also have* $p \mid b$, *then* γ *has a period of length* $\operatorname{ord}(b)$ *modulo* u *and a pre-period of length* N, *where* N *is the smallest positive integer such that* $t \mid b^N$.

Proof. We first assume that γ has a periodic representation, i.e.,

$$\begin{aligned} \gamma &= (.c_1 \ldots c_N\overline{c_{N+1} \ldots c_{N+k}})_b \\ &= \sum_{i=1}^{N} c_i b^{-i} + \left(\sum_{j=0}^{\infty} b^{-jk}\right)\left(\sum_{i=N+1}^{N+k} c_i b^{-i}\right) \\ &= \sum_{i=1}^{N} c_i b^{-i} + \left(\frac{b^k}{b^k - 1}\right)\left(\sum_{i=N+1}^{N+k} c_i b^{-i}\right). \end{aligned}$$

Hence γ is the sum of rational numbers and thus rational. Note that this also covers the case of finite representations by setting $k = 0$.

For the other direction, we can assume that $0 < \gamma < 1$ is such that $\gamma = \frac{r}{s}$, where $\gcd(r, s) = 1$ and $s = ut$ with $\gcd(b, u) = 1$ and for every prime $p \mid t$, we also have $p \mid b$. Let us denote by N the smallest positive integer such that $t \mid b^N$.

Since $t \mid b^N$, we have that $a = b^N/t$ is a positive integer. Hence,

$$b^N \gamma = b^N \frac{r}{ut} = \frac{ar}{u}.$$

We can write

$$\frac{ar}{u} = v + \frac{c}{u},$$

using the Euclidean Algorithm to write $ar = vu + c$ with $0 \leq c < u$ and $0 \leq v < b^N$, since $0 < b^N\gamma < b^N$ and hence $0 < b^N\gamma = v + \frac{c}{u} < v + 1$ and $b^N > b^N\gamma = v + \frac{c}{u} > v$. If $u = 0$, then $vut = b^N r$ and since $\gcd(u, b) = 1$ we get $u \mid r$. This would imply that $\frac{r}{s} = \frac{r}{ut}$ is not in reduced form, a contradiction. Thus, $0 < c < u$.

We now want to show that $\gcd(u, c) = 1$. For this let $d = \gcd(u, c)$, hence $d \mid ut = s$ and $d \mid (vu + c) = ar$. Since $\gcd(r, s) = 1$ this implies that $d \mid a$, so that there exists an integer ℓ with $d\ell t = b^N$ and thus $d \mid b$. As $d \mid u$ and $\gcd(u, b) = 1$ we also get $\gcd(d, b) = 1$ and together with $d \mid b$ we conclude that $d = 1$.

Let us write $v = (v_n \dots v_0)_b$ and $\frac{c}{u} = (.c_1 \dots)_b$ with $\gamma_0 = \frac{c}{u}$ and

$$c_k = \lfloor b\gamma_{k-1} \rfloor, \quad \gamma_k = b\gamma_{k-1} - \lfloor b\gamma_{k-1} \rfloor.$$

If $u = 1$, then γ has a finite representation to the base b as $\gamma = \frac{v+c}{b^N}$ and $v, c \in \mathbb{Z}$.

If $u > 1$, then we can consider the order of b modulo u, denoted by d. Thus, $b^d = u\ell + 1$ for some integer ℓ.

Then

$$b^d \frac{c}{u} = \frac{(u\ell + 1)c}{u} = \ell c + \frac{c}{u}.$$

However, we also have that

$$b^d \frac{C}{u} = b^d \left(\sum_{i=1}^{d} c_i b^{-i} + \gamma_d b^{-d} \right),$$

using Equation 5, so that

$$b^d \frac{C}{u} = \sum_{i=1}^{d} c_i b^{d-i} + \gamma_d.$$

Putting these two together, we get

$$b^d \frac{C}{u} = \sum_{i=1}^{d} c_i b^{d-i} + \gamma_d = \ell c + \frac{c}{u}.$$

Thus, their fractional parts $0 < \gamma d < 1$ and $0 < \frac{c}{u} < 1$ are equal $\gamma_d = \frac{c}{u}$ and thus $\gamma_0 = \gamma_d = \frac{c}{u}$, leading to the period length d and $c_{k+d} = c_k$ for all $k \geq 1$.

Thus, $\frac{c}{u}$ has a periodic representation,

$$\frac{c}{u} = (.\overline{c_1 \dots c_d})_b.$$

Thus,

$$b^N\gamma = v + \frac{c}{u} = (v_n \dots v_0 . \overline{c_1 \dots c_d})_b$$

and dividing by b^N shifts the representation by N to

$$\gamma = (.0 \dots 0 v_n \dots v_0 \overline{c_1 \dots c_d})_b.$$

Hence the pre-period of γ is of length N (beginning with $N-(n+1)$ zeroes), and the period is of length d.

We are left with showing that there does not exist a regrouping of the representation with shorter period or pre-period length.

Assume by contradiction that γ has a shorter pre-period M and period length k, i.e.,

$$\begin{aligned}\gamma &= (.c_1 \dots c_M \overline{c_{M+1} \dots c_{M+k}})_b \\ &= \sum_{i=1}^{M} c_i b^{-i} + \left(\frac{b^k}{b^k-1}\right)\left(\sum_{i=M+1}^{M+k} c_i b^{-i}\right) \\ &= \frac{(b^k-1)\sum_{i=1}^{M} c_i b^{M-i} + \sum_{i=1}^{k} c_{M+i} b^{k-i}}{b^M(b^k-1)}.\end{aligned}$$

Since $\gamma = \frac{r}{s}$ with coprime r, s we get that $s \mid b^M(b^k-1)$. As $s = ut$ with $\gcd(u,b) = 1$, we get $t \mid b^M$ and $u \mid (b^k-1)$. By definition N is the smallest integer such that $t \mid b^N$, hence $M \geq N$. Similarly, from $u \mid (b^k-1)$, we know there exists an integer ℓ such that $u\ell = b^k-1$, which is equivalent to $b^k \equiv 1 \mod u$. As the order of b modulo u is d, we get that $d \mid k$ and thus $d \leq k$.

Hence the pre-period length can not be shorter than N, and the period length can not be shorter than d. □

This proof also allows us to determine quickly the period and pre-period length.

Additionally, if γ has a representation which does not end and is not periodic, γ must be irrational.

10.2 Finite Continued Fractions

Using the Euclidean algorithm, we can represent rational numbers using continued fractions.

Example 10.8. *Let us consider $\frac{62}{23}$. Then using the Euclidean algorithm we can write*

$$\begin{aligned}62 &= 2 \cdot 23 + 16, \\ 23 &= 1 \cdot 16 + 7, \\ 16 &= 2 \cdot 7 + 2, \\ 7 &= 3 \cdot 2 + 1.\end{aligned}$$

By dividing each side with the respective divisor, we get

$$\begin{aligned}\frac{62}{23} &= 2 + \frac{16}{23} = 2 + \frac{1}{23/16},\\ \frac{23}{16} &= 1 + \frac{7}{16} = 1 + \frac{1}{16/7},\\ \frac{16}{7} &= 2 + \frac{2}{7} = 2 + \frac{1}{7/2},\\ \frac{7}{2} &= 3 + 1/2.\end{aligned}$$

Combining these we get

$$\begin{aligned}\frac{62}{23} &= 2 + \frac{1}{23/16}\\ &= 2 + \frac{1}{1 + \frac{1}{16/7}}\\ &= 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{7/2}}}\\ &= 2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{2}}}}.\end{aligned}$$

Definition 10.9. A *finite continued fraction* is of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cfrac{\vdots}{a_{n-1} + \cfrac{1}{a_n}}}}},$$

where a_i are positive real numbers for $i > 0$ and $a_0 \geq 0$ and we write it as $[a_0; a_1 \ldots, a_n]$.

If the a_i are integers, we call the continued fraction *simple.*

Example 10.10. *In the example before, we wrote* $\frac{62}{23} = [2; 1, 2, 3, 2]$.

In fact, every finite simple continued fraction is a rational number and vice versa.

Theorem 10.11. *Every finite simple continued fraction is a rational number and every rational number can be expressed by a finite simple continued fraction.*

Proof. We first prove that every finite simple continued fraction is a rational number by induction.

For $n = 1$, we have

$$[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1},$$

which is rational.

Now we assume that for any continued fraction of the form $[a_0; a_1, \ldots, a_k]$ with a_i integers is a rational number. Then

$$[a_0; a_1, \ldots, a_k, a_{k+1}] = a_0 + \frac{1}{[a_1; a_2, \ldots, a_{k+1}]}.$$

By the induction hypothesis $[a_1; a_2, \ldots, a_{k+1}] = \frac{r}{s}$ is a rational number. Thus

$$[a_0; a_1, \ldots, a_k, a_{k+1}] = a_0 + \frac{1}{r/s} = \frac{a_0 r + s}{r}$$

is also a rational number.

For the other direction we let $x = \frac{a}{b}$, where a, b are integers and $b > 0$.

Let $r_0 = a, r_1 = b$, then using the Euclidean algorithm, we can write

$$\begin{aligned} r_0 &= r_1 a_1 + r_2, \\ r_1 &= r_2 a_2 + r_3, \\ &\vdots \\ r_{n-3} &= r_{n-2} a_{n-2} + r_{n-1}, \\ r_{n-2} &= r_{n-1} a_{n-1} + r_n, \\ r_{n-1} &= r_n a_n, \end{aligned}$$

with $0 < r_{i+1} < r_i$ for all $i \in \{1, \ldots, n-1\}$ and a_i are positive integers.

We can rewrite the equations as

$$\begin{aligned} \frac{a}{b} = \frac{r_0}{r_1} &= a_1 + \frac{r_2}{r_1} = a_1 + \frac{1}{r_1/r_2}, \\ \frac{r_1}{r_2} &= a_2 + \frac{r_3}{r_2} = a_2 + \frac{1}{r_2/r_3}, \\ &\vdots \\ \frac{r_{n-3}}{r_{n-2}} &= a_{n-2} + \frac{r_{n-1}}{r_{n-2}} = a_{n-2} + \frac{1}{r_{n-2}/r_{n-1}}, \\ \frac{r_{n-2}}{r_{n-1}} &= a_{n-1} + \frac{r_n}{r_{n-1}} = a_{n-1} + \frac{1}{r_{n-1}/r_n}, \\ \frac{r_{n-1}}{r_n} &= a_n. \end{aligned}$$

We can substitute the value of r_1/r_2 in the first equation using the term in the second equation and get

$$\frac{a}{b} = a_1 + \frac{1}{a_2 + \frac{1}{r_2/r_3}}.$$

Similarly, we can substitute the value of r_2/r_3 and continuing like this, we obtain

$$\frac{a}{b} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots \cfrac{}{a_{n-1} + \frac{1}{a_n}}}}}.$$

Thus, $\frac{a}{b} = [a_1; a_2, \dots, a_n]$. □

Note that this representation is not unique.

From the identity $a_n = (a_n - 1) + \frac{1}{1}$ we get that

$$[a_0; a_1, \dots, a_n] = [a_0; a_1, \dots, a_{n-1}, a_n - 1, 1],$$

whenever $a_n > 1$.

Example 10.12. *We have that*

$$\frac{7}{11} = [0; 1, 1, 1, 3] = [0; 1, 1, 1, 2, 1].$$

In fact, one can show that every rational number allows for exactly two representations as finite simple continued fractions, one having an odd number of terms, the other with an even number of terms.

Definition 10.13. Let $[a_0; a_1 \dots, a_n]$ be a finite continued fraction and let $k \in \{0, \dots, n\}$.

The kth *convergent* is a given by the partial continued fraction $c_k = [a_0; a_1 \dots, a_k]$.

We give an algorithm to compute $c_k = \frac{p_k}{q_k}$.

Theorem 10.14. *Let $a_0, \dots, a_n$ be real numbers and $a_j > 0$ for $j > 0$. We define the sequence $p_0, \dots, p_n$ and $q_0, \dots, q_n$ recursively by*

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

for $k \in \{2, \dots, n\}$.

Then, $c_k = \frac{p_k}{q_k}$.

Proof. We prove this theorem with induction. For $k = 0$, we have

$$c_0 = [a_0] = \frac{p_0}{q_0}.$$

For $k = 1$, we get

$$c_1 = [a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{p_1}{q_1}.$$

Assume the statement holds for k, where $2 \leq k < n.$
That is

$$c_k = [a_0; a_1, \ldots, a_k] = \frac{p_k}{q_k} = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}}.$$

We note that by definition of convergents we have that

$$c_k = [a_0; a_1, \ldots, a_k] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \cfrac{}{a_k}}},$$

while

$$c_{k+1} = [a_0; a_1, \ldots, a_k, a_{k+1}] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots \cfrac{}{a_k + \frac{1}{a_{k+1}}}}} = [a_0; a_1, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}].$$

Thus,

$$\begin{aligned} c_{k+1} &= [a_0; a_1, \ldots, a_k, a_{k+1}] = [a_0; a_1, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}] \\ &= \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} \\ &= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} \\ &= \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} \\ &= \frac{p_{k+1}}{q_{k+1}}. \end{aligned}$$

□

Example 10.15. *Let us consider* $\frac{173}{55} = [3; 6, 1, 7]$. *We can compute the sequences* p_i, q_i *as*

$$\begin{aligned} p_0 &= 3, & q_0 &= 1, \\ p_1 &= 3 \cdot 6 + 1 = 19, & q_1 &= 6, \\ p_2 &= 1 \cdot 19 + 3 = 22, & q_2 &= 1 \cdot 6 + 1 = 7, \\ p_3 &= 7 \cdot 22 + 19 = 173, & q_3 &= 7 \cdot 7 + 6 = 55. \end{aligned}$$

Hence the convergents are given by

$$\begin{aligned} c_0 &= \frac{p_0}{q_0} = \frac{3}{1} = 3, \\ c_1 &= \frac{p_1}{q_1} = \frac{19}{6}, \\ c_2 &= \frac{p_2}{q_2} = \frac{22}{7}, \\ c_3 &= \frac{p_3}{q_3} = \frac{173}{55}. \end{aligned}$$

Theorem 10.16. *Let $c_k = \frac{p_k}{q_k}$ be the kth convergent of the finite continued fraction $[a_0; a_1, \ldots, a_n]$, where $k \in \{1, \ldots, n\}$. Then*

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$

Proof. We again use induction.

For $k = 1$, we have

$$p_1 q_0 - p_0 q_1 = (a_0 a_1 + 1) \cdot 1 - a_0 a_1 = 1 = (-1)^{1-1}.$$

Assume that the claim is true for an integer $k \in \{1, \ldots, n-1\}$, that is

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$

Then

$$\begin{aligned} p_{k+1} q_k - p_k q_{k+1} &= (a_{k+1} p_k + p_{k-1}) q_k - p_k (a_{k+1} q_k + q_{k-1}) \\ &= p_{k-1} q_k - p_k q_{k-1} = -(-1)^{k-1} = (-1)^k. \end{aligned}$$

□

Example 10.17. *Let us consider the same example from before: $\frac{173}{55} = [3; 6, 1, 7]$. Then*

$$\begin{aligned} p_0 q_1 - p_1 q_0 &= 3 \cdot 6 - 19 \cdot 1 = -1, \\ p_1 q_2 - p_2 q_1 &= 19 \cdot 7 - 22 \cdot 6 = 1, \\ p_2 q_3 - p_3 q_2 &= 22 \cdot 55 - 173 \cdot 7 = -1. \end{aligned}$$

As another consequence, we see that the convergents of a finite simple continued fraction are in lowest terms, i.e., $c_k = \frac{p_k}{q_k}$ with $\gcd(p_k, q_k) = 1$.

Corollary 10.18. *Let $c_k = \frac{p_k}{q_k}$ be the kth convergent of the finite simple continued fraction $[a_0; a_1, \ldots, a_n]$. Then $\gcd(p_k, q_k) = 1$.*

Proof. Let $d = \gcd(p_k, q_k)$. Since

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1},$$

we must have $d \mid (-1)^{k-1}$ and thus $d = 1$. □

Corollary 10.19. *Let $c_k = \frac{p_k}{q_k}$ be the kth convergent of the finite simple continued fraction $[a_0; a_1, \dots, a_n]$. Then*

$$c_k - c_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$$

for all $k \in \{1, \dots, n\}$. Further,

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

for all $k \in \{2, \dots, n\}$.

Proof. We write

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

Similarly,

$$c_k - c_{k-2} = \frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{p_k q_{k-2} - p_{k-2} q_k}{q_k q_{k-2}}.$$

Since $p_k = a_k p_{k-1} + p_{k-2}$ and $q_k = a_k q_{k-1} + q_{k-2}$, we get that

$$\begin{aligned} p_k q_{k-2} - p_{k-2} q_k &= (a_k p_{k-1} + p_{k-2}) q_{k-2} - p_{k-2}(a_k q_{k-1} + q_{k-2}) \\ &= a_k(p_{k-1} q_{k-2} - p_{k-2} q_{k-1}) = a_k(-1)^{k-2} = a_k(-1)^k. \end{aligned}$$

□

The convergents are nesting the continued fraction:

Theorem 10.20. *Let c_k be the kth convergent of the finite simple continued fraction $[a_0; a_1, \dots, a_n]$. Then,*

$$c_0 < c_2 < c_4 < \cdots < c_5 < c_3 < c_1.$$

Proof. From Corollary 10.19, we get that

$$c_k - c_{k-2} = \frac{a_k(-1)^k}{q_k q_{k-2}}.$$

Thus, when k is odd, we have $c_k - c_{k-2} = -\frac{a_k}{q_k q_{k-2}}$ and thus $c_k < c_{k-2}$ and when k is even, we get $c_k > c_{k-2}$. Thus, $c_1 > c_3 > c_5 > \dots$ and $c_0 < c_2 < c_4 < \dots$.

It remains to show that $c_{2i+1} > c_{2i}$ for all $i \geq 0$.

Again, using Corollary 10.19, we have

$$c_{2i} - c_{2i-1} = \frac{(-1)^{2i-1}}{q_{2i} q_{2i-1}} < 0,$$

which implies $c_{2i-1} > c_{2i}$. We can compare any c_{2j} with $c_{2\ell-1}$ as

$$c_{2\ell-1} > c_{2\ell+2j-1} > c_{2\ell+2j} > c_{2\ell}.$$

□

Example 10.21. *Let us consider again* $\frac{173}{55} = [3; 5, 1, 7]$. *then*

$$c_0 = 3 < c_2 = \frac{22}{7} \sim 3.1428 < c_3 = \frac{173}{55} \sim 3.1454 < c_1 = \frac{19}{6} \sim 3.166.$$

Thus, convergents provide good approximations of the value of the continued fraction.

Exercise 10.22. *Show that for all positive integers* k *we have that* $q_k \geq k$.

10.3 Infinite Continued Fractions

What happens if we let a continued fraction go on forever?

We start with a sequence of real numbers $a_0, a_1 \ldots$, with $a_i > 0$ for $i > 0$ and define recursively

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

Definition 10.23. A *continued fraction* is of the form

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}$$

and we write it as $[a_0; a_1, a_2 \ldots]$.

Theorem 10.24. *Let* a_i *be integers and* $a_j > 0$ *for* $j > 0$ *and let* $c_k = [a_0; a_1, \ldots, a_k]$ *be the kth convergent. Then, there exists some real number* α *such that*

$$\lim_{k \to \infty} c_k = \alpha.$$

Proof. We will show that the infinite sequence of even numbered $a_0, a_2, \ldots$, is increasing and has an upper bound, i.e., $a_0 < a_2 < \ldots < a$ and the odd numbered $a_1, a_3, \ldots$, is decreasing and has a lower bound, i.e., $a_1 > a_3 > \ldots > a$.

Let m be an even positive integer, then due to Theorem 10.20, we get that

$$c_1 > c_3 > \ldots > c_{m-1}, \quad c_m > \ldots > c_2 > c_0$$

and $c_{2i} < c_{2j+1}$ if $2i \leq m$ and $2j + 1 < m$. By considering all possible values for m, we get that

$$c_1 > c_3 > \ldots > c_{2n-1} > c_{2n+1} > \ldots, \quad \ldots > c_{2n} > c_{2n-1} > \ldots > c_2 > c_0$$

and $c_{2i} > c_{2j+1}$ for all i, j.

Thus, $\lim\limits_{i \to \infty} c_{2i+1} = \alpha_1$ and $\lim\limits_{i \to \infty} c_{2i} = \alpha_2$. We now want to show that $\alpha_1 = \alpha_2 = \alpha$.

Using Corollary 10.19, we have that

$$c_{2n+1} - c_{2n} = \frac{(-1)^{(2n+1)-1}}{q_{2n+1}q_{2n}} = \frac{1}{q_{2n+1}q_{2n}}.$$

Due to Exercise 10.22, we have that $q_k \geq k$, and we get

$$\frac{1}{q_{2n+1}q_{2n}} < \frac{1}{(2n+1)2n}$$

and thus $c_{2n+1} - c_{2n}$ tends to 0. Hence

$$\lim_{n\to\infty}(c_{2n+1} - c_{2n}) = \lim_{n\to\infty} c_{2n+1} - \lim_{n\to\infty} c_{2n} = 0.$$

□

While finite simple continued fractions are rationals, we now show that infinite simple continued fractions are irrational.

Theorem 10.25. *Let a_i be integers and $a_j > 0$ for $j > 0$. Then $[a_0; a_1, \ldots]$ is irrational.*

Proof. Let $\alpha = [a_0; a_1, \ldots]$ and let $c_k = \frac{p_k}{q_k} = [a_0; a_1, \ldots, a_k]$ be the kth convergent. For a positive integer n, we have due to Theorem 10.24 that $c_{2n} < \alpha < c_{2n+1}$ and hence

$$0 < \alpha - c_{2n} < c_{2n+1} - c_{2n}.$$

Due to Corollary 10.19, however, we have

$$c_{2n+1} - c_{2n} = \frac{1}{q_{2n+1}q_{2n}}$$

implying that

$$0 < \alpha - c_{2n} = \alpha - \frac{p_{2n}}{q_{2n}} < \frac{1}{q_{2n+1}q_{2n}}$$

and thus

$$0 < \alpha q_{2n} - p_{2n} < \frac{1}{q_{2n+1}}.$$

If $\alpha = \frac{a}{b}$ for a, b integers and $b \neq 0$, then

$$0 < \frac{aq_{2n}}{b} - p_{2n} < \frac{1}{q_{2n+1}}$$

and in turn

$$0 < aq_{2n} - bp_{2n} < \frac{b}{q_{2n+1}},$$

where $aq_{2n} - bp_{2n}$ is an integer.

However, as $q_{2n+1} \geq 2n + 1$ (due to Exercise 10.22), for each integer n there exists an integer N such that $q_{2N+1} > b$, so $\frac{b}{q_{2N+1}} < 1$. This leads to a contradiction as there is no integer $aq_{2n} - bp_{2n}$ with

$$0 < aq_{2n} - bp_{2n} < 1.$$

□

We now want to show also the other direction, i.e., every irrational number can be expressed as infinite simple continued fraction.

We can do the same as for rational numbers, with the simple tweak to compute always $\lfloor \cdot \rfloor$.

Let us consider $\alpha \in \mathbb{R}$. Then

$$x_0 = \alpha = \lfloor x_0 \rfloor + r_1 = \lfloor x_0 \rfloor + \frac{1}{\frac{1}{r_1}}$$

for $0 \leq r_1 < 1$. We can continue by setting $x_1 = \frac{1}{r_1} > 1$ and

$$x_1 = \lfloor x_1 \rfloor + r_2 = \lfloor x_1 \rfloor + \frac{1}{\frac{1}{r_2}}$$

and so on. That is for k a positive integer we define

$$a_k = \lfloor x_k \rfloor, \quad x_{k+1} = \frac{1}{x_k - a_k}.$$

Theorem 10.26. *Let α be an irrational number and consider $a_k = \lfloor x_k \rfloor$ where $x_{k+1} = \frac{1}{x_k - a_k}$ for $k \geq 0$, where $x_0 = \alpha$. Then $\alpha = [a_0; a_1, \ldots]$.*

Proof. From the definition of a_k we see that it is an integer for every k.

We now show that x_k is irrational for every k and thus $x_{k+1} = \frac{1}{x_k - a_k}$ exists as $x_k \neq a_k = \lfloor x_k \rfloor$. In fact, for $k = 0$ we have $x_0 = \alpha$ is irrational and thus $a_0 = \lfloor x_0 \rfloor \neq x_0$ and hence $x_1 = \frac{1}{x_0 - a_0}$ exists.

Assume that x_k is irrational. Then,

$$x_{k+1} = \frac{1}{x_k - a_k}$$

implies that $x_k = a_k + \frac{1}{x_{k+1}}$ and hence x_{k+1} is again irrational and hence $a_{k+1} = \lfloor x_{k+1} \rfloor \neq x_{k+1}$.

By the recursive definition we get that

$$\begin{aligned} \alpha = x_0 &= a_0 + \frac{1}{x_1} = [a_0; x_1] \\ &= a_0 + \frac{1}{a_1 + \frac{1}{x_2}} = [a_0; a_1, x_2] \\ &\vdots \\ &= [a_0; a_1, \ldots, a_k, x_{k+1}]. \end{aligned}$$

We are left with showing that $[a_0; a_1, \ldots, a_k, x_{k+1}]$ tends to α.

By Theorem 10.14, we get that

$$\alpha = [a_0; a_1, \ldots, a_k, x_{k+1}] = \frac{x_{k+1} p_k + p_{k-1}}{x_{k+1} q_k + q_{k-1}},$$

where $c_k = \frac{p_k}{q_k} = [a_0; a_1, \ldots, a_k]$ is the kth convergent. Hence

$$\begin{aligned}
\alpha - c_k &= \frac{x_{k+1}p_k + p_{k-1}}{x_{k+1}q_k + q_{k-1}} - \frac{p_k}{q_k} \\
&= \frac{p_{k-1}q_k - p_k q_{k-1}}{(x_{k+1}q_k + q_{k-1})q_k} \\
&= \frac{(-1)^k}{(x_{k+1}q_k + q_{k-1})q_k}.
\end{aligned}$$

Since $x_{k+1}q_k + q_{k-1} > a_{k+1}q_k + q_{k-1} = q_{k+1}$, we get that

$$|\alpha - c_k| < \frac{1}{q_k q_{k+1}}.$$

Using again Exercise 10.22, we get that $\frac{1}{q_k q_{k+1}}$ tends to zero. Thus, c_k tends to α, i.e.,

$$\lim_{k\to\infty} c_k = \lim_{k\to\infty} [a_0; a_1, \ldots, a_k] = [a_0; a_1, \ldots] = \alpha.$$

□

The representation of an irrational number as infinite simple continued fraction is also unique.

Theorem 10.27. *Let α be an irrational number. If $\alpha = [a_0; a_1, \ldots] = [b_0; b_1, \ldots]$ then $a_k = b_k$ for all $k \geq 0$.*

Proof. Since $c_0 = a_0, c_1 = a_0 + \frac{a}{a_1}$ we get by Theorem 10.20

$$a_0 < \alpha < a_0 + \frac{1}{a_1}.$$

We can write

$$\begin{aligned}
\alpha = [a_0; a_1, \ldots] &= \lim_{k\to\infty} [a_0; a_1, \ldots, a_k] \\
&= \lim_{k\to\infty} \left(a_0 + \frac{1}{[a_1; a_2, \ldots, a_k]} \right) \\
&= a_0 + \frac{1}{\lim_{k\to\infty} [a_1; a_2, \ldots, a_k]} \\
&= a_0 + \frac{1}{[a_1; a_2, \ldots]}.
\end{aligned}$$

Let $[a_0; a_1, \ldots] = [b_0; b_1, \ldots]$. We show by induction that $a_k = b_k$ for all $k \geq 0$. Note that for $k = 0$ we have $a_0 = \lfloor \alpha \rfloor = b_0$ and thus

$$a_0 + \frac{1}{[a_1; a_2, \ldots]} = b_0 + \frac{1}{[b_1; b_2, \ldots]}$$

which implies $[a_1; a_2, \ldots] = [b_1; b_2, \ldots]$. We can then repeat the argument for $[a_1; a_2, \ldots] = [b_1; b_2, \ldots]$, getting $a_1 = b_1$.

Assume that $a_k = b_k$ for some k and $[a_{k+1}; a_{k+2}, \ldots] = [b_{k+1}; b_{k+2}, \ldots]$. Using the same argument, we get that $a_{k+1} = b_{k+1}$ and $[a_{k+2}; a_{k+3}, \ldots] = [b_{k+2}; b_{k+3}, \ldots]$.

□

Example 10.28. *Let $\alpha = x_0 = \sqrt{3}$, then*

$$\begin{aligned} a_0 &= \lfloor x_0 \rfloor = 1, \quad r_1 = \sqrt{3} - 1 \quad \text{and} \quad x_1 = \frac{\sqrt{3}+1}{2}, \\ a_1 &= \lfloor x_1 \rfloor = 1, \quad r_2 = \frac{\sqrt{3}+1}{2} - 1 \quad \text{and} \quad x_2 = \sqrt{3}+1, \\ a_2 &= \lfloor x_2 \rfloor = 2, \quad r_3 = \sqrt{3} - 1 \quad \text{and} \quad x_3 = \frac{\sqrt{3}+1}{2}, \end{aligned}$$

since $x_3 = x_1$ we get a periodicity. Thus, $\sqrt{3} = [1; \overline{1, 2}]$. Since $[\overline{1, 2}] = \sqrt{3} - 1$ we can write

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

The convergents are a good approximation for α.

Theorem 10.29 (Dirichlet's Theorem on Diophantine Approximation). *If α is an irrational number, then there exist infinitely many rational numbers $\frac{p}{q}$ such that*

$$|\alpha - \frac{p}{q}| < \frac{1}{q^2}.$$

Proof. Let $c_k = \frac{p_k}{q_k}$ be the kth convergent of α. Then, by the proof of Theorem 10.26, we get that the infinitely many convergents are such rational approximations, as

$$|\alpha - \frac{p_k}{q_k}| < \frac{1}{q_k q_{k+1}}.$$

Since $q_k < q_{k+1}$, we immediately get the claim. □

There also exists the converse result:

Theorem 10.30 (Criteria of Legendre). *Let $\alpha \in \mathbb{R}$, $\frac{p}{q} \in \mathbb{Q}$. If*

$$|\alpha - \frac{p}{q}| < \frac{1}{2q^2},$$

then $\frac{p}{q}$ is a convergent of α.

In order to prove this, we first need to show the following.

Proposition 10.31. *Let $\alpha \in \mathbb{R}$ and let $c_k = \frac{p_k}{q_k}$ be the kth convergent. If r, s are integers with $s > 0$ and k is a positive integer with*

$$|s\alpha - r| < |q_k\alpha - p_k|,$$

then $s \geq q_{k+1}$.

Proof. Let us assume that $|s\alpha - r| < |q_k\alpha - p_k|$, but $1 \leq s < q_{k+1}$. We can write

$$\begin{aligned} p_k x + p_{k+1} y &= r, \\ q_k x + q_{k+1} y &= s. \end{aligned}$$

The existence of (x, y) follows from the fact that $\begin{pmatrix} p_k & p_{k+1} \\ q_k & q_{k+1} \end{pmatrix}$ has determinant $p_k q_{k+1} - p_{k+1} q_k = (-1)^{k-1}$ which means the matrix is invertible in $\mathbb{Z}$. Thus,

$$\begin{aligned} rq_k - sp_k &= y(p_{k+1}q_k - p_k q_{k+1}), \\ sp_{k+1} - rq_{k+1} &= x(p_{k+1}q_k - p_k q_{k+1}). \end{aligned}$$

By Theorem 10.16, we have

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

so that

$$y = (-1)^k (rq_k - sp_k).$$

Similarly, we get

$$x = (-1)^k (sp_{k+1} - rq_{k+1}).$$

If $x = 0$, then $sp_{k+1} = rq_{k+1}$, which implies $q_{k+1} \mid s$ (as $\gcd(p_{k+1}, q_{k+1}) = 1$), which contradicts our assumption $s < q_{k+1}$.

If $y = 0$, then $r = p_k x, s = q_k x$ so that

$$|s\alpha - r| = |x||q_k\alpha - p_k| \geq |q_k\alpha - p_k|,$$

which is also a contradiction.

Now we show that x, y have opposite signs. If $y < 0$, then $x > 0$ since $q_k x = s - q_{k+1} y > 0$ and $q_k > 0$. If $y > 0$, then $x < 0$ since $q_{k+1} y \geq q_{k+1} > s$ and thus $q_k x = s - q_{k+1} y < 0$.

By Theorem 10.20, we know that either $\frac{p_k}{q_k} < \alpha < \frac{p_{k+1}}{q_{k+1}}$ or $\frac{p_{k+1}}{q_{k+1}} < \alpha < \frac{p_k}{q_k}$. In either case, $q_k\alpha - p_k$ and $q_{k+1}\alpha - p_{k+1}$ have opposite signs.

We can write

$$\begin{aligned} |s\alpha - r| &= |(q_k x + q_{k+1} y)\alpha - (p_k x + p_{k+1} y)| \\ &= |x(q_k\alpha - p_k) + y(q_{k+1}\alpha - p_{k+1})|. \end{aligned}$$

Together with the fact that x, y have opposite signs and $q_k\alpha - p_k$ and $q_{k+1}\alpha - p_{k+1}$ have opposite signs, we get that $x(q_k\alpha - p_k)$ and $y(q_{k+1}\alpha - p_{k+1})$ have the same sign. Thus,

$$\begin{aligned}|s\alpha - r| &= |x||q_k\alpha - p_k| + |y||q_{k+1}\alpha - p_{k+1}| \\ &\geq |x||q_k\alpha - p_k| \geq |q_k\alpha - p_k|,\end{aligned}$$

which is a contradiction.

□

Corollary 10.32. *Let α be an irrational number and $c_k = \frac{p_k}{q_k}$ be the kth convergent. If r, s are integers with $s > 0$ and k is a positive integer such that*

$$|\alpha - \frac{r}{s}| < |\alpha - \frac{p_k}{q_k}|,$$

then $s > q_k$.

Proof. Assume by contradiction that $|\alpha - \frac{r}{s}| < |\alpha - \frac{p_k}{q_k}|$, but $s \leq q_k$. Thus,

$$s|\alpha - \frac{r}{s}| < q_k|\alpha - \frac{p_k}{q_k}|$$

and hence

$$|s\alpha - r| < |q_k\alpha - p_k|,$$

which contradicts Proposition 10.31. □

We are now ready to prove Legendre's criteria.

Proof. Assume by contradiction that $\frac{p}{q}$ is not a convergent. Then there exist successive convergents $\frac{p_k}{q_k}, \frac{p_{k+1}}{q_{k+1}}$ such that $q_k \leq q < q_{k+1}$. Due to Proposition 10.31, we get

$$|q_k\alpha - p_k| \leq |q\alpha - p| = q|\alpha - \frac{p}{q}| < \frac{1}{2q}.$$

We can divide by q_k to get

$$|\alpha - \frac{p_k}{q_k}| < \frac{1}{2qq_k}.$$

Since $|qp_k - pq_k| \geq 1$ (since else $\frac{p}{q} = \frac{p_k}{q_k}$), we get that

$$\begin{aligned}\frac{1}{qq_k} \leq \frac{|qp_k - pq_k|}{qq_k} &= |\frac{p_k}{q_k} - \frac{p}{q}| = \left|-\left(\alpha - \frac{p_k}{q_k}\right) + \left(\alpha - \frac{p}{q}\right)\right| \\ &\leq |\alpha - \frac{p_k}{q_k}| + |\alpha - \frac{p}{q}| < \frac{1}{2qq_k} + \frac{1}{2q^2}.\end{aligned}$$

Thus, $\frac{1}{2qq_k} < \frac{1}{2q^2}$ and in turn $2qq_k > 2q^2$, contradicting that $q \geq q_k$.

□

10.4 Attack on RSA

Apart from approximating real numbers with rationals, continued fractions also find applications in cryptography.

We can use a version of Legendre's criteria for rational numbers, saying that: if

$$|\frac{a}{b} - \frac{p}{q}| \leq \frac{1}{2q^2},$$

then $\frac{p}{q}$ is a convergent of $\frac{a}{b}$.

This result has been used by Wiener to attack the RSA cryptosystem whenever the decryption exponent d is small.

Theorem 10.33 (Wiener's Theorem)**.** *Let $p, q \in \mathcal{P}$ with $q < p < 2q$ and $n = pq$. Let $e < \varphi(n)$ be coprime to $\varphi(n)$ and $d \equiv e^{-1} \mod \varphi(n)$. If $d < \frac{n^{1/4}}{3}$, then given n, e one can efficiently recover p, q.*

Efficiently in this theorem refers to $\mathcal{O}(\log(n)^3)$.

Proof. Since $ed \equiv 1 \mod \varphi(n)$, there exists some $b \in \mathbb{Z}$ such that $ed - b\varphi(n) = 1$.

Dividing both sides with $d\varphi(n)$, we get

$$\frac{e}{\varphi(n)} - \frac{b}{d} = \frac{1}{d\varphi(n)}.$$

Since $q < p$ we also get that $q < n^{1/2}$ and since $p < 2q$

$$p + q - 1 \leq 2q + q - 1 = 3q - 1 < 3\sqrt{n}.$$

Note that $\varphi(n) = (p-1)(q-1) = n - p - q + 1$, thus

$$n - \varphi(n) = p + q - 1 < 3\sqrt{n}.$$

This means, $\frac{b}{d}$ is a good approximation of $\frac{e}{n}$ as

$$\begin{aligned} |\frac{e}{n} - \frac{b}{d}| &= |\frac{ed - bn}{nd}| \\ &= |\frac{(ed - b\varphi(n)) - (bn - b\varphi(n))}{nd}| \\ &= |\frac{1 - b(n - \varphi(n))}{nd}| \leq \frac{3b\sqrt{n}}{nd} = \frac{3b}{d\sqrt{n}}. \end{aligned}$$

As $e < \varphi(n)$ we get that $be < b\varphi(n) = ed - 1 < ed$. Hence, $b < d < \frac{n^{1/4}}{3}$. It follows that

$$|\frac{e}{n} - \frac{b}{d}| \leq \frac{3b\sqrt{n}}{nd} \leq \frac{3\frac{n^{1/4}}{3}\sqrt{n}}{nd} = \frac{n^{3/4}}{nd} = \frac{1}{dn^{1/4}} < \frac{1}{2d^2},$$

where the last inequality used $2d < n^{1/4}$.

Hence, we can apply Legendre's criteria and get that $\frac{b}{d}$ is a convergent of $\frac{e}{n}$. Since both e, n are public, we now only have to compute the convergents of $\frac{e}{n}$ in order to find candidates for $\frac{b}{d}$. We use a candidate for $\frac{b}{d}$ to compute a candidate for $\varphi(n) = \frac{ed-1}{b}$. We then use the trick from Proposition 8.2 to factor n.

□

Recall the revised version of RSA, using the Carmichael function $\lambda(n) = \text{lcm}(p-1, q-1)$ instead of $\varphi(n) = (p-1)(q-1)$.

Exercise 10.34. *Prove Wiener's theorem using $\lambda(n)$ instead of $\varphi(n)$.*

Example 10.35. *Let $n = 6667$ and $e = 4331$. We can compute the convergents $\frac{p_i}{q_i}$ of $\frac{e}{n}$ and test if $\frac{eq_i-1}{p_i}$ is $\varphi(n)$.*

We start with computing the continued fraction using the Euclidean algorithm

$$\frac{4331}{6667} = [0; 1, 1, 1, 5, 1, 5, 1, 2, 5, 3].$$

Then the sequences p_i, q_i as

$$p_0 = a_0 = 0, \qquad q_0 = 1.$$

Since $q_0 = 1$ it cannot be d, since $e \neq 1$. Thus, we continue computing

$$p_1 = a_1 p_0 + 1 = 1, \qquad q_1 = a_1 = 1.$$

Again, $q_1 = 1$ cannot be d, since $e \neq 1$.

Then

$$p_2 = a_2 \cdot p_1 + p_0 = 1, \qquad q_2 = a_2 \cdot q_1 + q_0 = 2.$$

Also this case we can exclude as $d = 2$ is not a unit modulo $\varphi(n)$ (which is even).

Thus we compute

$$p_3 = a_3 \cdot p_2 + p_1 = 2, \qquad q_3 = a_3 \cdot q_2 + q_1 = 3.$$

Now we can check if

$$\frac{eq_3 - 1}{p_3} = 6496$$

is $\varphi(n)$ by solving

$$n - \varphi(n) + 1 = p + q = 6667 - 6469 + 1 = 172,$$
$$\sqrt{(p+q)^2 - 4n} = p - q = \sqrt{172^2 - 4 \cdot 6667} = 54,$$

thus $(p+q) + (p-q) = 172 + 54 = 226 = 2p$ and thus $p = 113$ and $q = 113 - 54 = 59$.

Exercise 10.36. *Perform the same attack as in Example 10.35 but using $\lambda(n)$.*

An easy countermeasure against Wiener's attack is to choose e small enough (which also speeds up the encryption process) such that $d >> \frac{n^{1/4}}{3}$.

10.5 Periodic Continued Fractions

Definition 10.37. A simple infinite continued fractions is called *periodic*, if there exist positive integers k, N such that for all $n \geq N$ we have $a_n = a_{n+k}$. We then write $[a_0; a_1, \ldots, a_{N-1}, \overline{a_N, \ldots, a_{N+k-1}}]$.

We have seen before that a representation to the base b which is periodic gives a rational number. For continued fractions, we get special irrational numbers.

Definition 10.38. We say that a real number α is *quadratic irrational*, if α is irrational and a root of a quadratic polynomial with integer coefficients, that is

$$a\alpha^2 + b\alpha + c = 0,$$

where $a, b, c \in \mathbb{Z}$ and $a \neq 0$.

Example 10.39. *Let* $\alpha = 2 + \sqrt{3}$. *Since* $\alpha^2 - 4\alpha + 1 = (7 + 4\sqrt{3}) - 4(2 + \sqrt{3}) + 1 = 0$. *Thus,* α *is quadratic irrational.*

We now show that an infinite simple continued fraction of α is periodic if and only if α is quadratic irrational.

Clearly, there are several roots of quadratic polynomials that are rationals and we can exclude.

Lemma 10.40. *Let* α *be a real number. Then* α *is quadratic irrational if and only if there exist integers* a, b, c *with* $b > 0$ *and* $c \neq 0$ *and* b *not a perfect square, such that*

$$\alpha = \frac{a + \sqrt{b}}{c}.$$

Proof. If α is quadratic irrational, then there exist integers A, B, C such that

$$A\alpha^2 + B\alpha + C = 0.$$

From the quadratic formula we know that

$$\alpha = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}.$$

Since α is a real number, we have that $B^2 - 4AC > 0$ and since α is irrational, we want that $B^2 - 4AC$ is not a square and thus $A \neq 0$. Define $a = -B, b = B^2 - 4AC$ and $c = 2A$ we get the required form

$$\alpha = \frac{a + \sqrt{b}}{c}.$$

Conversely, if $\alpha = \frac{a+\sqrt{b}}{c}$, where $a, b, c \in \mathbb{Z}$ and $b > 0$ is not a square and $c \neq 0$, we get by Theorem 2.2, that α is irrational. Since further

$$c^2\alpha^2 - 2ac\alpha + (a^2 - b) = 0,$$

α is quadratic irrational. □

Lemma 10.41. *If α is a quadratic irrational number and $r, s, t, u \in \mathbb{Z}$ then $\frac{r\alpha+s}{t\alpha+u}$ is either rational or quadratic irrational.*

Proof. From Lemma 10.40, there exist integers a, b, c such that $b > 0$ is not a square and $c \neq 0$ and

$$\alpha = \frac{a+\sqrt{b}}{c}.$$

Thus,

$$\begin{aligned}
\frac{r\alpha+s}{t\alpha+u} &= \frac{\frac{r(a+\sqrt{b})}{c}+s}{\frac{t(a+\sqrt{b})}{c}+u} \\
&= \frac{(ar+cs)+r\sqrt{b}}{(at+cu)+t\sqrt{b}} \\
&= \frac{((ar+cs)+r\sqrt{b})((at+cu)-t\sqrt{b})}{((at+cu)+t\sqrt{b})((at+cu)-t\sqrt{b})} \\
&= \frac{((ar+cs)(at+cu)-rtb)+(r(at+cu)-t(ar+cs))\sqrt{b}}{(at+cu)^2-t^2b}.
\end{aligned}$$

Thus, by Lemma 10.40, $\frac{r\alpha+s}{t\alpha+u}$ is quadratic irrational, unless $r(at+cu)-t(ar+cs)=0$, in which case the number is rational. □

Example 10.42. *Let us consider the constant sequence $a_i = 1$ for all i. That is*

$$\alpha = 1 + \frac{1}{1+\frac{1}{1+\cdots}}.$$

Since $\alpha = 1 + \frac{1}{\alpha}$ we can solve for α, getting $\alpha = \frac{1+\sqrt{5}}{2}$, the golden ratio. The convergents are defined through the Fibonacci sequence, as $p_i = F_{i+2}, q_i = F_{i+1}$, where the Fibonacci sequence is defined as $F_0 = 0, F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$.

We are now ready to prove our main result.

Theorem 10.43 (Lagrange's Theorem or the Continued Fractions Theorem)**.** *The infinite simple continued fraction of an irrational number is periodic if and only if the number is quadratic irrational.*

Proof. We start by proving that a periodic simple continued fraction is quadratic irrational.

Let $\alpha = [a_0; a_1, \ldots, a_{N-1}, \overline{a_N, \ldots, a_{N+k}}]$. Define

$$\beta = [\overline{a_N; a_{N+1}, \ldots, a_{N+k}}] = [a_N; a_{N+1}, \ldots, a_{N+k}, \beta].$$

Let c_k be the convergent of $[a_N; a_{N+1}, \ldots, a_{N+k}]$, then by Theorem 10.14, we get that

$$\beta = \frac{\beta p_k + p_{k-1}}{\beta q_k + q_{k-1}}.$$

Since the continued fraction of β is infinite, β is irrational and

$$q_k\beta^2 + (q_{k-1} - p_k)\beta - p_{k-1} = 0,$$

thus β is quadratic irrational. Let c'_k now be the convergents of the continued fraction $[a_0; a_1, \ldots, a_{N-1}]$ Since $\alpha = [a_0; a_1, \ldots, a_{N-1}, \beta]$, we get from Theorem 10.14 that

$$\alpha = \frac{\beta p'_{N-1} + p'_{N-2}}{\beta q'_{N-1} + q'_{N-2}}.$$

Thus, since β is quadratic irrational we can apply Lemma 10.41 and get that α is quadratic irrational.

In order to show the other direction, that is: any quadratic irrational number is a simple periodic continued fraction, we require two additional results. Thus the proof is continued afterwards. □

Example 10.44. *Let $\alpha = [3; \overline{1, 2}]$. Define $\beta = [\overline{1; 2}]$, so that $\alpha = [3; \beta]$. Clearly, we have that $\beta = [1; 2, \beta]$, that is*

$$\beta = 1 + \frac{1}{2 + \frac{1}{\beta}} = \frac{3\beta + 1}{2\beta + 1}.$$

Thus, we get $2\beta^2 - 2\beta - 1 = 0$ and can solve this as

$$\beta = \frac{1 + \sqrt{3}}{2}.$$

Since $\alpha = 3 + \frac{1}{\beta}$ we get that

$$\alpha = 3 + \frac{2}{1 + \sqrt{3}} = 2 + \sqrt{3}.$$

Lemma 10.45. *If α is a quadratic irrational, then α can be written as*

$$\frac{P + \sqrt{d}}{Q},$$

where $P, Q, d \in \mathbb{Z}$ and $Q \neq 0, d > 0$ is not a square and $Q \mid (d - P^2)$.

Proof. This is almost the same statement as in Lemma 10.40, except for the part $Q \mid (d - P^2)$. Hence, Lemma 10.40 implies that

$$\alpha = \frac{a + \sqrt{b}}{c},$$

where $a, b, c \in \mathbb{Z}$ and $c \neq 0, b > 0$ is not a square. We multiply the numerator and the denominator with $|c|$ to get

$$\alpha = \frac{a|c| + \sqrt{bc^2}}{c|c|}.$$

Let $P = a|c|, Q = c|c|$ and $d = bc^2$. Then $P, Q, d \in \mathbb{Z}$ and $Q \neq 0$, $d > 0$ is not a square and finally $Q \mid (d - P^2)$ since

$$d - P^2 = bc^2 - a^2c^2 = c^2(b - a^2) = \pm Q(b - a^2).$$

□

Definition 10.46. Let $\alpha = \frac{a+\sqrt{b}}{c}$ be a quadratic irrational. The *conjugate* of α is $\alpha' = \frac{a-\sqrt{b}}{c}$.

Lemma 10.47. *If the quadratic irrational α is the root of the polynomial $Ax^2 + Bx + C = 0$, then α' is the second root.*

Proof. From the quadratic formula, we have that $Ax^2 + Bx + C = 0$ has the two roots

$$\frac{-B \pm \sqrt{B^2 - 4AC}}{2A}.$$

If α is a root, then $\alpha = \frac{a+\sqrt{b}}{c}$, where $a = -B, b = B^2 - 4AC$ and $c = 2A$. Thus, $\alpha' = \frac{a-\sqrt{b}}{c}$ is the second root. □

Lemma 10.48. *If $\alpha_1 = \frac{a_1+b_1\sqrt{d}}{c_1}, \alpha_2 = \frac{a_2+b_2\sqrt{d}}{c_2}$, are quadratic irrationals or rationals, then*

1. $(\alpha_1 + \alpha_2)' = \alpha_1' + \alpha_2'$.
2. $(\alpha_1 - \alpha_2)' = \alpha_1' - \alpha_2'$.
3. $(\alpha_1\alpha_2)' = \alpha_1'\alpha_2'$.
4. $\left(\frac{\alpha_1}{\alpha_2}\right)' = \frac{\alpha_1'}{\alpha_2'}$.

Exercise 10.49. *Prove Lemma 10.48.*

We now give an algorithm for finding the periodic continued fraction.

Theorem 10.50. *Let α be a quadratic irrational number, and write $\alpha = \frac{P_0+\sqrt{d}}{Q_0}$, where $Q_0 \neq 0$, $d > 0$ is not a square and $Q_0 \mid (d - P_0^2)$. Define recursively*

$$\begin{aligned} \alpha_k &= \frac{P_k + \sqrt{d}}{Q_k}, \\ a_k &= \lfloor \alpha_k \rfloor, \\ P_{k+1} &= a_k Q_k - P_k, \\ Q_{k+1} &= \frac{d - P_{k+1}^2}{Q_k}, \end{aligned}$$

for $k \geq 0$. Then $\alpha = [a_0; a_1, \ldots]$.

Proof. We use induction to show that $P_k, Q_k \in \mathbb{Z}$ and $Q_k \neq 0$, $Q_k \mid (d - P_k^2)$.

For $k = 0$, Lemma 10.45 implies $P_0, Q_0 \in \mathbb{Z}$ and $Q_0 \neq 0$, $Q_0 \mid (d - P_0^2)$.

Assume that for k the statement is true, i.e., $P_k, Q_k \in \mathbb{Z}$ and $Q_k \neq 0$, $Q_k \mid (d - P_k^2)$.

Then

$$P_{k+1} = a_k Q_k - P_k \in \mathbb{Z}.$$

Further,

$$Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k} = \frac{d - (a_k Q_k - P_k)^2}{Q_k} = \frac{d - P_k^2}{Q_k} + 2a_k P_k - a_k^2 Q_k.$$

Since $Q_k \mid (d - P_k^2)$ we get that $Q_{k+1} \in \mathbb{Z}$. Since d is not a square, we see that $d \neq P_{k+1}^2$ and $Q_{k+1} = \frac{d-P_{k+1}^2}{Q_k} \neq 0$. From the definition of Q_{k+1} we also get the condition that $Q_{k+1} \mid (d - P_{k+1}^2)$.

Finally, we want to show that $\alpha = [a_0; a_1, \ldots]$. Using Theorem 10.26, we equivalently want to show that $\alpha_{k+1} = \frac{1}{\alpha_k - a_k}$.

We can write

$$\begin{aligned}
\alpha_k - a_k &= \frac{P_k + \sqrt{d}}{Q_k} - a_k \\
&= \frac{P_k + \sqrt{d} - a_k Q_k}{Q_k} \\
&= \frac{\sqrt{d} - P_{k+1}}{Q_k} \\
&= \frac{(\sqrt{d} - P_{k+1})(\sqrt{d} + P_{k+1})}{Q_k(\sqrt{d} + P_{k+1})} \\
&= \frac{d - P_{k+1}^2}{Q_k(\sqrt{d} + P_{k+1})} \\
&= Q_{k+1} \frac{1}{\sqrt{d} + P_{k+1}} \\
&= \frac{1}{\alpha_{k+1}}.
\end{aligned}$$

□

Example 10.51. *Let $\alpha = \frac{3+\sqrt{7}}{2}$. Then we can write*

$$\alpha = \frac{6 + \sqrt{28}}{4},$$

and thus set $P_0 = 6, Q_0 = 4, d = 28$.

Hence we can compute $a_0 = \lfloor \alpha \rfloor = 2$ and

$$\begin{aligned}
P_1 &= 2 \cdot 4 - 6 = 2, & \alpha_1 &= \frac{2+\sqrt{28}}{6}, \\
Q_1 &= \frac{28-2^2}{4} = 6, & a_1 &= \lfloor \alpha_1 \rfloor = 1, \\
P_2 &= 1 \cdot 6 - 2 = 4, & \alpha_2 &= \frac{4+\sqrt{28}}{2}, \\
Q_2 &= \frac{28-4^2}{6} = 2, & a_2 &= \lfloor \alpha_2 \rfloor = 4, \\
P_3 &= 4 \cdot 2 - 4 = 4, & \alpha_3 &= \frac{4+\sqrt{28}}{6}, \\
Q_3 &= \frac{28-4^2}{2} = 6, & a_3 &= \lfloor \alpha_3 \rfloor = 1, \\
P_4 &= 1 \cdot 6 - 4 = 2, & \alpha_4 &= \frac{2+\sqrt{28}}{4}, \\
Q_4 &= \frac{28-2^2}{6} = 4, & a_4 &= \lfloor \alpha_4 \rfloor = 1, \\
P_5 &= 1 \cdot 4 - 2 = 2, & \alpha_5 &= \frac{2+\sqrt{28}}{6}, \\
Q_5 &= \frac{28-2^2}{4} = 6, & a_5 &= \lfloor \alpha_5 \rfloor = 1,
\end{aligned}$$

since $P_5 = P_1, Q_5 = Q_1$ we get a periodicity, i.e.,

$$\frac{3+\sqrt{7}}{2} = [2; \overline{1, 4, 1, 1}].$$

We are now ready to finish Lagrange's theorem.

Proof. Let α be a quadratic irrational, so that we can write

$$\alpha = \frac{P_0 + \sqrt{d}}{Q_0}.$$

By Theorem 10.50, we get that $\alpha = [a_0; a_1, \ldots]$ where

$$\begin{aligned}
\alpha_k &= \frac{P_k + \sqrt{d}}{Q_k}, \\
a_k &= \lfloor \alpha_k \rfloor, \\
P_{k+1} &= a_k Q_k - P_k, \\
Q_{k+1} &= \frac{d - P_{k+1}^2}{Q_k},
\end{aligned}$$

for $k \geq 0$.

We can write $\alpha = [a_0; a_1, \ldots, a_{k-1}, \alpha_k]$. Let c_k be the convergent. Due to Theorem 10.14, we get that

$$\alpha = \frac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}}.$$

Taking conjugates on both sides, we can use Lemma 10.48 to get

$$\alpha' = \frac{p_{k-1}\alpha'_k + p_{k-2}}{q_{k-1}\alpha'_k + q_{k-2}}.$$

Solving for α'_k, we find that

$$\alpha'_k = -\frac{q_{k-2}}{q_{k-1}}\left(\frac{\alpha' - \frac{p_{k-2}}{q_{k-2}}}{\alpha' - \frac{p_{k-1}}{q_{k-1}}}\right).$$

Recall that the convergents $\frac{p_{k-2}}{q_{k-2}}, \frac{p_{k-1}}{q_{k-1}}$ tend to α, thus

$$\frac{\alpha' - \frac{p_{k-2}}{q_{k-2}}}{\alpha' - \frac{p_{k-1}}{q_{k-1}}}$$

tends to 1.

Hence, there exists an integer N, such that $\alpha'_k < 0$ for $k \geq N$. Since $\alpha_k > 0$, we get

$$\alpha_k - \alpha'_k = \frac{P_k + \sqrt{d}}{Q_k} - \frac{P_k - \sqrt{d}}{Q_k} = \frac{2\sqrt{d}}{Q_k} > 0.$$

Hence $Q_k > 0$ for $k \geq N$.

Since $Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k}$, we get

$$Q_k \leq Q_k Q_{k+1} = d - P_{k+1}^2 \leq d$$

and in turn

$$P_{k+1}^2 \leq d = P_{k+1}^2 - Q_k Q_{k+1}$$

hence

$$-\sqrt{d} < P_{k+1} < \sqrt{d}.$$

From the inequalities ($0 \leq Q_k \leq d, -\sqrt{d} < P_{k+1} < \sqrt{d}$ for $k \geq N$) we see that only a finite number of values are possible for P_k, Q_k. However, as there are infinitely many integer $k > N$, there must exist two integers $i \neq j$ such that $P_i = P_j$ and $Q_i = Q_j$ which implies $\alpha_i = \alpha_j$.

Consequently, we get a periodicity as $a_i = a_j$ and thus a periodic continued fraction

$$\alpha = [a_0; a_1, \ldots, a_{i-1}, \overline{a_i, \ldots, a_{j-1}}].$$

□

Exercise 10.52. *Show that if $\frac{a}{b}$ is a convergent of $\sqrt{n}$ then $\frac{b}{a}$ is a convergent of $\frac{1}{\sqrt{n}}$.*

Finally, we can consider continued fractions, which are purely periodic.

Definition 10.53. A simple continued fraction $[a_0; a_1, \ldots]$ is called *purely periodic*, if there exists an integer n such that $a_k = a_{n+k}$ for all positive integers k, i.e.,

$$[a_0; a_1, \ldots] = [\overline{a_0; a_1 \ldots, a_{k-1}}].$$

These continued fractions belong to special quadratic irrationals.

Definition 10.54. A quadratic irrational α is called *reduced*, if $\alpha > 1$ and $-1 < \alpha' < 0$.

Theorem 10.55. *The simple continued fraction of a quadratic irrational α is purely periodic, if and only if α is reduced.*

Proof. For the first direction, assume that α is a reduced quadratic irrational.

Recall from Theorem 10.50 that the continued fraction is found via $\alpha_0 = \alpha, a_k = \lfloor \alpha_k \rfloor, \alpha_{k+1} = \frac{1}{\alpha_k - a_k}$.

Hence $\frac{1}{\alpha_{k+1}} = \alpha_k - a_k$ and its conjugate is $\frac{1}{\alpha'_{k+1}} = \alpha'_k - a_k$.

We now show by induction that $-1 < \alpha'_k < 0$, so that all α_k are reduced.

For $k = 0$, we get that $\alpha_0 = \alpha$, which we assumed is reduced and hence $-1 < \alpha'_0 < 0$.

Assume the claim is true for k, i.e., $-1 < \alpha'_k < 0$.

Then, since $\alpha > 1$ we also have $a_k \geq 1$ for all k and thus

$$\frac{1}{\alpha'_{k+1}} = \alpha'_k - a_k < -1,$$

so that

$$-1 < \alpha'_{k+1} < 0$$

for all k.

Thus,

$$-1 < \alpha'_k = a_k + \frac{1}{\alpha'_{k+1}} < 0,$$

which implies that

$$-1 - \frac{1}{\alpha'_{k+1}} < a_k < -\frac{1}{\alpha'_{k+1}}.$$

Thus we get that

$$a_k = \lfloor -\frac{1}{\alpha'_{k+1}} \rfloor.$$

As in Lagrange's Theorem for continued fractions, we again get that there exist $i < j$ with $\alpha_i = \alpha_j$ and hence

$$a_{i-1} = \lfloor -\frac{1}{\alpha'_{i-1}} \rfloor = \lfloor -\frac{1}{\alpha'_{j-1}} \rfloor.$$

Since then also

$$\alpha_{i-1} = a_{i-1} + \frac{1}{\alpha_i} = a_{j-1} + \frac{1}{\alpha_j} = a_{j-1}$$

we get $\alpha_{i-1} = \alpha_{j-1}$. We can continue in this way, until we get

$$\alpha_0 = \alpha_{j-i}$$

and hence

$$\alpha = [\overline{a_0; a_1, \ldots, a_{j-i-1}}].$$

For the other direction, we assume that α is quadratic irrational and has a purely periodic continued fraction

$$\alpha = [\overline{a_0; a_1, \ldots, a_k}] = [a_0; a_1, \ldots, a_k, \alpha].$$

Hence

$$\alpha = \frac{\alpha p_k + p_{k-1}}{\alpha q_k + q_{k-1}}$$

where $\frac{p_k}{q_k}, \frac{p_{k-1}}{q_{k-1}}$ are the kth and $(k-1)$th convergent of α. We can rewrite this to get

$$\alpha^2 q_k + \alpha(q_{k-1} - p_k) - p_{k-1} = 0$$

and hence α is a root of the quadratic polynomial $x^2 q_k + x(q_{k-1} - p_k) - p_{k-1}$.

Let us consider the quadratic irrational

$$\beta = [\overline{a_k; a_{k-1}, \ldots, a_0}] = [a_k; a_{k-1}, \ldots, a_0, \beta].$$

Again, we get that

$$\beta = \frac{\beta p'_k + p'_{k-1}}{\beta q'_k + q'_{k-1}},$$

where $\frac{p'_k}{q'_k}, \frac{p'_{k-1}}{q'_{k-1}}$ are the kth and $(k-1)$th convergent of β.

From Exercise Sheet 6, Problem 2.3 we have that

$$\frac{p_k}{p_{k-1}} = [a_k; a_{k-1}, \ldots, a_0] = \frac{p'_k}{q'_k},$$
$$\frac{q_k}{q_{k-1}} = [a_k; a_{k-1}, \ldots, a_1] = \frac{p'_{k-1}}{q'_{k-1}}.$$

Since convergents are in lowest terms, we get that

$$p_k = p'_k, \quad p_{k-1} = q'_k, \quad q_k = p'_{k-1}, \quad q_{k-1} = q'_{k-1}.$$

We can insert these values to get

$$\beta = \frac{\beta p_k + q_k}{\beta p_{k-1} + q_{k-1}}$$

and hence

$$\beta^2 p_{k-1} + \beta(q_{k-1} - p_k) - q_k = 0.$$

We multiply this by $-\frac{1}{\beta^2}$ to get

$$-p_{k-1} - \frac{1}{\beta}(q_{k-1} - p_k) + \left(-\frac{1}{\beta}\right)^2 q_k = 0.$$

Thus, $-\frac{1}{\beta}$ is the second root of $x^2 q_k + x(q_{k-1} - p_k) - p_{k-1}$.

Thus, α and $-\frac{1}{\beta}$ are conjugates, i.e., $\alpha' = -\frac{1}{\beta}$.

Since $\beta = [\overline{a_k; a_{k-1}, \ldots, a_0}]$ we get that $\beta > 1$ and hence

$$-1 < -\frac{1}{\beta} = \alpha' < 0,$$

which shows that α is reduced.

□

Let us consider $\sqrt{d}$, for d a positive integer, which is not a square. Clearly, $\sqrt{d}$ is not purely periodic, but almost. That is, if we consider $\alpha = \lfloor \sqrt{d} \rfloor + \sqrt{d} > 1$, we get

$$-1 < \alpha' = \lfloor \sqrt{d} \rfloor - \sqrt{d} < 0$$

and hence α is reduced. Thus,

$$\sqrt{d} = [a_0; \overline{a_1, \ldots, a_n}]$$

is almost purely periodic.

10.6 Factoring using Continued Fractions

Recall Fermat's factorization algorithm, where we search for t, s such that $n = t^2 - s^2$, as then $n = (t - s)(t + s)$.

We can generalize this method, as it is enough to find positive integers x, y which satisfy the weaker condition

$$x^2 \equiv y^2 \mod n,$$

and $0 < y < x < n$ and $x + y \neq n$.

In this case, $n \mid (x^2 - y^2)$ and $n \nmid (x - y)$, $n \nmid (x + y)$. Thus, $\gcd(n, x - y)$ and $\gcd(n, x + y)$ are non-trivial divisors of n.

We can use the continued fraction of $\sqrt{n}$ to find solutions to the congruence

$$x^2 \equiv y^2 \mod n.$$

We first need the following result.

Lemma 10.56. *Let r, s, t, u be rational numbers and n be a positive integer, which is not a square. If $r + s\sqrt{n} = t + u\sqrt{n}$, then $r = t, s = u$.*

Proof. If $r + s\sqrt{n} = t + u\sqrt{n}$ but $s \neq u$, then

$$\sqrt{n} = \frac{r-t}{u-s},$$

which is a contradiction to $\sqrt{n}$ being irrational. Thus, $u = s$ and hence also $r = t$. □

Theorem 10.57. *Let n be a positive integer, which is not a square. Define*

$$\begin{aligned} \alpha_k &= \frac{P_k + \sqrt{n}}{Q_k}, \\ a_k &= \lfloor \alpha_k \rfloor, \\ P_{k+1} &= a_k Q_k - P_k, \\ Q_{k+1} &= \frac{n - P_{k+1}^2}{Q_k} \end{aligned}$$

for $k \geq 0$ and $\alpha_0 = \sqrt{n}$.

Let $\frac{p_k}{q_k}$ be the kth convergent of the continued fraction of $\sqrt{n}$.

Then,

$$p_k^2 - nq_k^2 = (-1)^{k-1} Q_{k+1}.$$

Proof. Since $\sqrt{n} = [a_0; a_1, \ldots, a_k, \alpha_{k+1}]$, by Theorem 10.14, we get that

$$\sqrt{n} = \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}}.$$

We can insert that $\alpha_{k+1} = \frac{P_{k+1} + \sqrt{n}}{Q_{k+1}}$ to get

$$\sqrt{n} = \frac{(P_{k+1} + \sqrt{n})p_k + Q_{k+1} p_{k-1}}{(P_{k+1} + \sqrt{n})q_k + Q_{k+1} q_{k-1}}.$$

Thus, rewriting this we get

$$nq_k + (P_{k+1} q_k + Q_{k+1} q_{k-1})\sqrt{n} = (P_{k+1} p_k + Q_{k+1} p_{k-1}) + p_k \sqrt{n}.$$

By Lemma 10.56, we get that

$$\begin{aligned} nq_k &= P_{k+1} p_k + Q_{k+1} p_{k-1}, \\ p_k &= P_{k+1} q_k + Q_{k+1} q_{k-1}. \end{aligned}$$

Thus, by multiplying with q_k, respectively with p_k we get

$$\begin{aligned} nq_k^2 &= P_{k+1} p_k q_k + Q_{k+1} p_{k-1} q_k, \\ p_k^2 &= P_{k+1} q_k p_k + Q_{k+1} q_{k-1} p_k. \end{aligned}$$

Hence

$$p_k^2 - nq_k^2 = Q_{k+1}(q_{k-1} p_k - p_{k-1} q_k) = (-1)^{k-1} Q_{k+1}.$$

□

The continued fraction factorization algorithm, thus considers the continued fraction of $\sqrt{n}$ and due to Theorem 10.57, we have

$$p_k^2 \equiv (-1)^{k-1} Q_{k+1} \mod n.$$

If k is odd and $Q_{k+1} = s^2$ for some integer s, then we can use $p_k^2 \equiv s^2 \mod n$ to factor n.

Example 10.58. *Let* $n = 1037$ *and* $\alpha = \sqrt{1037} = \frac{0+\sqrt{1037}}{1}$, *i.e., we set* $P_0 = 0, Q_0 = 1$.

We then generate the terms P_k, Q_k, α_k, a_k *and search for square* Q_k*. In fact,* $Q_1 = 13$ *is not a square but* $Q_2 = 49 = 7^2$*. We get that* $p_1^2 \equiv Q_2 \equiv 7^2 \mod 1037$ *and by computing the sequence* p_i *we get* $p_1 = 129$.

Thus,

$$129^2 - 7^2 \equiv (129 - 7)(129 + 7) \equiv 0 \mod 1037.$$

We can compute gcd$(122, 1037) = 61$ *and gcd*$(136, 1037) = 17$.

11 Non-Linear Diophantine Equations

Any equation where we are only interested in integer solutions is called Diophantine equation. In Chapter 1.4 we have studied linear Diophantine equations and have seen how all solutions (if any exists) can be found. What happens if we consider non-linear Diophantine equations? Unfortunately, there is no general method for solving all non-linear Diophantine equations.

However, if we focus on special types of equations, e.g. $x^2 + y^2 = z^2$, we can provide all solutions.

A related equation is the Pell equation, of the form $x^2 - dy^2 = n$. These equations can be solved using continued fractions from Chapter 10.

This will lead us to consider the more general equation $x^n + y^n = z^n$ for $n > 2$ and clearly we will not be interested in the trivial solution $(0, 0, 0)$. Fermat's last theorem then tells us that no non-trivial solution to this equation exists. This result is probably the most famous one within elementary number theory. This statement of Fermat has puzzled mathematicians for 350 years, until finally, in 1995, Andrew Wiles was able to prove it.

While the proof for a general n lies beyond the scope of this lecture, we will prove it for the case $n = 4$.

11.1 Pythagorean Triples

Recall the famous theorem of Pythagoras, which states that in a right-angled triangle with sides x, y, z (where z denotes the hypothenuse), we have that

$$x^2 + y^2 = z^2.$$

Thus to find all possible right-angled triangles with sides of integer length, we want to find all integer solutions to the non-linear Diophantine equation $x^2 + y^2 = z^2$.

Definition 11.1. A *Pythagorean triple* is a solution $(x, y, z) \in \mathbb{Z}^3$ with

$$x^2 + y^2 = z^2.$$

Example 11.2. *For example,* $x = 3, y = 4, z = 5$ *is a Pythagorean triple.*

Unlike most non-linear Diophantine equations, we can describe all Pythagorean triples. Before proving this, we will require some more results.

Definition 11.3. A Pythagorean triple (x, y, z) is called *primitive* if $\gcd(x, y, z) = 1$.

Example 11.4. *The Pythagorean triple* $(3, 4, 5)$ *is primitive, while* $(6, 8, 10)$ *is not.*

Let (x, y, z) be a Pythagorean triple with $\gcd(x, y, z) = d$. Then, there exist integers x_1, y_1, z_1 with $x = dx_1, y = dy_1, z = dz_1$ and $\gcd(x_1, y_1, z_1) = 1$. In addition, as

$$x^2 + y^2 = z^2,$$

we also get that

$$x_1^2 + y_1^2 = (x/d)^2 + (y/d)^2 = (z/d)^2 = z_1^2.$$

Thus, from a non-primitive Pythagorean triple we can form a primitive Pythagorean triple.

On the other hand, any multiple of a Pythagorean triple will again be a Pythagorean triple. That is: if (x, y, z) is a Pythagorean triple, i.e., $x^2 + y^2 = z^2$, then (dx, dy, dz) is also a Pythagorean triple as

$$(dx)^2 + (dy)^2 = d^2(x^2 + y^2) = d^2z^2 = (dz)^2.$$

Consequently, all Pythagorean triples can be found forming multiples of primitive Pythagorean triples. Thus, we will only be interested in finding primitive solutions.

The first lemma tells us that any two integers in a primitive Pythagorean triple are coprime.

Lemma 11.5. *Let (x, y, z) be a primitive Pythagorean triple. Then*

$$gcd(x, y) = gcd(x, z) = gcd(y, z) = 1.$$

Proof. Let $d = \gcd(x, y)$, and assume by contradiction that $d > 1$, so that there exists some prime p with $p \mid d$. Thus, we also have $p \mid x$ and $p \mid y$, which in turn gives that $p \mid (x^2 + y^2) = z^2$. As then $p \mid \gcd(x, y, z) = 1$, we get the desired contradiction. The other two cases are analogous. □

The next lemma tells us about the parity of the integers in a Pythagorean triple.

Lemma 11.6. *If (x, y, z) is a primitive Pythagorean triple, then either x is even and y is odd or x is odd and y is even.*

Proof. By Lemma 11.5, we know that $\gcd(x, y) = 1$, thus x and y cannot both be even. On the other hand, if x, y are both odd, then

$$x^2 \equiv y^2 \equiv 1 \mod 4,$$

and hence

$$z^2 \equiv x^2 + y^2 \equiv 2 \mod 4.$$

As 2 is not a quadratic residue modulo 4, we get a contradiction. □

The final lemma tells us that two coprime integers whose product is a square, must already be squares themselves.

Lemma 11.7. *Let r, s, t be positive integers such that gcd$(r, s) = 1$ and $rs = t^2$. Then, there exist integers m, n such that $r = m^2, s = n^2$.*

Exercise 11.8. *Prove Lemma 11.7 using the Fundamental Theorem of Arithmetic.*

We can now describe all Pythagorean triples. By Lemma 11.6, we may assume that y is even and x, z are odd.

Theorem 11.9. *The positive integers (x, y, z) form a primitive Pythagorean triple with y even if and only if there exist coprime integers $0 < n < m$ such that either m is odd and n is even, or m is even and n is odd and*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2.$$

Proof. For the first direction, let (x, y, z) be a primitive Pythagorean triple with even y. Due to Lemma 11.6, we then have that x, z are odd.

Thus, $z + x$ and $z - x$ are both even, i.e., there exist positive integers r, s with

$$r = (z + x)/2, \quad s = (z - x)/2.$$

Note that $\gcd(r, s) = 1$. In fact, if $\gcd(r, s) = d$ then $d \mid (r + s) = z$ and $d \mid (r - s) = x$. Hence $d \mid \gcd(x, z) = 1$.

As $x^2 + y^2 = z^2$, we get

$$y^2 = z^2 - x^2 = (z + x)(z - x)$$

and hence

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

Using Lemma 11.7 there exist positive integers m, n such that $r = m^2$ and $s = n^2$. We can hence write x, y, z in terms of m, n as

$$\begin{aligned} x &= r - s = m^2 - n^2, \\ y &= \sqrt{4rs} = \sqrt{4m^2n^2} = 2mn, \\ z &= r + s = m^2 + n^2. \end{aligned}$$

We note that $\gcd(m, n) = 1$.

In fact, if $\gcd(m, n) = d$, then $d \mid (m^2 - n^2) = x$, and $d \mid 2mn = y$ and finally $d \mid (m^2 + n^2) = z$. Thus, $d \mid \gcd(x, y, z) = 1$. Since m, n cannot both be odd (if both are odd then $x = m^2 - n^2$ is even, which we excluded) we get that either m is even and n is odd or m is odd and n is even. This shows that every primitive Pythagorean triple has the desired form.

For the other direction, we want to show that every triple

$$\begin{aligned} x &= m^2 - n^2, \\ y &= 2mn, \\ z &= m^2 + n^2 \end{aligned}$$

with $m > n$ positive coprime integers of different parity forms a primitive Pythagorean triple.

First note that $x = m^2 - n^2, y = 2mn, z = m^2 + n^2$ forms a Pythagorean triple as

$$\begin{aligned} x^2 + y^2 &= (m^2 - n^2)^2 + (2mn)^2 = (m^4 - 2m^2n^2 + n^4) + 4m^2n^2 \\ &= m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2 = z^2. \end{aligned}$$

To show that the triple is primitive, assume that gcd$(x, y, z) = d > 1$, then there exists a prime p, such that $p \mid d$.

As x is odd, we have that $p \neq 2$ in fact $x = m^2 - n^2$ and m, n have opposite parity. As $p \mid x, z$ we also get $p \mid (x + z) = 2m^2$ and $p \mid (z - x) = 2n^2$.

Thus, $p \mid m, n$ which contradicts gcd$(m, n) = 1$.

□

Example 11.10. *Let $m = 5, n = 2$. Then Theorem 11.9 tells us that*

$$\begin{aligned} x &= m^2 - n^2 = 21, \\ y &= 2mn = 20, \\ z &= m^2 + n^2 = 29 \end{aligned}$$

is a primitive Pythagorean triple.

11.2 Pell's Equation

We now want to study Diophantine equations of the form

$$x^2 - dy^2 = n,$$

where d, n are given integers. Note that if $d < 0, n < 0$ then there are no solutions. If $d < 0$ and $n > 0$, then $|x| \leq \sqrt{n}, |y| \leq \sqrt{n/|d|}$, hence there are only finitely many solutions.

If d is a square, say $d = D^2$, then

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

Hence any solution of $x^2 - dy^2 = n$ corresponds to a solution of

$$\begin{aligned} x + Dy &= a, \\ x - Dy &= b, \\ ab &= n. \end{aligned}$$

In this case, there are again only finitely many solutions (in fact, for any factorization a, b there exists at most one solution (x, y) in the integers).

Thus, we will assume that d, n are positive integers and d is not a square. As before, if (x, y) is a solution to the Pell's Equation, then $(\pm x, \pm y)$ is as well. We thus only consider positive solutions $x, y > 0$.

We can use continued fractions to study a Diophantine equation, called *generalized Pell's equation*:

$$x^2 - dy^2 = n,$$

where d is a given positive integer, not a square and we are interested in positive integer solutions (x, y).

Theorem 11.11. *Let d, n be nonzero integers. If $d > 0$ is not a square and $|n| < \sqrt{d}$, then for any solution $(x, y) \in \mathbb{Z}^2$ with $y \neq 0$ to the generalized Pell equation*

$$x^2 - dy^2 = n,$$

we have that $\frac{x}{y}$ is a convergent of $\sqrt{d}$.

Proof. Let us rewrite the generalized Pell's equation as $x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d}) = n$. If $n > 0$, then $x - y\sqrt{d} > 0$, and hence $\frac{x}{y} - \sqrt{d} > 0$.

Since $0 < n < \sqrt{d}$, we get that

$$\frac{x}{y} - \sqrt{d} = \frac{x - \sqrt{d}y}{y} = \frac{x^2 - dy^2}{y(x + y\sqrt{d})} < \frac{n}{y(2y\sqrt{d})} < \frac{\sqrt{d}}{2y^2\sqrt{d}} = \frac{1}{2y^2}.$$

Since

$$0 < \frac{x}{y} - \sqrt{d} < \frac{1}{2y^2},$$

we can apply the Legendre Criteria, which tells us that $\frac{x}{y}$ must be a convergent of $\sqrt{d}$.

If $n < 0$, we divide the generalized Pell's equation by $-d$ to get

$$y^2 - \frac{1}{d}x^2 = -\frac{n}{d}.$$

We can argue in the same manner as before, as $-\frac{n}{d} > 0$ to get that $\frac{y}{x}$ is a convergent of of $\frac{1}{\sqrt{d}}$. Thus, using Exercise 10.52 we get that $\frac{x}{y}$ is a convergent of $\sqrt{d}$. □

This theorem tells us that the solutions of the generalized Pell's equation are given by the convergents of $\sqrt{d}$. Thus, we want to make use of Theorem 10.57, i.e., we define $\alpha_0 = \sqrt{d}$, $\alpha_k = \frac{P_k + \sqrt{d}}{Q_k}$, $a_k = \lfloor \alpha_k \rfloor$ and $P_{k+1} = a_k Q_k - P_k, Q_{k+1} = \frac{d - P_{k+1}^2}{Q_k}$, for k a non-negative integer. Let $\frac{p_k}{q_k}$ denote the kth convergent of the continued fraction of $\sqrt{d}$. Then

$$p_k^2 - dq_k^2 = (-1)^{k-1} Q_{k+1}.$$

With this we can see how the odd convergents $\frac{p_{2k-1}}{q_{2k-1}}$ corresponds to a solution of the Pell's equation

$$x^2 - dy^2 = 1.$$

Theorem 11.12. *Let d be a positive integer which is not a square. Let $\frac{p_k}{q_k}$ denote the kth convergent of $\sqrt{d}$. Let n denote the period length of the continued fraction of $\sqrt{d}$. If n is even, the positive solutions to*

$$x^2 - dy^2 = 1$$

are $x = p_{jn-1}, y = q_{jn-1}$, for j a positive integer. If n is odd, the positive solutions to $x^2 - dy^2 = 1$ are $x = p_{2jn-1}, y = q_{2jn-1}$ for j a positive integer.

Proof. By Theorem 11.11, we get that a solution x, y of $x^2 - dy^2 = 1$ is such that $\frac{x}{y}$ is a convergent of $\sqrt{d}$, i.e., $x = p_k, y = q_k$.

Recall that the continued fraction of $\sqrt{d}$ is found via $\alpha_0 = \sqrt{d} = \frac{P_0 + \sqrt{d}}{Q_0}$, with $P_0 = 0, Q_0 = 1$ and $\sqrt{d} = [a_0; \overline{a_1, \ldots, a_n}]$.

From Theorem 10.57, we get that

$$p_k^2 - dq_k^2 = (-1)^{k-1} Q_{k+1}.$$

As $\sqrt{d}$ has period length n, we get that $Q_{jn} = Q_0 = 1$ for all positive integers j. In fact, since $\alpha_{n+1} = \alpha_n$ we also have $P_{n+1} = P_1, Q_{n+1} = Q_1$. By definition

$$Q_{n+1} = \frac{d - P_{n+1}^2}{Q_n} = \frac{d - P_1^2}{Q_0} = Q_1$$

and since $P_{n+1} = P_1$ we also get $Q_n = Q_0$.

Hence

$$p_{jn-1}^2 - dq_{jn-1}^2 = (-1)^{jn} Q_{jn} = (-1)^{jn}.$$

If n is even, then $x = p_{jn-1}, y = q_{jn-1}$ is a solution to $x^2 - dy^2 = 1$ and if n is odd, we can consider $2jn - 1$ instead.

We now want to show that the equation $x^2 - dy^2 = 1$ has no other solutions. For this we show that $Q_{k+1} = 1$ implies that $n \mid (k+1)$, so that $Q_{k+1} = Q_{jn}$ and that $Q_j \neq -1$ for any positive integer j.

If $Q_{k+1} = 1$, then $\alpha_{k+1} = P_{k+1} + \sqrt{d}$. Since $\alpha_{k+1} = [a_{k+1}; a_{k+2}, \ldots]$, the continued fraction of α_{k+1} is purely periodic. Thus, we can use Theorem 10.55 to get that $-1 < \alpha'_{k+1} = P_{k+1} - \sqrt{d} < 0$. Since P_{k+1} is an integer, we can only have $P_{k+1} = \lfloor \sqrt{d} \rfloor = P_1$. Hence we can compare α_{k+2} and α_1 :

$$\begin{aligned}
&P_0 = 0, \quad Q_0 = 1, \quad \alpha_0 = \sqrt{d}, \quad a_0 = \lfloor \sqrt{d} \rfloor, \\
&P_1 = a_0 Q_0 - P_0 = \lfloor \sqrt{d} \rfloor, \quad Q_1 = \frac{d - P_1^2}{Q_0} = d - \lfloor \sqrt{d} \rfloor^2, \quad \alpha_1 = \frac{\lfloor \sqrt{d} \rfloor + \sqrt{d}}{d - \lfloor \sqrt{d} \rfloor^2}, \\
&P_{k+1} = \lfloor \sqrt{d} \rfloor, \quad Q_{k+1} = 1, \quad \alpha_{k+1} = \lfloor \sqrt{d} \rfloor + \sqrt{d}, \quad a_{k+1} = 2\lfloor \sqrt{d} \rfloor, \\
&P_{k+2} = a_{k+1} Q_{k+1} - P_{k+1} = 2\lfloor \sqrt{d} \rfloor - \lfloor \sqrt{d} \rfloor = \lfloor \sqrt{d} \rfloor = P_1, \quad Q_{k+2} = d - \lfloor \sqrt{d} \rfloor^2 = Q_1,
\end{aligned}$$

which implies $\alpha_{k+2} = \alpha_1$ and hence $n \mid (k+1)$.

For the second point, we note that $Q_j = -1$ implies that $\alpha_j = -P_j - \sqrt{d}$ and since α_j is purely periodic, we get $-1 < \alpha'_j = -P_j + \sqrt{d} < 0$ and $\alpha_j = -P_j - \sqrt{d} > 1$.

We can rewrite this as $P_j > \sqrt{d}$ and $P_j < -1 - \sqrt{d}$, which are contradictions.

□

Theorem 11.13. *Let d be a positive integer which is not a square. Let $\frac{p_k}{q_k}$ denote the kth convergent of $\sqrt{d}$. Let n denote the period length of the continued fraction of $\sqrt{d}$. If n is even, the equation*

$$x^2 - dy^2 = -1$$

has no non-trivial integer solutions. If n is odd, the positive integer and the solutions of $x^2 - dy^2 = -1$ are $x = p_{(2j-1)n-1}, y = q_{(2j-1)n-1}$ for j a positive integer.

Exercise 11.14. *Prove Theorem 11.13.*

Example 11.15. *Since $\sqrt{14} = [3, \overline{1, 2, 1, 6}]$, we get that the positive solutions of $x^2 - 14y^2 = 1$ are given by p_{4j-1}, q_{4j-1}, for j a positive integer. The smallest positive solution is given by $p_3 = 15, q_3 = 4$.*

Theorem 11.16. *Let d be a positive non-square integer. Let x_1, y_1 be the smallest positive solution to the Pell equation $x^2 - dy^2 = 1$. Then, all positive solutions are given by*

$$x_k + y_k\sqrt{d} = (x_1 + y_1\sqrt{d})^k,$$

for k a positive integer.

Proof. We start by showing that x_k, y_k is a solution.

Note that by taking conjugates, we get

$$x_k - y_k\sqrt{d} = (x_1 - y_1\sqrt{d})^k$$

as the conjugate of a power is the power of the conjugate.

Thus,

$$\begin{aligned} x_k^2 - dy_k^2 &= (x_k + y_k\sqrt{d})(x_k - y_k\sqrt{d}) = (x_1 + y_1\sqrt{d})^k(x_1 - y_1\sqrt{d})^k \\ &= (x_1^2 - dy_1^2)^k = 1. \end{aligned}$$

Thus, x_k, y_k is a solution for any positive integer k.

Next, we want to show that all solutions are of this form.

For this, we assume that x', y' is a positive solution, which is not of the form x_k, y_k. Then, there exists an integer n such that

$$(x_1 + y_1\sqrt{d})^n < x' + y'\sqrt{d} < (x_1 + y_1\sqrt{d})^{n+1}.$$

We multiply this with $(x_1 + y_1\sqrt{d})^{-n}$ to get

$$1 < (x_1 - y_1\sqrt{d})^n(x' + y'\sqrt{d}) < x_1 + y_1\sqrt{d},$$

where we have used that $x_1 - y_1\sqrt{d} = (x_1 + y_1\sqrt{d})^{-1}$.

Now, we define s, t to be the integers with

$$s + t\sqrt{d} = (x_1 - y_1\sqrt{d})^n(x' + y'\sqrt{d}).$$

We then get that

$$\begin{aligned} s^2 - dt^2 &= (s - t\sqrt{d})(s + t\sqrt{d}) \\ &= (x_1 + y_1\sqrt{d})^n(x' - y'\sqrt{d})(x_1 - y_1\sqrt{d})^n(x' + y'\sqrt{d}) \\ &= (x_1^2 - dy_1^2)^n(x'^2 - dy'^2) = 1. \end{aligned}$$

Hence, s, t is a solution of $x^2 - dy^2 = 1$ and

$$1 < s + t\sqrt{d} < x_1 + y_1\sqrt{d}.$$

As we also have $s + t\sqrt{d} > 1$ we get that

$$0 < (s + t\sqrt{d})^{-1} < 1$$

and thus

$$\begin{aligned} s &= \frac{1}{2}\Big((s + t\sqrt{d}) + (s - t\sqrt{d})\Big) > 0 \\ t &= \frac{1}{2\sqrt{d}}\Big((s + t\sqrt{d} - (s - t\sqrt{d})\Big) > 0. \end{aligned}$$

Hence, s, t is a positive solution and $s \geq x_1, t \geq y_1$ as we have chosen x_1, y_1 to be the smallest positive solution. Together with $s + t\sqrt{d} < x_1 + y_1\sqrt{d}$ we get a contradiction. Thus, x', y' must be of the form x_k, y_k. □

Example 11.17. *The smallest positive solution of the equation* $x^2 - 13y^2 = 1$ *is* $x_1 = 649, y_1 = 180$. *Hence all positive solutions are given by*

$$x_k + y_k\sqrt{13} = (649 + 180\sqrt{13})^k.$$

For example $x_2 = 842401, y_2 = 233640$.

11.3 Fermat's Last Theorem

We have seen that the non-linear Diophantine equation $x^2 + y^2 = z^2$ has infinitely many solutions. What happens if we take larger powers?

Theorem 11.18 (Fermat's Last Theorem)**.** *The equation*

$$x^n + y^n = z^n$$

has no integer solutions if $n \geq 3$.

This famous statement of Fermat has challenged mathematicians for centuries. As Fermat only provided the proof for the case $n = 4$, claiming that the general case works similarly. It is unlikely that he did know the proof of the statement, as the only proof available today, due to Andrew Wiles, uses different tools (such as a novel connection to algebraic geometry) than the proof he gave for $n = 4$. However, trying to prove the statement, many novel and interesting results have been found along the way, such as

Theorem 11.19 (Euler)**.** *The non-linear Diophantine equation $x^3 + y^3 = z^3$ has no non-trivial integer solutions.*

and

Theorem 11.20 (Germain)**.** *Let $p, 2p + 1 \in \mathcal{P}$, then $x^p + y^p = z^p$ has no integer solution with $xyz \neq 0$ when $p \nmid xyz$.*

The proof for $n = 4$ uses *infinite descent*, which shows that a Diophantine equation has no solution by showing that for each solution one would find a smaller one, contradicting the well-ordering property.

We will show a slightly stronger statement, that is $x^4 + y^4 = z^2$ has no non-trivial integer solution, as any solution to $x^4 + y^4 = z^4 = (z^2)^2$ gives raise to a solution of $x^4 + y^4 = z^2$.

Theorem 11.21. *The non-linear Diophantine equation*

$$x^4 + y^4 = z^2$$

has no non-trivial integer solution.

Proof. Assume by contradiction that the equation has a non-trivial integer solution (x, y, z). As then also $(\pm x, \pm y, \pm z)$ is a solution, we can assume that x, y, z are all positive integers.

We can also assume that $\gcd(x, y) = 1$. In fact, if $\gcd(x, y) = d > 1$, then there exist positive integers x_1, y_1 with $x = dx_1, y = dy_1$. Since

$$x^4 + y^4 = (dx_1)^4 + (dy_1)^4 = d^4(x_1^4 + y_1^4) = z^2,$$

implying that $d^4 \mid z^2$ and thus $d^2 \mid z$. Hence there exists a positive integer z_1 such that $z = d^2 z_1$ and hence

$$x^4 + y^4 = (dx_1)^4 + (dy_1)^4 = d^4(x_1^4 + y_1^4) = z^2 = d^4 z_1^2,$$

implying that $x_1^4 + y_1^4 = z_1^2$ is another, smaller, solution with $\gcd(x_1, y_1) = 1$. Thus, we can always assume that $\gcd(x, y) = 1$.

Thus, let us suppose that (x, y, z) is a positive integer solution with $\gcd(x, y) = 1$ and derive another positive integer solution (x_1, y_1, z_1) with $\gcd(x_1, y_1) = 1$ but with $z_1 < z$.

As $x^4 + y^4 = z^2$ we also get that $(x^2)^2 + (y^2)^2 = z^2$ and thus (x^2, y^2, z) is a Pythagorean triple. Let $d = \gcd(x^2, y^2)$, if $d > 1$, then there exists a prime p with $p \mid x^2, y^2$ and thus $p \mid \gcd(x, y) = 1$.

As the Pythagorean triple (x^2, y^2, z) is primitive, we can apply Theorem 11.9 and get that there exist positive coprime integers $m > n$ with opposite parity and

$$\begin{aligned} x^2 &= m^2 - n^2, \\ y^2 &= 2mn, \\ z &= m^2 + n^2. \end{aligned}$$

Hence

$$x^2 + n^2 = m^2$$

and as $\gcd(m, n) = 1$ we get that (x, n, m) is a primitive Pythagorean triple. If m is odd and n is even, we can again apply Theorem 11.9 to get that there exist r, s coprime positive integers with opposite parity, such that

$$\begin{aligned} x &= r^2 - s^2, \\ n &= 2rs, \\ m &= r^2 + s^2. \end{aligned}$$

Since m is odd and $\gcd(m, n) = 1$ we also get that $\gcd(m, 2n) = 1$. As $y^2 = 2n \cdot m$, Lemma 11.7 tells us that there exist positive integers z' and w with

$$m = z'^2, \quad 2n = w^2.$$

As w is even, there exists some positive integer v such that $w = 2v$ and hence

$$v^2 = n/2 = rs.$$

We can again apply Lemma 11.7 and get that there are positive integers x', y' such that

$$r = x'^2, \quad s = y'^2.$$

Again, as $\gcd(r, s) = 1$ we get $\gcd(x', y') = 1$ and hence

$$x'^4 + y'^4 = r^2 + s^2 = m = z'^2,$$

where x', y', z' are positive integers with $\gcd(x', y') = 1$. Additionally, from

$$z' \leq z'^4 = m^2 < m^2 + n^2 = z$$

it follows that $z' < z$.

Hence we have found another solution (x', y', z') to $x^4 + y^4 = z^2$ with a smaller z'.

To complete the proof, we assume that $x^4 + y^4 = z^2$ has at least one integer solution. By the well-ordering property, we know that among the solutions in $\mathbb{N}^3$ there exists a solution with smallest value for z. However, as we have shown that one integer solution leads to a second one with a smaller z, this leads to a contradiction. □

There are still several unsolved conjectures which have emerged from Fermat's Last Theorem, for example

Conjecture 11.22 (Beal's Conjecture)**.** *Let $a, b, c \geq 3$ be positive integers. The non-linear Diophantine equation $x^a + y^b = z^c$ has no non-trivial integer solution with gcd$(x, y) =$ gcd$(x, z) =$ gcd$(y, z) = 1$.*

If you prove this conjecture or find a counterexample, Andrew Beal has offered a prize of $ 100'000. In 1844 Catalan conjectured that the only consecutive positive integers that are both powers of integers are $8 = 2^3$ and $9 = 3^2$.

Theorem 11.23 (Catalan's Conjecture)**.** *Let $m, n \geq 2$ be positive integers. The non-linear Diophantine equation $x^m - y^n = 1$ has no solutions in $\mathbb{N}^2$, except for $x = 3, y = 2, m = 2, n = 3$.*

This conjecture (as you can see we call it a Theorem) was proven in 2002 by Mihailescu.

Finally, as an attempt to unify the Catalan conjecture and Fermat's Last Theorem, we get the last conjecture:

Conjecture 11.24 (Fermat-Catalan Conjecture)**.** *The non-linear Diophantine equation $x^a + y^b = z^c$ has at most finitely many solutions with gcd$(x, y) =$ gcd$(x, z) =$ gcd$(y, z) = 1$ and $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} < 1$.*

While the conjecture is still open, we do have several examples which satisfy the hypothesis, e.g.

$$\begin{aligned} 1 + 2^3 &= 3^2, \\ 2^5 + 7^2 &= 3^4, \\ 7^3 + 13^2 &= 2^9. \end{aligned}$$

12 Sums of Squares

In this section we want to answer two questions: which integers are the sum of two squares and what is the least integer n such that every positive integer is the sum of n squares.

We start with the first question, considering the sum of two squares. Clearly not every integer is the sum of two squares.

Example 12.1. 3 *and* 15 *are not the sum of two squares while* $5 = 1^2 + 2^2$ *and* $4 = 2^2 + 0^2$.

Since $a^2 \equiv 0, 1 \mod 4$, we must also have that $x^2 + y^2 \equiv 0, 1, 2 \mod 4$. Hence we can already exclude all integers which are 3 modulo 4.

This distinction is however not enough, as also 15 is not a sum of two squares. In fact, we have to consider their prime factorizations.

Proposition 12.2. *Let* m, n *be positive integers, which are both sums of two squares, then* mn *is also the sum of two squares.*

Proof. Let $m = a^2 + b^2, n = c^2 + d^2$, for integers a, b, c, d. Then

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

□

Example 12.3. *As* $5, 4$ *are the sum of two squares,* $20 = 2^2 + 4^2$ *is as well.*

Hence we will focus first on the primes. Clearly 2 is the sum of two squares as

$$2 = 1^2 + 1^2.$$

Since we can exclude all $p \equiv 3 \mod 4$, it is enough to consider primes $p \equiv 1 \mod 4$.

Lemma 12.4. *Let* $p \in \mathcal{P}$ *such that* $p \equiv 1 \mod 4$. *Then, there exist integers* x, y *such that* $x^2+y^2 = kp$ *for some positive integer* $k < p$.

Proof. Recall from Theorem 9.26, that -1 is a quadratic residue modulo p. Thus, there exists an integer $a < p$ such that $a^2 \equiv -1 \mod p$, which is equivalent to $a^2 + 1 = kp$ for some integer k. Hence $x^2 + y^2 = kp$ for $x = a$ and $y = 1$. Finally, since

$$kp = x^2 + y^2 \leq (p - 1)^2 + 1 < p^2$$

we get that $k < p$. □

In fact, all primes which are congruent to 1 modulo 4 are sums of two squares.

Theorem 12.5. *Let* $p \in \mathcal{P}$ *such that* $p \equiv 1 \mod 4$. *Then, there exist integers* x, y *with* $x^2+y^2 = p$.

Proof. Let $m < p$ be the smallest positive integer such that $x^2 + y^2 = mp$ from Lemma 12.4.

Assume by contradiction that $m > 1$ and let a, b be such that

$$a \equiv x \mod m, \quad b \equiv y \mod m$$

and

$$-m/2 < a \leq m/2, \quad -m/2 < b \leq m/2.$$

It follows that

$$a^2 + b^2 \equiv x^2 + y^2 \equiv mp \equiv 0 \mod m.$$

Thus, there exists an integer k such that

$$a^2 + b^2 = km.$$

We can rewrite this as

$$(a^2 + b^2)(x^2 + y^2) = (km)(mp) = km^2p.$$

By Proposition 12.2, we get that

$$(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2.$$

Since $a \equiv x, b \equiv y \mod m$ we get

$$ax + by \equiv x^2 + y^2 \equiv 0 \mod m, \quad ay - bx \equiv xy - yx \equiv 0 \mod m.$$

Thus,

$$\left(\frac{ax + by}{m}\right)^2 + \left(\frac{ay - bx}{m}\right)^2 = \frac{km^2p}{m^2} = kp$$

is the sum of two squares.

If we can show that $0 < k < m$, we get a contradiction to m being the smallest integer such that mp is the sum of two squares.

Due to the choice of a, b we get that

$$a^2 \leq m^2/4, \quad b^2 \leq m^2/4$$

and hence

$$0 \leq km = a^2 + b^2 \leq 2(m^2/4) = m^2/2$$

which implies $k \leq m/2$. Now we only need to show that $k \neq 0$.

If $k = 0$, then $a^2 + b^2 = 0$ implies that $a = b = 0$ and hence $x \equiv y \equiv 0 \mod m$. Equivalently, $m \mid x$ and $m \mid y$, thus $m^2 \mid (x^2 + y^2) = mp$. This would imply that $m \mid p$ and as $m < p$, we get $m = 1$. □

We can now put everything together, to get

Theorem 12.6. *Let n be a positive integer. Then, n is a sum of two squares if and only if each prime factor of n which is congruent to 3 modulo 4 occurs with an even power.*

Proof. Assume that there are no primes congruent to 3 modulo 4, which appear in the prime factorization of n with an odd power. We write $n = t^2u$ and $u = \prod_{i=1}^{k} p_i$ is the product of primes. Thus, no primes congruent to 3 modulo 4 appear in u.

By Proposition 12.2 each prime in u can be written as the sum of two squares.

That is, there exist integers x, y such that $x^2 + y^2 = u$.

We then get that n is also the sum of two squares as

$$n = (tx)^2 + (ty)^2.$$

For the other direction, assume that n is the sum of two squares, i.e., there exist two integers x, y such that $x^2 + y^2 = n$ and that there exists a prime $p \equiv 3 \mod 4$ which appears in the prime factorization of n with odd power $2j + 1$.

Let $\gcd(x, y) = d$ and define $a = x/d, b = y/d$, and $m = n/d^2$. Then $\gcd(a, b) = 1$ and

$$a^2 + b^2 = m.$$

Let p^k be the largest power of p which divides d. Then m is divisible by $p^{2j-2k+1}$ and $2j - 2k + 1 \geq 1$, thus $p \mid m$.

If $p \mid a$, then $p \mid (m - a^2) = b^2$ which contradicts that $\gcd(a, b) = 1$. Hence, $p \nmid a$ and there exists an integer z such that $az \equiv b \mod p$.

Thus,

$$a^2 + b^2 \equiv a^2 + (az)^2 \equiv a^2(1 + z^2) \mod p.$$

Since $a^2 + b^2 = m$ and $p \mid m$, we get that

$$a^2(1 + z^2) \equiv 0 \mod p.$$

This implies that $1 + z^2 \equiv 0 \mod p$ and hence $z^2 \equiv -1 \mod p$. This gives a contradiction to Theorem 9.26. □

We now turn to the second question: how many squares would we need to sum to get any integer? Three are not enough, e.g. 7 is not the sum of three squares.

Several mathematicians have claimed and tried to prove that 4 squares are enough. The first proof was published by Lagrange in 1770.

To prove this result, we first need the following

Lemma 12.7. *Let m, n be positive integers which are the sum of four squares, then mn is also the sum of four squares.*

Exercise 12.8. *Prove Lemma 12.7.*

Lemma 12.9. *Let $p \in \mathcal{P}$ be odd. Then, there exists a positive integer $k < p$ such that*

$$kp = x^2 + y^2 + z^2 + w^2$$

has a integer solution.

Proof. We start by showing that there are integers $0 \leq x, y < p$ such that

$$x^2 + y^2 + 1 \equiv 0 \mod p.$$

For this we consider the quadratic residues modulo p together with 0, $S = \{0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2\}$ and

$$T = \{-1 - s \mid s \in S\}.$$

Observe that S and T are disjoint. In fact, if there exist $s, s' \in S$ such that $s = -1 - s'$ then $s + s' = -1 \equiv 3 \mod 4$, but the sum of two squares cannot be 3 modulo 4. Thus, $S \cup T$ contains $p + 1$ distinct integers.

By the pigeonhole principle, there are two integers which are congruent modulo p, i.e., there exist $0 \leq x, y \leq \frac{p-1}{2}$, such that

$$x^2 \equiv -1 - y^2 \mod p.$$

Hence, $x^2 + y^2 + 1^2 + 0^2 = kp$ for some positive integer k. In fact, $k = 0$ is excluded as $x^2 + y^2 + 1 = 0$ implies that -1 is a sum of two squares.

Finally, from $x^2 + y^2 + 1 \leq 2\left(\frac{p-1}{2}\right)^2 + 1 < p^2$ it follows that $k < p$. □

Theorem 12.10. *Let $p \in \mathcal{P}$. Then, the equation $x^2 + y^2 + z^2 + w^2 = p$ has an integer solution.*

Proof. If $p = 2$, then we have $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Thus, we can assume that p is odd. From Lemma 12.9, we know that there exists a smallest positive integer m such that

$$x^2 + y^2 + z^2 + w^2 = mp$$

has a integer solution.

We hence want to show that $m = 1$.

Assume by contradiction that $m > 1$. If m is even, then either x, y, z, w are all odd, all even, or two are odd and two are even. In all these cases, we can rearrange the integers such that

$$x \equiv y \mod 2, \quad z \equiv w \mod 2.$$

Thus, $\frac{x-y}{2}, \frac{x+y}{2}, \frac{z-w}{2}, \frac{z+w}{2}$ are integers and

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

Hence we have found $n = m/2 < m$ which is also such that np is the sum of four squares, a contradiction to the minimality of m.

If m is odd, we consider the integers $-m/2 < a, b, c, d < m/2$ with

$$a \equiv x, b \equiv y, c \equiv z, d \equiv w \mod m.$$

Clearly,

$$x^2 + y^2 + z^2 + w^2 \equiv a^2 + b^2 + c^2 + d^2 \mod m$$

and hence there exists some integer k such that $a^2 + b^2 + c^2 + d^2 = km$ and due to the choice of a, b, c, d we get that

$$0 \leq a^2 + b^2 + c^2 + d^2 < 4\left(\frac{m}{2}\right)^2 = m^2,$$

hence $0 \leq k < m.$

If $k = 0$, we have $a = b = c = d = 0$ and hence $m \mid x, y, z, w$ and $m^2 \mid (x^2 + y^2 + z^2 + w^2) = mp$ implies that $m \mid p$, which is impossible as $1 < m < p.$

Hence we have $k > 0$ and

$$\left(x^2 + y^2 + z^2 + w^2\right)\left(a^2 + b^2 + c^2 + d^2\right) = m^2 kp.$$

By Lemma 12.7, we have

$$\begin{aligned}(ax + by + cz + dw)^2 + (bx - ay + dz - cw)^2 \\ +(cx - dy - az + bw)^2 + (dx + cy - bz - aw)^2 = m^2 kp.\end{aligned}$$

Each of the four terms is divisible by m as

$$\begin{aligned}ax + by + cz + dw \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \mod m,\\ bx - ay + dz - cw \equiv yx - xy + wz - wz \equiv 0 \mod m,\\ cx - dy - az + bw \equiv zx - wy - xz + yw \equiv 0 \mod m,\\ dx + cy - bz - aw \equiv wx + zy - yz - xw \equiv 0 \mod m.\end{aligned}$$

Hence we can consider the integers x', y', z', w' defined as

$$\begin{aligned}x' &= \frac{ax + by + cz + dw}{m},\\ y' &= \frac{bx - ay + dz - cw}{m},\\ z' &= \frac{cx - dy - az + bw}{m},\\ w' &= \frac{dx + cy - bz - aw}{m}.\end{aligned}$$

For which we have that

$$x'^2 + y'^2 + z'^2 + w'^2 = \frac{m^2 kp}{m^2} = kp,$$

which contradicts the minimality of m such that mp can be written as sum of four squares, as $k < m$. Thus, $m = 1$.

□

We are now ready to state the main result.

Theorem 12.11. *Every positive integer is the sum of four squares.*

Proof. Let n be a positive integer. By Theorem 12.10, each prime factor of n can be written as sum of four squares. Applying Lemma 12.7, also n is the sum of four squares. □

13 Finite Fields and more Applications

14 Glance at Algebraic Number Theory

In Elementary Number Theory, we were considering basic properties of the integers $\mathbb{Z} \subset \mathbb{Q}$, such as divisibility, primality and factorization. Algebraic number theory is interested in the same properties, but over extension fields of $\mathbb{Q}$ and their respective integers.

Definition 14.1. A *number field* is a finite field extension K of $\mathbb{Q}$, i.e., a field which is a $\mathbb{Q}$-vector space of finite dimension. This dimension is called *degree* and denoted by $k = [K : \mathbb{Q}]$.

Example 14.2. $\mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$ *is a number field of degree 2.*

Definition 14.3. We say that $\alpha \in K$ is an *algebraic integer* if α is a root of a monic polynomial with coefficients in $\mathbb{Z}$. The set of algebraic integers is denoted by $\mathcal{O}_K$.

Example 14.4. *Since* $x^2 - 2 = 0$, $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ *is an algebraic integer.*

Note that this is inline with the definition of integers over $\mathbb{Q}$:

Proposition 14.5. $\mathbb{Z}$ *are the algebraic integers of* $\mathbb{Q}$.

Proof. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with coefficients $a_i \in \mathbb{Z}$. Assume $\frac{p}{q} \in \mathbb{Q}$ is such that $q \neq 1, -1$ and is in lowest terms. If $\frac{p}{q}$ is a root of $f(x)$, then

$$q^n f(\frac{p}{q}) = p^n + a_{n-1}qp^{n-1} + \cdots + a_0q^n = 0.$$

Hence modulo q, we have that

$$p^n + a_{n-1}qp^{n-1} + \cdots + a_0q^n \equiv p^n \equiv 0 \mod q,$$

and this contradicts gcd$(p, q) = 1$. □

Definition 14.6. The quadratic number field $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$, where $i = \sqrt{-1}$ is called the *Gaussian rationals.*

We will focus in the rest of this chapter on $\mathbb{Q}(i)$, however most of the introduced concepts extend to any number field K.

Proposition 14.7. *The algebraic integers of* $\mathbb{Q}(i)$ *are given by*

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

and called Gaussian integers.

Proof. Let $\gamma = a + bi$ with $a, b \in \mathbb{Z}$, then γ is the root of the monic polynomial

$$x^2 - 2ax + (a^2 + b^2).$$

$\square$

Exercise 14.8. *Finish the proof, by showing: if $\alpha = r + si$, with $r, s \in \mathbb{Q}$, and α is the root of a monic polynomial with integer coefficients, then $r, s \in \mathbb{Z}$.*

Algebraic integers are closed under addition, multiplication and subtraction (in fact they form a ring).

Exercise 14.9. *Let $\alpha = r + is, \beta = t + iu$ with $r, s, t, u \in \mathbb{Z}$. Show that $\alpha + \beta, \alpha - \beta, \alpha\beta \in \mathbb{Z}[i]$.*

Definition 14.10. Let $\alpha, \beta \in \mathbb{Z}[i]$. We say that α divides β, denoted by $\alpha \mid \beta$, if there exists $\gamma \in \mathbb{Z}[i]$ such that $\beta = \alpha\gamma$.

Example 14.11. $(2 - i) \mid (13 + i)$ *since*

$$(2 - i)(5 + 3i) = 13 + i.$$

On the other hand $(3 + 2i) \nmid (6 + 5i)$ *as*

$$\frac{6 + 5i}{3 + 2i} = \frac{28}{13} + \frac{3}{13}i \notin \mathbb{Z}[i].$$

Having divisibility established, we can ask for units in $\mathbb{Z}[i]$.

Definition 14.12. A Gaussian integer ε is called *unit*, if $\varepsilon \mid 1$. For ε a unit, we call $\varepsilon\alpha$ the associate of α.

Theorem 14.13. *A Gaussian integer $\varepsilon = a+bi$ is a unit if and only if it has norm $N(\varepsilon) = a^2+b^2 = 1$.*

Proof. If ε is a unit, then there exists a $\nu \in \mathbb{Z}[i]$ such that $\varepsilon\nu = 1$. Hence

$$1 = N(\varepsilon\nu) = (ac - bd)^2 + (ad + cb)^2 = (a^2 + b^2)(c'2 + d^2) = N(\varepsilon)N(\nu).$$

Since $N(\varepsilon), N(\nu) \in \mathbb{N}$, we get that $N(\nu) = N(\varepsilon) = 1$.

Conversely, assume that $N(\varepsilon) = 1$ and consider its conjugate $\varepsilon' = a - bi$. Then

$$\varepsilon\varepsilon' = (a + bi)(a - bi) = a^2 + b^1 = N(\varepsilon) = 1$$

and hence $\varepsilon \mid 1$. $\square$

Theorem 14.14. *The units in the Gaussian integers are $1, -1, i, -i$.*

Proof. From Theorem 14.13, we know that $\varepsilon = a + bi$ is a unit if and only if $N(\varepsilon) = a^2 + b^2 = 1$. Since $a, b \in \mathbb{Z}$, we can only have

$$(a, b) \in \{(0, 1), (1, 0), (0, -1), (-1, 0)\}.$$

□

We can then also define primes.

Definition 14.15. A Gaussian integer π is a Gaussian prime, if π is not a unit and is divisible only by units and its associates.

It follows that any Gaussian prime has 8 divisors:

$$1, -1, -i, -i, \pi, -\pi, i\pi, -i\pi.$$

Theorem 14.16. *If π is a Gaussian integer with $N(\pi) = p$, then π, π' are Gaussian primes, and p is not.*

Proof. Assume that $\pi = \alpha\beta$ for $\alpha, \beta \in \mathbb{Z}[i]$. Then

$$p = N(\pi) = N(\alpha\beta) = N(\alpha)N(\beta).$$

Since $N(\alpha), N(\beta) \in \mathbb{N}$, we must have $N(\alpha) = 1$ or $N(\beta) = 1$ and hence either α or β is a unit and thus π a Gaussian prime.

Since $N(\pi) = \pi\pi' = p$ it follows that p is not a Gaussian prime and since $N(\pi') = p$ also π' is a Gaussian prime. □

Example 14.17. $2 - i$ *is a Gaussian prime since*

$$N(2 - i) = 2^2 + 1^2 = 5.$$

Primes also do what they are supposed to do:

Lemma 14.18. *If π is a Gaussian prime and $\alpha, \beta \in \mathbb{Z}[i]$ such that $\pi \mid \alpha\beta$, then $\pi \mid \alpha$ or $\pi \mid \beta$.*

Proof. Assume $\pi \nmid \alpha$, then $\varepsilon\pi \nmid \alpha$ for ε a unit. Since the only divisors of π are

$$1, -1, i, -i, \pi, -\pi, i\pi, -i\pi$$

we get that $\gcd(\alpha, \pi) = 1$. Hence (by the generalization of Bézout's theorem) there exist $\mu, \nu \in \mathbb{Z}[i]$ such that

$$1 = \mu\pi + \nu\alpha,$$

and multiplying both sides with β we get

$$\beta = \pi(\mu\beta) + \nu(\alpha\beta)$$

and as $\pi \mid \alpha\beta$ we get that $\pi \mid \beta$. □

We can further define an version of the Euclidean Algorithm for Gaussian integers and define the greatest common divisor as usual:

Definition 14.19. Let $\alpha, \beta \in \mathbb{Z}[i]$. Then we define the *greatest common divisor* as $\gcd(\alpha, \beta) = \gamma$ with

1. $\gamma \mid \alpha, \gamma \mid \beta$,
2. if $\delta \mid \alpha$ and $\delta \mid \beta$ then $\delta \mid \gamma$.

We say that α and β are coprime if $\gcd(\alpha, \beta) = 1$.

This all brings us to one fundamental question (pun intended).

Does the Fundamental Theorem of Arithmetic still hold over algebraic integers?

For $\mathbb{Z}[i]$, the answer is yes, and this will be the final Theorem of this lecture. However, this is not true for any number field.

Example 14.20. *Let us consider $\mathbb{Q}(\sqrt{-5})$ with the algebraic integer $\mathbb{Z}[\sqrt{-5}]$. Then*

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

Fortunately, we do have a similar result: Every ideal can be uniquely decomposed into prime ideals. The proof is clearly omitted, but you can see the parallels between $\mathbb{Z}$ and any $\mathcal{O}_K$.

Theorem 14.21 (Unique Factorization for Gaussian Integers)**.** *Let $\gamma \in \mathbb{Z}[i] \setminus \{0\}$ not be a unit, then γ can be written uniquely as a product of Gaussian primes.*

Uniquely, as usual refers to unique up to reordering.

Proof. We proceed by induction on $N(\gamma)$.

Since $\gamma \neq 0$ is not a unit we have that $N(\gamma) \neq 1$ and hence $N(\gamma) \geq 2$.

If $N(\gamma) = 2$, then γ is a Gaussian prime and can thus be written as product of Gaussian primes.

If $N(\gamma) > 2$, we assume that every Gaussian integer δ with $N(\delta) < N(\gamma)$ can be written as product of Gaussian primes.

Note that if γ is a Gaussian prime, then clearly it can be written as product of Gaussian primes. Thus assume that $\gamma = \alpha\beta$ for $\alpha, \beta \in \mathbb{Z}[i]$ not units. Thus, $N(\alpha), N(\beta) > 1$.

Since

$$2 \leq N(\gamma) = N(\alpha)N(\beta),$$

we get that $2 \leq N(\alpha), N(\beta) < N(\gamma)$. By the hypothesis, α and β can be written as product of Gaussian primes, thus $\gamma = \alpha\beta$ can too.

To show uniqueness, we again proceed via induction.

Since $\gamma \neq 0$ is not a unit, we have $N(\gamma) \geq 2$. Note that if $N(\gamma) = 2$, then γ is already a Gaussian prime, which by definition cannot be divisible by any Gaussian integer except units. Thus, γ can be written uniquely as product of Gaussian primes (itself).

We assume that for any $\delta \in \mathbb{Z}[i]$ with $N(\delta) < N(\gamma)$, the statement is true, that is δ can be written uniquely as product of Gaussian primes.

Now assume γ can be written in two ways

$$\gamma = \pi_1 \cdots \pi_s = \rho_1 \cdots \rho_t,$$

for Gaussian primes π_i, ρ_i.

Since $\pi_1 \mid \pi_1 \cdots \pi_s$ we get that $\pi_1 \mid \rho_1 \cdots \rho_t$. By Lemma 14.18, we get that $\pi_1 \mid \rho_i$ for some i. We can assume that $\pi_1 \mid \rho_1$. Since ρ_1 is a Gaussian prime, it is only divisible by units and its associates. Thus, we get that

$$\rho_1 = \varepsilon \pi_1,$$

for some unit ε.

Thus,

$$\pi_1 \pi_2 \cdots \pi_s = \varepsilon \pi_1 \rho_2 \cdots \rho_t.$$

Dividing both sides by π_1 we get

$$\pi_2 \cdots \pi_s = \varepsilon \rho_2 \cdots \rho_t.$$

Since $N(\pi_1) \geq 2$ we get that

$$1 \leq N(\pi_2 \cdots \pi_s) < N(\pi_1 \cdots \pi_s) = N(\gamma)$$

and we can apply the induction hypothesis, getting that

$$\pi_2 \cdots \pi_s = \varepsilon \rho_2 \cdots \rho_t$$

has a unique factorization into Gaussian primes. That is $s = t$ and $\pi_i = \rho_i$. □

References

[1] G. A. Jones and J. M. Jones. *Elementary number theory*. Springer Science & Business Media, 1998.

[2] K. H. Rosen. *Elementary number theory*. Pearson Education London, 2011.

[3] V. Weger. *Information Set Decoding in the Lee Metric and the Local to Global Principle for Densities*. PhD thesis, University of Zurich, 2020.