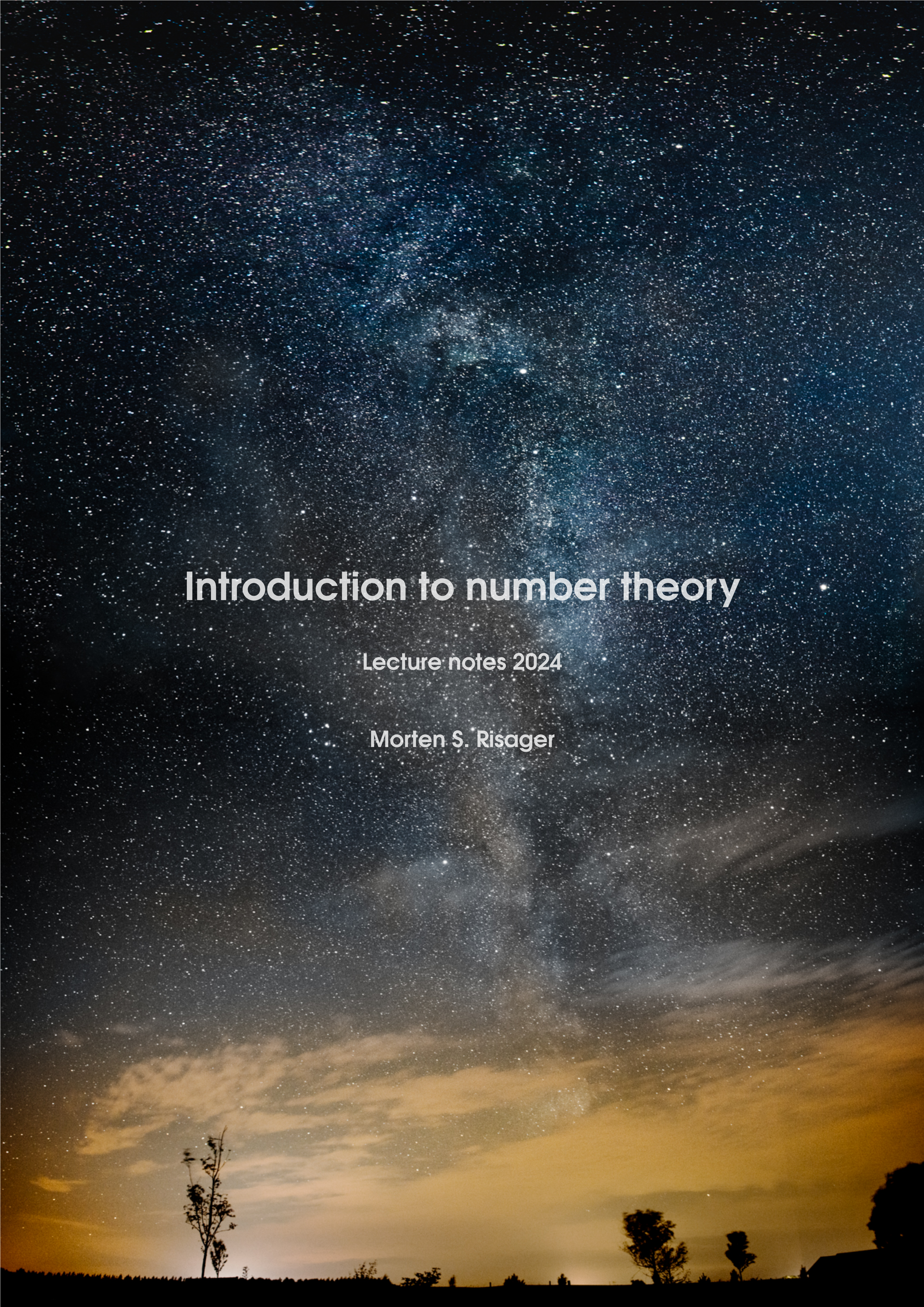


Introduction to number theory

Lecture notes 2024

Morten S. Risager

These are notes for the 7 week course “Introduction to Number Theory” at the University of Copenhagen.
Cover photo kindly provided by Christian Rasmussen.

Please send comments and corrections to risager@math.ku.dk
Last compiled with LaTeX 2_ε on April 10, 2024.

Contents

Introduction

Number theory has a long history in mathematics. Indeed its problems and concepts have played a formative role in many branches of mathematics. Even today it is a vibrant and active part of modern mathematics, and it continues to offer new insights and stimulate the creation of new mathematical subdisciplines and theories.

Historically there is a clear tendency that number theory has been driven by the desire to tackle specific problems, e.g.: Does there exist positive integer solutions to the equation

$$x^n + y^n = z^n$$

for $n \geq 3$ (the answer is no)? Are there infinitely many twin primes (we do not know)? Trying to answer such questions has often taken precedence, rather than generalizing the theory as much as possible. This comment should not be taken as an indication that number theory does not use or develop deep theories, but merely as statement of what motivates and drives many number theorists.

This text gives an introduction to the many facets of number theory, including tastes of its algebraic, analytic, metric, Diophantine and geometric incarnations. We assume the reader has taken a first course in algebra and has familiarity with groups as well as modular arithmetic.

The text is somewhat brief at points, and we strongly encourage the reader to dive into other texts on number theory to get a more multifaceted view on the subject. Several are listed in the bibliography and they all offer their own unique views on the topic.

1. Divisibility and primes

1.1 Notation and basic properties

We denote by

- $\mathbb{N}$ the set of natural numbers $1,2,3,\ldots$,
- $\mathbb{Z}$ the set of integers,
- $\mathbb{Q}$ the set of rationals,
- $\mathbb{R}$ the set of real numbers, and
- $\mathbb{C}$ the set of complex numbers.

If $a,b \in \mathbb{Z}$ we say that a *divides* b and write $a \mid b$ if there exists $c \in \mathbb{Z}$ such that $b = ac$. We call a a *factor* of b. If a does *not* divide b we write $a \nmid b$.

Proposition 1.1.1 Let $a,b,c,d \in \mathbb{Z}$. Then

(i) if $a \mid b$ and $b \mid c$ then $a \mid c$.
(ii) if $a \mid b$ and $c \mid d$ then $ac \mid bd$.
(iii) if $m \neq 0$ then $a \mid b$ if and only if $ma \mid mb$.
(iv) if $d \mid a$ and $a \neq 0$ then $|d| \leq |a|$.

Proof. See Exercise 1.5. ■

1.2 Euclidean division and greatest common divisor

We start by stating and proving a fundamental property of the integers that we learn already in elementary school.

Theorem 1.2.1 — Euclidean division. Let $a,b \in \mathbb{Z}$ with $b \neq 0$. Then there exist unique integers q, r satisfying $0 \leq r < |b|$ and $a = bq + r$.

Proof. The case $a = 0$ is left as an easy exercise. See exercise 1.7.

We first reduce to the case $a,b > 0$. If $b < 0$ we let $b' = -b$ and a unique solution to $a = b'q' + r'$ with $0 \leq r' < b'$ gives a unique solution $q = -q'$, $r = r'$ to $a = bq + r$ with $0 \leq r < |b|$. Hence we may assume $b > 0$. If $a < 0$ and $b > 0$ we let $a' = -a$. Then a unique solution to $a' = bq' + r'$ gives a unique solution $q = -q' - 1$, $r = b - r'$ to $a = bq + r$ with $0 \leq r < |b|$. We may therefore assume $a, b > 0$.

If $a, b > 0$ consider

$$Q = \{n \in \mathbb{Z} | n \geq 0, a - bn \geq 0\}.$$

This set is non-empty ($0 \in Q$) and bounded (if $n > a/b$ then $a - bn < 0$). Let $q \in Q$ be its maximal element. Then $r = a - bq < b$ since if $a - bq \geq b$ then $a - b(q+1) \geq 0$ which contradicts the maximality of q. This proves existence in this case.

To prove uniqueness suppose q', r' is another set of integers satisfying the conclusion. Then $q' \in Q$ so $q' \leq q$. If $q' < q$ then

$$r' = a - bq' = a - b(q + (q' - q)) = r - b(q' - q) \geq b$$

which is a contradiction. Hence $q = q'$ and $r = r'$, which proves uniqueness in this case. ■

▪ **Example 1.1** The integers q, r from Euclidean division can be found by standard long division: Given $a = 36948, b = 2100$ we find

$$\begin{array}{l} 36948 : 2100 = 17 \\ \underline{2100} \\ 15948 \\ \underline{14700} \\ \ \ 1248 \end{array}$$

so $36948 = 2100 \cdot 17 + 1248$ i.e. $q = 17$, $r = 1248$. ▪

As an example of the power of Theorem 1.2.1 we prove a simple result about division. This will be somewhat easier to prove after we have proved the fundamental theorem of arithmetic below (Theorem 1.4.2) but the following simple proof shows that it can be proved without the use of unique factorization.

Proposition 1.2.2 Assume $m^2 \mid b^2$. Then $m \mid b$.

Proof. Certainly there exist natural numbers l such that $m \mid bl$ (e.g. $l = m$). By the well-ordering principle we can let l_0 be the smallest such number. Let n, k be the integers such that $b^2 = m^2 n$, $bl_0 = mk$. Notice that $mbk = b^2 l_0 = m^2 n l_0$ so $bk = mnl_0$. By Theorem 1.2.1 we can write $k = ql_0 + r$ with $0 \leq r < l_0$. But then

$$br = b(k - ql_0) = mnl_0 - bql_0 = m(nl_0 - qk)$$

so m divides br. By the minimality of l_0 we must have $r = 0$. But then $bl_0 = mk = mql_0$ which shows that $b = mq$. ■

Definition 1.2.1 Given $a, b \in \mathbb{Z}$ not both zero we define their *greatest common divisor* as as the largest natural number which divides both a and b, i.e.

$$\gcd(a, b) = \max\{d \in \mathbb{N} : d \mid a, d \mid b\}.$$

We define $\gcd(0, 0) = 0$

We note that 1 divides any integer, and that if $d \mid a$ then $|d| \leq |a|$ so the maximum in the above definition is over a finite non-empty set.

Proposition 1.2.3 Let $a, b \in \mathbb{Z}$. Then

$$gcd(a,b) = gcd(b,a) = gcd(-a,b) = gcd(a,-b) = gcd(a,b \pm a)$$

Proof. We prove that $gcd(a,b) = gcd(a,b+a)$. The other identities are proved a similar way. Let $g_1 = gcd(a,b)$ and $g_2 = gcd(a,a+b)$. Since $g_1 \mid a$ and $g_1 \mid b$ we have $g_1 \mid a+b$ so g_1 is a common divisor of a and $a+b$. It follows that $g_1 \leq g_2$. Similarly g_2 is a divisor of a and $a+b$ and therefore also of a and $b = (a+b)-a$. Hence $g_2 \leq g_1$ which completes the proof. ■

The greatest common divisor of two integers a,b can be computed effectively as follows: We have $\gcd(a,0) = \gcd(a,\pm a) = |a|$. If $ab \neq 0$, $|a| \neq |b|$ we may use Proposition 1.2.3 to reduce to the case $a > b > 0$. Using Theorem 1.2.1 we write $a = bq + r$ with $0 \leq r < b$. By repeated use of Proposition 1.2.3 we see that $\gcd(a,b) = \gcd(r,b)$. If $r = 0$ we have $\gcd(a,b) = b$. If not we repeat the above argument with $a' = b$, $b' = r$. This procedure will eventually terminate since r goes down by at least one in each step. This procedure is called *Euclid's algorithm*.

■ **Example 1.2** Consider $a = 567$ and $b = 32$. We use Euclid's algorithm and find

$$\begin{aligned}
567 &= 17 \cdot 32 + 23 && \text{so } \gcd(567,32) = \gcd(23,32) \\
32 &= 1 \cdot 23 + 9 && \text{so } \gcd(32,23) = \gcd(9,23) \\
23 &= 2 \cdot 9 + 5 && \text{so } \gcd(23,9) = \gcd(5,9) \\
9 &= 1 \cdot 5 + 4 && \text{so } \gcd(9,5) = \gcd(4,5) \\
5 &= 1 \cdot 4 + 1 && \text{so } \gcd(5,4) = \gcd(1,4) \\
4 &= 4 \cdot 1 + 0 && \text{so } \gcd(4,1) = \gcd(0,1) = 1
\end{aligned}$$

and we may conclude that $\gcd(567,32) = 1$. ■

We see that this procedure constructs integers $a_0 = a$, $b_0 = r_0 = b$,

$$a_i = q_i b_{i-1} + r_i \tag{1.1}$$

with $0 \leq r_i < r_{i-1}$. This ends when $r_n = 0$ and in this case $r_{n-1} = gcd(a,b)$.

Theorem 1.2.4 — Bezout's identity. Let a, b be integers not both zero. Then there exist an integer solution $x, y \in \mathbb{Z}$ to the equation

$$\gcd(a,b) = ax + by.$$

Proof. One way of proving this is to take the procedure described immediately before the theorem and then use backwards substitution. Here is another proof that has the advantage of giving an alternative characterization of $\gcd(a,b)$:

Consider

$$S = \{ax + by > 0 | x, y \in \mathbb{Z}\} \subseteq \mathbb{N}$$

Clearly S is non-empty. Let $g = ax_0 + by_0 \in S$ be its smallest element. Then $g \mid a$ since if not $a = gq + r$ with $0 < r < g$ by Theorem 1.2.1. But since $r = a - gq = a - qax_0 - by_0q = a(1-qx_0) - by_0q \in S$ this contradicts the minimality of g. By the same argument $g \mid b$. Hence g is a common divisor i.e. $g \leq \gcd(a,b)$.

Clearly $gcd(a,b) \mid ax_0 + bx_0 = g$ so $gcd(a,b) \leq g$, and we may conclude that $gcd(a,b) = g$. ■

R We notice that the proof of Theorem 1.2.4 actually proves that for any $a, b \in \mathbb{Z}$ we have

$$gcd(a,b) = \min\{ax + by > 0 | x, y \in \mathbb{Z}\}.$$

From this observation we easily deduce the following corollary:

Corollary 1.2.5 Let $a,b \in \mathbb{Z}$. Then $\gcd(na,nb) = |n|\gcd(a,b)$.

■ **Example 1.3** In the proof of Theorem 1.2.4 we used the well-ordering principle for $\mathbb{N}$ i.e. that any non-empty subset of the natural numbers contains a smallest element to prove the existence of solutions to the integer equation $gcd(a,b) = ax+by$. If we want to actually find such a solution we may use the procedure described above for finding $gcd(a,b) = r_{n-1}$: We see from (1.1) that we can express r_{n-1} as an integer linear combination of a_{n-1} and b_{n-2}. Doing successive substitution of the previous equation we arrive at the result.

With the integers from Example 1.2 we find that

$$\begin{aligned} gcd(567,32) = 1 &= 5-1\cdot 4 \\ &= 5-1\cdot(9-1\cdot 5) = -9+2\cdot 5 \\ &= -9+2\cdot(23-2\cdot 9) = 2\cdot 23-5\cdot 9 \\ &= 2\cdot 23-5\cdot(32-23) = -5\cdot 32+7\cdot 23 \\ &= -5\cdot 32+7\cdot(567-17\cdot 32) = 7\cdot 567-124\cdot 32 \end{aligned}$$

so we find a solution $x = 7$, $y = -124$. ■

Definition 1.2.2 Let $a,b \in \mathbb{Z}$. We call a,b *coprime* or *relatively prime* if $gcd(a,b) = 1$.

Proposition 1.2.6

(i) The integers a,b are coprime if and only if $1 = ax+by$ for some $x,y \in \mathbb{Z}$.
(ii) Let $d = \gcd(a,b)$. Then the integers a/d and b/d are coprime.
(iii) Assume a,b are coprime and $a \mid c$ and $b \mid c$. Then $ab \mid c$.
(iv) Assume a,b are coprime and $a \mid bc$. Then $a \mid c$.

Proof. The claim in (i) follows directly from the remark after Theorem 1.2.4. The remaining 3 claims all use (i).

To prove (ii) we use again Theorem 1.2.4 and divide $ax+by = d$ by d. Then (i) proves the claim. To see (iii) we note that on the assumptions we have $c = ea$ and $c = fb$ so by (i) we have $c = c(ax+by) = fbax+eaby = ab(fx+ey)$ which proves the claim. To prove (iv) we note if a,b are relatively prime and $bc = da$ then by (i) we have $c = c(ax+by) = cax+day = a(cx+dy)$ which shows that $a \mid c$. ■

1.3 Diophantine equations

Let $p(X_1,\dots,X_n) \in \mathbb{Z}[X_1,\dots,X_n]$ be a polynomial in n variables with integer coefficients. We want to find *integer* solutions to the equation $p(X_1,\dots,X_n) = 0$. Such equations are usually called *Diophantine equations* and they are of central importance in number theory.

1.3.1 Linear equations

We are now ready to discuss this in the simplest possible case namely the case $p(X,Y) = aX+bY-c$ where $a,b,c \in \mathbb{Z}$:

Theorem 1.3.1 Assume $a,b,c \in \mathbb{Z}$ with a,b not both zero. Let $d = \gcd(a,b)$. Then the equation

$$ax+by = c$$

has integer solutions if and only if $d \mid c$. If $d \mid c$ the complete solution consists of all pairs of the form

$$(x,y) = \frac{c}{d}(x_0,y_0) + n \cdot \left(\frac{b}{d}, -\frac{a}{d}\right)$$

where $n \in \mathbb{Z}$. Here (x_0,y_0) is any particular solution to $ax+by = gcd(a,b)$.

Proof. If an integer solution (x,y) exists then since d divides a and b it also divides $ax+by = c$.

If on the other hand $d \mid c$ then we pick a solution (x_0,y_0) of $ax_0+by_0 = d$ which is possible by Bezout's identity (Theorem 1.2.4). It is then clear that $\frac{c}{d}(x_0,y_0)$ is a solution to $ax+by = c$. Let now (x,y) be any integer solution. Then $(u,v) = (x,y) - \frac{c}{d}(x_0,y_0)$ is an integer solution to

$$au+bv = 0$$

and therefore also to

$$\frac{a}{d}u + \frac{b}{d}v = 0 \tag{1.2}$$

It follows from Proposition 1.2.6 (ii) that a/d and b/d are coprime. By Proposition 1.2.6 (iv) we can conclude that $b/d \mid u$, i.e. $u = nb/d$ for some $n \in \mathbb{Z}$. Substituting back into 1.2 we find that $v = -(a/d)n$. We have now proved that any integer solution is of the form

$$(x,y) = \frac{c}{d}(x_0,y_0) + n\left(\frac{b}{d}, -\frac{a}{d}\right)$$

for some integer n. It is easy to see – by direct verification – that all such integer pairs are indeed solutions. ■

■ **Example 1.4** We find all solution to

$$1485x + 1745y = 15$$

We start by finding the greatest common divisor of 1485 and 1745. Using division with remainder we have

$$\begin{aligned}
1745 &= 1 \cdot 1485 + 260\\
1485 &= 5 \cdot 260 + 185\\
260 &= 1 \cdot 185 + 75\\
185 &= 2 \cdot 75 + 35\\
75 &= 2 \cdot 35 + 5\\
35 &= 7 \cdot 5 + 0
\end{aligned}$$

so by the discussion before Theorem 1.2.4 we have $\gcd(1485,1745) = 5$, and since $5 \mid 15$ there are infinitely many solutions. Doing backwards substitution we find

$$\begin{aligned}
5 &= 75 - 2 \cdot 35\\
&= 75 - 2(185 - 2 \cdot 75) = 5 \cdot 75 - 2 \cdot 185\\
&= 5 \cdot (260 - 185) - 2 \cdot 185 = 5 \cdot 260 - 7 \cdot 185\\
&= 5 \cdot 260 - 7 \cdot (1485 - 5 \cdot 260) = 40 \cdot 260 - 7 \cdot 1485\\
&= 40 \cdot (1745 - 1485) - 7 \cdot 1485\\
&= 40 \cdot 1745 - 47 \cdot 1485
\end{aligned}$$

Using Theorem 1.3.1 we find that the complete solution is

$$(x,y) = 3 \cdot (-47,40) + n\left(\frac{1745}{5}, -\frac{1485}{5}\right) = (-141,120) + n \cdot (349,-297)$$

■

1.4 Primes

We recall the definition of primes:

Definition 1.4.1 A natural number $p > 1$ is called a *prime* if its only divisors are 1 and p. A natural number $n > 1$ which is not a prime is called a *composite* number.

We note that by this definition 1 is neither composite or prime. Historically 1 has been considered a prime for a long time, but certain theorems become easier to formulate if this is not so.

■ **Example 1.5** This is the first 100 primes: $2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97,101,103,107,109,113,127,131,137,139,149,151,157,163,167,173,179,181,191,193,197,199,211,223,227,229,233,239,241,251,257,263,269,271,277,281,283,293,307,311,313,317,331,337,347,349,353,359,367,373,379,383,389,397,401,409,419,421,431,433,439,443,449,457,461,463,467,479,487,491,499,503,509,521,523,541$.

Short lists like this can be easily found by hand. For a given n we note that if n is composite then $n = ab$ where either a or b is at most $\sqrt{n}$. Hence if we have checked that n has no factors less than $\sqrt{n}$ it must be prime. (See Exercise 1.8). Using Eratosthenes' sieve we can find a complete list of small primes. Much longer lists can be found online e.g. at primes.utm.edu. ■

R There is a very clever algorithm (published in 2004) based on Fermat's little theorem (See Corollary 2.3.2) which checks whether a number is prime or not. The algorithm is called AKS after its inventors Agrawal, Kayal and Saxena. We will encounter several algorithms later which verifies whether a number is prime or not, but a major interest in AKS is that it is the first algorithm that *provably* runs in 'computational time' bounded by a polynomial in $\log(p)$ where p is the number we want to investigate if it is a prime or not. Hence the required time is polynomial in the number of digits of p. For more information see [AKS04; Gra05].

Maybe the most important fact about prime numbers is the fundamental theorem of arithmetic. The crucial result we need to prove it, uses the divisibility results from Section 1.2:

Lemma 1.4.1 — Euclid. Let $a, b \in \mathbb{Z}$ and assume p is a prime. If $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof. If $p \mid a$ we are done. Assume not: Then $\gcd(p,a) = 1$, for if $\gcd(p,a) \neq 1$ then since $1, p$ are the only divisors of p then $\gcd(p,a) = p$ which in particular means that $p \mid a$ but we have assumed this not to be the case, i.e. $\gcd(p,a) = 1$. Using Bezout (Theorem 1.2.4) we find that there exist integers x_0, y_0 such that $x_0 p + y_0 a = 1$. Multiplying this by b we find that

$$x_0 pb + y_0 ab = b$$

Since $p \mid ab$ we see that $p \mid b$ which finishes the proof. ■

1.4.1 The fundamental theorem of arithmetic

We are now ready to prove the main result:

Theorem 1.4.2 — The fundamental theorem of arithmetic. Every natural number $n > 1$ can be written as a product of primes. The product is unique up to permutation of terms.

We interpret 1 as being written as the empty product over primes.

Proof. Let $X \subseteq \mathbb{N}$ be the set of natural numbers which *can not* be written as a product of primes. To see that X is the empty set assume that it is not, and let n be its smallest member. Then n cannot be a prime (then it is clearly a product of primes), so it has a factorization $n = ab$ where $a, b < n$. But by minimality a, b are not in X so they can both be written as a product of primes, which implies that n is a product of primes. But then n is not in X which shows that X is the empty set. Hence every $n > 1$ can be written as a product of primes.

To show that such a product is unique we assume that

$$p_1 p_2 \cdots p_d = q_1 \cdots q_l$$

By successive use of Lemma 1.4.1 we find that $p_d = q_j$ for some $j = 1, \ldots l$. By possibly renaming the q_i's we may assume that $p_d = q_l$. Cancelling by q_l we find

$$p_1 p_2 \cdots p_{d-1} = q_1 \cdots q_{l-1}$$

Repeating this argument d times we find

$$1 = q_1 \cdots q_{l-d}$$

But this is only possible if $l = d$, which means we have removed all primes q_j on the right. The claim follows. ■

R The fundamental theorem of arithmetic says that every natural number can be factored in primes. Is factoring a given number n 'easy'or 'hard'? We discussed earlier that the AKS-algorithm determines whether a number n is prime or not, and does so in polynomial time in the digits of n, i.e. determining whether a number is prime is 'easy'. If n is *not* a prime the AKS algorithm does not give a factorization of n. It is a big unsolved problem if there exist a polynomial time algorithm which *factors* n. There is an algorithm due to Schor [Sho94; Sho97] which can do prime factorizations on quantum computers in polynomial time. However quantum computing is still in its infancy, so this has not had great practical use so far. As we shall see later some of the most used cryptosystems like RSA relies on the fact that noone knows how to factor 'easily'.

Theorem 1.4.3 There are infinitely many prime numbers.

Proof. We will construct infinitely many prime numbers recursively. 2 is a prime. Assume now that we have a list of n primes $p_1, p_2, \ldots p_n$. Multiplying them together, adding 1, and then using the fundamental theorem of arithmetic (Theorem 1.4.2) we have

$$p_1 p_2 \cdots p_n + 1 = q_1 q_2 \ldots q_l \tag{1.3}$$

where $q_1, \ldots q_l$ are (not necessarily distinct) primes. We now notice that $q_j \neq p_i$ for all i, j since if $p_i = q_j = p$ then by (1.3) we find $p \mid 1$ which is impossible. Letting p_{n+1} be the smallest of the q_j's we have added one extra prime to our list. Doing this recursively we see that we can construct arbitrarily many primes. ■

The first few terms in the sequence of primes constructed in the proof of Theorem 1.4.3 are

$$2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, 5471, 52662739, \ldots$$

This is usually called the Euclid-Mullin sequence.

Conjecture 1.4.4 The Euclid-Mullin sequence contains all primes.

The numerical evidence for this conjecture is very sparse. Only the first 51 terms are known (the last term found September 2012). For primes less than 100 we do not know if 41, 47, 67, 73, 79, 83 are in the Euclid-Mullin sequence.

Even if we know that there are at infinitely many primes we have of course only explicitly computed finitely many. The largest known prime is $2^{82589933}-1$ which is a monstrous number with 24862048 decimal digits. It was found in December 2018. If you want to join the prime-finding community go to GIMPS or PrimeGrid. The only thing you have to do is to run a piece of software on your computer.

It was fairly straightforward to prove that there are infinitely many primes. Consider two coprime integers a and b. Then it is natural to ask if there are infinitely many primes of the form $an+b$ i.e. infinitely many primes which has remainder b if we divide by a. This is indeed so, but except for a few simple choices of a and b this turns out to be significantly harder to prove. It was first proved by Dirichlet more that 2000 years after Euclid's result (Theorem 1.4.3). See [Apo76, Thm 7.9] for an accessible proof.

1.4.2 On the number of primes less than a given size

Consider the function $\pi(x)$ which counts the number of primes less than a given size

$$\pi(x)=\#\{p\leq x|p \text{ prime}\}.$$

where x is any real number. Theorem 1.4.3 can be formulated as $\pi(x)\to\infty$ as $x\to\infty$. The proof of Theorem 1.4.3 can be used to show a bit more. One can use the proof to see that $\pi(x)\geq\log_2(\log_2(x))$ (See Exercise 1.13). Much more is true: By a relatively elementary argument one can show that for $x>2$ we have $\pi(x)\geq\frac{1}{6}\frac{x}{\log(x)}$ ([Apo76, Thm 4.6]) as well as an analogous upper bound $6\frac{x}{\log(x)}$. Riemann was probably the first to fully understand the link between $\pi(x)$ and the Riemann zeta function

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

which we shall study more in Chapter 5. Hadamard and de la Vallée Poussin proved in 1896, using Riemann's insights, that in fact

$$\pi(x)\sim\frac{x}{\log(x)}, \tag{1.4}$$

meaning that the quotient of the two sides converges to 1 as $x\to\infty$. This result is called the prime number theorem and its validity was conjectured independently by Gauss and Legendre 100 years earlier. The prime number theorem is very powerful, but we expect a much stronger result to be true: The Riemann hypothesis, which is usually stated in terms of the zeros of $\zeta(s)$, is equivalent to the following conjecture:

Conjecture 1.4.5 For every $\varepsilon>0$ we have $\pi(x)-\int_2^x\frac{1}{\log(t)}dt=O(x^{1/2+\varepsilon})$.

1.4.3 Pythagorean triples

We now discuss another example of a Diophantine equation: Consider the polynomial equation

$$P(X,Y,Z)=X^2+Y^2-Z^2=0.$$

By Pythagoras' theorem solutions with $X,Y,Z>0$ to this equation corresponds to side lengths in right triangles. Given an integer solution (e.g. $(X,Y,Z)=(3,4,5)$) we can always multiply this by an integer m and get another integer solution (mX,mY,mZ). Such solutions will always have m as a common factor. Solutions (X,Y,Z) without common factor are called *primitive*. Note that if two of X, Y, Z has a common factor the third has the same factor.

Observe now that no primitive solution has $Z=0$, and if (X,Y,Z) is a primitive solution then $(X,Y,-Z)$ is also a primitive solution. Since X and Y has no common factor they cannot both be even. We claim that they also cannot both be odd. If they were then Z^2 would be of the form $2+4k$ for some k. But no perfect square is of this form, so one of X, Y is even and the other is odd. Given a primitive solution (X,Y,Z) we have that (Y,X,Z) is also a solution and this mapping interchanges the primitive solutions with X even with the primitive solutions with X odd.

We now parametrize all primitive solutions.

Theorem 1.4.6 The primitive integer solution to the equation

$$X^2+Y^2=Z^2 \tag{1.5}$$

with X odd, Y even and $Z>0$ are exactly the triples

$$(X,Y,Z)=(p^2-q^2,-2pq,p^2+q^2)$$

where p,q are coprime integers with $p\geq 0$ satisfying $p-q$ is odd.

Proof.

We recall that there is a bijection between primitive solution of (1.5) and the rational points on the unit circle, i.e. rational solutions of the equation

$$X^2+Y^2=1.$$

This is seen as follows:

Given a primitive solution $x^2+y^2=z^2$ with $z>0$ then $(X,Y)=(x/z,y/z)$ is a rational number on the unit circle. Furthermore given a rational point $(X',Y')=(x'/z',y'/w')$ with $z',w'>0$ on the unit circle then consider $(x'w')^2+(y'z')^2=(z'w')^2$. It is immediate from Proposition 1.2.2 that if two of the three numbers $x'w'$, $y'z'$, and $z'w'$ has a common factor then so does the third. Hence we can divide by this common factor m . It follows that we can write $(X',Y')=(a/c,b/c)$ where (a,b,c) is a primitive solution to (1.5) with $c>0$. The Pythagorean triples with X odd and Y even correspond exactly to those rational points on the circle $(a/c,b/c)$ with a odd and b even.

We now parametrize all rational points on the unit circle. Consider $P=(1,0)$ and another rational point $Q=(q_1,q_2)\neq P$ on the unit circle. Then the line between them $y=\alpha(x-1)$ has rational slope $\alpha=q_2/(q_1-1)$. On the other hand, given a rational slope $\alpha\in\mathbb{Q}$ the line $y=\alpha(x-1)$ and $x^2+y^2=1$ intersects at a point Q which satisfies

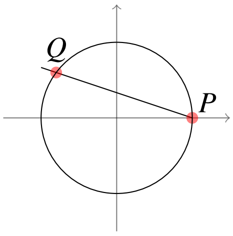
$$x^2+\alpha^2(x-1)^2-1=(1+\alpha^2)x^2-2\alpha^2x+\alpha^2-1=0$$

which has the two solutions

$$\frac{2\alpha^2\pm\sqrt{4\alpha^4-4(1+\alpha^2)(\alpha^2-1)}}{2(1+\alpha^2)}=\frac{2\alpha^2\pm 2}{2(1+\alpha^2)}=1,\frac{\alpha^2-1}{\alpha^2+1}.$$

In particular we note that Q has rational coordinates:

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



If $\alpha = \frac{p}{q}$ is an irreducible fraction with $p \geq 0$, we find that $Q = \left(\frac{p^2-q^2}{p^2+q^2}, \frac{-2pq}{p^2+q^2}\right)$. It is straightforward to see that the second coordinate is of the form b/c with b even precisely if $p-q$ is odd. By the above discussion the result follows. The Pythagorean triple $(1,0,1)$ is covered by $p=1$, $q=0$ which corresponds to $\alpha = \infty$. ■

The above theorems might give the impression that it is relatively straightforward to determine if integer polynomial equations have integer solutions. *This is wrong*. Most often it is very difficult to determine all integer solutions. To illustrate this consider Fermat's equation

$$x^n + y^n = z^n, \text{ for } n \geq 3.$$

It took almost 400 years between 1637 when Fermat thought that he had proved that this does not have any integer solutions satisfying $xyz \neq 0$ until A. Wiles (and his collaborators) finally found a definitive proof in 1995.

1.5 Exercises for Chapter 1

Exercise 1.1 Compute $\gcd(455, 1235)$.

Exercise 1.2 Find all integer solutions to $455x + 1235y = 130$.

Exercise 1.3 Find all integer solutions to $455x + 1235y = 143$.

Exercise 1.4 What are the possible reminders when dividing a square n^2 by 3? By 4? By 5? By 6?

Exercise 1.5 Prove Proposition 1.1.1

Exercise 1.6 In each of the following, apply the division algorithm to find q and r such that $a = bq + r$ with $0 \leq r < |b|$:

$$(a,b) = (302,19), \quad (a,b) = (829,31), \qquad (a,b) = (300,-17), \quad , \quad (a,b) = (449,4),$$

Exercise 1.7 Prove Theorem 1.2.1 in the case $a = 0$. ☕

Exercise 1.8 Prove that $n \in \mathbb{N}$ with $n > 1$ is a prime if and only if n has no non-trivial factors less than or equal to $\sqrt{n}$.

Exercise 1.9 Find all integer solution to $1485x + 1745y = \gcd(1485, 1745)$.

Exercise 1.10 Show that Proposition 1.2.6 (iii), (iv) fails if we do *not* assume a, b to be coprime.

Exercise 1.11 — Eratosthenes' Sieve. Assume that $P = \{p_1, p_2, \dots p_k\}$ are the smallest k primes. Erase from the list $p_k+1, p_k+2, \dots, p_k^2$ all multiples of $p_1, p_2, \dots p_k$ and add the remaining numbers to P. Show that P now contains all prime numbers less than p_k^2. This may be used to easily find complete lists of primes of moderate size. ☕

Exercise 1.12 Find, using nothing put pen and paper, all primes less than 200.

Exercise 1.13 Let p_n be the n-th prime, and let $\pi(x) = \#\{p_n \leq x\}$. Show that $\pi(x) \geq \lfloor \log_2(\log_2(x)) \rfloor + 1$. (Hint: Use Theorem 1.4.3 to show that $p_n \leq 2^{2^{n-1}}$.) ☕

Exercise 1.14 Show that there are infinitely many primitive Pythagorean triangles, i.e. right triangles whose side lengths are integers and pairwise coprime.

Exercise 1.15 Prove Proposition 1.2.2 using the theory of primes.

Exercise 1.16 Show that there are infinitely many primes of the form $4n-1$. (Hint: Assume $p_1, \dots p_n$ are of the desired form and consider the prime factorization of $4p_1 \cdots p_n - 1$)

Exercise 1.17 Prove that no integer in the sequence $11, 111, 1111, \dots$ is a perfect square. Hint: What are the possible remainders when dividing a perfect square by 4?

Exercise 1.18 Assume that $a^b - 1$ is a prime where $a, b \in \mathbb{N}$ with $b \geq 2$. Show that $a = 2$ and b is prime. Primes of this form are called Mersenne primes. Most of the largest known primes are Mersenne primes.

Exercise 1.19 Show that there does not exist a Pythagorean triple (x, y, z) where x, y, z are all primes.

2. Modular arithmetic

2.1 Basic structures

We recall the definition of a ring

Definition 2.1.1 A *ring* R is a set with two binary operations $+,\cdot$ (usually called addition and multiplication), and two elements $0,1 \in R$ such that

(i) $(R,+,0)$ is an abelian group, and for every $a,b,c \in R$ we have

(ii) $1 \cdot a = a \cdot 1 = a$, i.e 1 is a multiplicative identity,

(iii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, i.e. multiplication is associative,

(iv) $a \cdot (b+c) = a \cdot b + a \cdot c$, i.e. multiplication is distributive from the right,

(v) $(a+b) \cdot c = a \cdot c + b \cdot c$, i.e. multiplication is distributive from the left.

■ **Example 2.1** The following are all examples of rings

- $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ (with the usual two binary operations $+,\cdot$) are all examples of commutative (or abelian) rings, i.e. rings where the multiplication is commutative.
- Let $n > 1$. The set of n by n matrices with coefficients in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ denote $M_n(\mathbb{Z})$, $M_n(\mathbb{R})$, $M_n(\mathbb{Q})$, and $M_n(\mathbb{C})$ equipped with the usual matrix addition and matrix multiplication are all examples of non-commutative rings. In this course we will almost exclusively be considering commutative rings.
- Let $n \in \mathbb{N}$. The set of equivalence classes of integers modulo n, $\mathbb{Z}/n\mathbb{Z}$ with addition and multiplication defined by

$$\begin{aligned}(a+n\mathbb{Z})+(b+n\mathbb{Z}) &:= (a+b)+n\mathbb{Z}\\ (a+n\mathbb{Z})\cdot(b+n\mathbb{Z}) &:= a\cdot b+n\mathbb{Z}\end{aligned}$$

It is straightforward to verify that these operations are well-defined and that they make $\mathbb{Z}/n\mathbb{Z}$ a commutative ring. You have already seen in your basic algebra course that $(\mathbb{Z}/n\mathbb{Z},+)$ is an abelian group. We shall use both $a+n\mathbb{Z}$, $[a]_n$, and a mod n to denote the equivalence class a modulo n. If, on the other hand, we write $a = b \pmod n$ we mean that $n \mid (a-b)$ which is equivalent to the equivalence classes a mod n and b mod n being equal.

■

Definition 2.1.2 Let R be a ring and let $a \in R$. We say that a is *invertible* or that it is *a unit* if there exists a $b \in R$ such that $ab = ba = 1$. The set of invertible elements is denoted by $R^\times$.

Notice that if a is invertible then a corresponding b is uniquely determined: If both $ab = ba = 1$ and $ab' = b'a = 1$ then $b = b(ab') = (ba)b' = b'$. We denote this element by a^{-1}. We notice also that if $a, b, c \in R$ with c invertible then $ac = bc$ implies $a = b$ by multiplication from the right with c^{-1}.

It is straightforward to verify the following proposition (See Exercise 2.1) :

Proposition 2.1.1 Let $(R, +, \cdot)$ be a ring. The set $(R^\times, \cdot)$ of invertible elements with $\cdot$ is a group.

■ **Example 2.2** We have

- $\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Q}^\times = \mathbb{Q} \backslash \{0\}$, $\mathbb{R}^\times = \mathbb{R} \backslash \{0\}$, $\mathbb{C}^\times = \mathbb{C} \backslash \{0\}$.
- We have

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{x \bmod n \in \mathbb{Z}/n\mathbb{Z} | \gcd(x, n) = 1\}. \tag{2.1}$$

It follows from Proposition 1.2.3 that the set on the right is well-defined. If $x \bmod n \in \mathbb{Z}/n\mathbb{Z}$ is invertible then there exist $y \bmod n \in \mathbb{Z}/n\mathbb{Z}$ such that $xy = 1 + kn$ for some $k \in \mathbb{Z}$. But then by Proposition 1.2.6 (i) we have $\gcd(x, n) = 1$. On the other hand if $\gcd(x, n) = 1$ then again by Proposition 1.2.6 (i) there exist y, k such that $1 = yx + kn$ which shows that $(x \bmod n) \cdot (y \bmod n) = 1 \bmod n$.

■

Definition 2.1.3 Let R be a ring. If all non-zero elements are invertible then R is called a *division ring* or a *skew field*. If additionally R is commutative then R is called a *field*.

■ **Example 2.3** By Example 2.2 we see that $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are fields and $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if $n = p$ is a prime. This field is usually denoted $\mathbb{F}_p$. ■

2.2 Modular arithmetic

We will investigate further the ring $\mathbb{Z}/n\mathbb{Z}$.

Proposition 2.2.1 The equation

$$ax = b \pmod{n} \tag{2.2}$$

has a solution if and only if $\gcd(a, n) \mid b$.

Proof. Let $g = \gcd(a, n)$. Assume x is a solution. Then $n \mid ax - b$ so $ax - b = nc$ for some integer c and hence $g \mid b$. Assume on the other hand $g \mid b$. Note that by Proposition 1.2.6 (ii) we have $\gcd(a/g, n/g) = 1$. By (2.1) a/g is a unit in $\mathbb{Z}/(n/g)\mathbb{Z}$, so there exists a y such that $ya/g = 1 + kn/g$. Multiplying by b we find that $x = yb/g$ solves (2.2). ■

■ **Example 2.4**

- Note that $x = 4 \pmod{8}$ and $x = 0 \pmod{8}$ are two different solutions to $2x = 0 \pmod{8}$. Hence there is not necessarily uniqueness in Proposition 2.2.1.
- Consider solutions to $3x = 7 \pmod{5}$. Euclidean division gives

$$\begin{aligned} 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

so $\gcd(5, 3) = 1$ and $1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5$. It follows that $3^{-1} = 2 \pmod{5}$ so we may multiply by 2 to find the unique solution $x = 2 \cdot 7 = 4 \pmod{5}$.

■

2.3 Euler's φ-function

We now consider the function

$$\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^{\times} = \#\{1 \leq a \leq n \,|\, \gcd(a,n) = 1\} \tag{2.3}$$

called *Euler's φ-function*.

■ **Example 2.5** If we want to find $\varphi(6)$ we have to count how many of $1,2,3,4,5$ are coprime to 6. But this is is exactly $1,5$, so $\varphi(6) = 2$. ■

It is obvious that $\varphi(1) = 1$. It follows from Example 2.3 that if p is a prime $\varphi(p) = p-1$. More generally we have

$$\varphi(p^n) = p^n - p^{n-1} = p^n(1-p^{-1}). \tag{2.4}$$

To see this we note that we are counting all the numbers $1,2,\dots,p^n$ except for those that have a factor in common with p^n. But if $gcd(a,p^n) > 1$ then using that p is a prime we see that $gcd(a,p) > 1$ which means that p divides a. Hence the numbers we are excluding are exactly $p,2p,3p,\dots,p^n$ and the claim follows.

Theorem 2.3.1 — Euler. Assume $gcd(x,n) = 1$. Then $x^{\varphi(n)} = 1 \pmod{n}$.

Proof. From basic algebra we have Lagrange's theorem which implies that for a finite group G we have $g^{\#G} = 1$. Applying this to $G = (\mathbb{Z}/n\mathbb{Z})^{\times}$ gives the result by (2.1) and (2.3). ■

Corollary 2.3.2 — Fermat's little theorem. Let p be a prime. Then $a^p = a \pmod{p}$ for every $a \in \mathbb{Z}$.

Proof. For $p \mid a$ both sides are zero and the claim is trivial. For $p \nmid a$ we have $\gcd(a,p) = 1$ and Euler's theorem and (2.4) gives that $a^{p-1} = 1 \pmod{p}$. Multiplying by a gives the result. ■

We note that the above proof is somewhat anachronistic. Historically Lagrange's theorem was a generalization of Fermat's little theorem. For a more elementary proof of Euler's theorem we can argue as follows: Since $gcd(x,n) = 1$ multiplication by x gives a permutation of the elements $G = \{a \mod n | gcd(a,n) = 1\}$. It follows that

$$\prod_{a\in G} ax = \prod_{a\in G} a \pmod{n}.$$

Since $\gcd(\prod_{a\in G} a, n) = 1$ it follows from Bezout's theorem that there exists an integer b such that $b\prod_{a\in G} a = 1 \pmod{n}$. Multiplying by this b finishes the proof of Theorem 2.3.1 .

2.3.1 The Chinese remainder theorem

In order to find the values of Euler's φ-function on general integers we need the Chinese remainder theorem.

Theorem 2.3.3 — The Chinese remainder theorem. Let $a_1,\dots a_l \in \mathbb{Z}$ and let $n_1,\dots,n_l$ be pairwise coprime. Then the system of l equations

$$x = a_i \pmod{n_i}, \quad i = 1,\dots,l$$

has an integer solution. This solution is unique modulo $n_1 \cdots n_l$.

Proof. For $l = 1$ the claim is clear: Choose $x = a_1$. Assume $l = 2$ and consider the equation in t given by

$$a_1 + n_1 t = a_2 \pmod{n_2}.$$

As $\gcd(n_1, n_2) = 1$ Proposition 2.2.1 ensures that there is a solution to this. Indeed we may take $t = (a_2 - a_1) n_1^{-1} \pmod{n_2}$. Letting $x = a_1 + n_1 t$ we find that this solves the two equations. Assume two solutions x, y. Then subtracting them we find that $x - y = 0 \pmod{n_i}$. Then by Proposition 1.2.6 (iii) we have that $n_1 n_2 \mid x - y$ which shows uniqueness modulo $n_1 n_2$.

Assume now that the theorem holds for a given l. Then we want to show that it holds also for $l+1$. So assume we have a solution to

$$x = a_i \pmod{n_i}, \quad i = 1, \dots, l$$

Then we want to show that we can find a solution to

$$y = a_i \pmod{n_i}, \quad i = 1, \dots, l+1$$

We consider now the equation

$$x + t n_1 n_2 \cdots n_l = a_{l+1} \pmod{n_{l+1}} \tag{2.5}$$

As $\gcd(n_1 \cdots n_l, n_{l+1}) = 1$ Proposition 2.2.1 ensures that there is a solution to this. Indeed we may take $t = (a_{l+1} - x)(n_1 \cdots n_l)^{-1} \pmod{n_{l+1}}$. Letting $y = x + t n_1 n_2 \cdots n_l$ we find that this solves all $l+1$ equations. Uniqueness is proved like the case $l = 2$. ■

▪ **Example 2.6** The Chinese mathematician Sun Tzu asked in a late 3rd century book for the smallest solution to the equations

$$\begin{aligned} x &= 2 \pmod{3} \\ x &= 3 \pmod{5} \\ x &= 2 \pmod{7}. \end{aligned}$$

Using Theorem 2.3.3 we see immediately that a solution exist. Recalling the proof we see that in order to solve the two first equations we solve, in t the equation

$$2 + t \cdot 3 = 3 \pmod{5}.$$

We easily find that $t = 2$ solves this, and hence $2 + 2 \cdot 3 = 8$ is a solution of the two first equations. To get a solution of all three equations we need to solve in t the equation

$$8 + t \cdot 3 \cdot 5 = 2 \pmod{7}.$$

Since $15 = 1 \pmod{7}$ we find that $t = -6 = 1 \pmod{7}$ solves the equation, and $x = 8 + 1 \cdot 15 = 23$ solves all three equations. Since all solution are of the form $x = 23 + k \cdot 3 \cdot 5 \cdot 7$ (and all integers of this form are indeed solutions), this is also the smallest solution. ▪

Lemma 2.3.4 Let m, n be coprime integers. The mapping between groups

$$\begin{aligned} \psi : (\mathbb{Z}/mn\mathbb{Z})^\times &\to (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \\ c \bmod mn &\mapsto (c \bmod m, c \bmod n) \end{aligned}$$

is a bijection.

Proof. Notice that the map is independent of choice of representative. Note also that if $c \bmod mn \in (\mathbb{Z}/mn\mathbb{Z})^\times$ then $\gcd(c,mn) = 1$. It follows that $\gcd(c,n) = 1$ since $\gcd(c,n) \mid \gcd(c,mn) = 1$. The same argument shows that $\gcd(c,m) = 1$. It follows that $\psi(c \bmod mn) \in (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ so the map is indeed well-defined.

Notice that the Chinese remainder theorem gives directly that the map

$$\begin{aligned}\overline{\psi} : \mathbb{Z}/mn\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\\ c \bmod mn &\mapsto (c \bmod m, c \bmod n)\end{aligned}$$

is a bijection. As ψ is the restriction of $\overline{\psi}$ to $(\mathbb{Z}/mn\mathbb{Z})^\times$ it follows that ψ is injective.

To see that it is surjective we have to show that if $\overline{\psi}(c \bmod mn) \in (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$ then $c \bmod mn \in (\mathbb{Z}/mn\mathbb{Z})^\times$. But assume that a prime $p \mid \gcd(c,mn)$. Then by Euclid's lemma (Lemma 1.4.1) we have $p \mid m$ or $p \mid n$. But this means that $p \mid \gcd(c,m) = 1$ or $p \mid \gcd(c,n) = 1$ which cannot be the case. So no such prime exists, and we have $\gcd(c,mn) = 1$ which shows that $c \bmod mn \in (\mathbb{Z}/mn\mathbb{Z})^\times$. Hence ψ is surjective, which finishes the proof. ■

In fact a bit more is true. One can show that ψ is a *group isomorphism*. Indeed $\overline{\psi}$ is a *ring isomorphism* (we have not defined what this means) but since we do not need it we settle for the above statement. We need it to be able to conclude the following:

Corollary 2.3.5 Let m,n be coprime integers. Then $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof. This follows immediately from Lemma 2.3.4, and the definition of φ. ■

Combining Corollary 2.3.5 with (2.4) we find immediately that

$$\varphi(n) = n\prod_{p\mid n}(1-p^{-1}). \tag{2.6}$$

2.4 Primitive roots modulo n.

Recall that if g is an element of a group G then the *order of* g, $\operatorname{ord}(g)$, is the smallest natural number n such that g^n is the neutral element of the group. By Lagrange theorem the order of a group element divides the group order $\#G$. We know also that if g^m equals the neutral element in G then $\operatorname{ord}(g) \mid m$ as can be proved by Euclidean division.

Definition 2.4.1 Let n be a natural number. An integer $a \in \mathbb{Z}$ is called *a primitive root modulo* n if $a \bmod n \in (\mathbb{Z}/n\mathbb{Z})^\times$ has order $\varphi(n)$.

■ **Example 2.7** Recall Example 2.5. We have $(5 \bmod 6)^2 = 25 \bmod 6 = 1 \bmod 6$. It follows that $5 \bmod 6$ has order $2 = \varphi(6)$. I.e. 5 is a primitive root modulo 6. ■

Note that if a is a primitive root mod n then by the definition of $\varphi(n)$ we have that $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic with $a \bmod n$ being a generator. It is a natural question to ask whether to a given n primitive roots modulo n exist. We will prove that if n is prime this is indeed the case. In order to prove this we need to study roots of polynomials:

2.4.1 Roots of polynomials.

Consider the polynomial $f(x) = x^2 - 1 \in (\mathbb{Z}/8\mathbb{Z})[x]$. It is straightforward to verify that this has roots $1,3,5,7 \bmod 8$. Hence this is an example of a degree 2 polynomial with 4 roots. If we are working over a *field* polynomials cannot have such an abundance of roots.

Proposition 2.4.1 Let k be a field and let $0 \neq f \in k[x]$ be a polynomial over k. Then f has *at most* $\deg(f)$ roots.

We note that $f(x) = x^2 - 2 \in (\mathbb{Z}/3\mathbb{Z})[x]$ has no roots in $\mathbb{Z}/3\mathbb{Z}$ since modulo 3 we have $f(0) = -2$, $f(1) = -1$, $f(2) = 2$.

Proof. The proof is induction in $\deg(f)$. For polynomials of degree 0, i.e. constants, the claim is clear. Assume now that the claim holds for polynomials of degree at most n. Let

$$f(x) = a_{n+1}x^{n+1} + \cdots a_1 x^1 + a_0 \in k[x]$$

be a polynomial of degree $n+1$. If there are no roots in k we are done. So assume $\alpha \in k$ is a root. Then

$$f(x) = f(x) - f(\alpha) = a_{n+1}(x^{n+1} - \alpha^{n+1}) + \cdots a_1(x^1 - \alpha)$$

Since $x^i - \alpha^i = \sum_{j=0}^{i-1} x^j \alpha^{i-1-j}(x-\alpha)$ this implies that $f(x) = (x-\alpha)g(x)$ where $\deg(g) \leq n$.

If $\beta \neq \alpha$ is a root of f then $0 = (\beta - \alpha)g(\beta)$ and since $\beta - \alpha \neq 0$ we may multiply by its inverse (since k is a field) and find $g(\beta) = 0$. By induction hypothesis this can be true for at most n different β and it follows that f has at most $n+1$ roots. ■

Recall that if p is a prime then $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field.

Proposition 2.4.2 Let p be a prime and d a divisor of $p-1$. Then $f(x) = x^d - 1 \in \mathbb{F}_p[x]$ has *exactly* d roots.

Proof. Write $p - 1 = dl$, and consider $e(x) = x^{p-1} - 1 \in \mathbb{F}_p[x]$. By Euler's theorem (Theorem 2.3.1) all non-zero elements of $\mathbb{F}_p$ are roots of this polynomial, i.e. it has $p-1$ different roots. We notice also the factorization

$$e(x) = (x^d)^l - 1 = (x^d - 1)((x^d)^{l-1} + (x^d)^{l-2} + \cdots + 1) = f(x)g(x),$$

where $g(x) \in \mathbb{F}_p[x]$ has degree $p-1-d$. By Proposition 2.4.1 f has at most d roots and g has at most $p-1-d$ roots but since their product has $p-1$ different roots f must have at least d roots and g must have at least $p-1-d$ roots which proves the claim. ■

Lemma 2.4.3 Let G be a group. Assume $g_1, g_2 \in G$ are commuting elements with coprime finite orders n_1,n_2. Then their product g_1g_2 has order n_1n_2.

Proof. Let $n = \operatorname{ord}(g_1g_2)$. Since g_1 and g_2 commutes $(g_1g_2)^{n_1n_2} = (g_1^{n_1})^{n_2}(g_2^{n_2})^{n_1} = 1$ so $n \mid n_1n_2$. On the other hand we have $g_1^n g_2^n = 1$. Raising this to the n_2'th power and using $g_2^{n_2} = 1$ we find $g_1^{nn_2} = 1$ so $n_1 \mid nn_2$. Since n_1 and n_2 are coprime we get from Proposition 1.2.6 (iv) that $n_1 \mid n$. A similar argument shows that $n_2|n$, which then by Proposition 1.2.6 (iii) implies that $n_1n_2 \mid n$. Hence we have $n = n_1n_2$. ■

We are now ready to prove the main result of this section.

Theorem 2.4.4 Primitive roots modulo p exist for every prime number p.

Proof. By the fundamental theorem of arithmetic we can factor $\varphi(p) = p - 1 = p_1^{l_1} \cdots p_k^{l_k}$ into a product of powers of distinct primes. If we can show that for every $i = 1, \ldots k$, we can find an element a_i of $\mathbb{F}_p^\times$ with order $p_i^{l_i}$, then by successive use of Lemma 2.4.3 we find that $a = a_1a_2 \ldots a_k$ has order $\varphi(p)$ which proves that there exists a primitive root modulo p.

To show that there exists an elements of order $p_i^{l_i}$, we observe that by Proposition 2.4.2 we see that there are $p_i^{l_i} - p_i^{l_i - 1}$ elements of order $p_i^{l_i}$ since the roots of $x^{p_i^{l_i}} - 1 = 0$ which are not roots of $x^{p_i^{l_i-1}} - 1 = 0$ have order $p_i^{l_i}$: For such a root a_i satisfies $a_i^{p_i^{l_i}} = 1$ so $\operatorname{ord}(a_i) \mid p_i^{l_i}$ i.e. $\operatorname{ord}(a_i) = p_i^l$ for some $0 \leq l \leq l_i$. But if $l < l_i$ then a_i is a root of $x^{p_i^{l_i-1}} - 1 = 0$ which we have assumed it is not. This finishes the proof. ■

Since a primitive root modulo p induces an element in $\mathbb{F}_p^\times$ of order $\varphi(p) = \#\mathbb{F}_p^\times$ we conclude the following corollary:

Corollary 2.4.5 Let p be a prime. Then $\mathbb{F}_p^\times$ is cyclic.

Theorem 2.4.4 settles the question of the existence of primitive roots modulo primes. There are no primitive roots modulo 8 (Exercise 2.2), so some restriction on n needs to be assumed. It turns out that primitive roots modulo n exists precisely if $n = 2, 4, p^e$, or $2p^e$ where p is any odd prime and $e \in \mathbb{N}$. We shall not prove this but please consult [JJ98, Theorem 6.7] for an accessible proof.

Proposition 2.4.6 Let n be a natural number and assume that there exist primitive roots modulo n. Then $\varphi(\varphi(n))$ of the numbers $1, 2, \ldots, n-1$ are primitive roots modulo n.

Proof. If a is a primitive root modulo n then $a \pmod n$ is a generator of $(\mathbb{Z}/n\mathbb{Z})^\times$. We see the number we are looking for equals the number of $1 \le r \le \varphi(n)$ where $a^r \pmod n$ is a generator of $(\mathbb{Z}/n\mathbb{Z})^\times$. But $a^r \pmod n$ is a generator precisely if for every $1 \le c \le \varphi(n)$ the equation $a^{ry} = a^c \pmod n$ has a solution. This happens precisely if $ry = c \pmod{\varphi(n)}$ has a solution. But by Proposition 2.2.1 this happens precisely if $\gcd(r, \varphi(n)) \mid c$ for all c which happens precisely if $\gcd(r, \varphi(n)) = 1$. Hence we are counting the number of elements in the set

$$\{1 \le r \le \varphi(n) | \gcd(r, \varphi(n)) = 1\}$$

which is exactly $\varphi(\varphi(n))$. ■

We remark that the proof of Proposition 2.4.6 shows that if a is a primitive root modulo n then set of all primitive roots are the integers b such that $b = a^r \bmod n$ for some $\gcd(r, \varphi(n)) = 1$.

Example 2.8 We want to find all primitive roots modulo 7. Recall that $\varphi(7) = 6$, so we are looking for all natural numbers a such that $a \bmod 7$ has order 6, or said differently that $a \bmod 7$ is a generator for $(\mathbb{Z}/7\mathbb{Z})^\times$. Note that $3^2 = 2 \pmod 7$, $3^3 = 6 \pmod 7$ so $3 \bmod 7$ does not have order 1,2, or 3. Since the order is a divisor of the order of the group. The group order is 6 so we may conclude that $3 \bmod 7$ has order 6 and is therefore a generator. By the proof of Proposition 2.4.6 the element $3^r \bmod 7$ is a generator precisely if $\gcd(r, 6) = 1$ which happens precisely for $r = 1, 5 \pmod 6$. Note that $3^5 = 5 \pmod 7$.

Therefore 3,5 are the only primitive roots modulo 7 which are less than 6. Note that that this agrees with $\varphi(\varphi(7)) = \varphi(6) = \varphi(2)\varphi(3) = 2$.

Hence a is a primitive root modulo 7 if and only if $a = 3 \pmod 7$ or $a = 5 \pmod 7$. ■

2.4.2 Artin's conjecture

Conjecture 2.4.7 [Artin's conjecture] Let $a \in \mathbb{Z} \backslash \{-1\}$ with $a \neq b^2$. Then there are infinitely many primes p such that a is a primitive root modulo p

This is a long-standing and important conjecture. On the one hand we do not know a single a for which there are infinitely many primes p such that a is a primitive root modulo p. On the other hand we know – due to Heath-brown [Hea86] – that it is true whenever a is a prime with at most two exceptions. In particular it is true for either $a = 2, 3$, or 5 but we do not know which of the three. Heath-brown also showed that it holds whenever a is square-free (i.e. a being a product of different primes) with at most 3 exceptions.

Hooley showed [Hoo67] that Artin's conjecture follows from a generalization of the Riemann hypothesis.

2.5 Local obstructions

When we want to determine whether a specific diophantine equation has integer solutions this can sometimes be ruled out by clever congruence considerations.

■ **Example 2.9** Consider the Diophantine equation

$$x^5 - x^2 + x - 3 = 0,$$

i.e. we are looking for integer roots of the polynomial $f(x) = x^5 - x^2 + x - 3$. If such a root exist we can reduce it modulo n (where n is any integer) and we will have that x satisfies $f(x) = 0 \pmod{n}$. In this case it turns out to be convenient to consider $n = 4$. We can then verify that $f(0) = 1$, $f(1) = 2$, $f(2) = 3$ and $f(3) = 2$, in particular these numbers are all non-zero modulo 4, and hence no such integer solution can exist. We say that there is a *local obstruction* to $f(x) = 0$ having integer solutions.

Note that it is straightforward to verify that $f(x)$ has real roots as $f(x) \to \infty$ as $x \to \infty$, and $f(x) \to -\infty$ as $x \to -\infty$, so by the intermediate value theorem $f(x_0) = 0$ for some real x_0. ■

■ **Example 2.10** Consider the Diophantine equation

$$3 = x^2 + y^2.$$

It is easy to verify that any square x^2 is either 0 or 1 modulo 4. Hence any expression $x^2 + y^2$ must be either 0, 1, or 2 modulo 4. But since 3 is 3 modulo 4 this Diophantine equation does not have a solution. Notice that this argument generalizes to proving that the equation

$$p = x^2 + y^2 \tag{2.7}$$

does not have solutions whenever p is equal to 3 modulo 4. We will later in Theorem 6.1.3 that if p is a prime which is *not* equal to 3 modulo 4 then (2.7) does indeed have a solution. ■

Local obstructions are useful for proving that there are no solutions to a Diophantine equation. In other cases there are no local obstructions (e.g. if the Diophantine equation has solutions there can be no local obstruction). There are families of Diophantine equations where the existence of both solutions modulo p^n for every prime power and a real solution suffices to conclude that the Diophantine equation has an integer solution. Such a result is called a *local to global principle*.

2.6 Exercises for Chapter 2

Exercise 2.1 Prove Proposition 2.1.1.

Exercise 2.2 Show that there are no primitive roots modulo 8.

Exercise 2.3 Show that there are no primitive roots modulo 2^n for any $n \geq 3$.

Exercise 2.4 Find all primitive roots modulo 17.

Exercise 2.5 — Freshman's dream. Let a, b be integers and let p be a prime. Prove that $(a+b)^p = a^p + b^p \pmod{p}$.

Exercise 2.6 Determine if $x^5 = 2 \pmod{2003}$ has a solution. Note that 2003 is a prime.

Exercise 2.7 Prove that the Diophantine equation $f(x) = 0$ has no solution when $f(x)$ is one of the following: a) $x^3 - x + 1$, b) $x^3 + x^2 - x + 1$, c) $x^3 + x^2 - x + 3$.

Exercise 2.8 Seven pirates try to share a stolen pile of identical diamonds equally between themselves. Unfortunately, six diamonds are left over, and in the fight over them, one pirate is thrown overboard and gets eaten by sharks. The remaining six pirates, still unable to share the diamonds equally since two are left over, again fight, and another is killed. When the remaining five share the diamonds, one diamond is left over, and it is only after yet another pirate is thrown overboard that an equal sharing is possible. What is the minimum number of diamonds that the pirates have stolen?

Exercise 2.9 For which values n is $\varphi(n)$ odd? Show that there exists integers n with $\varphi(n) = 2, 4, 6, 8, 10, 12$ but not 14.

Exercise 2.10 Find the smallest integer n such that $\varphi(n)/n \leq 1/4$

Exercise 2.11 Show that if $n > 4$ is composite then $(n-1)! = 0 \bmod n$.

Exercise 2.12 Assume $a = -1$ or that a is a perfect square. Show that a is not a primitive root modulo p for any prime $p > 3$. Determine whether a is a primitive root modulo 3. Compare with Artin's Conjecture 2.4.7.

Exercise 2.13 (Hard) Let p be an odd prime. Let g be a primitive root modulo p. Prove that either g or $g + p$ is a primitive roots modulo p^2. In particular this shows that primitive roots modulo p^2 exists One can show that primitive roots modulo p^e exist for any $e \geq 1$. See e.g. [JJ98, Thm 6.7].

Exercise 2.14 Find all integer solutions to each of the equations

$$\begin{aligned} 3x &= 4 \pmod{123} \\ 5x &= 23 \pmod{123} \\ 5x &= 234 \pmod{2002}. \end{aligned}$$

3. Cryptography

The basic idea of cryptography is that we want to send coded messages between two persons (call them Alice and Bob) without anyone else being able to read and/or change the message. A major benefit of modern cryptosystems is that they allow Alice and Bob to exchange secret messages without having secretly exchanged the keys they are using to encrypt and decrypt their messages. They can use keys that they construct and then exchange in an open non-encrypted form of communication (like the internet). In fact we all use such encrypted systems every day in our daily interactions with modern digital technology. We will now describe the principles in some of these cryptosystems.

We will always assume that the message is a number or a string of numbers. Clearly any text can be translated to a string of numbers. For instance one can use the unicode-values of the standard characters. See also [Ste09, p. 3.3.2] for an even more basic implementation.

In the two cryptographic settings we will describe in some detail (Diffie-Hellman and RSA) a central role is played by large primes. We therefore start by discussing techniques to verify if a number is prime or not.

3.1 Primality testing

We want to find various ways to verify if a number n is a prime. The naive way is of course to see if any $1 < d \leq \sqrt{n}$ divides n. If not n is indeed a prime. This method of testing for primality is very slow

There are several ways of characterizing primes. Here are a few basic ones:

Theorem 3.1.1 — Wilson. A number $p > 1$ is a prime if and only if $(p-1)! = -1 \pmod{p}$.

Proof. The statement is clear for $p = 2$ so assume $p > 2$. If p is a prime then every $1, 2, \ldots p-1$ has multiplicative inverses in $\mathbb{F}_p$ since it is a field. If b is its own inverse then $b^2 - 1 = (b-1)(b+1)$ is divisible by p so by Euclid's lemma 1.4.1 p divides $b-1$ or $b+1$. But this means that b equals 1 or $p-1$. Since all the other integers less that $p-1$ has a unique inverse different from itself it follows that $(p-1)! = p-1 = -1 \pmod{p}$.

Let on the other hand $(p-1)! = -1 \pmod{p}$. If we assume that p is not a prime then it has a non-trivial factor $1 < l < p$. It follows that $0 = -1 \pmod{l}$ which is a contradiction since an integer $l > 1$ cannot divide 1. ■

In terms of efficiency using Wilson's theorem to check for primality is horribly slow as it is very time consuming to find $(p-1)!$ if p is large.

Theorem 3.1.2 Let $p > 1$. Then p is a prime if and only if $a^{p-1} = 1 \pmod{p}$ for every $a \neq 0 \pmod{p}$.

Proof. Assume p is prime. Then by Theorem 2.3.1 and (2.4) we have $a^{p-1} = 1 \pmod{p}$.

If on the other hand $a^{p-1} = 1 \pmod{p}$ for every $a \neq 0 \pmod{p}$ then if p is not a prime let $1 < l < p$ be a non-trivial factor. Then $l^{p-1} = 1 \pmod{l}$ which implies that $l|1$ which is impossible. By contradiction we conclude that p must be a prime. ■

3.1.1 Carmichael numbers

By Theorem 3.1.2 we can test if n is a prime number by verifying $a^{n-1} = 1$ for all a not divisible by n. One could speculate if it was enough to verify this for all a which are relatively prime to n. This is not the case: There exists "many" composite numbers n such that $a^{n-1} = 1$ for all a which are relatively prime to n. Such numbers are called Carmichael numbers:

Definition 3.1.1 A *Carmichael* number n is a composite number which satisfies that $a^{n-1} = 1 \pmod{n}$ for every a which is relatively prime to n.

■ **Example 3.1** We want to show that 561 is a Carmichael number. Note that $561 = 3 \cdot 11 \cdot 17$. Assume that a is relatively prime to 561. Then a is also relatively prime to 3, 11, and 17. It then follows from Euler's theorem 2.3.1 that

$$a^{560} = a^{2 \cdot 280} = 1 \pmod{3}, \quad a^{560} = a^{10 \cdot 56} = 1 \pmod{11}, \quad a^{560} = a^{16 \cdot 35} = 1 \pmod{17}$$

It follows that $a^{560} - 1$ is divisible by 3, 11, and 17, and therefore by Proposition 1.2.6 (iii) also by 561. Hence $a^{560} = 1 \pmod{561}$, so 561 is a Carmichael number. ■

R There are many Carmichael numbers: 561, 1105, 1729, 2465, 2821, 6601, 8911 are all the Carmichael numbers less than 10000. Ahlford, Granville, and Pomerance [AGP94] proved in 1994 that there are infinitely many Carmichael numbers. It is a wide open problem to determine asymptotics for the number of Carmichael numbers less than a given x.

3.1.2 Miller-Rabin's primality test

The Miller-Rabin primality test is based on the following theorem:

Theorem 3.1.3 Let $p > 1$ be an integer, and write $p - 1 = 2^k m$ where m is odd. Then p is a prime if and only if for every $a \neq 0 \pmod{p}$

$$\text{either} \quad a^m = 1 \pmod{p} \quad \text{or} \quad a^{2^r m} = -1 \pmod{p} \text{ for some } 0 \le r < k. \tag{3.1}$$

Proof. Assume that $p > 1$ is prime. By Theorem 3.1.2 $1 = a^{p-1} = a^{m2^k} \pmod{p}$, so

$$(a^{m2^{k-1}} + 1)(a^{m2^{k-1}} - 1) = 0 \pmod{p}.$$

By Euclid's lemma 1.4.1 this implies that $a^{m2^{k-1}} = \pm 1 \pmod{p}$. If $a^{m2^{k-1}} = -1 \pmod{p}$ we are done. If not we can use the same argument to conclude that $a^{m2^{k-2}} = \pm 1 \pmod{p}$. Continuing to strip off a power of 2 if $a^{m2^r} = 1 \pmod{p}$ until $r = 0$ we find that $a^m = \pm 1 \pmod{p}$ which shows that (3.1) holds.

Assume now instead that (3.1) holds. If $a^m = 1 \pmod{p}$ then

$$a^{p-1} = a^{m2^k} = (a^m)^{2^k} = 1 \pmod{p}.$$

If $a^{2^r m} = -1 \pmod{p}$ then

$$a^{p-1} = (a^{2^r m})^{2^{k-r}} = ((-1)^2)^{2^{k-r-1}} = 1 \pmod{p}.$$

In any case we have $a^{p-1} = 1 \pmod{p}$ so by Theorem 3.1.2 p is a prime. ■

Given an odd number p, the existence of a single $a \neq 0 \pmod{p}$ not satisfying (3.1) suffices for proving that p is not a prime.

If (3.1) holds for a given $a \neq 0 \pmod{p}$ we say that p is a *pseudo-prime to base a*. Hence a prime is a number which is a pseudo-prime to *any* base $a \neq 0 \pmod{p}$. If we have tested that p is a pseudo-prime to sufficiently many bases we might start to suspect that maybe it is indeed a prime. This can be made precise and there is a way to use this to verify that p is a prime with a sufficiently high probability. We will not go into the details of how this is defined but mention only that such probabilistic tests are usually much faster than deterministic tests. And for applications in cryptosystems we might be content with knowing that the communication is secure with probability $\geq 1 - \varepsilon$ with the size of ε depending on the concrete case. If I am encrypting my bank account information $\varepsilon = 10^{-10}$ might suffice, whereas if the national security is at stake I might want a smaller ε.

R The Miller-Rabin primality test as described above is usually used as a probabilistic test. It turns out that if we knew a generalization of the Riemann hypothesis, then we could prove that if p is a pseudo-prime to base a for the first $2\log p$ bases then p is indeed a prime. See [Bac90] for a proof.

3.1.3 Modular exponentiation

In order to make good use of Theorem 3.1.2 as a primality testing tool we must have efficient ways of computing $a^n \pmod{m}$. This is called *modular exponentiation*. If a and m are huge number it is very inefficient to simply compute $a^n \pmod{m}$ by simply computing $a \bmod m, a^2 \bmod m, a^3 \bmod m, \dots, a^n \bmod m$ by successive multiplication by a and reducing modulo m. It is much more efficient to write n in binary and then use that $a^{2^k} = (a^{2^{k-1}})^2$. This dramatically reduces the number of multiplications needed. We illustrate by an example:

■ Example 3.2 We want to compute $3^{75} \pmod{100}$. The naive approach uses 75 multiplications in $(\mathbb{Z}/100\mathbb{Z})^\times$ (note that 3 and 100 are relatively prime). Using Eulers' theorem we see that $3^{\varphi(100)} = 1 \pmod{100}$. Using (2.6) we find that $\varphi(100) = 100(1-1/2)(1-1/5) = 40$. It follows that $3^{75} = 3^{35} \pmod{100}$. We now write 35 in binary, i.e. we find ε_i such that $35 = \sum_{i=0}^{k} \varepsilon_i 2^i$. An easy way to do this is as follows:

35 is odd so	$\varepsilon_0 = 1,$
$(35-1)/2 = 17$ is odd so	$\varepsilon_1 = 1,$
$(17-1)/2 = 8$ is even so	$\varepsilon_2 = 0,$
$(8-0)/2 = 4$ is even so	$\varepsilon_3 = 0,$
$(4-0)/2 = 2$ is even so	$\varepsilon_4 = 0,$
$(2-0)/2 = 1$ is odd so	$\varepsilon_5 = 1.$

This implies that 35 is 100011 in binary. We now compute the 2^i powers of 3 $\pmod{100}$.

$$\begin{aligned}
3^{2^0} &= 3 \pmod{100} \\
3^{2^1} &= (3^{2^0})^2 = 3^2 = 9 \pmod{100} \\
3^{2^2} &= (3^{2^1})^2 = 9^2 = 81 \pmod{100} \\
3^{2^3} &= (3^{2^2})^2 = 81^2 = 61 \pmod{100} \\
3^{2^4} &= (3^{2^3})^2 = 61^2 = 21 \pmod{100} \\
3^{2^5} &= (3^{2^4})^2 = 21^2 = 41 \pmod{100}
\end{aligned}$$

It follows that $3^{35} = 3^{2^5+2^1+2^0} = 3^{2^5}3^{2^1}3^{2^0} = 41 \cdot 9 \cdot 3 = 7 \pmod{100}$. This method is much more efficient than the naive multiplication. We have only made 7 multiplications (and 5 divisions by 2). ■

3.2 Concrete cryptosystems

We are now equipped with effective tools for

1. finding large primes (Section 3.1.2)
2. doing modular exponentiation (Section 3.1.3) , and
3. solving the equation $ax = 1 \pmod{n}$ when $\gcd(a,n) = 1$ using Bezout's theorem 1.2.4 and Remark 1.3

These tools will be instrumental in the concrete cryptosystems we are now going to describe. We should warn that there are many delicate points when one wants to *actually* implement such systems in order not to introduce more or less subtle vulnerabilities. We will not discuss such points here but only focus on the general mechanism.

3.2.1 Diffie–Hellman

The Diffie–Hellman key exchange protocol is a way for Alice and Bob to agree on a secret number that they can use to encrypt and decrypt messages that they send to each other. It allows them to agree on a secret number that only they know, even if anyone can listen to their communication. The protocol was proposed by W. Diffie and M.E. Hellman in the 1970s [DH76], and is still being used in various cryptosystems.

It is a so-called symmetric key exchange meaning that the secret key (a number) is used for both encryption and decryption.

Agreeing on a key

The Diffie–Hellman key exchange protocol consists of the following steps.

Agreeing on a secret number

1. Alice and Bob agree in public on a prime p and a random number $1 < g < p$.
2. Alice secretly chooses an integer n_A and computes $g^{n_A} \pmod{p}$.
3. Bob secretly chooses an integer n_B and computes $g^{n_B} \pmod{p}$.
4. Alice and Bob sends, possibly on an insecure line, the results of their computations to the other.
5. The secret shared key is now

$$s = (g^{n_A})^{n_B} = (g^{n_B})^{n_A} \pmod{p},$$

which both Alice and Bob can compute.

This protocol enables Alice and Bob to find a secret key that only they know, and even if they have only communicated over insecure channels they have managed to agree on a number s that only they know how to compute. They can now use this number to encode and decode their messages (using standard tools like AES, Twofish, Serpent, Blowfish, CAST5, Grasshopper, RC4 or similar).

■ **Example 3.3** Here is a small example of what Alice and Bob needs to compute. In more realistic examples the numbers are of course much larger. Even for these small examples it is convenient to use a computer to do the computations.

1. $p = 101$, $g = 41$.
2. $n_A = 56$, $g^{n_A} = 95 \pmod{101}$.
3. $n_B = 22$, $g^{n_B} = 65 \pmod{101}$.
4. Alice sends 95 to Bob and receives 65 from him.
5. Alice computes $s = 65^{56} = 36 \pmod{101}$, and Bob computes $s = 95^{22} = 36 \pmod{101}$, so 36 is the secret key.

■

The Discrete Log Problem

It is reasonable to consider if someone listening to Alice and Bob's communication (call him Charlie) can find s based on the information available to him. He does after all have access to both g, p, $g^{n_A} \pmod p$, and $g^{n_B} \pmod p$. One thing he could try to do is to compute $g^i \pmod p$ for every $i = 1, 2, ..$ until he finds an i_0 such that $g^{i_0} = g^{n_A} \pmod p$. Then $\mathrm{ord}(g) \mid n_A - i_0$ so $i_0 = n_A + k \cdot \mathrm{ord}(g)$ which implies that

$$(g^{n_B})^{i_0} = g^{n_B i_0} = g^{n_B(n_A + k\mathrm{ord}(g))} = g^{n_A n_B} = s \pmod p,$$

i.e. Charlie has found the secret key.

This is indeed a way to break this type of code. The upshot is that if p is large and Alice has not been extremely unlucky in her choice of parameters this will be *extremely* time-consuming, to the extent where it is practically impossible using current technology. We have run into a particular case of the discrete log problem.

Problem 3.1 — The discrete log problem. Let G be a finite group and let $g \in G$. Given an element a in the cyclic group generated by g, find n such that

$$g^n = a$$

In general solving the discrete log problem is *believed* to be computationally infeasible. No general algorithm is known, which is polynomial in the number of digits of the size of the group G. There are groups (Like $(\mathbb{Z}/n\mathbb{Z}, +)$) where solving the discrete logarithm problem is easy, but in general, and for the group $(\mathbb{Z}/p\mathbb{Z})^\times$ it is considered very hard. Analogous to factoring into primes there is a quantum computer algorithm developed by Schor [Sho94] which solves this in polynomial time, so if the technology of quantum computers computers matures sufficiently, Alice and Bob need to be careful when using the Diffie–Hellman protocol. And at all times they need to choose the size of p in a way where they are not vulnerable to this type of attack.

Man in the Middle attack

The Diffie–Hellman key exchange is also vulnerable to another kind of attack called the man-in-the-middle attack. The problem is the following:

What if, when Alice and Bob transmit their respective values $g^{n_A} \pmod p$ and $g^{n_B} \pmod p$ to each other, Charlie manages to substitute $g^{n_A} \pmod p$ by $g^{n_C} \pmod p$ and also $g^{n_B} \pmod p$ by $g^{n_C} \pmod p$ without Alice and Bob noticing. Here n_C is a value that Charlie chooses.

Then Alice computes $s_A = (b^{n_C})^{n_A} \pmod p$ believing this is the shared secret, while Bob computes $s_B = (b^{n_C})^{n_B} \pmod p$ believing this is the shared secret. But Charlie can compute both s_A, and s_B since he knows $g^{n_A} \pmod p$, $g^{n_B} \pmod p$, and n_C. Hence Charlie can completely control the encrypted correspondence between Alice and Bob.

3.2.2 RSA

A more flexible and much more widely used protocol is the RSA protocol invented by R. Rivest, A. Shamir, and L. Adleman in the 1970'ies [RSA78]. This is a so-called asymmetric algorithm which uses different "keys" for encrypting and decrypting.

Constructing private and public keys

In RSA Alice needs to construct 2 keys. One for encrypting and one for decrypting. What she needs to do is the following:

Constructing keys

1. Choose secretly two large primes p_1, p_2.
2. Compute secretly $n_A = p_1 p_2$ and $\varphi(n_A) = (p_1 - 1)(p_2 - 1)$, and
3. Choose a "random" $1 < e_A < \varphi(n_A)$ which is coprime to $\varphi(n_A)$.
4. Find secretly a solution d_A to the equation $e_A x = 1 \pmod{\varphi(n_A)}$ (using Bezout's identity).
5. Make public the public key (e_A, n_A).
6. Keep secret the private key (d_A, n_A).

If Bob now wants to send the message $a \bmod n_A$ to Alice he simply encrypts his message by computing $a^{e_A} \bmod n_A$ and sends it to Alice. Alice then computes $(a^{e_A})^{d_A} \bmod n_A$ and uses the following Proposition:

Proposition 3.2.1 Let n be a product of distinct primes. Assume $ed = 1 \pmod{\varphi(n)}$. Then for every a we have

$$a^{ed} = a \pmod n.$$

Proof. Notice that $\varphi(n) = \prod_{p|n}(p-1)$. Since distinct primes are relatively prime it follows from Proposition 1.2.6 (iii) that it suffices to prove that $a^{ed} = a \pmod p$ for every prime dividing n. If a is divisible by p this is clear since both sides equal 0. If a is not divisible by p the numbers a and p are coprime, and Theorem 2.3.1 then gives that

$$a^{ed} = a^{ed-1}a = a^{\varphi(n)k}a = a^{(p-1)l_p}a = a \pmod p,$$

which completes the proof. ■

Note that in the proof of Proposition 3.2.1 we do not use that ed is a product of integers, but only that it equals 1 mod $\varphi(n)$. We could just as well have formulated it for an integer $m = 1 \bmod \varphi(n)$, and then concluded that $a^m = a \bmod n$. The reason it is formulated with a product $m = ed$ is that this shows directly that Alice can compute $(a^{e_A})^{d_A} \bmod n_A$ and will get as result the original message $a \bmod n_A$. This is the basic idea of RSA.

Now Bob has a secure way to send messages to Alice. If Bob wants to be able to receive encrypted messages he needs to go through the same procedure as Alice to construct his own public key (e_B, n_B) and private key (d_B, n_B). If he makes the public key public Alice (or anyone else) can encrypt a message $b \bmod n_B$ by computing $b^{e_B} \bmod n_B$ and sending this coded messages to Bob who can decrypt it using his private key.

■ **Example 3.4** Let us compute a (unrealistically small) set of RSA-keys for Alice.

1. Choose the primes $p_1 = 43$, $p_2 = 67$.
2. $n_A = 43 \cdot 67 = 2881$, $\varphi(n_A) = 42 \cdot 66 = 2772$.
3. We choose $e_A = 1003$.
4. $1003x = 1 \pmod{2772}$ has solution 655.
5. The public key is $(1003, 2881)$.
6. The private key is $(655, 2881)$.

Alice now puts the public key on her website. Bob wants to send her the number 1330 which is the time he wants her to meet at their secret place the next day. He computes $1330^{1003} \bmod 2881 = 2259 \bmod 2881$ and sends Alice 2259. She computes $2259^{655} \bmod 2881 = 1330 \bmod 2881$ and now knows that Bob wants to meet her at 13.30.

In real life applications the primes are typically several 100 digits long. ■

Keep it secret, keep it safe

The security on RSA rests on a very simple observation: It is very easy to multiply two large primes $n = p_1 \cdot p_2$, but if all we know is the result n, it seems very hard to find, in a reasonable amount of time, the two prime factors p_1, p_2.[1]

If Charlie could somehow compute the prime factorization of n_A he would be able to compute $\varphi(n_A)$ and then he could solve the equation $e_A x = 1 \pmod{\varphi(n)}$ meaning that he could find d_A. Once he knows d_A he can decrypt any encrypted message to Alice he can get his hands on. Hence it is crucial that Alice does not treat the two primes p_1, p_2, or $\varphi(n_A)$ carelessly. In fact once the keys (e_A, n_A), (d_A, n_A) have been generated the safest thing she can do is probably to delete them completely. Many people suspect that without knowing the prime factorization of n_A beforehand it is generally as difficult to find d_A as to factor n_A.

If Charlie knows p_1, p_2 he can compute $\varphi(n_A)$ and break the code. Knowing $\varphi(n_A)$ and n_A is in fact essentially equivalent to knowing the prime factors p_1, p_2 as they are the roots of the polynomial

$$x^2 + (\varphi(n_A) - (n_A + 1))x + n_A,$$

which follows from Exercise 3.3.

3.3 Exercises for Chapter 3

Exercise 3.1 — Korselt's criterion. Let n be a composite square-free number. Assume that $p - 1 \mid n - 1$ for every p dividing n. Show that n is a Carmichael number.

Exercise 3.2 Show that 1105, 1729, and 2465 are Carmichael numbers.

Exercise 3.3 Let n be a product of two primes p_1, p_2. Show that the polynomial

$$x^2 + (\varphi(n) - (n+1))x + n$$

has p_1 and p_2 as its roots.

Exercise 3.4 Find the last two digits of 5^{75} and 7^{75}.

[1] I dare you to find the prime factors of
$n =$159542902770478353477333649649796581389938839451613607718093662563072803655525608627699609028760
74683622288154113013374670636273789063661078805497874071102398808291120799306047641864281161403791
13482778195649341783699438770737541361816167097612982009724078014971271538123606653607727522296003
21587160692562661
which is a product of two primes. The primes were computed and multiplied together on my laptop in about a second. This is a realistic size n for RSA.

4. Quadratic reciprocity

In the field $\mathbb{F}_p$ it is easy to solve first degree equations $ax+b=0 \pmod p$. Since $\mathbb{F}_p$ is a field this has a solution whenever $a \neq 0 \bmod p$ given by $x = a^{-1}(-b) \pmod p$ where $a^{-1} \bmod p$ is the multiplicative inverse of $a \bmod p$ in $\mathbb{F}_p$.

Consider now a second degree equation of the form

$$ax^2+bx+c=0 \pmod p \tag{4.1}$$

where we assume $a \neq 0 \pmod p$. By Proposition 2.4.1 this equation can have at most 2 solutions. Assume that $p \neq 2$ (See Exercise 4.1 for the case $p=2$.) To understand when it has solutions we complete the square, write $D = b^2-4ac$ and find

$$\begin{aligned} 0 = ax^2+bx+c &= \frac{1}{4a}\left(4a^2x^2+4abx+4ac\right) \\ &= \frac{1}{4a}\left((2ax+b)^2-b^2+4ac\right) = \frac{1}{4a}\left((2ax+b)^2-D\right) \pmod p \end{aligned}$$

This small computation reduces the question of existence of solutions to (4.1) to the question of existence of solutions to

$$y^2 = D \pmod p. \tag{4.2}$$

Putting $y=2ax+b$ we see that (4.1) has solutions if and only if (4.2) has solutions. If $D=0 \pmod p$ equation 4.2 has exactly one solution namely $y=0$, and if $D \neq 0 \pmod p$ and (4.2) has a solution (call it $\sqrt{D}$) then it has two distinct solutions namely $\pm\sqrt{D}$. In this case it follows that the solutions to (4.1) are given by the familiar formula

$$\frac{1}{2a}\left(-b \pm \sqrt{D}\right).$$

We will now develop methods for determining whether the equation $y^2 = D \pmod p$ has solutions or not.

4.1 Quadratic residues and Legendre symbols

Definition 4.1.1 Let p be a prime. An integer $a \neq 0 \pmod p$ is called a quadratic residue modulo p if $y^2 = a \pmod p$ has a solution. If not a is called a quadratic non-residue.

We note that $a \in \mathbb{Z}$ not divisible by p is a quadratic residue modulo p if and only $a \bmod p \in \mathbb{F}_p^\times$ is a square in $\mathbb{F}_p^\times$ i.e. $a \bmod p = b^2$ for some $b \in \mathbb{F}_p^\times$, and a quadratic non-residue if and only if $a \bmod p$ is not a square in $\mathbb{F}_p^\times$.

■ **Example 4.1** Let $p = 7$. We compute all squares modulo p

$y \bmod 7$	0	1	2	3	4	5	6
$y^2 \bmod 7$	0	1	4	2	2	4	1

and we see that 1, 2 and 4 are quadratic residues and 3,5,6 are quadratic non-residues modulo 7 ■

Definition 4.1.2 Let $p > 2$ be a prime and let $a \in \mathbb{Z}$. We define the Legendre symbol by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a = 0 \pmod p \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

We note that

$$\text{if } a_1 = a_2 \pmod p \text{ then } \left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right). \tag{4.3}$$

We note also that $\left(\frac{a}{p}\right) = 0$ if and only if $a = 0 \pmod p$. It follows that the map

$$\begin{array}{rccc} \psi : & \mathbb{F}_p^\times & \to & \{\pm 1\} \\ & a \bmod p & \mapsto & \left(\frac{a}{p}\right) \end{array} \tag{4.4}$$

is well-defined. Note that the set $\{\pm 1\}$ equipped with ordinary multiplication is a group of order 2.

Lemma 4.1.1 The map ψ is a surjective group homomorphism.

Proof. Note that $f \in \mathbb{F}_p$ satisfies $\psi(f) = 1$ if and only if f is a square in $\mathbb{F}_p^\times$. By Corollary 2.4.5 $\mathbb{F}_p^\times$ is cyclic, so let g be a generator. Hence $g^{p-1} = g^0 = 1 \bmod p$, and $p-1$ is the smallest number with this property. The elements of $\mathbb{F}_p^\times$ are precisely

$$g^1, g^2, \dots g^{\frac{p-3}{2}}, g^{\frac{p-1}{2}}, g^{\frac{p+1}{2}}, \dots, g^{p-1}.$$

The squares of these gives

$$g^2, g^4, \dots g^{p-3}, \overset{\overset{g^0}{\shortparallel}}{g^{p-1}}, \overset{\overset{g^2}{\shortparallel}}{g^{p+1}}, \dots, \overset{\overset{g}{\shortparallel}}{g^{2(p-1)}}$$

so $f \in \mathbb{F}_p^\times$ is a square precisely if $f = g^{2i}$ for some i. It follows that $\psi(g^j) = (-1)^j$. But this is clearly a group homomorphism since

$$\psi(g^i g^j) = \psi(g^{i+j}) = (-1)^{i+j} = (-1)^i(-1)^j = \psi(g^i)\psi(g^j).$$

Observing that $\psi(g) = -1$, and $\psi(g^2) = 1$ shows that ψ is surjective. ■

Corollary 4.1.2 Let p be a prime and let $a, b \in \mathbb{Z}$. Then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Proof. If $p \mid ab$ then by Lemma 1.4.1 we have $p \mid a$ or $p \mid b$, so both sides of the equation are zero. If $p \nmid ab$ then $ab \bmod p \in \mathbb{F}_p^\times$ and by Lemma 4.1.1 we have

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

■

Corollary 4.1.3 Let $Q_p = \{a \bmod p \in \mathbb{F}_p^\times | a \text{ is a quadratic residue modulo } p\}$. Then Q_p is a subgroup of $\mathbb{F}_p^\times$ of index 2. In particular there are the same number of squares as non-squares in $\mathbb{F}_p^\times$.

Proof. We have $Q_p = \ker\psi$, from which the result follows that Q_p is a subgroup. It follows from the isomorphism theorem that $Im(\psi) = \{\pm 1\}$ is isomorphic to the quotient $\mathbb{F}_p^\times/\ker\psi$ so $\#Q_p = (p-1)/2$ from which the claim follows. Note also that it follows from the proof of Lemma 4.1.1 that the squares are exactly $g^2, g^4, \ldots, g^{p-1}$ ■

4.2 Quadratic reciprocity

Consider the following question: Let p, q be two different primes. What is the relation (if any) between the solvability of the equation $x^2 = p \pmod q$ and the solvability of $x^2 = q \pmod p$? Or said using Legendre symbols: What is the relation between $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$

This is the content of the main theorem of this chapter:

Theorem 4.2.1 — Quadratic reciprocity. Let p, q be different odd primes. Then

(i) $\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$,

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

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

We note that in case (ii) the right-hand side depends only on $p \bmod 4$ since if $p = a \pmod 4$ then $(p-1)/2 = (a-1)/2 + 2k$ for a $k \in \mathbb{Z}$. In case (iii) the right-hand side depends only on $p \bmod 8$ since if $p = a \pmod 8$ then $(p^2-1)/8 = (a^2-1)/8 + 2k'$ for a $k' \in \mathbb{Z}$.

R The quadratic reciprocity theorem was first conjectured by Legendre and Euler and first rigorously proved by Gauss, probably in 1796. Gauss gave several proofs and called it the "aureum theorema" (golden theorem) in his diary. There are now more than 300 proofs (see e.g. [Bau15, Ch. 15]). We will make an elegant proof which uses Gauss sums. Gauss sums are important tools in number theory. For a very elementary proof using nothing more than the Chinese remainder theorem see e.g [Rou91].

■ **Example 4.2** Before diving into the proof of quadratic reciprocity let us see how it can be used to determine if -14 is a quadratic residue modulo 2503 which can easily be verified to be a prime.

We compute

$$\begin{aligned}
\left(\frac{-14}{2503}\right) &= \left(\frac{-1}{2503}\right)\left(\frac{2}{2503}\right)\left(\frac{7}{2503}\right) && \text{by Corollary 4.1.2}\\
&= (-1)^{\frac{2503-1}{2}}(-1)^{\frac{2503^2-1}{8}}(-1)^{\frac{2503-1}{2}\frac{7-1}{2}}\left(\frac{2503}{7}\right) && \text{by Quadratic reciprocity}\\
&= (-1)1(-1)\left(\frac{2503}{7}\right)\\
&= \left(\frac{4}{7}\right) && \text{by (4.3) since } 2503 = 357\cdot 7+4\\
&= \left(\frac{2}{7}\right)^2 = 1 && \text{by Corollary 4.1.2}
\end{aligned}$$

so -14 is a quadratic residue modulo 2503. Indeed $x^2 = -14$ has solutions ± 274 ▪

Proposition 4.2.2 — Euler's criterion. Let $p > 2$ be a prime and $a \in \mathbb{Z}$. Then $\left(\frac{a}{p}\right) = 1$ if and only if $a^{(p-1)/2} = 1 \pmod{p}$.

Proof. Recall the homomorphism ψ from (4.4). The map $\rho : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, defined by $\rho(a \bmod p) = a^{(p-1)/2} \bmod p$ is a group homomorphism (Exercise 4.2), so $\ker(\rho)$ is a subgroup of $\mathbb{F}_p^\times$ i.e. $\ker(\rho) \leq \mathbb{F}_p^\times$. We have also $Q_p = \ker\psi \leq \ker\rho \leq \mathbb{F}_p^\times$ since if $g \in \ker\psi$ then $g = h^2$ so $\rho(g) = g^{(p-1)/2} = h^{p-1} = 1$, since $\mathbb{F}_p^\times$ has order $p-1$. Since Q_p has index 2, $\ker\rho$ will have index 1 or 2 in $\mathbb{F}_p^\times$. But if it has index 1 then every $g \in \mathbb{F}_p^\times$ is a root of $x^{(p-1)/2} - 1$ which contradicts Proposition 2.4.1, so $\ker\rho$ must have index 2 in $\mathbb{F}_p^\times$. But this implies that $\#Q_p = \#\ker\rho = (p-1)/2$ which forces $Q_p = \ker\rho$ which shows the result. ■

Proposition 4.2.3 Let $p > 2$ be a prime and let $a \in \mathbb{Z}$. Then $\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}$.

Proof. If $p \mid a$ both sides are zero so suppose not. We notice that $a^{(p-1)/2} \bmod p$ is a solution to $x^2 = 1 \bmod p$. By Proposition 2.4.2 there are exactly two solutions to this equation and since $\pm 1 \bmod p$ are indeed solutions we must have $a^{(p-1)/2} = \pm 1 \pmod{p}$.

Proposition 4.2.2 says that a is a quadratic residue precisely if $a^{(p-1)/2} = 1 \pmod{p}$ so, if a is a quadratic non-residues we must have $a^{(p-1)/2} = -1 \pmod{p}$, since there are no other possible values for it. ■

We can now prove Theorem 4.2.1 (ii):

Corollary 4.2.4 Let p be an odd prime. Then $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Proof. By Proposition 4.2.3 with $a = -1$ we find $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \pmod{p}$, so $\left(\frac{-1}{p}\right) - (-1)^{(p-1)/2}$ is divisible by p. Since $\left(\frac{-1}{p}\right) - (-1)^{(p-1)/2} \in \{0, \pm 2\}$ and $p > 2$ this implies the claim. ■

4.2.1 Algebraic integers

Before continuing to prove the rest of the quadratic reciprocity theorem, we need a small intermezzo about algebraic integers. We need to work in congruences in a slightly more general setting than we have done so far.

Definition 4.2.1 A complex number ζ is called *algebraic* if it is a root in non-zero polynomial with integer coefficients, i.e. if $f(\zeta) = 0$ for some $0 \neq f \in \mathbb{Z}[x]$. If ζ is root of a monic polynomial it is called an *algebraic integer*. The set of algebraic numbers are denoted by $\overline{\mathbb{Q}}$ and the set of algebraic integers are denoted by $\overline{\mathbb{Z}}$.

■ **Example 4.3**

- If $n \in \mathbb{Z}$ then $n \in \overline{\mathbb{Z}}$ since n is a root of $x - n$.
- $(1+\sqrt{13})/2$ is an algebraic integer since it is a root of $x^2 - x - 3$
- $54 + \sqrt[17]{2}$ is an algebraic integer since it is a root of $(x-54)^{17} - 2$
- Let $n \in \mathbb{N}$. Then $\zeta_n = e^{\frac{2\pi i}{n}}$ is an algebraic integer since it is a root of $x^n - 1$
- Let $n, m \in \mathbb{Z}$. Then $n + im$ is an algebraic integer since it is a root of $(x-n)^2 + m^2$

■

Definition 4.2.2 Let ζ be an algebraic number. Then $d = \min\{\deg(p) | p(\zeta) = 0, p \in \mathbb{Z}[x]\}$ is called the degree of ζ.

We note that ζ is rational if and only if ζ is algebraic and of degree 1. If ζ is algebraic of degree 2 we call ζ a *quadratic irrational*.

R There are many complex numbers which are not algebraic. In fact the algebraic numbers are countable (See Exercise 4.4), and since the complex numbers are uncountable most complex numbers are non-algebraic. We call them *transcendental*. Proving that specific numbers are transcendental is usually rather tricky. Examples of provably transcendental numbers are $\sum_{i=1}^{\infty} 10^{-i!}$, e, π, e^{π}, $2^{\sqrt{2}}$. On the other hand there are many numbers which are conjectured but not proved to be transcendental like $\pi \pm e$, γ, $\zeta(3)$ and many others. The study of such properties is usually called transcendence theory (Consult [Wal79]).

Since $\overline{\mathbb{Z}} \subseteq \mathbb{C}$ we can multiply, and subtract two algebraic integers, and – perhaps surprisingly – the result is still an algebraic integer as we see from the following result:

Theorem 4.2.5 The set $\overline{\mathbb{Z}}$ is a subring of $\mathbb{C}$, and $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$.

We will not prove Theorem 4.2.5, but refer to [Jar14, Cor 2.28 and Cor. 2.12]. We shall only use the first part the theorem.

Theorem 4.2.6 The rational algebraic integers are precisely the integers i.e.

$$\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$$

Proof. We have already seen in the above examples that $\mathbb{Z} \subseteq \overline{\mathbb{Z}} \cap \mathbb{Q}$. Let $\zeta = \frac{m}{n}$ be a rational algebraic integer which is a root of the monic polynomial $f(x) = x^k + \sum_{i=0}^{k-1} a_i x^i$ with integer coefficients. We may assume that $\gcd(m,n) = 1$ and $n \geq 1$. Inserting ζ in f, multiplying by n^k and subtracting m^k we find

$$\sum_{i=0}^{k-1} a_i m^i n^{k-i} = -m^k, \tag{4.5}$$

so since n is a clearly a factor in the left-hand side we see that $n \mid m^k$ which implies that $n = 1$ since $\gcd(m,n) = 1$. But then $\zeta = m \in \mathbb{Z}$ which completes the proof. ■

We define congruences in the algebraic integers as follows: For $a, b, c \in \overline{\mathbb{Z}}$ we write $a \cong b \pmod{c}$ if there exist a $d \in \overline{\mathbb{Z}}$ such that $a - b = cd$.

Proposition 4.2.7 Suppose $a \cong b \pmod{c}$ where $a, b, c \in \mathbb{Z}$. Then $a = b \pmod{c}$.

Proof. Since $a \cong b \pmod{c}$ there exist a $d \in \overline{\mathbb{Z}}$ such that $a - b = cd$. But this implies that $d \in \mathbb{Q}$ so by Theorem 4.2.6 we have $d \in \mathbb{Z}$ which proves the claim. ■

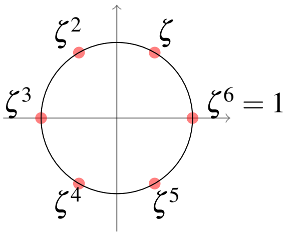


Figure 4.1: 6th roots of 1

R The theory of algebraic numbers is vast, fascinating, and important in many modern mathematical theories. Here we are only barely touching the surface. For a more thorough introduction consult [Hec81; Jar14; Mar77; Neu99].

Definition 4.2.3 An nth root of 1 is a complex number $\zeta \in \mathbb{C}$ such that $\zeta^n = 1$. The root is called *primitive* if $\zeta^k \neq 1$ for $1 \leq k < n$.

Note that both primitive and non-primitive roots of 1 are algebraic integers as they are roots of $f(x) = x^n - 1$

Proposition 4.2.8 The nth roots of 1 are precisely $\zeta_n^k = e^{\frac{2\pi i k}{n}}$ where $0 \leq k < n$. The primitive nth roots of 1 are precisely $\zeta_n^k = e^{\frac{2\pi i k}{n}}$ where $0 \leq k < n$ and $\gcd(n,k) = 1$.

Proof. See Exercise 4.9 ■

■ **Example 4.4** The 6th primitive roots of 1 are $\zeta_6 = e^{2\pi i/6}$ and $\zeta_6^5 = e^{2\pi i 5/6}$. All 6th roots of 1 are illustrated in Figure 4.1 . ■

If $n \in \mathbb{N}$ we will always write $\zeta_n = e^{2\pi i/n}$ which is an nth primitive root of 1.
We consider the set

$$\mathbb{Z}[\zeta_n] = \{a_0 + a_1\zeta_n + a_2\zeta_n^2 + \ldots a_{n-1}\zeta_n^{n-1} | a_i \in \mathbb{Z}\}.$$

We notice immediately that $\mathbb{Z}[\zeta_n]$ is a subring of $\overline{\mathbb{Z}}$. We can now prove Theorem 4.2.1 (iii):

Proof. Let p be an odd prime. Consider $\zeta = \zeta_8 = e^{2\pi i/8} \in \mathbb{Z}[\zeta_8]$ which is an 8th primitive root of 1. Note that $\zeta^{-1} = \zeta^7 \in \mathbb{Z}[\zeta_8]$. We have

$$0 = \zeta^8 - 1 = (\zeta^4 + 1)(\zeta^4 - 1) = (\zeta^2 + \zeta^{-2})\zeta^2(\zeta^4 - 1)$$

Since ζ is an 8th primitive root of 1 it follows that $\zeta^2 + \zeta^{-2} = 0$. If we let $\tau = \zeta + \zeta^{-1}$, then $\tau^2 = \zeta^2 + \zeta^{-2} + 2 = 2$. It follows from Proposition 4.2.3 that $\tau^{p-1} = 2^{(p-1)/2} = \left(\frac{2}{p}\right) \pmod{p}$ and by multiplying the underlying equality by τ we find that

$$\tau^p \simeq \tau \left(\frac{2}{p}\right) \pmod{p}$$

Since the binomial coefficients $\binom{p}{i}$ are divisible by p if $1 \leq i \leq p-1$ (See Exercise 4.10). It follows from the binomial formula that for

$$x, y \in \overline{\mathbb{Z}} \text{ we have } (x+y)^p \simeq x^p + y^p \pmod{p}. \tag{4.6}$$

Using this for $x = \zeta$, $y = \zeta^{-1}$ we see that

$$\zeta^p + \zeta^{-p} \simeq \tau \left(\frac{2}{p}\right) \pmod{p} \tag{4.7}$$

We now have to go through the 4 cases $p = \pm 1, \pm 3 \pmod 8$:

If $p = 1 \pmod 8$ then $\zeta^{\pm p} = \zeta^{\pm 1}$ so (4.7) reads $\tau \cong \tau \left(\frac{2}{p}\right) \pmod p$ so multiplying by τ and using $\tau^2 = 2$ we find $2 \cong 2\left(\frac{2}{p}\right) \pmod p$. We can now use Proposition 4.2.7 to conclude that $2 = 2\left(\frac{2}{p}\right) \pmod p$. Multiplying by an integer b satisfying $2b = 1 \pmod p$ (Use $\gcd(2, p) = 1$ and Bezout to find such b) we see that $1 = \left(\frac{2}{p}\right) \pmod p$. We conclude that $p \mid (\left(\frac{2}{p}\right) - 1)$ and since $\left(\frac{2}{p}\right) - 1 \in \{0, \pm 2\}$ we find that in this case $\left(\frac{2}{p}\right) = 1$.

If $p = -1 \pmod 8$ then $\zeta^{\pm p} = \zeta^{\mp 1}$ so we find $\tau \cong \tau \left(\frac{2}{p}\right) \pmod p$ as before so we can again conclude $\left(\frac{2}{p}\right) = 1$.

If $p = 3 \pmod 8$ then $\zeta^p = \zeta^3 = \zeta^4 \zeta^{-1} = -\zeta^{-1}$ and $\zeta^{-p} = -\zeta$ so $\zeta^p + \zeta^{-p} = -\tau$ and (4.7) reads $-\tau \cong \tau \left(\frac{2}{p}\right) \pmod p$. Arguing as before this leads to $\left(\frac{2}{p}\right) = -1$.

If $p = -3 \pmod 8$ then $\zeta^p = \zeta^{-3} = \zeta^{-4}\zeta^1 = -\zeta^1$ and $\zeta^{-p} = -\zeta^{-1}$ so again $\zeta^p + \zeta^{-p} = -\tau$ and we find $\left(\frac{2}{p}\right) = -1$.

■

4.2.2 Gauss sums

In order to generalize the proof of Theorem 4.2.1 (ii) presented above we introduce some very important sums:

Definition 4.2.4 Let p be an odd prime. The Gauss sum associated to $a \in \mathbb{Z}$ is the sum

$$g_p(a) = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{an}.$$

We note that since $\zeta_p^{a+p} = \zeta_p^a$ since ζ_p is a pth root of 1 we have $g_p(a+p) = g_p(a)$ so the Gauss sum depends only on a mod p. We note also that since ζ_p lies in the ring $\mathbb{Z}[\zeta_p]$ we have $g_p(a) \in \mathbb{Z}[\zeta_p]$.

■ **Example 4.5** Let $p = 5$. We have $\zeta_5 = e^{2\pi i/5}$ and

n	0	1	2	3	4
$\left(\frac{n}{5}\right)$	0	1	-1	-1	1

$$g_5(0) = 0 + 1 + (-1) + (-1) + 1 = 0$$

$$g_5(1) = e^{\frac{2\pi i}{5}} - e^{\frac{2\pi i2}{5}} - e^{\frac{2\pi i3}{5}} + e^{\frac{2\pi i4}{5}} = 2\cos(\frac{2\pi}{5}) - 2\cos(\frac{2\pi 3}{5}) = 2\frac{-1+\sqrt{5}}{4} - 2\frac{-1-\sqrt{5}}{4} = \sqrt{5}$$

$$g_5(2) = e^{\frac{2\pi i2}{5}} - e^{\frac{2\pi i4}{5}} - e^{\frac{2\pi i6}{5}} + e^{\frac{2\pi i8}{5}} = e^{\frac{2\pi i2}{5}} - e^{\frac{2\pi i4}{5}} - e^{\frac{2\pi i}{5}} + e^{\frac{2\pi i3}{5}} = -g_5(1) = -\sqrt{5}$$

$$g_5(3) = e^{\frac{2\pi i3}{5}} - e^{\frac{2\pi i6}{5}} - e^{\frac{2\pi i9}{5}} + e^{\frac{2\pi i12}{5}} = e^{\frac{2\pi i3}{5}} - e^{\frac{2\pi i}{5}} - e^{\frac{2\pi 4}{5}} + e^{\frac{2\pi i2}{5}} = -g_5(1) = -\sqrt{5}$$

$$g_5(4) = e^{\frac{2\pi i4}{5}} - e^{\frac{2\pi i8}{5}} - e^{\frac{2\pi i12}{5}} + e^{\frac{2\pi i16}{5}} = e^{\frac{2\pi i4}{5}} - e^{\frac{2\pi i3}{5}} - e^{\frac{2\pi 2}{5}} + e^{\frac{2\pi i}{5}} = g_5(1) = \sqrt{5}$$

■

The next lemma shows that this pattern holds much more generally.

Lemma 4.2.9 Let p be a prime. Then for any $a \in \mathbb{Z}$ we have

$$g_p(a) = \left(\frac{a}{p}\right) g_p(1)$$

Proof. If $a = 0 \pmod p$ then the legendre symbol is zero so we have to show that in this case we have $g_p(a) = 0$. But we have $g_p(a) = g_p(0) = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right)$ which equals 0 by Corollary 4.1.3.

Assume now that $a \not\equiv 0 \pmod{p}$. Then

$$\begin{aligned}
\left(\frac{a}{p}\right) g_p(a) &= \sum_{n=0}^{p-1} \left(\frac{a}{p}\right)\left(\frac{n}{p}\right) \zeta_p^{an} \\
&= \sum_{n=0}^{p-1} \left(\frac{an}{p}\right) \zeta_p^{an} && \text{by Corollary 4.1.2} \\
&= \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{n} = g_p(1)
\end{aligned}$$

where in the penultimate equality we have used the following reasoning: The summands only depend on n mod p. Since $\gcd(a,p) = 1$ we see that multiplication by a gives a bijection from $\mathbb{Z}/p\mathbb{Z}$ to itself so an mod p runs through the same set as n mod p and the sum is unchanged. Multiplying both sides by $\left(\frac{a}{p}\right) = \pm 1$ gives the result. ■

We will often write $g_p = g_p(1)$.

Lemma 4.2.10 Let $n \in \mathbb{N}$ and $x, y \in \mathbb{Z}$. Then

$$\frac{1}{n}\sum_{a=0}^{n-1} \zeta_n^{(x-y)a} = \begin{cases} 1 & \text{if } x = y \pmod{n} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. If $x = y \pmod{n}$ then $\zeta_n^{x-y} = 1$ and the claim is clear. If not then $\zeta_n^{x-y} \neq 1$ and we may use the formula for the geometric series to see that

$$\sum_{a=0}^{n-1} \zeta_n^{(x-y)a} = \frac{\zeta_n^{(x-y)n} - 1}{\zeta_n^{(x-y)} - 1} = 0$$

since $\zeta_n^n = e^{2\pi i n/n} = 1$. ■

Theorem 4.2.11 Let $a \not\equiv 0 \pmod{p}$. Then $g_p(a)^2 = (-1)^{(p-1)/2} p$. In particular $|g_p(a)| = \sqrt{p}$.

Proof. It suffices to prove the claim for $a = 1$, since by Lemma 4.2.9 $g_p(a)^2 = g_p(1)^2 \left(\frac{a}{p}\right)^2 = g_p^2$. (Recall that we write $g_p = g_p(1)$).

Note that by Lemma 4.2.9 and Corollary 4.1.2 we have – if $a \not\equiv 0 \pmod{p}$ – that $g_p(a)g_p(-a) = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g_p^2 = \left(\frac{-1}{p}\right) g_p^2 = (-1)^{(p-1)/2} g_p^2$, where we have used Corollary 4.2.4. Also $g_p(0) = 0$ by Lemma 4.2.9. The proof of the claim will follow from two different computations of the expression $\sum_{a=0}^{p-1} g_p(a) g_p(-a)$. By the above observation it equals $(p-1)(-1)^{(p-1)/2} g_1^2$. Using the definition of $g_p(a)$ we find

$$\begin{aligned}
(p-1)(-1)^{(p-1)/2} g_p^2 = \sum_{a=0}^{p-1} g_p(a) g_p(-a) &= \sum_{a=0}^{p-1}\sum_{n=0}^{p-1}\sum_{m=0}^{p-1} \left(\frac{n}{p}\right)\left(\frac{m}{p}\right) \zeta_p^{an} \zeta_p^{-am} \\
&= \sum_{n=0}^{p-1}\sum_{m=0}^{p-1} \left(\frac{n}{p}\right)\left(\frac{m}{p}\right) \sum_{a=0}^{p-1} \zeta_p^{a(n-m)} \\
&= p \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)\left(\frac{n}{p}\right) = p(p-1)
\end{aligned}$$

where in the penultimate equality we have used Lemma 4.2.10. Diving by $p-1$ gives the result. ■

We are now ready to prove the main part of quadratic reciprocity namely Theorem 4.2.1 (i).

Proof. Let $p^* = (-1)^{(p-1)/2}p$. Then according to Theorem 4.2.11 we have $g_p^2 = p^*$.

By Proposition 4.2.3 we have $(p^*)^{(q-1)/2} = \left(\frac{p^*}{q}\right) \pmod{q}$. Combining these we find that

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

Multiplying by g_p we no longer have a congruence in $\mathbb{Z}$ but only in $\overline{\mathbb{Z}}$. We get

$$g_p^q \overset{\sim}{=} g_p \left(\frac{p^*}{q}\right) \pmod{q}$$

Using (4.6) we see that the left-hand side satisfies

$$g_p^q = \left(\sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta_p^n\right)^q \overset{\sim}{=} \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)^q \zeta_p^{qn} \pmod{q}$$

Since $\left(\frac{n}{p}\right)^q = \left(\frac{n}{p}\right)$ the right-hand side equals $g_p(q)$ which by Lemma 4.2.9 equals $\left(\frac{q}{p}\right)g_p$. Putting it all together we have proved

$$g_p \left(\frac{p^*}{q}\right) \overset{\sim}{=} g_p \left(\frac{q}{p}\right) \pmod{q}. \tag{4.8}$$

Multiplying by g_p and using Theorem 4.2.11 and Proposition 4.2.7 we find that

$$p^* \left(\frac{p^*}{q}\right) = p^* \left(\frac{q}{p}\right) \pmod{q}$$

Since $\gcd(p^*, q) = 1$ we can multiply by an $(p^*)^{-1}$ satisfying $p^*(p^*)^{-1} = 1 \pmod{q}$ which gives that

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right) \pmod{q}$$

from which we may conclude that $\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$. To finish we note that

$$\left(\frac{p^*}{q}\right) = \left(\frac{(-1)^{(p-1)/2}p}{q}\right) = \left(\frac{-1}{q}\right)^{(p-1)/2} \left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right)$$

which finishes the proof. ■

■ **Example 4.6** We want to determine if $5x^4 + 35x^2 + 3 = 0 \pmod{541}$ has any integer solutions. We first notice that if this has a solution x_0 then $y_0 = x_0^2$ will be a solution to $5y^2 + 35y + 3 = 0 \pmod{541}$ which has discriminant $D = 35^2 - 4 \cdot 5 \cdot 3 = 1165$. We need to verify if the discriminant is a square modulo 541 to see if this is even possible. So we compute using Theorem 4.2.1

$$\begin{aligned}\left(\frac{1165}{541}\right) &= \left(\frac{83}{541}\right) = (-1)^{(83-1)(541-1)/4}\left(\frac{541}{83}\right) = \left(\frac{43}{83}\right) = (-1)^{(83-1)(43-1)/4}\left(\frac{83}{43}\right)\\ &= -\left(\frac{40}{43}\right) = -\left(\frac{2}{43}\right)^2\left(\frac{2}{43}\right)\left(\frac{5}{43}\right) = -(-1)^{(43^2-1)/8}(-1)^{(43-1)(5-1)/4}\left(\frac{43}{5}\right) = \left(\frac{3}{5}\right)\\ &= -1\end{aligned}$$

But this means, that $5y^2 + 35y + 3 = 0 \pmod{541}$ has no solutions and therefore $5x^4 + 35x^2 + 3 = 0 \pmod{541}$ also cannot have any solutions. ■

4.3 Exercises for chapter 4

Exercise 4.1 Find all solutions to all second degree equations in $\mathbb{F}_2$.
Exercise 4.2 Let G be an abelian group. Prove that $\rho_n : G \to G$ defined by $\rho_n(g) = g^n$ is a group homomorphism.
Exercise 4.3 Compute $\left(\frac{5}{107}\right)$, $\left(\frac{3}{1871}\right)$, $\left(\frac{5!}{41}\right)$.
Exercise 4.4 Prove that there are only countably many algebraic numbers (recall that a countable union of countable sets is again countable).
Exercise 4.5 Determine which of the following degree 2 equations have integer solutions:

$$x^2+4x+2=0 \bmod 11, \quad x^2+7x+1=0 \bmod 59, \quad x^2+7x+1=0 \bmod 61.$$

Exercise 4.6 Prove, using quadratic reciprocity, that for a prime $p \geq 5$ we have

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p = 1, 11 \bmod 12, \\ -1 & \text{if } p = 5, 7 \bmod 12. \end{cases}$$

Exercise 4.7 In this exercise you will give a direct proof that $\left(\frac{-3}{p}\right) = 1$ when $p = 1 \bmod 3$.

1. Show that $(\mathbb{Z}/p\mathbb{Z})^*$ has an element c of order 3
2. Show that $(2c+1)^2 = -3 \bmod p$.
3. Conclude that $\left(\frac{-3}{p}\right) = 1$.
4. Show independently, using quadratic reciprocity, that $\left(\frac{-3}{p}\right) = 1$.

Exercise 4.8 You may use without proof that $2^{13}-1 = 8191$ is prime. How many natural numbers $x \leq 8191$ satisfy the equation

$$x^2 = 5 \pmod{8191}.$$

Exercise 4.9 Prove Proposition 4.2.8
Exercise 4.10 Let p be a prime. Show that if $1 \leq i \leq p-1$ then $\binom{p}{i}$ is divisible by p.
Exercise 4.11 (Jacobi symbols) Let n be an odd positive number. Factor it like $n = \prod_{i=1}^{k_n} p_i^{e_i}$. Then we define the Jacobi symbol $\left(\frac{a}{n}\right)$ by

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k_n} \left(\frac{a}{p_i}\right)^{e_i}$$

Show that in general $\left(\frac{a}{n}\right) = 1$ does *not* imply that $x^2 = a \pmod{n}$ has a solution.

Show that

1. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ for integers a, b.
2. $\left(\frac{-1}{n}\right) = n \pmod 4$.
3. $\left(\frac{2}{n}\right) = 1$ if $n = \pm 1 \pmod 8$, and -1 otherwise.
4. Assume further that a is positive and odd. Show that

$$\left(\frac{a}{n}\right) = (-1)^{(a-1)(n-1)/4}\left(\frac{n}{a}\right).$$

Exercise 4.12 Let p, q be different odd primes and let $q^* = (-1)^{\frac{q-1}{2}} q$. Show that $x^2 = p \pmod{q}$ has an integer solution if and only if $x^2 = q^* \pmod{p}$ has an integer solution.
Exercise 4.13 For which primes does $x^2+9x+19 = 0 \pmod{p}$ have integer solutions? How many solutions $\bmod p$ does it have?

5. Arithmetic functions and Dirichlet series

5.1 Arithmetical functions

Definition 5.1.1 An arithmetic function is a map

$$f : \mathbb{N} \to \mathbb{C}$$

Note that the set of arithmetical functions are in bijective correspondence to the set of complex sequences under $f \mapsto \{f(n)\}_{n=1}^{\infty}$. As such, without making further assumptions, arithmetic functions are not more nor less interesting than complex sequences.

■ **Example 5.1** The following are all clearly arithmetical functions and it is very easy to cook up other examples:

1. $u(n) = 1$
2. $N(n) = n$
3. Euler's φ function
4. Fix p. The Legendre symbol $\left(\frac{n}{p}\right)$.
5. $I(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$
6. $\tau(n) = \sum_{d|n} 1$, the number of divisors of n.
7. $\sigma(n) = \sum_{d|n} d$, the sum of divisors of n.
8. Let $k \in \mathbb{C}$. $\sigma_k(n) = \sum_{d|n} d^k$,

In the sums the $d \mid n$ means that we sum over positive divisors.

■

Definition 5.1.2 An arithmetical function f is called multiplicative if

$$f(mn) = f(n)f(m) \tag{5.1}$$

whenever m, n are coprime natural numbers. If (5.1) holds for *all* $m, n \in \mathbb{N}$ the arithmetical function f is called completely multiplicative.

All the arithmetical functions from Example 5.1 are multiplicative. (See Exercise 5.1). The arithmetical functions u, N, $\left(\frac{n}{p}\right)$, I are completely multiplicative (See Exercise 5.2).

We note that if n has prime factorization $n = p_1^{l_1} \cdots p_k^{l_k}$ with $p_i \neq p_j$ for $i \neq j$ then

$$\begin{aligned} f(n) = &\quad f(p_1^{l_1}) \cdots f(p_k^{l_k}) && \text{if } f \text{ is multiplicative} \\ = &\quad f(p_1)^{l_1} \cdots f(p_k)^{l_k} && \text{if } f \text{ is completely multiplicative} \end{aligned}$$

Proposition 5.1.1 If $n = p_1^{l_1} \cdots p_k^{l_k}$ then

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

Proof. Since

$$\begin{aligned} \sigma(p^l) &= 1 + p + p^2 + \cdots + p^l = \frac{p^{l+1} - 1}{p - 1} \\ \tau(p^l) &= 1 + 1 + 1 + \cdots + 1 = l + 1 \end{aligned}$$

the proof is immediate.

■

We note that it follows directly from Proposition 5.1.1 that $\tau(n)$ is odd if and only if l_i is even for each i which happens if and only if n is a square, i.e. $n = a^2$ for some $a \in \mathbb{N}$.

5.1.1 Perfect numbers

We now describe an ancient notion going back at least to Euclid, namely that of perfect numbers:

Definition 5.1.3 A natural number $n \in \mathbb{N}$ is called *perfect* if n equals the sum of its proper positive divisors.

We note that formulated in terms of the divisor function we have that a n is perfect if and only if $n = \sigma(n) - n$, i.e. $2n = \sigma(n)$

■ **Example 5.2** The number 6 is perfect since $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6$. In the same way we can check that 28, 496, 8128, 33550336, 8589869056 are perfect numbers. Using a computer one can verify that these are the only perfect numbers less that 10^{10}. ■

Theorem 5.1.2 The number n is perfect and even if and only if $n = 2^{p-1}(2^p - 1)$ where p and $2^p - 1$ are primes.

The "if" part of this theorem goes back to Euclid, but the "only if" part was a conjecture from around year 1000 until it was proven by Euler in the 18th century.

Proof. The "if" part follows from observing that if p and $2^p - 1$ are prime then 2^{p-1} and $2^p - 1$ are coprime and by Proposition 5.1.1 we have

$$\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = \frac{2^p - 1}{2 - 1}(1 + 2^p - 1) = 2 \cdot 2^{p-1}(2^p - 1) = 2n$$

which shows that n is perfect.

To prove the only if part we assume that n is perfect and even and write $n = 2^{p-1}q$ with $p, q \in \mathbb{N}$, $p \geq 2$, and q odd. We note that $q > 1$ since otherwise $n = 2^{p-1}$ but $\sigma(2^{p-1}) = 2^p - 1 \neq 2 \cdot 2^{p-1}$.

Using that n is perfect we see that

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

so by Theorem 1.2.6 (iv) $2^p - 1 \mid q$. Writing $q = r(2^p - 1)$ we find $\sigma(q) = 2^p r$. Hence

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

If $r > 1$ then q, r, and 1 are 3 different divisors of q so $\sigma(q) \geq q + r + 1 = \sigma(q) + 1$ which is impossible; Hence $r = 1$. It follows that $\sigma(q) = 1 + q$ which means that q only has divisors 1 and q which means that $q = 2^p - 1$ is prime. But this can only happen if p is also prime (see Exercise 1.18) which finishes the proof. ■

This theorem classifies even perfect numbers, but doesn't say much about their existence. Also it makes no claim about odd perfect numbers.

Conjecture 5.1.3 There are no odd perfect numbers, but infinitely many even perfect numbers.

It has been verified that there are no odd perfect numbers less than 10^{1500}. Note that by Theorem 5.1.2 there is a 1-1 correspondence between even perfect numbers and Mersenne primes (see Exercise 1.18). See mersenne.org/primes for a list of all 49 known Mersenne primes. Hence we know also 49 even perfect numbers.

5.1.2 Convolution of arithmetical functions

Definition 5.1.4 Let f, g be arithmetical functions. Then we define their *Dirichlet convolution* $f * g$ by

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d)$$

■ **Example 5.3** $\sigma(n) = \sum_{d|n} d = N * u(n)$, $\tau = \sum_{d|n} 1 = u * u(n)$ ■

Let

$$\begin{aligned} A &= \{f \text{ arithmetical functions}\} \\ G &= \{f \in A | f(1) \neq 0\} \\ M &= \{f \in G | f \text{ is multiplicative}\} \end{aligned}$$

Notice that if f is multiplicative then $f(m) = f(m)f(1)$ so if $f \neq 0$ then we have $f(1) = 1$.

Theorem 5.1.4 $(A, *)$ is an abelian semigroup i.e. for every $f, g, h \in A$ we have

$$f * g \in A, \quad \text{and} \quad (f * g) * h = f * (g * h), \quad \text{and} \quad f * g = g * f$$

Proof. It is clear that $f * g \in A$.

We note that we can write $f * g(n)$ as the sum over all expressions $f(a)g(b)$ where a,b are natural numbers multiplying to n, i.e.

$$f * g(n) = \sum_{ab=n} f(a)g(b).$$

It follows immediately that $f*g = g*f$. To see that Dirichlet convolution is associative we note that

$$(f*g)*h(n) = \sum_{ab=n} f*g(a)h(b) = \sum_{ab=n}\sum_{cd=a} f(c)g(d)h(b) = \sum_{cdb=n} f(c)g(d)h(b)$$

and similarly

$$f*(g*h)(n) = \sum_{ab=n} f(a)g*h(b) = \sum_{ab=n}\sum_{cd=b} f(a)g(c)h(d) = \sum_{acd=n} f(a)g(c)h(d)$$

which proves the claim. ■

We recall from Example 5.1 that $I(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$

Theorem 5.1.5 $(G,*)$ is an abelian group with identity I.

Proof. It is clear that for any $f \in A$ we have $f*I(n) = I*f(n) = \sum_{d|n} I(d)f(n/d) = f(n)$. If $f \in G$ we need to show that there exists another arithmetical function f^{-1} satisfying $f^{-1}*f(n) = \sum_{d|n} f^{-1}(d)f(n/d) = I(n)$. But if $f(1) \neq 0$ we can construct such a function recursively by $f^{-1}(1) = 1/f(1)$ and

$$f^{-1}(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d\neq n}} f^{-1}(d)f(n/d).$$

which proves that $(G,*)$ is an abelian group. ■

Theorem 5.1.6 $(M,*)$ is a subgroup of $(G,*)$

Proof. It is clear that I is multiplicative.

We need to show that if F,G are multiplicative then so is $F*G$. If m,n are coprime natural numbers consider the following map between sets of positive divisors

$$\begin{aligned} \{d \mid m\} \times \{e \mid n\} &\rightarrow \{f \mid mn\} \\ (d,e) \quad &\mapsto \quad de. \end{aligned}$$

We claim that this is a bijection: It is surjective since if $f \mid mn$ we may define $d = \gcd(f,m)$ and $e = \gcd(f,n)$. It is clear from Proposition 1.2.6 (iii) that $de \mid f$. If $f \neq de$ we let $f = d \cdot e \cdot g$ with $g \neq 1$. Let $p \mid g$ be a prime. Then since $f \mid mn$ Euclid's Lemma 1.4.1 implies that $p \mid m$ or $p \mid n$. If $p \mid n$ we see that $pe \mid f$. We have also $pe \mid mn$. Since pe is coprime with m (A common prime factor would be a common prime factor of both m and n but they have no common factor other than 1) Theorem 1.2.6 (iv) implies that $pe \mid n$. Hence pe is a common divisor of f and n, which contradicts e being their greatest common divisor. If instead $p \mid m$ we are lead to the same contradiction, and we may conclude that $g = 1$ which means that the map is surjective.

To see that it is injective assume that $de = d'e'$ with $d,d' \mid m$ and $e,e' \mid n$. Then d,e' are coprime, and e, d' are coprime. By Proposition 1.2.6 (iv) we may conclude that $d \mid d'$, $d' \mid d$, $e \mid e'$, and $e' \mid e$ which implies that $(d,e) = (d',e')$.

Using this we see that

$$\begin{aligned}
F*G(mn) &= \sum_{f|nm} F(f)\,G\left(\frac{mn}{f}\right)\\
&= \sum_{d|m}\sum_{e|n} F(de)G\left(\frac{mn}{de}\right)\\
&= \sum_{d|m}\sum_{e|n} F(d)F(e)G\left(\frac{m}{d}\right)G\left(\frac{n}{e}\right)\\
&= \sum_{d|m} F(d)G\left(\frac{m}{d}\right)\sum_{e|n} F(e)G\left(\frac{n}{e}\right) = F*G(m)\cdot F*G(n)
\end{aligned}$$

To show that if F is multiplicative then so is F^{-1} we assume that it is not and let n be the smallest natural number such that there exists a factorization $n = ml$ with m,l coprime natural numbers such that $F^{-1}(ml) \neq F^{-1}(m)F^{-1}(l)$. Notice that multiplicative functions satisfies $F(1) = 1$ so $1 = I(1) = F*F^{-1}(1) = F(1)F^{-1}(1) = F^{-1}(1)$. This implies that $n \neq 1$.

Note that for all coprime natural numbers a,b with $ab < n$ we have $F^{-1}(ab) = F^{-1}(a)F^{-1}(b)$. Hence using the above isomorphism we find that

$$\begin{aligned}
I(ml) = F^{-1}*F(ml) &= \sum_{f|ml} F^{-1}(f)\,F\left(\frac{ml}{f}\right)\\
&= \sum_{d|m}\sum_{e|l} F^{-1}(de)F\left(\frac{ml}{de}\right)\\
&= \sum_{\substack{d|m\\ e|l\\ de\neq ml}} F^{-1}(de)F\left(\frac{ml}{de}\right) + F^{-1}(ml)F(1)\\
&= \sum_{\substack{d|m\\ e|l\\ de\neq ml}} F^{-1}(d)F^{-1}(e)F\left(\frac{m}{d}\right)F\left(\frac{l}{e}\right) + F^{-1}(ml)F(1)\\
&= \sum_{\substack{d|m\\ e|l}} F^{-1}(d)F^{-1}(e)F\left(\frac{m}{d}\right)F\left(\frac{l}{e}\right) + F^{-1}(ml) - F^{-1}(m)F^{-1}(l)\\
&= \sum_{d|m} F^{-1}(d)F\left(\frac{m}{d}\right)\sum_{e|l} F^{-1}(e)F\left(\frac{l}{e}\right) + F^{-1}(ml) - F^{-1}(m)F^{-1}(l)\\
&= I(m)I(l) + F^{-1}(ml) - F^{-1}(m)F^{-1}(l) \neq I(m)I(l)
\end{aligned}$$

which is a contradiction. Hence F^{-1} is indeed multiplicative.

■

This theorem allows us to prove the following “two out of three” result:

Corollary 5.1.7 Let f,g,h be arithmetical functions satisfying $f*g = h$. If two of f,g,h are multiplicative then so is the third.

Proof. This follows in a straightforward manner from Theorem 5.1.6: If f,g are multiplicative then so is $f*g = h$. If f,h are multiplicative then so is $f^{-1}*h = g$, and if g,h are multiplicative then so is $g^{-1}*h = f$. ■

5.1.3 The Möbius function

We now define a very important function called the Möbius function. Clearly $u \in G$. By Theorem 5.1.5 this has an inverse with respect to $*$. By general group theory such an inverse is unique in G (but clearly also in A since $f * g(1) = f(1)g(1)$), which makes the following well-defined:

Definition 5.1.5 The Möbius function is the unique arithmetical function satisfying $\mu * u = I$.

It follows from Theorem 5.1.6 and the fact that u is multiplicative that μ is multiplicative.

Theorem 5.1.8

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n \text{ is the product of } k \text{ different primes} \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let μ' be the right-hand side. We have $\mu' * u(1) = \sum_{ab=1} \mu'(a)u(b) = \mu'(1)u(1) = 1 \cdot 1 = I(1)$. For $n = p_1^{l_1} \cdots p_k^{l_k} > 1$ we observe that

$$\mu' * u(n) = \sum_{d|n} \mu'(d) = \sum_{d|p_1 \cdots p_k} \mu'(d) \tag{5.2}$$

$$= \sum_{j=0}^{k} \binom{k}{j} (-1)^j = (1-1)^k = 0 = I(n) \tag{5.3}$$

$$\tag{5.4}$$

It follows that $\mu' * u = I$ so by uniqueness we have $\mu = \mu'$. ■

Theorem 5.1.9 — Möbius inversion. Let $f, g \in A$ then $f = u * g$ if and only if $g = f * \mu$

Proof. If $f = u * g$ then $f * \mu = u * g * \mu = u * \mu * g = I * g = g$. If $g = f * \mu$ then $u * g = u * f * \mu = u * \mu * f = I * f = f$ ■

5.2 Dirichlet series

In the last section we discussed arithmetical functions. Very often it is useful to try to make a generating function from such a series. A Dirichlet series is one particularly useful such generating series.

Definition 5.2.1 Let f be an arithmetical function. Then the corresponding Dirichlet series is defined, for $s \in \mathbb{C}$ by

$$D_f(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

We note that there is no requirement in this definition about convergence of the series, but if the series is divergent everywhere the series is not so useful. Following Riemann it is customary to write $s = \sigma + it \in \mathbb{C}$ with $\sigma, t \in \mathbb{R}$.

We note that if $\sigma \geq a$ then since $|n^s| = n^\sigma \geq n^a$ we have

$$\frac{|f(n)|}{|n^s|} \leq \frac{|f(n)|}{n^a}. \tag{5.5}$$

It then follows from the comparison test that if $D_f(s)$ is absolutely convergent at $s = a + ib$ then $D_f(s)$ is absolutely convergent in the half-plane $\sigma \geq a$.

Theorem 5.2.1 Assume that $\sum_{n=1}^{\infty} |f(n)n^{-s}|$ is not always convergent nor always divergent. Then there exist σ_a such that $D_f(s)$ converges absolutely if $\sigma > \sigma_a$, and does not converge absolutely if $\sigma < \sigma_a$. This number is called the *abscissa of absolute convergence*.

Proof. Let $\sigma_a = \inf\{a \in \mathbb{R} | \exists b \in \mathbb{R} : D_f(a+ib) \text{ converges absolutely}\}$. By assumption we are taking infimum over an non-empty set. If $s = \sigma + it$ with $\sigma > \sigma_a$ we have that $D_f(s)$ converges absolutely by the observation following (5.5). If $s = \sigma + it$ with $\sigma < \sigma_a$ we have that $D_f(s)$ is not absolutely convergent: If it were then σ would be in the set we are taking infimum over which it cannot be, since σ is strictly less than the infimum. ■

If D_f is *always* absolutely convergent then we define $\sigma_a = -\infty$ and if D_f is never absolutely convergent we define $\sigma_a = \infty$.

■ **Example 5.4** The Riemann zeta function is defined as the Dirichlet series related to u, i.e. $\zeta(s) := D_u(s)$. We note that $\sum_{n=1}^{\infty} \frac{1}{n}$ is divergent so we must have $\sigma_a \geq 1$. At the same time we have for $n \geq 1$ and $\sigma > 0$ that $\frac{1}{n^\sigma} \leq \int_{n-1}^{n} t^{-\sigma} dt$ and it follows that for $\sigma > 1$ we have

$$\sum_{n=1}^{\infty} \frac{1}{|n^s|} \leq 1 + \int_1^{\infty} t^{-\sigma} dt = 1 - \frac{1}{1-\sigma} \tag{5.6}$$

which implies that $\sigma_a \leq 1$. Hence $\sigma_a = 1$. ■

Lemma 5.2.2 Assume $|f(n)| \leq Cn^c$. Then D_f is absolutely convergent for $\sigma > 1 + c$, i.e. the abscissa of absolute convergence is less than or equal to $1 + c$.

Proof. This follows directly from Example 5.4 and the comparison test. ■

We can now show that there is a precise relation between multiplication of Dirichlet series and Dirichlet convolution of the corresponding arithmetical functions.

Theorem 5.2.3 Assume f_1, f_2, f_3 are arithmetical functions satisfying $|f_i(n)| \leq Cn^c$ then we have $D_{f_1}(s)D_{f_2}(s) = D_{f_3}(s)$ for σ sufficiently large if and only if $f_1 * f_2 = f_3$.

Proof. Assume $f_1 * f_2 = f_3$. Since for σ sufficiently large we have that D_{f_1}, D_{f_2} are absolutely convergent we have, using Cauchy products, that

$$\begin{aligned} D_{f_1}(s)D_{f_2}(s) &= \sum_{n=1}^{\infty} \frac{f_1(n)}{n^s} \sum_{m=1}^{\infty} \frac{f_2(m)}{m^s} = \sum_{n,m=1}^{\infty} \frac{f_1(n)f_2(m)}{(nm)^s} \\ &= \sum_{k=1}^{\infty} \frac{\sum_{nm=k} f_1(n)f_2(m)}{k^s} = \sum_{k=1}^{\infty} \frac{f_1 * f_2(k)}{k^s} = D_{f_3}(s) \end{aligned}$$

for σ sufficiently large.

Assume on the other hand that $D_{f_1}(s)D_{f_2}(s) = D_{f_3}(s)$ for σ large enough. Then by the above computations we have that

$$0 = \sum_{k=1}^{\infty} \frac{f_1 * f_2(k) - f_3(k)}{k^s} \tag{5.7}$$

But an absolutely convergent Dirichlet series is uniquely determined by its coefficients (See Exercise 5.5). ■

■ **Example 5.5** Note that $|\mu(n)| \leq 1$ so D_μ is absolutely convergent for $\sigma > 1$ by Lemma 5.2.2. Note also that $D_I(s) = 1$. It then follows from Theorem 5.2.3 and the definition of the Möbius function that $D_\mu(s)D_u(s) = 1$. Since $D_u(s) = \zeta(s)$ we see that $\zeta(s)$ has no zeroes for $\sigma > 1$. We note also that for $\sigma > 1$ we have

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

In fact $D_\mu(s)$ has abcissa of absolute convergence equal to 1 as follows from the above and Exercise 5.6. ■

Euler products

Let p_n be the n'th prime.

Theorem 5.2.4 Let g be a multiplicative arithmetic function and assume that $\sum_{n=1}^{\infty} g(n)$ converges absolutely. Then this sum can be expressed as an infinite product

$$\sum_{n=1}^{\infty} g(n) = \prod_{p \text{ prime}} \sum_{k=0}^{\infty} g(p^k) := \lim_{l\to\infty} \prod_{n=1}^{l} \sum_{k=0}^{\infty} g(p_n^k).$$

If furthermore g is completely multiplicative we have

$$\sum_{n=1}^{\infty} g(n) = \prod_{p \text{ prime}} \frac{1}{1-g(p)}.$$

Proof. Consider $P_l = \prod_{n=1}^{l} \sum_{k=0}^{\infty} g(p_n^k)$. Since $\sum_{k=0}^{\infty} g(p^k)$ is a subsum of an absolutely convergent sum it is itself absolutely convergent. Hence we find, using successive Cauchy multiplication, that

$$\begin{aligned} P_l &= \sum_{h=0}^{\infty} \sum_{k_1+k_2+\cdots k_l = h} g(p_1^{k_1})\cdots g(p_l^{k_l}) \\ &= \sum_{h=0}^{\infty} \sum_{k_1+k_2+\cdots k_l = h} g(p_1^{k_1}\cdots p_l^{k_l}) \end{aligned}$$

which is also absolutely convergent. By absolute convergence we may rearrange as we please, and we find, using the fundamental theorem of arithmetic, that for every n whose prime factors are all less than or equal to p_l, the term $g(n)$ appears and appears exactly once. Let $A_l = \{n | n = p_1^{k_1}\cdots p_l^{k_l}, k_i \geq 0\}$. Then we have shown that $P_l = \sum_{n\in A_l} g(n)$. It follows that

$$\left|\sum_{n=1}^{\infty} g(n) - P_l\right| = \left|\sum_{n\notin A_l} g(n)\right| \leq \sum_{n\notin A_l} |g(n)| \leq \sum_{n>p_l} |g(n)|$$

which can be made arbitrarily small by making l large since $\sum_{n=1}^{\infty} g(n)$ is absolutely convergent. This proves the first claim.

The second claim follows after we observe that $g(p^k) = g(p)^k$. For this implies, since the terms in a convergent series goes to zero, that $|g(p)| < 1$, and hence the sum $\sum_{k=0}^{\infty} g(p^k)$ is really a convergent geometric series which equals $(1-g(p))^{-1}$. This finishes the proof. ■

Definition 5.2.2 We say that $D_f(s)$ admits an Euler product if $D_f(s) = \prod_{p \text{ prime}} D_{f,p}(s)$ where

$$D_{f,p}(s) = \sum_{k=0}^{\infty} \frac{f(p^k)}{p^{ks}}.$$

We notice that $n \mapsto f(n)$ is multiplicative (respectively completely multiplicative) if and only if $n \mapsto f(n)n^{-s}$ is multiplicative (respectively completely multiplicative). Combining this observation with Theorem 5.2.4 we arrive at the following result:

Corollary 5.2.5 Assume f is a multiplicative arithmetic function and that $D_f(s)$ is absolutely convergent in some halfplane. Then $D_f(s)$ admits an Euler product. If f is completely multiplicative then

$$D_{f,p}(s) = \frac{1}{(1-f(p)p^{-s})}.$$

■ **Example 5.6** The arithmetical function u is completely multiplicative so

$$\zeta(s) = D_u(s) = \prod_p (1-p^{-s})^{-1}$$

which is the Euler product of the Riemann zeta function. ■

■ **Example 5.7** The Möbius function is multiplicative so

$$\frac{1}{\zeta(s)} = \prod_p \sum_{k=0}^{\infty} \mu(p^k)p^{-ks} = \prod_p (1-p^{-s})$$

where we have used Theorem 5.1.8. ■

■ **Example 5.8** Fix a prime q and consider $\chi(n) = \left(\frac{n}{q}\right)$ which is completely multiplicative by Corollary 4.1.2. The corresponding Dirichlet series is usually denoted $L(s,\chi)$ and we find

$$L(s,\chi) = \prod_p (1-\chi(p)p^{-s})^{-1}$$

■

The Riemann zeta function

The Riemann zeta function $\zeta(s)$ is one of the most fundamental functions in all of number theory. We have only described its most basic properties. We have shown, in Example 5.4 that if $\sigma > 1$ then it can be defined as the absolutely convergent Dirichlet series $D_u(s)$ which in this region is free of zeroes. Also we have seen that in this same region it is given by a convergent infinite Euler product. Consider the function

$$\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s). \tag{5.8}$$

Here $\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt$ (when $\sigma > 0$) is the Euler Gamma function which admits a continuation as a meromorphic function to $s \in \mathbb{C}$. Riemann [Rie59] proved the following theorem:

Theorem 5.2.6 The Riemann zeta function $\zeta(s)$ admits a meromorphic continuation to $s \in \mathbb{C}$ with a simple pole in $s = 1$. The function $\xi(s)$ defined by (5.8) satisfies the functional equation

$$\xi(s) = \xi(1-s).$$

Moreover all the zeroes of $\xi(s)$ are in the critical strip $0 \le \sigma \le 1$.

For a proof of this and a wealth of other information about the Riemann zeta function consult [Ivi85; KV92; Tit86]

Conjecture 5.2.7 — The Riemann hypothesis. All zeros of $\xi(s)$ lie on the critical line $\Re(s) = 1/2$.

We have already seen one equivalent formulation of this namely Conjecture 1.4.5. Here is another equivalent formulation:

Conjecture 5.2.8 For every $\varepsilon > 0$ $\dfrac{\sum_{n\le x}\mu(n)}{x^{1/2+\varepsilon}}$ is bounded.

R The Riemann hypothesis has not been proved despite many attempts. Hardy [Har14] proved that there are infinitely many zeros on the critical line. Selberg [Sel42] proved that a positive (but unspecified) proportion of the zeroes lie on the critical line. This has been improved several times with a 2012 result of Feng [Fen12] as the current record: Feng proved that at least 41.28% of all zeros of ζ lies on the critical line. See [Bor+08] for a treasure of information about the Riemann hypothesis.

5.3 Exercises for chapter 5

Exercise 5.1 Show that all the arithmetical functions of Example 5.1 are multiplicative.

Exercise 5.2 Show that u, N, I, and $\left(\frac{n}{p}\right)$ are completely multiplicative.

Exercise 5.3 Is $2^{10}\cdot(2^{11}-1)$ perfect? Hint: 23.

Exercise 5.4 Show that $\sum_{d|n}|\mu(d)| = \prod_{p|n}2$.

Exercise 5.5 Let D_f be a Dirichlet series with finite abcissa of absolute convergence σ_a. In this exercise we will show that D_f determines f uniquely.

Assume that there exist a complex sequence $s_k = \sigma_k + it_k$ with $\sigma_k \to \infty$ when $k \to \infty$, satisfying that $D_f(s_k) = 0$ for all k sufficiently large. We will show that this implies that $f(n) = 0$ for all n.

(i) Assume that f is not identically zero, and choose $N \in \mathbb{N}$ minimal such that $f(N) \neq 0$. Show that

$$f(N) = -N^{s_k}\sum_{n=N+1}^{\infty} f(n)n^{-s_k}.$$

(ii) Let $c > \sigma_a$. Show that for k sufficiently large we have

$$|f(N)| \le N^{\sigma_k}(N+1)^{-(\sigma_k-c)}\sum_{n=N+1}^{\infty}|f(n)|n^{-c}$$

(iii) Conclude, by letting $k \to \infty$, that $f(N) = 0$, which gives a contradiction and therefore $f(n) = 0$ for all $n \in \mathbb{N}$.

Exercise 5.6 In this exercise we show that the reciprocal of the primes diverges. Let p_n denote the n'th prime. We start by assuming that $\sum_{n=1}^{\infty} p_n^{-1}$ is convergent with sum l.

(i) Show that there exist $N \in \mathbb{N}$ such that $\left|\sum_{n>N} p_n^{-1}\right| = \left|l - \sum_{n=1}^{N} p_n^{-1}\right| \le 1/2$.

(ii) Show that $\sum_{k=1}^{\infty}\left(\sum_{n>N} p_n^{-1}\right)^k$ is absolutely convergent.

(iii) Let $W = p_1\cdots p_N$. For $r \in \mathbb{N}$ consider $Wr+1$. Show that the prime factorization of $Wr+1$ contains only primes $p > p_N$.

(iv) Show, using Cauchy multiplication, that $\displaystyle\sum_{\substack{n=q_1\cdots q_k\\ q_i \text{ prime}\\ q_i>p_N}}\frac{1}{n} = \left(\sum_{n>N} p_n^{-1}\right)^k$ where the left-hand side denotes the reciprocals of all natural numbers which can be written of precisely k primes all bigger that p_N.

(v) Show that $\sum_{r=1}^{\infty}\frac{1}{Wr+1} \le \sum_{k=1}^{\infty}\left(\sum_{n>N} p_n^{-1}\right)^k$

(vi) Derive a contradiction and conclude that $\sum_{n=1}^{\infty} p_n^{-1}$ cannot be convergent.

Exercise 5.7 Let $g(n)$ be the sum of primitive nth roots of 1, i.e.

$$g(n) = \sum_{\substack{\zeta^n=1 \\ \zeta^m \neq 1 \\ \text{for } 0<m<n}} \zeta.$$

Show that $\mu(n) = g(n)$; i.e. $\mu(n)$ is the sum of primitive nth roots of 1.

Exercise 5.8 Let $k \in \mathbb{N}$. A number n is called *k-perfect* if $\sigma(n) = kn$. It is not known if there are infinitely many k-perfect numbers for any k. The following are the known 3-perfect numbers: 120, 672, 523776, 459818240, 1476304896, 51001180160. Show that they are indeed 3-perfect.

Exercise 5.9 Prove Gottschalck's theorem: Let n be a k-perfect number such that 2 divides n precisely m times. Then $2^m(2^{m+1}-1)$ divides kn.

6. Sums of squares

In this chapter we shall investigate questions concerning sums of squares, but before we dive into this we make a short digression into more general sums of powers. We start by the trivial observation that the number of l'th powers less than or equal to x is at essentially $x^{1/l}$ namely exactly the integers m^l with $m \leq x^{1/l}$. Hence the set of l'th powers is very *sparse* in the set of integers. By comparison the prime number theorem (1.4) implies that there are many more primes, than l'th powers.

6.0.1 Waring's problem

Let $l \in \mathbb{N}$ be a natural number. Waring's problem is the following: Does there exist a number s such that every natural number n can be written as the sum of at most s l'th powers, or said differently such that the Diophantine equation

$$n = x_1^l + \cdots + x_s^l \tag{6.1}$$

has at least one solution in non-negative integers.

The answer is yes. Hilbert [Hil09] showed that for every l such an s exist. Obviously we may ask – and this question also goes back to Waring – what the smallest such number is? We call this number $g(l)$. Trivially $g(1) = 1$. One may verify by simple computations (See exercise 6.1) that $g(2) \geq 4$, $g(3) \geq 9$, $g(4) \geq 19$. Waring conjectured that these inequalities attains the actual values. In fact it was later conjectured that this holds much more generally, namely that $g(l) = 2^l + [(3/2)l] - 2$ for every $l \in \mathbb{N}$. Here square bracket denotes the integer part.

6.1 Sums of squares

We shall now consider in more detail the case $l = 2$, i.e. we shall consider the case of sums of squares. Lagrange proved that $g(2) = 4$.

Theorem 6.1.1 — Lagrange. Every natural number can be written as a sum of at most 4 squares.

We will prove this theorem in Section 6.1.5 with a much more recent proof using geometric number theory.

Let $k \in \mathbb{N}$. Let

$$S_k = \{n \in \mathbb{Z} | n = x_1^2 + \cdots + x_k^2, x_i \in \mathbb{Z}\}.$$

Hence S_k denotes the subset of $\mathbb{N} \cup \{0\}$ of integers that can be written as a sum of at most k squares. We clearly have $S_1 \subseteq S_2 \subseteq S_3 \subseteq \cdots$. Proving Lagrange's theorem 6.1.1 is equivalent to proving that $S_4 = \mathbb{N} \cup \{0\}$. We will also see that $S_i \neq \mathbb{N} \cup \{0\}$ for $i = 1,2,3$. Hence 3 squares does not suffice. Before giving a proof of Lagrange's theorem 6.1.1 we describe explicitly S_1, S_2, S_3.

6.1.1 Squares

The set S_1 is simply the set of squares

$$S_1 = \{0,1,4,9,16,25,36,49,\ldots\}.$$

6.1.2 Sums of two squares

The set S_2 is the set of numbers that can be written as the sum of two squares i.e. the sum of two numbers from the set S_1. Clearly 3 cannot be written as the sum of two numbers from S_1 as $0,1$ are the only two numbers from S_1 which are less than 3. Similar simple considerations show that 6,7, and 11 do not lie in S_2. We have

$$S_2 = \{0,1,2,4,5,8,9,10,13,\ldots\}$$

Lemma 6.1.2 The set S_2 is closed under multiplication.

Proof. This is most easily proved using complex numbers. If $s_1, s_2 \in S_2$ then $s_j = a_j^2 + b_j^2 = |z_j|^2$ where $z_j = a_j + ib_j \in \{a + ib | a, b \in \mathbb{Z}\} = \mathbb{Z}[i]$. We notice that clearly $z_1 \cdot z_2 \in \mathbb{Z}[i]$. But for every $z = a + ib \in \mathbb{Z}[i]$ we have $|z|^2 = a^2 + b^2 \in S_2$. In particular $s_1 s_2 = |z_1 z_2|^2 \in S_2$. ■

Notice also that the proof gives a way of finding the representation of $s_1 s_2$ as the sum of two squares since

$$\begin{aligned}(a_1^2+b_1^2)(a_2^2+b_2^2) = |z_1 z_2|^2 = |z_1 \overline{z_2}|^2 &= |(a_1 a_2 + b_1 b_1) + i(-a_1 b_2 + b_1 a_2)|^2 \qquad (6.2)\\ &= (a_1 a_2 + b_1 b_2)^2 + (-a_1 b_2 + b_1 a_2)^2 \qquad (6.3)\end{aligned}$$

■ **Example 6.1** We have $8 = 2^2 + 2^2$ and $10 = 3^2 + 1^2$. But then $80 = 8 \cdot 10 = |2 + i2|^2 |3 + i|^2 = |4 + 8i|^2 = 4^2 + 8^2$. ■

The fact that S_2 is closed under multiplication makes it natural to consider which primes can be written as a sum of two squares. Clearly 2=1+1 is a sum of two squares.

Theorem 6.1.3 — Euler. Every prime $p = 1 \pmod 4$ is a sum of 2 squares.

Proof. By Theorem 4.2.1 (ii) we have $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = 1$ so there exist $u, r \in \mathbb{Z}$ such that $-1 = u^2 - rp$. By division modulo p we may assume $0 < u \leq p - 1$ which forces

$$0 < r = \frac{u^2+1}{p} \leq \frac{p^2+1-2p+1}{p} < p.$$

We hence have $rp = 1 + u^2$ with $0 < r < p$.

Consider

$$m = \min\{n \in \mathbb{N} | np \in S_2\}.$$

By the above considerations the sum of which we are taking the minimal element is non-empty and the minimum is strictly less than p. We claim that $m = 1$ from which it follows that $p \in S_2$.

To see that $m = 1$ we write $mp = a_1^2 + b_1^2$. We can choose representatives a_2 for a_1 mod m and b_2 for b_1 mod m satisfying $|a_2|, |b_2| \leq m/2$. Then

$$a_2^2 + b_2^2 = a_1^2 + b_1^2 = mp = 0 \pmod{m}$$

which implies that $a_2^2 + b_2^2 = sm$ with $0 \leq s \leq m/2 < m$.

If $s = 0$ then $a_2 = b_2 = 0$ so $a_1 = b_1 = 0 \pmod{m}$. Hence $m^2 | a_1^2 + b_1^2 = pm$ which implies that $m|p$ which implies $m \in \{1, p\}$. But $m < p$ so $m = 1$ and we are done.

We will show that $s > 0$ leads to a contradiction: We use the expression (6.2) to see that

$$(a_1a_2 + b_1b_2)^2 + (-a_1b_2 + b_1a_2)^2 = (a_1^2 + b_1^2)(a_2^2 + b_2^2) = mpsm = m^2sp$$

But

$$a_1a_2 + b_1b_2 = a_1^2 + b_1^2 = mp = 0 \pmod{m}, \text{ and } -a_1b_2 + b_1a_2 = -a_1b_1 + b_1a_1 = 0 \pmod{m}$$

so $a_1a_2 + b_1b_2$, $-a_1b_2 + b_1a_2$ are divisible by m and we find that

$$\left(\frac{a_1a_2 + b_1b_2}{m}\right)^2 + \left(\frac{-a_1b_2 + b_1a_2}{m}\right)^2 = sp.$$

But since $s < m$ this contradicts m being the smallest integer such that mp can be written as a sum of 2 squares. This finishes the proof. ■

R There are many other proofs of this theorem. Zagier found a delightful one-sentence proof, see [Zag90].

We can now describe the set S_2 completely:

Theorem 6.1.4 A natural number n is a sum of 2 squares if and only if every $p = 3 \pmod{4}$ has an even (possibly zero) exponent in the prime factorization of n.

Proof. Assume that every $p = 3 \pmod{4}$ has an even (possibly zero) exponent in the prime factorization of n. Then $n = 2^e p_1^{e_1} \cdots p_k^{e_k} m^2$ where $p_i = 1 \pmod{4}$. Since $2 = 1^2 + 1^2$, $m^2 = m^2 + 0^2$, and $p_i = a_i^2 + b_i^2$ by Theorem 6.1.3, we find – since S_2 is closed under multiplication – that n is the sum of two squares.

Assume that $n = x^2 + y^2$. If $\gcd(x,y) = d > 1$ then $d^2 \mid n$ and we consider $n/d^2 = (x/d)^2 + (y/d)^2$. We notice that every prime factor of n/d^2 comes with the same parity as in n. In particular any prime which divides n an odd number of times will still be a divisor of n/d^2. Hence we can assume, without loss of generality that $\gcd(x,y) = 1$.

Assume that $p \mid n$. Then $x^2 + y^2 = 0 \pmod{p}$, i.e. $x^2 = -y^2 \pmod{p}$. We notice that $\gcd(y,p) = 1$ for if $p \mid y$ then also $p \mid x$, but we have assumed that $\gcd(x,y) = 1$. Hence using Bezout we may find $z \in \mathbb{Z}$ such that $yz = 1 \pmod{p}$, and it follows that $(zx)^2 = z^2(-y^2) = -1 \pmod{p}$. But hence -1 is a quadratic residue modulo p this implies, by Theorem 4.2.1 (ii), that $p = 1 \pmod{4}$. Hence no prime $p = 3 \pmod{4}$ can occur an odd number of times in the prime factorization of n, which finishes the proof. ■

We now know exactly which natural numbers are in S_2. But we can go even further and count the number of ways a number can be written as a number of 2 squares, i.e. we want to understand

$$r_2(n) := \#\{(x,y) \in \mathbb{Z}^2 | x^2 + y^2 = n\} \tag{6.4}$$

We see that $r_2(1) = \#\{(\pm 1, 0), (0, \pm 1)\} = 4$, $r_2(2) = \#\{(\pm 1, 1), (\pm 1, -1)\} = 4$. From Theorem 6.1.4 we see that $r_2(n) = 0$ if any $p = 3 \pmod 4$ appears an odd number of times in the prime factorization of n.

To find a more explicit expression for $r_2(n)$ it is convenient to look at the Gaussian integers.

6.1.3 Gaussian integers

Consider the set $\mathbb{Z}[i] = \{x + iy | x, y \in \mathbb{Z}\}$ which is called the ring of Gaussian integers. It is straightforward to verify that this is indeed a ring. We have already seen (Example 4.3) that $\mathbb{Z}[i]$ is a subset of the set of algebraic integers $\overline{\mathbb{Z}}$, and since it is a subring of $\mathbb{C}$ it is an integral domain (i.e. a non-zero commutative ring in which the product of non-zero elements is non-zero).

Euclidean rings

Definition 6.1.1 An integral domain R is called a Euclidean ring if there exist a function

$$d : R \backslash \{0\} \to \mathbb{N} \cup \{0\}$$

satisfying

(i) $d(ab) \geq d(b)$ for $a, b \neq 0$.

(ii) for all $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that

$$a = bq + r, \text{ where } r = 0 \text{ or } d(r) < d(b).$$

The function d is called a Euclidean function on R. Note that the notion is clearly modelled on the classical case of Theorem 1.2.1, but there is also subtle differences. For instance the remainder need not be unique. Also the inequality (i) is in a certain sense superfluous. If an integral domain admits a d-function satisfying only (ii) then it also admits another d-function satisfying both (i) and (ii).

Proposition 6.1.5 Let R be a Euclidean ring with Euclidean function d. Then for a, b non-zero elements $d(ab) = d(b)$ if and only if $a \in R^\times$.

Proof. If $a \in R^\times$ there exist $c \in R$ such that $ac = 1$. But by (i) we have $d(b) = d(abc) \geq d(ab)$ and $d(ab) \geq d(b)$, so $d(ab) = d(b)$.

If $d(ab) = d(b)$ with $a, b \neq 0$ we claim that a is a unit. Assume not: We can divide b by ab and find $b = qab + r$ with $r = 0$ or $d(r) < d(ab)$ i.e.

$$b(1 - qa) = r, \text{ with } r = 0 \text{ or } d(r) < d(ab) = d(b).$$

Since a is not a unit $(1 - qa)$ is non-zero so r cannot be zero. Hence we have $d(b(1 - qa)) < d(b)$. But at the same time (i) gives $d(b(1 - qa)) \geq d(b)$ which is a contradiction. ■

Corollary 6.1.6 Let R be a Euclidean domain with Euclidean function d. Then $d(a) = d(1)$ if and only if a is a unit, i.e $a \in R^\times$.

Proof. If u is a unit then so is its inverse u^{-1}. Using Proposition 6.1.5 we find $d(1) = d(u^{-1}u) = d(u)$. If $d(u) = d(1)$ then by (ii) there exist q, r such that $1 = qu + r$. We claim that $r = 0$ which shows that u is a unit. For if not then $d(r) < d(u) = d(1)$. But at the same time $d(r) = d(r \cdot 1) \geq d(1)$ by (i) which is a contradiction. ■

Proposition 6.1.7 The Gaussian integers $\mathbb{Z}[i]$ is a Euclidean ring with Euclidean function $d(z) = z\bar{z}$.

Proof. We have already discussed why $\mathbb{Z}[i]$ is an integral domain. We verify easily that $d(ab) = |ab|^2 = |a|^2\,|b|^2 \geq d(b)$ i.e. (i) is satisfied.

Let $a, b \in \mathbb{Z}[i]$ with $b \neq 0$ and consider the complex number $z = a/b = x + iy$ with $x, y \in \mathbb{R}$. Choose $n_1, n_2 \in \mathbb{Z}$ such that $|n_1 - x| \leq 1/2$ and $|n_2 - y| \leq 1/2$. Let $q = n_1 + in_2$. If we let $r = a - qb$ then either $r = 0$ or $d(r) = |a - qb|^2 = |b|^2\,|a/b - q|^2 = |b|^2\,|x + iy - (n_1 + in_2)|^2 < |b|^2 = d(b)$ which verifies (ii). ■

■ **Example 6.2** The following can also be verified to be Euclidean rings

- Any field F with Euclidean function $d(f) = 1$.
- The ring $\mathbb{Z}$ with Euclidean function $d(n) = |n|$.
- Let $\zeta_3 = e^{\frac{2\pi i}{3}}$. We note that $\zeta_3^2 + \zeta_3 + 1 = 0$. Then $\mathbb{Z}[\zeta_3] = \{a + b\zeta_3 | a, b \in \mathbb{Z}\}$ (The Eisenstein integers) is a Euclidean ring with Euclidean function $d(a + b\zeta_3) = |a + b\zeta_3|^2 = a^2 + b^2 - ab$.
- The ring of polynomials $F[X]$ over a field F with Euclidean function $d(f) = deg(f)$.

■

Factorization in Euclidean rings

Let $a, b \in R$. We say that a, b are *associates* if $a = ub$ for a unit $u \in R^\times$. We say that *a divides b* and write $a \mid b$ if $b = ac$ for some $c \in R$. A non-zero, non-unit element a is called *irreducible* if its only divisors are units and associates of a. A *greatest common divisor* of a, b not both zero is an element $d \in R$ such that $d \mid a$ and $d \mid b$ and if d' is another element satisfying $d' \mid a$ and $d' \mid b$ then $d' \mid d$.

■ **Example 6.3** By Corollary 6.1.6 we see that the units in $\mathbb{Z}[i]$ are precisely those satisfying that $d(a + ib) = d(1) = 1$, i.e. the units are 1, i, -1, and $-i$. Geometrically these 4 elements rotate by 0, $\pi/2$, π, and $3\pi/2$. ■

In a Euclidean ring R greatest common divisors exist (but are generally not unique) and can be found in the same way as in the Euclidean algorithm. Also the “obvious” analogue of Bezout’s identity is true. (See [DF04, Theorem 4 p. 275]) and using these tools one can prove that in a Euclidean ring we have unique factorization (For a proof see [DF04, Theorem 14 p. 287], or go through the relevant parts of Chapter 1 making the appropriate changes.)

Theorem 6.1.8 Let R be a Euclidean domain. Then every non-zero element $r \in R$ which is not a unit can be written as a finite product of irreducibles of R. This product is unique up to permutation and multiplication of units.

We want to use this theorem to describe $r_2(n)$. To this end we need to find all irreducibles of $\mathbb{Z}[i]$.

Proposition 6.1.9 The irreducible elements of $\mathbb{Z}[i]$ are precisely the elements associated to one of the following:

(i) $\pi = 1 + i$.
(ii) $\pi = x + iy$ with $x^2 + y^2 = \pi\bar{\pi} = p = 1 \pmod 4, \quad x > |y| > 0$.
(iii) $q = 3 \pmod 4$.

Here p, q are primes in $\mathbb{N}$.

Proof. The numbers in (i) and (ii) are irreducible since $d(\pi)$ is prime: If $\pi = ab$ is a factorization then $d(\pi) = d(a)d(b)$ which is prime, which implies that $d(a)$ or $d(b)$ is 1. But then either a or b is a unit which means that π is irreducible.

An element q as in (iii) is irreducible since a non-trivial factorization $q = ab$ would imply $q^2 = d(q) = d(a)d(b)$. But since $d(a), d(b) \neq 1$ this is only possible if $q = d(b) = d(a) = d(x + iy) = x^2 + y^2$. But this contradicts Theorem 6.1.4.

This shows that all the listed elements are irreducible. To see that every irreducible is associated to one on the list we argue as follows: Let ρ be any irreducible element. We notice that if ρ is irreducible then $\overline{\rho}$ is irreducible also, since any non-trivial factorization $\overline{\rho} = ab$ gives a non-trivial factorization $\rho = \overline{a}\overline{b}$.

We have $d(\rho) = \rho\overline{\rho} \in \mathbb{N}$, which we can factor into primes in $\mathbb{N}$. Now we can factor all primes in $\mathbb{N}$ into irreducible in $\mathbb{Z}[i]$ of the listed form (Note that $2 = -i(1+i)(1+i)$). Hence using the uniqueness of factorization we see that ρ is associated to one of the listed irreducible. ■

Using the above properties of $\mathbb{Z}[i]$ we can determine $r_2(n)$ for any $n \in \mathbb{N}$:

Theorem 6.1.10 Let $n \in \mathbb{N}$ with prime factorization $n = 2^e p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_l^{f_l}$ where $p_i = 1 \pmod 4$ and $q_j = 3 \pmod 4$. Then

$$r_2(n) = \begin{cases} 0 & \text{if } f_j \text{ is odd for some } j = 1, \dots, l \\ 4\tau(p_1^{e_1} \cdots p_k^{e_k}) = 4\prod_{i=1}^{k}(e_i+1) & \text{otherwise.} \end{cases}$$

Proof. Write $p_i = \pi_i\overline{\pi_i}$ as in Proposition 6.1.9. Then we have a factorization into irreducible in $\mathbb{Z}[i]$:

$$n = (-i)^e(1+i)^{2e}\prod_{i=1}^{k}\pi_i^{e_i}\overline{\pi_i}^{e_i}\prod_{j=1}^{l}q_j^{f_j}.$$

Note that $n = x^2 + y^2$ if and only if $n = z\overline{z}$ where $z = x + iy$, so

$$r_2(n) = \#\{z \in \mathbb{Z}[i] : z \mid n, z\overline{z} = n\}.$$

To count the factors z of n satisfying $z\overline{z} = n$ we notice that any factor of n must factor in irreducibles as $z = u(1+i)^a\prod_{i=1}^{k}\pi_i^{a_i}\overline{\pi_i}^{b_i}\prod_{j=1}^{l}q_j^{c_j}$ for some $0 \le a \le 2e$, $0 \le a_i, b_i \le e_i$, $0 \le c_j \le f_j$. so we have

$$n = z\overline{z} = (-i)^a(1+i)^{2a}\prod_{i=1}^{k}\pi_i^{a_i+b_i}\overline{\pi_i}^{a_i+b_i}\prod_{j=1}^{l}q_j^{2c_j}$$

But by Theorem 6.1.8 this is only possible if $a = e$, $2c_j = f_j$ and $a_i + b_i = e_i$. It follows that $r_2(n) = 0$ if f_j is odd for some j. If on the other hand f_j is even we see that every factor is of the form

$$z = u(1+i)^e\prod_{i=1}^{k}\pi_i^{a_i}\overline{\pi_i}^{e_i-a_i}\prod_{j=1}^{l}q_j^{f_j/2}$$

and that every such expression is indeed a factor. Since there are 4 possible choices of units this implies that

$$r_2(n) = 4\#\{(a_1, \dots, a_k) | 0 \le a_i \le e_i\} = 4\prod_{i=1}^{k}(1+e_i).$$

■

■ **Example 6.4** Let us find all ways to write 221 as a sum of two squares. Note that $221 = 13 \cdot 17$ and $13, 17 = 1 \pmod 4$. We easily find that $13 = 3^2 + 2^2 = (3+2i)(3-2i)$, and $17 = 4^2 + 1^2 = (4+i)(4-i)$ By Theorem 6.1.10 we find that $r_2(221) = 4(1+1)(1+1) = 16$. Indeed the proof shows that $221 = x^2 + y^2$ if and only if $z = x + iy$ is of the form $z = u(3+2i)^{a_1}(3-2i)^{1-a_1}(4+$

$i)^{a_2}(4-i)^{1-a_2}$ with $0 \le a_i \le 1$. This means that $z = u(3 \pm 2i)(4 \pm i)$ with all possible choices of ±. This corresponds to $z = u(10 \pm 11i)$ or $z = u(14 \pm 5i)$ which gives the 16 representations

$$221 = (\pm 10)^2 + (\pm 11)^2 = (\pm 11)^2 + (\pm 10)^2 = (\pm 14)^2 + (\pm 5)^2 = (\pm 5)^2 + (\pm 14)^2,$$

with all possible choices of ±. ■

■ **Example 6.5** We find all ways to write $4168 = 2^3 521$ as a sum of two squares. Note that $521 = 1 \pmod 4$ so Theorem 6.1.10 gives $r_2(4168) = 4(1+1) = 8$ corresponding to factors of n of the type $z = u(1+i)^3(20 \pm i11) = u(-62+18i)$ or $u(-18+62i)$ corresponding to the 8 representations

$$4168 = (\pm 62)^2 + (\pm 18)^2 = (\pm 18)^2 + (\pm 62)^2$$

with all possible choices of ±. ■

6.1.4 Sums of three squares

It is easy to verify that not all natural numbers can be written as a sum of 3 squares, noticing that numbers which are sums of 3 squares can be written as $n = a + b$ where $a \in S_1$ is a square and $b \in S_2$ is a sum of two squares. We find

$$S_3 = \{0,1,2,3,4,5,6,8,9,10,11,12,13,14,16,\ldots\},$$

where we note that 7 and 15 are missing. We note also that although $3,5 \in S_3$ their product is not, so S_3 is *not* closed under multiplication. The following result holds[1]:

Theorem 6.1.11 $S_3 = \{n \in \mathbb{N} \cup \{0\} | n \neq 4^e(8k+7)\}$.

Note that any square is either 0,1,4 modulo 8 so if n is a sum of 3 square then $n \neq 7 \pmod 8$. If $n = 0 \pmod 4$ then since a square is either 0 or 1 modulo 4 we must have that all three squares are 0 modulo 4. But this implies that if $n = x^2 + y^2 + z^2$ then x,y,z are divisible by 2, so $n/4 = (x/2)^2 + (y/2)^2 + (z/2)^2 \in S_3$. We have shown that if $n \in S_3$ then $n \neq 7 + 8k$ and if $n = 4b \in S_3$ then $b \in S_3$. It follows that $S_3 \subseteq \{n \in \mathbb{N} \cup \{0\} | n \neq 4^e(8k+7)\}$.

Showing the opposite inclusion is much trickier, and we will not give the proof. See e.g. [Ank57] for a relatively simple proof, which in principle can be understood using the techniques of section 6.1.5.

6.1.5 Sums of four squares

We now describe S_4 which according to Lagrange's theorem 6.1.1 equals $\mathbb{N} \cup \{0\}$. It is possible to give an algebraic proof in the same spirit as Theorem 6.1.3 (See e.g. [JJ98, Theorem 10.6]), but here we give a more geometric proof using Minkowski theory. We start by noticing that it is enough to show that every prime is a sum of 4 squares. This follows immediately from the fundamental theorem of arithmetic and the following fact:

Lemma 6.1.12 The set S_4 is closed under multiplication.

Proof. This follows immediately from following identity which is straightforward to verify:

$$\begin{aligned}(a_1^2+b_1^2+c_1^2+d_1^2)(a_2^2+b_2^2+c_2^2+d_2^2) =&(a_1a_2-b_1b_2-c_1c_2-d_1d_2)^2\\ &+(a_1b_2+b_1a_2+c_1d_2-d_1c_2)^2\\ &+(a_1c_2-b_1d_2+c_1a_2+d_1b_2)^2\\ &+(a_1d_2+b_1c_2-c_1b_2+d_1a_2)^2.\end{aligned}$$

[1] There is some disagreement in the literature as to whether Legendre or Gauss gave the first correct proof of this result.

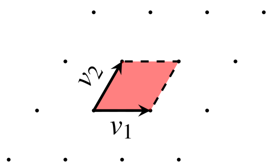


Figure 6.1: Fundamental domain

Analogous to the way that Lemma 6.1.2 can be proved using complex numbers, this lemma may be proved using quaternions. See e.g. [JJ98, Sec 10.5]. ■

Minkowski theory

Definition 6.1.2 A (full) lattice Λ in $\mathbb{R}^n$ is a subset $\Lambda \subseteq \mathbb{R}^n$ satisfying

$$\Lambda = \{\alpha_1 v_1 + \cdots \alpha_n v_n | \alpha_i \in \mathbb{Z}\}$$

where $(v_1, \ldots, v_n)$ is a basis for $\mathbb{R}^n$. The set $(v_1, \ldots, v_n)$ is also called a basis for Λ.

It is straightforward to verify that $(\Lambda, +)$ is a subgroup of $(\mathbb{R}^n, +)$.

■ **Example 6.6** $\mathbb{Z}^n = \{\alpha_1 e_1 + \cdots \alpha_n e_n\}$ where $(e_1, \ldots, e_n)$ is the standard basis of $\mathbb{R}^n$ is called the integer lattice. ■

Elements $v, w \in \mathbb{R}^n$ are called *equivalent* modulo Λ if $v - w \in \Lambda$. It is straightforward to verify that this is indeed an equivalence relation, and we shall write $v \sim_\Lambda w$.

Definition 6.1.3 If $(v_1, \ldots, v_n)$ is a basis for a lattice Λ then

$$F_\Lambda = \{t_1 v_1 + \cdots + t_n v_n | 0 \leq t_i < 1\}$$

is called a *fundamental domain* or a *fundamental mesh* for Λ.

Lemma 6.1.13 Let $v \in \mathbb{R}^n$. Then there exists a unique $w \in F_\Lambda$ such that $v \sim_\Lambda w$.

Proof. Since $(v_1, \ldots, v_n)$ is a basis for $\mathbb{R}^n$ there exist $r_1, \ldots, r_n \in \mathbb{R}$ such that $v = r_1 v_1 + \ldots + r_n v_n$. Let $\alpha_i = \lfloor r_i \rfloor$ where $\lfloor r \rfloor$ is the largest integer less than or equal to r. Define $w = v - \sum_{i=1}^n \alpha_i v_i$ which is then clearly in F_Λ and equivalent to v modulo Λ. Assume now that $w' \in F_\Lambda$ with $w' \sim_\Lambda v$. Write $w = \sum_{i=1}^n t_i v_i$, and $w' = \sum_{i=1}^n t_i' v_i$ with $0 \leq t_i, t_i' < 1$. Note that $-1 < t_i - t_i' < 1$. Since $w - w' \in \Lambda$ we have $t_i - t_i' \in \mathbb{Z}$ which is only possible if $t_i - t_i' = 0$, i.e. $w = w'$. ■

We note that an alternative way of formulating Lemma 6.1.13 is that we can write $\mathbb{R}^n$ as a disjoint union

$$\mathbb{R}^n = \bigcup_{l \in \Lambda} (F_\Lambda + l)$$

where for a set A we write $A + l = \{a + l | a \in A\}$.

Using Lemma 6.1.13 we can define the map $\phi_\Lambda : \mathbb{R}^n \to F_\Lambda$ sending v to the unique point w in F_Λ equivalent to v modulo Λ. We will prove the following result about this map:

Lemma 6.1.14 Let $X \subseteq \mathbb{R}^n$ be measurable with respect to Lebesgue measure. If $\operatorname{vol}(X) > \operatorname{vol}(F_\Lambda)$ then the restriction of ϕ_Λ to X, $\phi_\Lambda|_X$ is not injective.

Before proving this we recall a few facts about n-dimensional Lebesgue measure which we simply denote by vol:

1. Lebesgue measure is σ-additive, i.e. if $\{A_n\}_{n=1}^{\infty}$ are disjoint measurable sets then their union is measurable and $\mathrm{vol}(\cup_n A_n) = \sum_n \mathrm{vol}(A_n)$.
2. Lebesgue measure is translation invariant, i.e if A is measurable and $l \in \mathbb{R}^n$ then $A+l$ is measurable and $\mathrm{vol}(A+l) = \mathrm{vol}(A)$.
3. $$\mathrm{vol}(\{x \in \mathbb{R}^n \mid \|x\| < r\}) = r^n \frac{\pi^{n/2}}{\Gamma(n/2+1)} = r^n \cdot \begin{cases} \frac{(2\pi)^m}{n(n-2)\cdots 4\cdot 2} & \text{if } n = 2m \\ \frac{2^{m+1}\pi^m}{n\cdot(n-2)\cdots 3\cdot 1} & \text{if } n = 2m+1. \end{cases}$$
4. The measure of the parallelepiped spanned by $v_1, \dots, v_n$ equals the absolute value of determinant of the matrix whose columns are $v_1, \dots, v_n$, i.e. $\mathrm{vol}(\{\sum_{i=1}^n t_i v_i | 0 \le t_i < 1\}) = |\det(v_1\, v_2 \cdots v_n)|$.

Proof of Lemma 6.1.14. : We have

$$X = X \cap \mathbb{R}^n = X \cap \bigcup_{l\in\Lambda} (F_\Lambda + l) = \bigcup_{l\in\Lambda} X \cap (F_\Lambda + l) = \bigcup_{l\in\Lambda} X_l$$

where $X_l = X \cap (F_\Lambda + l)$ and the last union is disjoint. Note that if $x \in X_l$ then $\phi_\Lambda(x) = x - l$, so $\phi_\Lambda(X_l) = X_l - l$. By translation invariance of Lebesgue measure we have $\mathrm{vol}(\phi_\Lambda(X_l)) = \mathrm{vol}(X_l)$. If $\phi_\Lambda|_X$ were injective then by σ-additivity (and the fact that Λ is countable) we have

$$\mathrm{vol}(X) = \mathrm{vol}(\bigcup_{l\in\Lambda} X_l) = \sum_{l\in\Lambda} \mathrm{vol}(X_l) = \sum_{l\in\Lambda} \mathrm{vol}(\phi_\Lambda(X_l)) \le \mathrm{vol}(F_\Lambda)$$

which contradicts the assumption of the lemma. ■

Note that Lemma 6.1.14 has some resemblance to Dirichlet's pigeon-hole principle, which can be stated formally as follows: a map $\phi : A \to B$ between finite sets A, B cannot be injective if $\#A > \#B$. Lemma 6.1.14 shows that a set X cannot be mapped injectively to set with smaller volume if the map does not decrease volume.

Definition 6.1.4 A set $X \subseteq \mathbb{R}^n$ is called

1. *centrally symmetric* if $-x \in X$ when $x \in X$,
2. convex if when $v, w \in X$ then $tv + (1-t)w \in X$ for every $0 \le t \le 1$.

■ **Example 6.7** A ball centered at the origin is both centrally symmetric and convex. ■

Theorem 6.1.15 — Minkowski. Let Λ be a lattice in $\mathbb{R}^n$ with fundamental domain F_Λ. Let $X \subseteq \mathbb{R}^n$ be a convex, centrally symmetric measurable set satisfying $\mathrm{vol}(X) > 2^n \mathrm{vol}(F_\Lambda)$. Then X contains a non-zero lattice point $l \in \Lambda$.

Proof. Consider the lattice $2\Lambda = \{2v | v \in \Lambda\}$. If Λ has basis $v_1, \dots, v_n$ then 2Λ has basis $2v_1, \dots, 2v_n$ so 2Λ has fundamental domain $\mathrm{vol}(2F_\Lambda) = |\det(2(v_1\, v_2 \cdots v_n))| = 2^n\, |\det(v_1\, v_2 \cdots v_n)| = 2^n \mathrm{vol}(F_\Lambda)$, so $\mathrm{vol}(X) > \mathrm{vol}(2F_\Lambda)$. It follows from Lemma 6.1.14 that $\phi_{2\Lambda}|_X$ is not injective so there exist different $v, w \in X$ such that $\phi_{2\Lambda}(v) = \phi_{2\Lambda}(w)$, i.e. $v = w_0 + l_1$, $w = w_0 + l_2$ with $w_0 \in F_{2\Lambda}$ and $l_i \in 2\Lambda$. Clearly $l_1 \neq l_2$ since otherwise $v = w$.

Since X is centrally symmetric $-w \in X$. Since X is convex $\frac{1}{2}v + (1-\frac{1}{2})(-w) \in X$.

But
$$\frac{1}{2}v + (1-\frac{1}{2})(-w) = \frac{v-w}{2} = \frac{w_0 + l_1 - (w_0 + l_2)}{2} = \frac{l_1 - l_2}{2} \in \Lambda \backslash \{0\},$$
which finishes the proof. ■

Note that all three requirements of Theorem 6.1.15 are crucial (See Exercise 6.2).

We are now ready to prove the main theorem of this section:

Theorem 6.1.16 Every prime can be written as a sum of 4 squares.

Proof. Clearly $2 = 1^2 + 1^2 + 0^2 + 0^2$, so it suffices to prove the claim for odd primes. We note that by Corollary 4.1.3 there are $(p-1)/2$ squares in $\mathbb{F}_p^\times$. Clearly 0 is also a square so we find that

$$\#K = \#\{z \in \mathbb{F}_p | z = u^2, u \in \mathbb{F}_p\} = (p+1)/2$$

Since $-(1+z)$ runs through $\mathbb{F}_p$ when z runs through $\mathbb{F}_p$ we find that

$$\#L = \#\{z \in \mathbb{F}_p | -(1+z) = v^2, v \in \mathbb{F}_p\} = (p+1)/2$$

Since there are p elements in $\mathbb{F}_p$ there must be at least one z lying in $K \cap L$, i.e. a z such that $z = u^2 \pmod{p}$ and $-(1+z) = v^2 \pmod{p}$. Adding these equations we find that

$$-1 = u^2 + v^2 \pmod{p}$$

Consider now

$$\Lambda_{u,v} = \{(x,y,z,t)^t \in \mathbb{Z}^4 | z = ux + vy \pmod{p}, \quad t = vx - uy \pmod{p}\}$$

Then $\Lambda_{u,v}$ is a lattice with basis $\begin{pmatrix}1\\0\\u\\v\end{pmatrix}, \begin{pmatrix}0\\1\\v\\-u\end{pmatrix}, \begin{pmatrix}0\\0\\p\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\p\end{pmatrix}$. See Exercise 6.3. The volume of the corresponding fundamental domain equals

$$\mathrm{vol}(F_{\Lambda_{u,v}}) = \left| \det \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ u & v & p & 0 \\ v & -u & 0 & p \end{pmatrix} \right| = p^2.$$

Consider the set $X = \{x \in \mathbb{R}^4 | \, ||x|| < \sqrt{2p}\}$ which has volume

$$\mathrm{vol}(X) = (\sqrt{2p})^4 \frac{(2\pi)^2}{4 \cdot 2} = 2\pi^2 p^2 > 2^4 p^2 = 2^4 \mathrm{vol}(F_{\Lambda_{u,v}}).$$

By Minkowski's theorem 6.1.15 there exist a non-zero lattice element $0 \neq l \in \Lambda_{u,v} \cap X$. This l satisfies $0 < ||l||^2 < (\sqrt{2p})^2 = 2p$, and at the same time

$$\begin{aligned} ||l||^2 = x^2 + y^2 + z^2 + t^2 &= x^2 + y^2 + (u^2x^2 + v^2y^2 + 2uxvy) + (v^2x^2 + u^2y^2 - 2vxuy) \pmod{p} \\ &= (1 + u^2 + v^2)(x^2 + y^2) = 0 \pmod{p}, \end{aligned}$$

i.e. $x^2 + y^2 + z^2 + t^2$ is divisible by p. But since $0 < ||l||^2 < 2p$ this implies $x^2 + y^2 + z^2 + t^2 = p$. ■

We note that $0, 1$ can clearly be written as a sum of at most 4 squares, so Theorem 6.1.16 and Lemma 6.1.12 implies Lagrange's theorem 6.1.1.

6.2 Exercises for chapter 6

Exercise 6.1 Show that 7 can be written by no less that 4 squares, 23 requires 9 cubes, and 79 requires 19 fourth-powers. Conclude that $g(2) \geq 4$, $g(3) \geq 9$, $g(4) \geq 19$

Exercise 6.2 Show that if any of the requirements – convex, centrally symmetric, or $\mathrm{vol}(X) > 2^n \mathrm{vol}(F)$ – are left out, then Theorem 6.1.15 fails to hold. ☕

Exercise 6.3 Show that

$$\Lambda_{u,v} = \{(x,y,z,t)^t \in \mathbb{Z}^4 | z = ux + vy \pmod{p}, \quad t = vx - uy \pmod{p}\}$$

is a lattice with basis $\begin{pmatrix} 1 \\ 0 \\ u \\ v \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \\ v \\ -u \end{pmatrix}$, $\begin{pmatrix} 0 \\ 0 \\ p \\ 0 \end{pmatrix}$, and $\begin{pmatrix} 0 \\ 0 \\ 0 \\ p \end{pmatrix}$. ☕

Exercise 6.4 Find the factorization into irreducibles of $\mathbb{Z}[i]$ of the numbers $221 = 13 \cdot 17$, $234 = 2 \cdot 3^2 \cdot 13$, $702 = 2 \cdot 3^3 \cdot 13$, and $16660 = 2^2 \cdot 5 \cdot 7^2 \cdot 17$.

Exercise 6.5 Compute $r(n)$ and find all representations of n as a sum of two squares when $n = 221$, $n = 234$, $n = 702$, and $n = 16660$.

Exercise 6.6 Show that the average value of $r_2(n)$ equals π i.e. that

$$\frac{1}{n} \sum_{m=1}^{n} r_2(m) \to \pi \text{ as } n \to \infty.$$

Finding the correct rate of convergence is a very difficult unsolved problem in analytic number theory (Gauss' circle problem).

7. Continued fractions and approximations

Continued fractions provide a very useful tool in number theory. It is a tool with many applications, and we shall here look at a few of them

7.1 Continued fractions

A n-th order finite continued fraction is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}} \tag{7.1}$$

where $a_0 \in \mathbb{R}$, and $a_i > 0$ for $i \in \mathbb{N}$. We denote this by $[a_0, a_1, \ldots, a_n]$. We call n the *length* of the continued fraction. The continued fraction is called *simple* if $a_i \in \mathbb{Z}$.

We note that for $0 < j < n-1$

$$[a_0, a_1, \ldots, a_{n-1}, a_n] = [a_0, a_1, \ldots, a_j, [a_{j+1}, \ldots, a_n]] \tag{7.2}$$

which we shall use in particular for $j = 1$ and $j = n-2$ which can be written as

$$[a_0, a_1, \ldots, a_{n-1}, a_n] = a_0 + \frac{1}{[a_1, \ldots, a_n]} = [a_0, \ldots, a_{n-2}, a_{n-1} + 1/a_n] \tag{7.3}$$

■ **Example 7.1**

$$[7,2,3] = 7 + \cfrac{1}{2 + \cfrac{1}{3}} = 7 + \cfrac{1}{\cfrac{7}{3}} = 7 + \frac{3}{7} = \frac{51}{7}$$

■

Fix an n'th order finite continued fraction $x = [a_0,\dots,a_n]$. For $0 \le m \le n$ the continued fraction $[a_0,\dots,a_m]$ is called the m'th partial convergent of x. For $m = -2,\dots,n$ define numbers $p_m = p_m(a_0,\dots,a_m)$, $q_m = q_m(a_0,\dots,a_m)$ by

$$\begin{pmatrix} p_{-2} \\ q_{-2} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} p_{-1} \\ q_{-1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} p_m \\ q_m \end{pmatrix} = \begin{pmatrix} p_{m-1} & p_{m-2} \\ q_{m-1} & q_{m-2} \end{pmatrix} \begin{pmatrix} a_m \\ 1 \end{pmatrix} \text{ when } m \ge 0 \qquad (7.4)$$

Proposition 7.1.1 $[a_0,\dots,a_m] = \frac{p_m}{q_m}$.

Hence for simple finite continued fractions x the procedure (7.4) allows us to express x as a fraction.

Proof. This is a straightforward induction argument on m:

$$\frac{p_0}{q_0} = \frac{p_{-1}a_0 + p_{-2}}{q_{-1}a_0 + q_{-2}} = \frac{a_0}{1} = [a_0]$$

Assuming the statement holds for all continued fraction of lengths $m-1$ we find

$$\begin{aligned} [a_0,\dots,a_m] = [a_0,\dots,a_{m-1}+1/a_m] &= \frac{p_{m-2}(a_{m-1}+1/a_m)+p_{m-3}}{q_{m-2}(a_{m-1}+1/a_m)+q_{m-3}} \\ &= \frac{p_{m-2}(a_m a_{m-1}+1)+a_m p_{m-3}}{q_{m-2}(a_m a_{m-1}+1)+a_m q_{m-3}} = \frac{a_m(a_{m-1}p_{m-2}+p_{m-3})+p_{m-2}}{a_m(a_{m-1}q_{m-2}+q_{m-3})+q_{m-2}} \\ &= \frac{a_m p_{m-1}+p_{m-2}}{a_m q_{m-1}+q_{m-2}} = \frac{p_m}{q_m} \end{aligned}$$

where we have used that $p_{m-2}, p_{m-3}, q_{m-2}, q_{m-3}$ depend only on $a_0, \dots a_{m-2}$. ■

Proposition 7.1.2

$$\begin{aligned} p_n q_{n-1} - q_n p_{n-1} &= (-1)^{n+1} \\ p_n q_{n-2} - q_n p_{n-2} &= (-1)^n a_n \end{aligned}$$

Proof. By (7.4) we have

$$\begin{aligned} q_{n-1}p_n =& q_{n-1}(p_{n-1}a_n + p_{n-2}) \\ p_{n-1}q_n =& p_{n-1}(q_{n-1}a_n + q_{n-2}) \end{aligned}$$

Subtracting these two equations we find

$$p_n q_{n-1} - q_n p_{n-1} = -(p_{n-1}q_{n-2} - q_{n-1}p_{n-2})$$

Continuing in this way we find

$$p_n q_{n-1} - q_n p_{n-1} = (-1)^n (p_0 q_{-1} - q_0 p_{-1}) = (-1)^{n+1} \qquad (7.5)$$

We note also that again using (7.4) we have

$$\begin{aligned} p_n q_{n-2} - q_n p_{n-2} &= (p_{n-1}a_n + p_{n-2})q_{n-2} - (q_{n-1}a_n + q_{n-2})p_{n-2} \\ &= a_n(p_{n-1}q_{n-2} - q_{n-1}p_{n-2}) = (-1)^n a_n. \end{aligned}$$

where we have used (7.5). ■

Corollary 7.1.3 If $[a_0,\dots,a_n]$ is simple then for every n we have that p_n, q_n are relatively prime integers.

Proof. It is clear from the definition of p_n, q_n that they are integers with $q_n \geq 1$. If they have a common factor g Proposition 7.1.2 implies that $g \mid (-1)^{n+1}$ which implies that $g=1$, and we conclude that p_n, q_n are relatively prime. ■

It is obvious that a simple finite continued fraction $x=[a_0,\dots,a_n]$ is a rational number and according to Proposition 7.1.1 and Corollary 7.1.3 we have that $x=p_n/q_n$ where the fraction is written in lowest terms. In fact we can write any rational number as a continued fraction:

Lemma 7.1.4 Every rational number can be written as a simple continued fraction and every simple continued fraction is a rational number.

Proof. It is clear from the above that every simple continued fraction is a rational number. Given a rational number $q=a/b$ where we may assume that a,b are relatively prime and $b>1$ (If $b=1$ we have $q=[a]$ and the statement is clear.) we use Euclid's algorithm and find

$$\begin{aligned}
a &= a_0 b + r_1\\
b &= a_1 r_1 + r_2\\
r_1 &= a_2 r_2 + r_3\\
&\vdots\\
r_{n-1} &= a_n r_n + 0
\end{aligned}$$

where $a_i \in \mathbb{Z}$ and $a_i > 0$ for $i>0$, and $r_1 > r_2 > \dots > r_n = 1$. We find that

$$\begin{aligned}
q = \frac{a}{b} &= a_0 + \frac{r_1}{b} = a_0 + \cfrac{1}{\cfrac{b}{r_1}}\\
&= a_0 + \cfrac{1}{a_1 + \cfrac{r_2}{r_1}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\cfrac{r_1}{r_2}}}\\
& a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{r_3}{r_2}}} = \cdots = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}} = [a_0, a_1, \dots, a_n]
\end{aligned}$$

which shows that q can be written as a simple continued fraction. ■

7.1.1 Infinite continued fractions

We will now consider infinite continued fractions. These are limits of of finite continued fractions. Let $a_i \in \mathbb{R}$ and $a_i > 0$ for $i>0$. We denote

$$[a_0, a_1, a_3, \dots] = \lim_{n\to\infty} [a_0, \dots, a_n],$$

if the limit exists.

■ **Example 7.2** If $x = [1,1,1,\ldots]$ exists then $x > 1$ and $x = [1,x]$ i.e. $x = 1 + 1/x$ which implies that $x^2 - x - 1 = 0$, and we find that $x = \frac{1+\sqrt{5}}{2}$ which is the so-called golden ratio. ■

We will now show that $[a_0, a_1, \ldots]$ is well-defined if $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{N}$. We call such infinite continued fractions *simple*. For simple continued fractions we have $q_1 < q_2 < \cdots$. Furthermore $q_n = q_{n-1}a_n + q_{n-2} \geq 2q_{n-2}$. It follows, since $q_0 = 1$ and $q_1 \geq 1$, that for $n \geq 1$

$$q_n \geq 2^{(n-1)/2} \tag{7.6}$$

i.e q_n grows at least as fast as the terms of a geometric progression.

Theorem 7.1.5 Let $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{N}$ if $i > 0$. Then $c_n = [a_0, a_1, \ldots, a_n]$ converges as n goes to infinity.

Proof. We start by showing that c_{2n} and c_{2n+1} converge as n goes to infinity. Note that $q_n \geq 1$. By propositions 7.1.1 and 7.1.2 we have for $n \geq 2$

$$c_n - c_{n-2} = \frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_n q_{n-2}} \tag{7.7}$$

from which it follows that c_{2n} is strictly increasing, i.e. $c_{2(n-1)} < c_{2n}$, and c_{2n+1} is strictly decreasing. From the same propositions we find that

$$c_n - c_{n-1} = \frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}} \tag{7.8}$$

It follows that $c_{2n} < c_{2n-1} < c_1$, and $c_{2n+1} > c_{2n} > c_0$. Hence c_{2n} is an increasing sequence which is bounded from above and hence converges to some α_0. Similarly c_{2n+1} is a decreasing sequence bounded from below and hence converges to some α_1. To prove $\alpha_0 = \alpha_1$ we can use (7.8) and (7.6) to conclude that

$$\begin{aligned} |\alpha_0 - \alpha_1| &\leq |\alpha_0 - c_{2n}| + |c_{2n} - c_{2n-1}| + |c_{2n-1} - \alpha_1| \\ &= |\alpha_0 - c_{2n}| + \frac{1}{q_{2n}q_{2n-1}} + |c_{2n-1} - \alpha_1| \to 0 \end{aligned}$$

from which it follows that $\alpha_0 = \alpha_1$ and $c_n \to \alpha_0$. ■

The continued fraction procedure

We will now describe a procedure which, to any given $x \in \mathbb{R}$, finds a simple continued fraction $[a_0, a_1, \ldots]$ (finite or infinite) such that $x = [a_0, a_1, \ldots]$.

The continued fraction procedure For $x \in \mathbb{R}$

1. Write $x = a_0 + t_0$ where $a_0 \in \mathbb{Z}$ and $0 \leq t_0 < 1$.
2. As long as $t_n \neq 0$ write $1/t_n = a_{n+1} + t_{n+1}$ with $a_{n+1} \in \mathbb{N}$ and $0 \leq t_{n+1} < 1$

This associates to every real number a finite or infinite sequence of integers $a_0, a_1, \ldots$, with $a_i > 0$ for $i \geq 1$. We note if $t_n \neq 0$ then a small induction argument (See Exercise 7.4) shows that

$$x = [a_0, a_1, \ldots, a_{n+1} + t_{n+1}] \tag{7.9}$$

We note also that if x is rational then by the proof of Lemma 7.1.4 the continued fraction procedure gives a finite sequence and the corresponding continued fraction equals x.

■ **Example 7.3** Let $x = \sqrt{2}$. We have $\sqrt{2} = 1 + (\sqrt{2} - 1)$ and $0 < \sqrt{2} - 1 < 1$, so $a_0 = 1$ and $t_0 = \sqrt{2} - 1$. Continuing we find that $1/(\sqrt{2}-1) = \sqrt{2} + 1 = 2 + (\sqrt{2} - 1)$ so $a_1 = 2$ and $t_1 = \sqrt{2} - 1$. Since $t_1 = t_0$ we find $a_2 = a_1$ and $t_2 = t_1$. So the continued fraction procedure gives in this case $[1,2,2,2,\ldots]$, which we will also denote by $[1,\overline{2}]$ where the overline denotes that it continues periodically with 2's. We already know that this continued fraction is convergent. Call the limit y. Using the periodicity we see that $y - 1 = 1/(2 + (y-1))$, leading to $y = \sqrt{2}$. Hence $\sqrt{2} = [1,\overline{2}]$. ■

Theorem 7.1.6 Let $x \in \mathbb{R}$, and let $[a_0, a_1, \ldots]$ be the continued fraction coming from the continued fraction procedure. Let $c_n = \frac{p_n}{q_n}$ be the partial convergents and assume that the length of the continued fraction is at least $n+1$. Then

$$|x - c_n| \leq \frac{1}{q_n q_{n+1}} \tag{7.10}$$

If the length of the continued fraction is exactly $n+1$ we have $x = [a_0, a_1, \ldots a_{n+1}]$. In particular we have in both the finite and infinite case that $x = [a_0, a_1, \ldots]$.

Proof. We note that if $t_n \neq 0$ we have, by (7.9) and Proposition 7.1.1, that

$$x - c_n = \frac{p_n(a_{n+1} + t_{n+1}) + p_{n-1}}{q_n(a_{n+1} + t_{n+1}) + q_{n-1}} - \frac{p_n}{q_n} = \frac{p_{n+1} + p_n t_{n+1}}{q_{n+1} + q_n t_{n+1}} - \frac{p_n}{q_n} = \frac{p_{n+1}q_n - p_n q_{n+1}}{(q_{n+1} + q_n t_{n+1})q_n}$$

from which (7.10) follows using $q_n t_{n+1} \geq 0$ and Proposition 7.1.2. If $t_{n+1} = 0$ we see from the above computations that $x = p_{n+1}/q_{n+1} = [a_0, \ldots, a_{n+1}]$. If the continued fraction is infinite then (7.6) implies that $c_n \to x$ as $n \to \infty$. ■

We note that – in the above proof – if $t_{n+1} > 0$, then we have that $q_n t_{n+1} > 0$ and we find that, in this case, Eq. (7.10) is a strict inequality. Together with the following lemma, this shows that for irrational numbers the inequality in Eq. (7.10) can be strengthened to a strict inequality.

Lemma 7.1.7 The continued fraction procedure terminates after finitely many steps if and only if x is rational.

Proof. Use Theorem 7.1.6 and the proof of Lemma 7.1.4. ■

Using Theorem 7.1.6 and (7.6) we see that the continued fraction procedure gives a rational sequence c_n which converges as fast as $|x - c_n| \leq \sqrt{2}/2^n$.

Quadratic irrationals

In Section 4.2.1 we studied algebraic numbers. Given an algebraic number $\zeta \in \mathbb{C}$ there exist a polynomial with integer coefficients of minimal degree having ζ as a root. We denote this number *the degree of* ζ . Irrational numbers of degree 2 are called *quadratic irrationals*. Hence quadratic irrationals are non-rational numbers which are roots in integer polynomials of degree 2.

■ **Example 7.4** The number $\zeta_1 = (1+\sqrt{5})/2$ is a quadratic irrational since it is not rational, and it is a root of $x^2 - x - 1 = 0$. The number $\zeta_2 = \sqrt{2}$ is a quadratic irrational since it is not rational, and it is a root of $x^2 - 2 = 0$. ■

Definition 7.1.1 An infinite continued fraction $x = [a_0, a_1, \ldots]$ is called *periodic* if there exist N, h such that

$$a_n = a_{n+h}$$

for all $n > N$. The minimal choice of h is called the *period* of x. We write $x = [a_0, a_1, \ldots, a_N, \overline{a_{N+1}, \ldots, a_{N+h}}]$.

Example 7.5 1. For $x = \sqrt{2}$ we have (compare Example 7.3) $N = 0$ and $h = 1$ i.e. $\sqrt{2} = [1, \overline{2}]$.

2. For $x = (1+\sqrt{5})/2$ we have (compare Example 7.2) $N = -1$ (or $N = 0$) and $h = 1$. i.e. $(1+\sqrt{5})/2 = [\overline{1}]$.

3. If $x = [\overline{1,2,3}]$ then $x = [1,2,3,x]$, i.e.

$$x = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{x}}} = 1 + \cfrac{1}{2 + \cfrac{x}{3x+1}} = 1 + \frac{3x+1}{7x+2}$$

from which it follows that $(7x+2)x = 10x+3$, i.e. $7x^2 - 8x - 3 = 0$, which means that x is a quadratic irrational. Solving the quadratic equation we find that $x = \frac{4+\sqrt{37}}{7}$ (the other solution is negative, and x is clearly positive)

■

The next theorem says that what we saw in Example 7.5 holds in general:

Theorem 7.1.8 An infinite simple continued fraction $\alpha = [a_0, a_1, \ldots]$ is periodic if and only if α is a quadratic irrational.

Proof. Assume first that the continued fraction is periodic i.e.

$$\alpha = [a_0, a_1, \ldots, a_N, \overline{a_{N+1}, \ldots, a_{N+h}}] = [a_0, a_1, \ldots, a_N, \beta]$$

with $\beta = [\overline{a_{N+1}, \ldots, a_{N+h}}]$. Note that by periodicity $\beta = [a_{N+1}, \ldots, a_{N+h}, \beta]$ and by Proposition 7.1.1 we have

$$\beta = \frac{p'_{h-1}\beta + p'_{h-2}}{q'_{h-1}\beta + q'_{h-2}}$$

where $p'_i = p_i(a_{N+1}, \ldots, a_{N+1+i})$, $q'_i = q_i(a_{N+1}, \ldots, a_{N+1+i}) \in \mathbb{Z}$ from which it follows that β is a root of the degree 2 equation

$$q'_{h-1}\beta^2 + (q'_{h-2} - p'_{h-1})\beta - p'_{h-2} = 0.$$

Hence the degree of β is at most 2. If it is 1 then β would be rational, but then its continued fraction would be finite (Lemma 7.1.4) which it is not. It follows that β is a quadratic irrational and that $\alpha = [a_0, a_1, \ldots, a_N, \beta]$. Now we observe that $\beta' = k + 1/\beta$ is a quadratic irrational if β is a quadratic irrational and $k \in \mathbb{Z}$: Clearly β' cannot be rational and if β is a root of $f(x) = ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$ and $a, c \neq 0$ then β' is a root of $f'(x) = c(x-k)^2 + b(x-k) + a$ since

$$f'(\beta') = c\beta^{-2} + b\beta^{-1} + a = \beta^{-2}(c + b\beta + a\beta^2) = \beta^{-2} f(\beta) = 0.$$

Using (7.3) repeatedly shows that α is a quadratic irrational.

Assume on the other hand that $\alpha = [a_0, a_1, \ldots]$ is a quadratic irrational. Since α is not rational it is an infinite continued fraction. For every n we have by (7.2), $\alpha = [a_0, a_1, \ldots, a_{n-1}, r_n]$ where $r_n = [a_n, a_{n+1}, \ldots]$. We will show that the set of possible r_n's is finite. It follows that for some n, h we have $r_n = r_{n+h}$ which implies that $\alpha = [a_0, a_1, \ldots, a_{n-1}, \overline{a_n, a_{n+1}, a_{n+h-1}}]$, i.e. the continued fraction expansion is periodic.

To see that the set of r_n's is finite note that, since α is a quadratic irrational, there exist $a, b, c \in \mathbb{Z}$ with $ac \neq 0$, such that

$$0 = a\alpha^2 + b\alpha + c. \tag{7.11}$$

By Proposition 7.1.1

$$\alpha = \frac{p_{n-1}r_n + p_{n-2}}{q_{n-1}r_n + q_{n-2}}. \tag{7.12}$$

By combining (7.11) and (7.12) we see, after a small computation, that

$$\begin{aligned} 0 &= (ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2)r_n^2 \\ &\quad + (2ap_{n-1}p_{n-2} + b(p_{n-1}q_{n-2} + p_{n-2}q_{n-1}) + 2cq_{n-1}q_{n-2})r_n \\ &\quad + ap_{n-2}^2 + bp_{n-2}q_{n-2} + cq_{n-2}^2 \\ &= A_n r_n^2 + B_n r_n + C_n \end{aligned}$$

Note that $A_n, B_n, C_n \in \mathbb{Z}$ and $A_{n-1} = C_n$, and

$$B_n^2 - 4A_nC_n = (b^2 - 4ac)(p_{n-1}q_{n-2} - q_{n-1}p_{n-2})^2 = b^2 - 4ac \tag{7.13}$$

We claim that there are only finitely many possible values of A_n. If this is so then there are at most finitely many possible values of C_n since $A_{n-1} = C_n$. But then then there are also only finitely many values of B_n since $B_n^2 = b^2 - 4ac + 4A_nC_n$.

This means that all r_n's are roots of one of a list of finitely many polynomials, and hence there can only be finitely many r_n's. By the previous discussion this would conclude the proof.

To see that there are only finitely may possible values of A_n we recall from Theorem 7.1.6 that

$$\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{q_{n-1}q_n}$$

so $|q_{n-1}\alpha - p_{n-1}| < q_n^{-1} < q_{n-1}^{-1}$ i.e. $p_{n-1} = q_{n-1}\alpha + \delta_n q_{n-1}^{-1}$ where $|\delta_n| < 1$. Inserting this in the definition of A_n we see that

$$\begin{aligned} A_n &= a(q_{n-1}\alpha + \delta_n q_{n-1}^{-1})^2 + b(q_{n-1}\alpha + \delta_n q_{n-1}^{-1})q_{n-1} + cq_{n-1}^2 \\ &= (a\alpha^2 + b\alpha + c)q_{n-1}^2 + 2a\alpha\delta_n + a\delta_n^2 q_{n-1}^{-2} + b\delta_n = 2a\alpha\delta_n + a\delta_n^2 q_{n-1}^{-2} + b\delta_n \end{aligned}$$

It follows that $|A_n| \leq 2|a\alpha| + |a| + |b|$ which shows that there are at most finitely many possible values of A_n which finishes the proof.

■

We have now seen that

- an algebraic number is of degree 1 if and only if the continued fraction is finite (Lemma 7.1.4).
- an algebraic number is of degree 2 if and only if the continued fraction is periodic (Theorem 7.1.8).

so it is natural to ask if there is some property of the continued fraction expansion which characterizes the algebraic numbers of degree 3. This question is completely open.

7.2 Approximating real numbers with rationals

Since $\mathbb{Q}$ is dense in $\mathbb{R}$ we can approximate a real number α by a rational one to any precision. But what if we want to approximate α by a rational one with *small* denominator? Is this possible? Here is the first important result in this direction:

Theorem 7.2.1 — Dirichlet's approximation theorem. Let $\alpha \in \mathbb{R}$, and $n \in \mathbb{N}$. Then there exist co-prime integers $a, b \in \mathbb{Z}$, with $0 < b \leq n$ such that

$$\left|\alpha - \frac{a}{b}\right| \leq \frac{1}{b(n+1)}.$$

Proof. Consider first the case where $\alpha = \frac{p}{q} \in \mathbb{Q}$. If $0 < q \leq n$ we may choose $a = p$, $b = q$. Assume $q > n$. From the continued fraction algorithm we find $\alpha = [a_0, a_1 \ldots, a_k]$ and we have $1 = q_0 \leq q_1 < q_2 \cdots < q_k = q$. We choose $m < k$ such that $q_m \leq n < q_{m+1}$. Then $q_{m+1} \geq n+1$ and Theorem 7.1.6 gives the result with $a = p_m$, $b = q_m$.

If $\alpha \notin \mathbb{Q}$ we have $\alpha = [a_0, a_1, \ldots]$ and $q_m \to \infty$. We may choose m such that $q_m \leq n < q_{m+1}$, which again gives $q_{m+1} \geq n+1$ and Theorem 7.1.6 gives the result with $a = p_m$, $b = q_m$. ■

R Dirichlet's approximation theorem 7.2.1 is the beginning of an entire research topic called Diophantine approximation. For a much more thorough introduction check [Cas72; Ste16].

The proof we have presented here is constructive, as it allows us to use the continued fraction procedure to actually find the number numbers a, b such that a/b approximates α to the given precision. It is possible to give another simple (non-constructive) proof which uses only Dirichlet's pigeon-hole principle.

Corollary 7.2.2 For every $\alpha \in \mathbb{R}$ there exist infinitely many pairs $(a, b) \in \mathbb{Z}^2$ such that

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}. \tag{7.14}$$

Proof. If $\alpha \in \mathbb{Q}$ the result is clear, since we are not requiring a, b to be coprime: If $\alpha = p/q$ any $(a, b) = n(p, q)$ with $n \in \mathbb{N}$ will do.

If $\alpha \notin \mathbb{Q}$ then we can choose any $n = N_1$ and since $\frac{1}{b_1(N_1+1)} < \frac{1}{b_1^2}$ if $0 < b_1 \leq N_1$ we find the first pair (a_1, b_1) by using Theorem 7.2.1. Assume now that there are k different pairs $(a_1, b_1), \ldots, (a_k, b_k)$ satisfying (7.14).

Since α is not rational we have $\left|\alpha - \frac{a_i}{b_i}\right| > 0$, so we may choose $N_{k+1} \in \mathbb{N}$ such that

$$\frac{1}{N_{k+1}} < \min_{i=1,\ldots,k} b_i \left|\alpha - \frac{a_i}{b_i}\right|$$

Applying Theorem 7.2.1 with $n = N_{k+1}$ we get a pair (a_{k+1}, b_{k+1}) such that

$$\left|\alpha - \frac{a_{k+1}}{b_{k+1}}\right| < \frac{1}{(N_{k+1}+1)b_{k+1}} < \frac{1}{b_{k+1}^2}.$$

If $(a_{k+1}, b_{k+1}) = (a_j, b_j)$ for some $j \leq k$ then

$$\frac{1}{N_{k+1}} < \min_{i=1,\ldots,k} b_i \left|\alpha - \frac{a_i}{b_i}\right| \leq b_j \left|\alpha - \frac{a_j}{b_j}\right| = b_{k+1} \left|\alpha - \frac{a_{k+1}}{b_{k+1}}\right| \leq \frac{1}{N_{k+1}+1}$$

which is impossible, i.e. (a_{k+1}, b_{k+1}) is different from the first k pairs, and the proof is finished. ■

Definition 7.2.1 An irrational number $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ is called

- *badly approximable* if for some $C = C(\alpha) > 0$

$$\left|\alpha - \frac{a}{b}\right| \geq \frac{C}{b^2}$$

for every $\frac{a}{b} \in \mathbb{Q}$.

- *well approximable* if there exists $\varepsilon > 0$ such that

$$\left|\alpha - \frac{a}{b}\right| \leq \frac{1}{b^{2+\varepsilon}}$$

for infinitely many $\frac{a}{b} \in \mathbb{Q}$.

- *normally approximable* if it is not well approximable nor badly approximable.

Maybe surprisingly we can determine if α is badly approximable by looking at its continued fraction expansion.

Theorem 7.2.3 A number $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ is badly approximable if and only if the sequence $a_0, a_1, \ldots,$ produced by the continued fraction procedure is bounded.

Corollary 7.2.4 The set of badly approximable numbers is uncountable.

Proof. See Exercise 7.5 ■

Corollary 7.2.5 Every quadratic irrational is badly approximable.

Proof. See Exercise 7.6 ■

A measurable set A is said to have full Lebesgue measure if its complement has measure 0. Hence "almost every" number is in the set A.

Theorem 7.2.6 The set of normally approximable numbers has full Lebesgue measure.

It follows that the generic irrational number is normally approximable. The next theorem is deep, and in 1958 it earned Klaus Roth the Fields medal. The proof is well beyond the scope of these notes:

Theorem 7.2.7 — Roth. No algebraic irrational number is well approximable.

R Note that it follows from Roth's theorem 7.2.7 that all well-approximable numbers are transcendental (note that there are much easier ways to prove this). It is not known if algebraic numbers of degree $d > 2$ are normally approximable or badly approximable, but it is conjectured that they are all normally approximable.

7.3 Exercises for chapter 7

Exercise 7.1 Find the continued fraction of $13/9$.
Exercise 7.2 Evaluate the infinite continued fraction $[1, \overline{2, 1, 2}]$.
Exercise 7.3 Determine the continued fraction $(1+\sqrt{7})/3$.
Exercise 7.4 Prove (7.9). (Hint: (7.3)).
Exercise 7.5 Prove Corollary 7.2.4.
Exercise 7.6 Prove Corollary 7.2.5.
Exercise 7.7 Prove Theorem 7.1.5 by showing – using propositions 7.1.1 and 7.1.2, combined with (7.6) – that

$$|c_n - c_m| \leq \sqrt{2}\sum_{k=m}^{n} \frac{1}{2^k},$$

and conclude that c_n is a Cauchy sequence.

8. The ABC-conjecture

In the 1980s Oesterlé and Masser suggested the following important conjecture:

For an integer n we define the *radical*, $\operatorname{rad}(n)$ as the product of all distinct prime factors of n i.e.

$$\operatorname{rad}(n) = \prod_{p|n} p.$$

It is the largest square-free factor of n.

Conjecture 8.0.1 — ABC. For every $\varepsilon > 0$ there exists a constant $C_\varepsilon > 0$ such that for all mutually co-prime integers a,b,c satisfying $a+b=c$ we have

$$\max(|a|,|b|,|c|) \le C_\varepsilon(\operatorname{rad}(abc))^{1+\varepsilon}$$

The ABC-conjecture mixes the additive structure (by relating a,b,c by $a+b=c$) and the multiplicative structure (the radical of abc is defined through the factors of abc). In informal terms the conjecture implies that if a and b are positive numbers which contain large powers of small primes then c must contain small powers of larger primes.

■ **Example 8.1** Here are a couple of randomly chosen a, b which contain large powers of small primes, illustrating that their sum must have at least one small power of a large prime.

- $a = 2^{17}$ and $b = 5^{29}$ then $c = a+b = 1862645149230958341 97$ factors as

$$c = 7^2 \cdot 38013166310835884 53$$

- $a = 3^9$ and $b = 11^{10}$ then $c = a+b = 34522712163614$ factors as

$$c = 2 \cdot 587 \cdot 29406058061$$

- $a = (2\cdot 3)^{12}$ and $b = (5\cdot 7)^{15}$ then $c = a+b = 144884079282930643579211$ factors as

$$c = 52523171 \cdot 2758479286845241$$

■

The ABC-conjecture is surprisingly powerful, and it solves a lot of other conjectures in number theory, especially concerning diophantine equations. A long and extremely complex proposed proof by Mochizuki is currently under scrutiny by the mathematical community.

For one application of the ABC-conjecture note the following:

Wiles and Taylor proved, in the mid 1990'ies Fermat's last theorem, which we state below. The proof was long using advanced machinery about elliptic curves, modular functions, etc.

Theorem 8.0.2 — Fermat's last theorem. Let $n \geq 3$. The diophantine equation

$$x^n + y^n = z^n \tag{8.1}$$

has no solutions $x, y, z \in \mathbb{N}$.

The case $n = 3$ is due to Euler, $n = 4$ is due to Fermat, and $n = 5$ is due to Dirichlet and Legendre. The $n = 6$ case follows from the $n = 3$ case, and the $n = 7$ case was proved in 1839 by Lamé.

Using the ABC-conjecture we can get pretty close to a short proof of the rest of the theorem. Given a solution $(x, y, z) \in \mathbb{N}^3$ we would get immediately from the ABC-conjecture since $\operatorname{rad}(x^n y^n z^n) = \operatorname{rad}(xyz) \leq xyz \leq z^3$ that

$$z^n \leq C_\varepsilon z^{3(1+\varepsilon)}. \tag{8.2}$$

Clearly $z > 1$ so taking logs we find that

$$n - 3(1+\varepsilon) \leq \frac{\log C_\varepsilon}{\log z} \leq \frac{\log C_\varepsilon}{\log 2}$$

so Fermat's last theorem is true for $n > \log(C_\varepsilon)/\log(2) + 3(1+\varepsilon)$.

If we know the ABC-conjecture with any exponent ε_0 satisfying $n - 3(1+\varepsilon_0) > 0$ then by (8.2) we have $|z| \leq C_{\varepsilon_0}^{1/(n-3(1+\varepsilon_0))}$, i.e. given n there can only be finitely many z's and hence only finitely many solutions to Fermat's equation (8.1) for that given n.

If the ABC-conjecture holds with $\varepsilon = 1$ and $C = 1$ we find $z^n \leq z^6$. In particular $z^{n-6} \leq 1$ proves Fermat's last theorem if $n > 6$. Note that the cases $n = 3, 4, 5, 6$ have been resolved much earlier; See [Rib79].

Bibliography

[AKS04] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. “PRIMES is in P”. In: *Ann. of Math. (2)* 160.2 (2004), pp. 781–793 (cit. on p. 11).

[AGP94] W. R. Alford, Andrew Granville, and Carl Pomerance. “There are infinitely many Carmichael numbers”. In: *Ann. of Math. (2)* 139.3 (1994), pp. 703–722 (cit. on p. 26).

[Ank57] N. C. Ankeny. “Sums of three squares”. In: *Proc. Amer. Math. Soc.* 8 (1957), pp. 316–319 (cit. on p. 59).

[Apo76] Tom M. Apostol. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. New York: Springer-Verlag, 1976, pp. xii+338 (cit. on p. 13).

[Bac90] Eric Bach. “Explicit bounds for primality testing and related problems”. In: *Math. Comp.* 55.191 (1990), pp. 355–380 (cit. on p. 27).

[Bau15] Oswald Baumgart. *The quadratic reciprocity law*. A collection of classical proofs, Edited, translated from the German, and with contributions by Franz Lemmermeyer. Birkhäuser/Springer, Cham, 2015, pp. xiv+172 (cit. on p. 34).

[Bor+08] Peter Borwein et al., eds. *The Riemann hypothesis*. CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC. A resource for the afficionado and virtuoso alike. Springer, New York, 2008, pp. xiv+533 (cit. on p. 51).

[Cas72] J. W. S. Cassels. *An introduction to Diophantine approximation*. Facsimile reprint of the 1957 edition, Cambridge Tracts in Mathematics and Mathematical Physics, No. 45. Hafner Publishing Co., New York, 1972, pp. x+169 (cit. on p. 71).

[DH76] Whitfield Diffie and Martin E. Hellman. “New directions in cryptography”. In: *IEEE Trans. Information Theory* IT-22.6 (1976), pp. 644–654 (cit. on p. 28).

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. Third. Hoboken, NJ: John Wiley & Sons Inc., 2004, pp. xii+932 (cit. on p. 57).

[Fen12] Shaoji Feng. “Zeros of the Riemann zeta function on the critical line”. In: *J. Number Theory* 132.4 (2012), pp. 511–542 (cit. on p. 51).

[Gra05] Andrew Granville. “It is easy to determine whether a given integer is prime”. In: *Bull. Amer. Math. Soc. (N.S.)* 42.1 (2005), pp. 3–38 (cit. on p. 11).

[Har14] G. H. Hardy. “Sur les zéros de la fonction $zeta(s)$ de *Riemann*.” French. In: *C. R. Acad. Sci., Paris* 158 (1914), pp. 1012–1014 (cit. on p. 51).

[Hea86] D. R. Heath-Brown. “Artin’s conjecture for primitive roots”. In: *Quart. J. Math. Oxford Ser. (2)* 37.145 (1986), pp. 27–38 (cit. on p. 22).

[Hec81] Erich Hecke. *Lectures on the theory of algebraic numbers*. Vol. 77. Graduate Texts in Mathematics. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen. New York: Springer-Verlag, 1981, pp. xii+239 (cit. on p. 37).

[Hil09] David Hilbert. “Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n^{ter} Potenzen (Waringsches Problem)”. In: *Math. Ann.* 67.3 (1909), pp. 281–300 (cit. on p. 53).

[Hoo67] Christopher Hooley. “On Artin’s conjecture”. In: *J. Reine Angew. Math.* 225 (1967), pp. 209–220 (cit. on p. 22).

[Ivi85] Aleksandar Ivić. *The Riemann zeta-function*. A Wiley-Interscience Publication. The theory of the Riemann zeta-function with applications. New York: John Wiley & Sons Inc., 1985, pp. xvi+517 (cit. on p. 50).

[Jar14] Frazer Jarvis. *Algebraic number theory*. Springer Undergraduate Mathematics Series. Springer, Cham, 2014, pp. xiv+292 (cit. on pp. 36, 37).

[JJ98] Gareth A. Jones and J. Mary Jones. *Elementary number theory*. Springer Undergraduate Mathematics Series. London: Springer-Verlag London Ltd., 1998, pp. xiv+301 (cit. on pp. 22, 24, 59, 60).

[KV92] A. A. Karatsuba and S. M. Voronin. *The Riemann zeta-function*. Vol. 5. de Gruyter Expositions in Mathematics. Translated from the Russian by Neal Koblitz. Berlin: Walter de Gruyter & Co., 1992, pp. xii+396 (cit. on p. 50).

[Mar77] Daniel A. Marcus. *Number fields*. Universitext. New York: Springer-Verlag, 1977, pp. viii+279 (cit. on p. 37).

[Neu99] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Berlin: Springer-Verlag, 1999, pp. xviii+571 (cit. on p. 37).

[Rib79] Paulo Ribenboim. *13 lectures on Fermat’s last theorem*. Springer-Verlag, New York-Heidelberg, 1979, xvi+302 pp. (1 plate) (cit. on p. 74).

[Rie59] Bernhard Riemann. “Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse.” In: *Monatsberichte der Berliner Akademie* (1859), pp. 671–680 (cit. on p. 50).

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. “A method for obtaining digital signatures and public-key cryptosystems”. In: *Comm. ACM* 21.2 (1978), pp. 120–126 (cit. on p. 30).

[Rou91] G. Rousseau. “On the quadratic reciprocity law”. In: *J. Austral. Math. Soc. Ser. A* 51.3 (1991), pp. 423–425 (cit. on p. 34).

[Sel42] Atle Selberg. “On the zeros of Riemann’s zeta-function”. In: *Skr. Norske Vid. Akad. Oslo I.* 1942.10 (1942), p. 59 (cit. on p. 51).

[Sho94] Peter W Shor. “Algorithms for quantum computation: Discrete logarithms and factoring”. In: *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*. IEEE. 1994, pp. 124–134 (cit. on pp. 12, 29).

[Sho97] Peter W. Shor. “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”. In: *SIAM J. Comput.* 26.5 (1997), pp. 1484–1509 (cit. on p. 12).

[Ste09] William Stein. *Elementary number theory: primes, congruences, and secrets*. Undergraduate Texts in Mathematics. A computational approach. Springer, New York, 2009, pp. x+166 (cit. on p. 25).

[Ste16] Jörn Steuding, ed. *Diophantine analysis*. Trends in Mathematics. Course notes from the summer school held at the University of Würzburg, July 21–26, 2014. Birkhäuser/Springer, Cham, 2016, pp. xi+232 (cit. on p. 71).

[Tit86] Edward C. Titchmarsh. *The theory of the Riemann zeta-function*. Second. Edited and with a preface by D. R. Heath-Brown. New York: The Clarendon Press Oxford University Press, 1986, pp. x+412 (cit. on p. 50).

[Wal79] Michel Waldschmidt. *Transcendence methods*. Vol. 52. Queen’s Papers in Pure and Applied Mathematics. Available at the authors webpage. Kingston, Ont.: Queen’s University, 1979, 126 pp. (not consecutively paged) (cit. on p. 36).

[Zag90] D. Zagier. “A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares”. In: *Amer. Math. Monthly* 97.2 (1990), p. 144 (cit. on p. 55).

Index