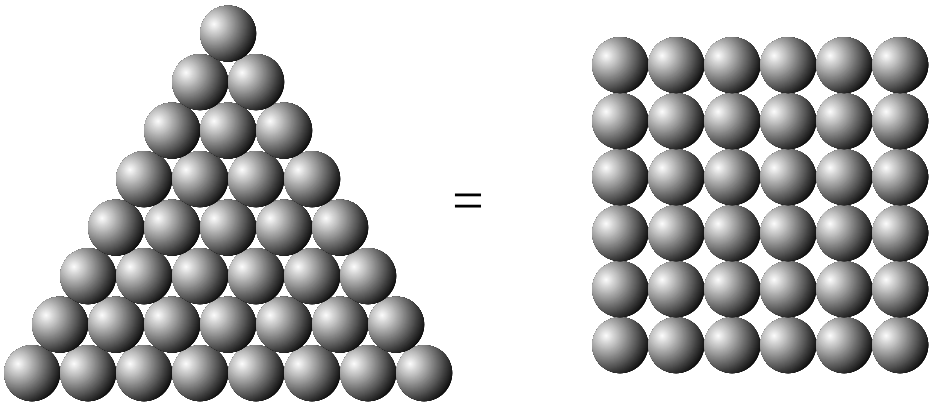
Elementary Number Theory

WISB321



F.Beukers

Department of Mathematics UU

2012

ELEMENTARY NUMBER THEORY

Frits Beukers

Fall semester 2013

Contents

Chapter 1

Integers and the Euclidean algorithm

1.1 Integers

Roughly speaking, number theory is the mathematics of the integers. In any systematic treatment of the integers we would have to start with the so-called *Peano-axioms* for the natural numbers, define addition, multiplication and ordering on them and then deduce their elementary properties such as the commutative, associatative and distributive properties. However, because most students are very familiar with the usual rules of manipulation of integers, we prefer to shortcut this axiomatic approach. Instead we simply formulate the basic rules which form the basis of our course. After all, we like to get as quickly to the parts which make number theory such a beautiful branch of mathematics.
We start with the natural numbers

$$\mathbb{N}: \ 1, 2, 3, 4, 5, \ldots$$

On $\mathbb{N}$ we have an addition $(+)$ and multiplication $(\times$ or $\cdot)$ law and a well-ordering $(>, <, \geq, \leq)$. By a well-ordering we mean that

1. For any distinct $a, b \in \mathbb{N}$ we have either $a > b$ or $a < b$.

2. From $a < b$ and $b < c$ follows $a < c$

3. There is a smallest element, namely 1. So $a \geq 1$ for all $a \in \mathbb{N}$.

We shall assume that we are all familiar with the usual rules of addition and multiplication.

1. For all $a, b \in \mathbb{N}$: $a + b = b + a$ and $ab = ba$ (commutativity of addition and multiplication).

2. For all $a, b, c \in \mathbb{N}$: $(a+b)+c = a+(b+c)$ and $(ab)c = a(bc)$ (associativity of addition and multiplication)

3. For all $a, b, c \in \mathbb{N}$: $a(b+c) = ab + ac$ (distributive law).

4. For all $a \in \mathbb{N}$: $1 \cdot a = a$.

5. For all $a \in \mathbb{N}$: $a + 1 > a$.

6. For all $a, b, c \in \mathbb{N}$: $b > c \Rightarrow a + b > a + c$ and $b \geq c \Rightarrow ab \geq ac$.

7. For all $a, b \in \mathbb{N}$: $a > b \Rightarrow$ there exists $c \in \mathbb{N}$ such that $a = b + c$.

We shall also use the following fact.

Theorem 1.1.1 *Every non-empty subset of* $\mathbb{N}$ *has a smallest element.*

Then there is the principle of induction.

Theorem 1.1.2 *Let* $S \subset \mathbb{N}$ *and suppose that*

1. $1 \in S$

2. *For all* $a \in \mathbb{N}$*:* $a \in S \Rightarrow a + 1 \in S$

Then $S = \mathbb{N}$.

Theorem 1.1.2 follows from Theorem 1.1.1 in the following way. Let S be as in Theorem 1.1.2 and consider the complement S^c. This set is either empty, in which case Theorem 1.1.2 is proven, or S^c is non-empty. Let us assume the latter. Theorem 1.1.1 states that S^c has a smallest element, which we denote by a. If $a = 1$, then $a \notin S$, violating the first condition of Theorem 1.1.2. If $a > 1$ then $a - 1 \notin S^c$. Hence $a - 1 \in S$ and $a \notin S$, violating the second condition. We conclude that S^c is empty, hence $S = \mathbb{N}$.
We call a subset $S \subset \mathbb{N}$ *finite* if there exists $m \in \mathbb{N}$ such that $s < m$ for all $s \in S$. There are two concepts which partially invert addition and multiplication.

1. **Subtraction** Let $a, b \in \mathbb{N}$ and $a > b$. Then there exists a unique $c \in \mathbb{N}$ such that $a = b + c$. We call c the *difference* between a and b. Notation; $a - b$.

2. **Divisibility** We say that the natural number b *divides* a if there exists $c \in \mathbb{N}$ such that $a = bc$. Notation: $b|a$, and b is called a *divisor* of a.

There are many well-known, almost obvious, properties which are not mentioned in the above rules, but which nevertheless follow in a more or less straightforward way. As an exercise you might try to prove the following properties.

1. For all $a, b, c \in \mathbb{N}$: $a + b = a + c \Rightarrow b = c$
2. For all $a, b, c \in \mathbb{N}$: $ab = ac \Rightarrow b = c$.
3. For all $a, b, d \in \mathbb{N}$: $d|a, d|b \Rightarrow d|(a + b)$
4. Any $a \in \mathbb{N}$ has finitely many divisors.
5. Any finite set of natural numbers has a biggest element.

Although divison of one number by another usually fails we do have the concept of *division with remainder*.

Theorem 1.1.3 (Euclid) *Let $a, b \in \mathbb{N}$ with $a > b$. Then either $b|a$ or there exist $q, r \in \mathbb{N}$ such that*

$$a = bq + r, \qquad r < b.$$

Moreover, q, r are uniquely determined by these (in)equalities.

Proof. Suppose b does not divide a. Consider all multiples of b which are less than a. This is a non-empty set, since $b < a$. Choose the largest multiple and call it bq. Then clearly $a - bq < b$. Conversely, if we have a multiple qb such that $a - bq < b$ then qb is the largest b-multiple $< a$. Our theorem follows by taking $r = a - bq$.

□

Another important concept in the natural numbers are *prime numbers*. These are natural numbers $p > 1$ that have only the trivial divisors $1, p$. Here are the first few:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots$$

Most of us have heard about them at a very early age. We also learnt that there are infinitely many of them and that every integer can be written in a unique way as a product of primes. These are properties that are not mentioned in our rules. So one has to prove them, which turns out to be not entirely trivial. This is the beginning of number theory and we will take these proofs up in this chapter.
In the history of arithmetic the number 0 was introduced after the natural numbers as the symbol with properties $0 \cdot a = 0$ for all a and $a + 0 = a$ for all a. Then came the negative numbers -1,-2,-3,... with the property that $-1 + 1 = 0, -2 + 2 = 0, \ldots$. Their rules of addition and multiplication are uniquely determined if we insist that these rules obey the commutative, associate and distributive laws of addition and multiplication. Including the infamous "minus times minus is plus" which causes so many high school children great headaches. Also in the history of mathematics we see that negative numbers and their arithmetic were only generally accepted at a surprisingly late age, the beginning of the 19th century.

From now on we will assume that we have gone through all these formal introductions and we are ready to work with the set of integers $\mathbb{Z}$, which consists of the natural numbers, their opposites and the number 0.
The main role of $\mathbb{Z}$ is to have extended $\mathbb{N}$ to a system in which the operation of subtraction is well-defined for any two elements. One may proceed further by extending $\mathbb{Z}$ to a system in which also element ($\neq 0$) divides any other. The smallest such system is well-known: $\mathbb{Q}$, the set of rational numbers. At several occasion they will also play an important role.

1.2 Greatest common divisors

Definition 1.2.1 *Let $a_1, \ldots, a_n \in \mathbb{Z}$, not all zero. The greatest common divisor of $a_1, \ldots, a_n$ is the largest natural number d which divides all a_i*

Notation: $(a_1, \ldots, a_n)$ or $\gcd(a_1, \ldots, a_n)$.

Definition 1.2.2 *Two numbers $a, b \in \mathbb{Z}$, not both zero, are called relatively prime if $\gcd(a, b) = 1$.*

Theorem 1.2.3 *Let $a_i \in \mathbb{Z}$ $(i = 1, \ldots, n)$ not all zero. Let $d = \gcd(a_1, \ldots, a_n)$. Then there exist $t_1, \ldots, t_n \in \mathbb{Z}$ such that $d = a_1 t_1 + \cdots + a_n t_n$*

Proof. Consider the set

$$S = \{a_1 x_1 + \cdots + a_n x_n \mid x_1, \cdots, x_n \in \mathbb{Z}\}$$

and choose its smallest positive element. Call it s. We assert that $d = s$. First note that every element of S is a multiple of s. Namely, choose $x \in S$ arbitrary. Then $x - ls \in S$ for every $l \in \mathbb{Z}$. In particular, $x - [x/s]s \in S$. Moreover, $0 \leq x - [x/s]s < s$. Because s is the smallest positive element in S , we have necessarily $x - [x/s]s = 0$ and hence $s|x$. In particular, s divides $a_i \in S$ for every i. So s is a common divisor of the a_i and hence $s \leq d$. On the other hand we know that $s = a_1 t_1 + \cdots + a_n t_n$ for suitable $t_1, \cdots, t_n$. From $d|a_i$ $\forall i$ follows that $d|s$. Hence $d \leq s$. Thus we conclude $d = s$. □

Corollary 1.2.4 *Assume that the numbers a, b are not both zero and that $a_1, \ldots, a_n$ are not all zero.*

i. Every common divisor of $a_1, \cdots, a_n$ divides $\gcd(a_1, \ldots, a_n)$.

Proof: This follows from Theorem 1.2.3. There exist integers $t_1, \ldots, t_n$ such that $\gcd(a_1, \ldots, a_n) = a_1 t_1 + \cdots + a_n t_n$. Hence every common divisor of $a_1, \ldots, a_n$ divides their greatest common divisor.

ii. *Suppose* $\gcd(a,b)=1$. *Then* $a|bc \Rightarrow a|c$.
Proof: $\exists x,y\in\mathbb{Z}:\ 1=ax+by$. So, $c=acx+bcy$. The terms on the right are divisible by a and consequently, $a|c$.

iii. *Let* p *be a prime. Then* $p|bc \Rightarrow p|b$ *or* $p|c$.
Proof: Suppose for example that $p\not|b$, hence $\gcd(b,p)=1$. From (ii.) we infer $p|c$.

iv. *Let* p *be a prime and suppose* $p|a_1a_2\cdots a_n$. *Then* $\exists i$ *such that* $p|a_i$.
Proof Use (iii.) and induction on n.

v. *Suppose* $\gcd(a,b)=1$. *then* $b|c$ and $a|c \Rightarrow ab|c$.
Proof: $\exists x,y\in\mathbb{Z}:\ 1=ax+by$. So, $c=acx+bcy$. Because both terms on the right are divisible by ab we also have $ab|c$.

vi. $\gcd(a_1,\ldots,a_n)=\gcd(a_1,\ldots,a_{n-2},(a_{n-1},a_n))$.
Proof: Every common divisor of a_{n-1} and a_n is a divisor of (a_{n-1},a_n) and conversely (see i.). So, the sets $a_1,\ldots,a_n$ and $a_1,\ldots,a_{n-2},(a_{n-1},a_n)$ have the same common divisors. In particular they have the same gcd.

vii. $\gcd(a,b)=d \Rightarrow \gcd(a/d,b/d)=1$.
Proof: There exist $x,y\in\mathbb{Z}$ such that $ax+by=d$. Hence $(a/d)x+(b/d)y=1$ and so any common divisor of a/d and b/d divides 1, i.e. $d=1$.

viii. $\gcd(a,b)=1 \iff$ there exist $x,y\in\mathbb{Z}:\ ax+by=1$.

1.3 Euclidean algorithm for $\mathbb{Z}$

In this section we describe a classical but very efficient algorithm to determine the gcd of two integers a,b and the linear combination of a,b which yields $\gcd(a,b)$. First an example. Suppose we want to determine (654321,123456) . The basic idea is that $\gcd(a,b)=\gcd(a-rb,b)$ for all $r\in\mathbb{Z}$. By repeatedly subtracting the smallest term from the largest, we can see to it that the maximum of the numbers between the gcd brackets decreases. In this way we get

$$\begin{aligned}
&\gcd(654321,123456)=\gcd(654321-5\cdot 123456,123456)=\gcd(37041,123456)\\
=\ &\gcd(37041,123456-3\cdot\gcd(37041)=\gcd(37041,12333)\\
=\ &\gcd(37041-3\cdot\gcd(12333,12333)=\gcd(42,12333)\\
=\ &\gcd(42,12333-293\cdot 42)=\gcd(42,27)\\
=\ &\gcd(42-27,27)=\gcd(15,27)\\
=\ &\gcd(15,27-15)=\gcd(15,12)\\
=\ &\gcd(15-12,12)=\gcd(3,12)=\gcd(3,0)=3
\end{aligned}$$

So we see that our greatest common divisor is 3. We also know that there exist integers x, y such that $3 = 654321x + 123456y$. To obtain such numbers we have to work in a more schematic way where we have put $a = 654321,\ b = 123456$,

$$\begin{array}{rl} & 654321 = 1a + 0b \\ & 123456 = 0a + 1b \\ 654321 = 5 \cdot 123456 + 37041 & 37041 = 1a - 5b \\ 123456 = 3 \cdot 37041 + 12333 & 12333 = -3a + 16b \\ 37041 = 3 \cdot 12333 + 42 & 42 = 10a - 53b \\ 12333 = 293 \cdot 42 + 27 & 27 = -2933a + 15545b \\ 42 = 1 \cdot 27 + 15 & 15 = 2943a - 15598b \\ 27 = 1 \cdot 15 + 12 & 12 = -5876a + 31143b \\ 15 = 1 \cdot 12 + 3 & 3 = 8819a - 46741b \\ 12 = 4 \cdot 3 + 0 & 0 = -123456a + 654321b \end{array}$$

In the left hand column we have rewritten the subtractions. In the righthand column we have written all remainders as linear combinations of $a = 654321$ and $b = 123456$.
In general, write $r_{-1} = a$ en $r_0 = b$ and inductively determine r_{i+1} for $i \geq 0$ by $r_{i+1} = r_{i-1} - [r_{i-1}/r_i] \cdot r_i$ until $r_{k+1} = 0$ for some k. Because $r_0 > r_1 > r_2 > \cdots \geq 0$ such a k occurs. We claim that $r_k = \gcd(a, b)$. This follows from the following observation, $\gcd(r_i, r_{i-1}) = \gcd(r_i, r_{i-1} - [r_{i-1}/r_i]r_i) = \gcd(r_i, r_{i+1}) = \gcd(r_{i+1}, r_i)$ for all i. Hence $\gcd(b, a) = \gcd(r_0, r_{-1}) = \gcd(r_1, r_0) = \cdots = \gcd(r_k, r_{k+1}) = \gcd(r_k, 0) = r_k$.
In our example we see in the right hand column a way to write 3 as a linear combination of $a = 654321$ and $b = 123456$. The idea is to start with $654321 = 1 \cdot a + 0 \cdot b$ and $b = 0 \cdot a + 1 \cdot b$ and combine these linearly as prescribed by the euclidean algorithm. We obtain consecutively the r_i as linear combination of 654321 and 123456 until

$$3 = 8819 \cdot 654321 - 46741 \cdot 123456.$$

In general, let r_i $(i \geq -1)$ be as above and suppose $r_k = 0$ and $r_i \neq 0$ $(i < k)$. Let

$$x_{-1} = 1,\ y_{-1} = 0,\ x_0 = 0,\ y_0 = 1$$

and inductively,

$$x_{i+1} = x_{i-1} - [r_{i-1}/r_i] \cdot x_i, \quad y_{i+1} = y_{i-1} - [r_{i-1}/r_i] \cdot y_i \quad (i \geq 0).$$

Then we can show by induction on i that $r_i = ax_i + by_i$ for all $i \geq -1$. In particular we have $\gcd(a, b) = r_k = ax_k + by_k$.
The proof of the termination of the euclidean algorithm is based on the fact that the remainders $r_1, r_2, \ldots$ form a strictly decreasing sequence of positive numbers.

In principle this implies that the number of steps required in the euclidean algorithm can be as large as the number a or b itself. This would be very bad if the numbers a, b would have more than 15 digits, say. However, *the very strong point* of the euclidean algorithm is that the number of steps required is very small compared to the size of the starting numbers a, b. For example, $3^{100} - 1$ and $2^{100} - 1$ are numbers with 48 and 31 digits respectively. Nevertheless the euclidean algorithm applied to them takes only 54 steps. Incidently, the gcd is 138875 in this case. All this is quantified in the following theorem.

Theorem 1.3.1 *Let $a, b \in \mathbb{N}$ with $a > b$ and apply the euclidean algorithm to them. Use the same notations as above and suppose that r_k is the last non-zero remainder in the algorithm. Then*

$$k < 2\frac{\log a}{\log 2}.$$

In other words, the number of steps in the euclidean algorithm is bounded by a linear function in the number of digits of a.

Proof. First we make an important obervation. Apply the first step of the euclidean algorithm to obtain $q, r \in \mathbb{Z}_{\geq 0}$ such that $a = bq + r$ with $0 \leq r < b$. Then we assert that $r < a/2$. Indeed, if $b > a/2$ then necessarily $q = 1$ and $r = a - b < a - a/2 = a/2$. If $b \leq a/2$ we have automatically $r < b \leq a/2$.
This observation can also be applied to any step $r_{i-1} = q_i r_i + r_{i+1}$ in the euclidean algorithm. Hence $r_{i+1} < r_{i-1}/2$ for every i. By induction we now find $r_1 < a/2,\ r_3 < a/4,\ r_5 < a/8, \ldots$ and in general $r_l < a/2^{(l+1)/2}$ for every odd l. When l is even we observe that $l - 1$ is odd, so $r_l < r_{l-1} < a/2^{l/2}$. So we find for all $l \in \mathbb{N}$ that $r_l < a/2^{l/2}$. In particular, $r_k < a/2^{k/2}$. Using the lower bound $r_k \geq 1$ our theorem now follows. □

In the exercises we will show that the better, and optimal, estimate $k < \log(a)/\log(\eta)$ with $\eta = (1 + \sqrt{5})/2$ is possible.

1.4 Fundamental theorem of arithmetic

Definition 1.4.1 *A prime number is a natural number larger than* 1*, which has only* 1 *and itself as positive divisor.*

Usually the following theorem is taken for granted since it is basically taught at elementary school. However, its proof requires some work and is an application of Corollary 1.2.4(iv).

Theorem 1.4.2 (Fundamental theorem of arithmetic) *Any integer larger than 1 can be written uniquely, up to ordering of factors, as the product of prime numbers.*

Proof. First we show that any $n \in \mathbb{N}_{>1}$ can be written as a product of primes. We do this by induction on n. For $n = 2$ it is obvious. Suppose $n > 2$ and suppose we proved our assertion for all numbers below n. If n is prime we are done. Suppose n is not prime. Then $n = n_1 n_2$, where $1 < n_1, n_2 < n$. By our induction hypothesis n_1 and n_2 can be written as a product of primes. Thus n is a product of primes.
We now prove our theorem. Let n be the smallest number having two different prime factorisations. Write

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

where p_i, q_j are all primes. Notice that $p_1 | q_1 \cdots q_s$. Hence according to Corollary 1.2.4(iv), $p_1 | q_t$ for some t. Since q_t is prime we have $p_1 = q_t$. Dividing out the common prime $p_1 = q_t$ on both factorisations we conclude that n/p_1 has also two different factorisations, contradicting the minimality of n. □

The proof of the above theorem relies on Corollary 1.2.4 of Theorem 1.2.3. The latter theorem relies on the fact that $\mathbb{Z}$ is a euclidean domain. In Theorem 13.2.3 we have given the analogue of Theorem 1.2.3 for general euclidean domains and in principle it is possible to prove a unique prime factorisation property for arbitrary commutative euclidean domains. We have not done this here but instead refer to standard books on algebra.

Definition 1.4.3 *Let $a_1, \ldots, a_n \in \mathbb{Z}$ be non-zero. The lowest common multiple of $a_1, \ldots, a_n$ is the smallest positive common multiple of $a_1, \ldots, a_n$.*

Notation: $\mathrm{lcm}(a_1, \ldots, a_n)$ or $[a_1, \ldots, a_n]$.
The following lemma is a straightforward application of Theorem 1.4.2,

Lemma 1.4.4 *Let $a, b \in \mathbb{N}$ be non-zero. Write*

$$a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \qquad b = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r},$$

where $p_1, \ldots, p_r$ are distinct primes and $0 \leq k_i, m_j$ $(i, j = 1, \ldots r)$. Then,

$$\gcd(a, b) = p_1^{\min(k_1, m_1)} \cdots p_r^{\min(k_r, m_r)}$$

and

$$\mathrm{lcm}(a, b) = p_1^{\max(k_1, m_1)} \cdots p_r^{\max(k_r, m_r)}.$$

Proof. Excercise.

Another fact which is usually taken for granted is that there are infinitely many primes. However, since it does not occur in our Axioms, we must give a proof.

Theorem 1.4.5 (Euclid) *There exist infinitely many primes.*

Suppose that there exist only finitely many primes $p_1, \ldots, p_n$. Consider the number $N = p_1 \cdots p_n + 1$. Let P be a prime divisor of N. Then $P = p_i$ for some i and $p_i | (p_1 \cdots p_n + 1)$ implies that $p_i | 1$. This is a contradiction, hence there exist infinitely many primes. □

1.5 Exercises

Exercise 1.5.1 *Prove,* $\forall n \in \mathbb{N}: \quad 1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$ *(use induction on* n*)*

Exercise 1.5.2 *Prove,* $2^n - 1$ is prime $\Rightarrow n$ is prime.
(The converse is not true, as shown by $89|2^{11} - 1$*.)*

Exercise 1.5.3 *Prove,* $2^n + 1$ is prime $\Rightarrow \ n = 2^k, \ k \geq 0$.
(Fermat thought that the converse is also true. However, Euler disproved this by showing that $641|2^{2^5} + 1$*.)*

Exercise 1.5.4 *(**) Prove,* $n^4 + 4^n$ is prime $\Rightarrow n = 1$.

Exercise 1.5.5 *Prove that there exist infinitely many primes* p *of the form* $p \equiv -1 (\text{mod } 4)$*. Hint: use a variant of Euclid's proof.*

Exercise 1.5.6 *Prove that there exist infinitely many primes* p *such that* $p + 2$ *is not a prime.*

Exercise 1.5.7 *(*)Let* $x, y \in \mathbb{N}$*. Prove that* $x + y^2$ *and* $y + x^2$ *cannot be both a square.*

Exercise 1.5.8 *Prove that* $n^2 \equiv 1 (\text{mod } 8)$ *for any odd* $n \in \mathbb{N}$.

Exercise 1.5.9 *Determine* $d = (4655, 12075)$ *and determine* $x, y \in \mathbb{Z}$ *such that* $d = 4655x + 12075y$.

Exercise 1.5.10 *Let* a, b *be relatively prime positive integers and* $c \in \mathbb{Z}$ *and consider the equation*

$$ax + by = c$$

in the unknowns $x, y \in \mathbb{Z}$.

1. *Show that there exists a solution.*
2. *Let* x_0, y_0 *be a solution. Show that the full solution set is given by*

$$x = x_0 + bt, \quad y = y_0 - at$$

   where t *runs through* $\mathbb{Z}$.

3. *Solve the equation* $23x + 13y = 3$ *in* $x, y \in \mathbb{Z}$ *completely*

Exercise 1.5.11 *Let* a, b *be any positive integers and* $c \in \mathbb{Z}$ *and consider the equation*

$$ax + by = c$$

in the unknowns $x, y \in \mathbb{Z}$.

1. *Show that the equation has a solution if and only if* $\gcd(a,b)$ *divides* c.
2. *Describe the full solution set of the equation.*
3. *Solve the equation* $105x + 121y = 3$ *in* $x, y \in \mathbb{Z}$ *completely.*

Exercise 1.5.12 *Let* $a, b \in \mathbb{N}$ *and suppose* $a > b$. *Choose* $r, q \in \mathbb{Z}$ *such that* $a = bq + r$ *and* $0 \leq r < b$.
a) Show that $r < a/2$.
Consider now the euclidean algoritm with the notations from the course notes. Let r_k *be the last non-zero remainder.*
b) Prove that $k < \log a / \log \sqrt{2}$.
Using the following steps we find an even better estimate for k,
c) Prove by induction on $n = k, k-1, \ldots, 1$ *that* $r_n \geq (\frac{1}{2}(1+\sqrt{5}))^{k-n}$.
d) Prove that $k < \log a / \log(\frac{1}{2}(1+\sqrt{5}))$.

Exercise 1.5.13 *To any pair* $a, b \in \mathbb{N}$ *there exist* $q, r \in \mathbb{Z}$ *such that* $a = qb + r$ *and* $|r| \leq b/2$. *Based on this observation we can consider an alternative euclidean algorithm.*
a) Carry out this algorithm for $a = 12075$ *and* $b = 4655$.
b) Suppose $a > b$ *and let* r_k *be the last non-zero remainder. Show that* $k < \log a / \log 2$.

Exercise 1.5.14 *Let* $a, m, n \in \mathbb{N}$ *and* $a \geq 2$. *Prove that* $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

Exercise 1.5.15 *(*) Let* α *be a positive rational number. Choose the smallest integer* N_0 *so that* $\alpha_1 = \alpha - 1/N_0 \geq 0$. *Next choose the smallest integer* $N_1 > N_0$ *such that* $\alpha_2 = \alpha_1 - 1/N_1 \geq 0$. *Then choose* N_2, *etcetera. Show that there exists an index* k *such that* $\alpha_k = 0$. *(Hint: First consider the case when* $\alpha_0 < 1$*).*
Conclude that every positive rational number α *can be written in the form*

$$\alpha = \frac{1}{N_0} + \frac{1}{N_1} + \cdots + \frac{1}{N_{k-1}}$$

where $N_0, N_1, \ldots, N_{k-1}$ *are distinct positive integers.*

Exercise 1.5.16 *In how many zeros does the number* $123!$ *end?*

Exercise 1.5.17 *Let* p *be prime and* $a \in \mathbb{N}$. *Define* $v_p(a) = \max\{k \in \mathbb{Z}_{\geq 0} |\ p^k | a\}$.
a) Prove that

$$v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots \quad \forall n.$$

b) Let $n \in \mathbb{N}$ *and write* n *in base* p, *i.e. write* $n = n_0 + n_1 p + n_2 p^2 + \cdots + n_k p^k$ *with* $0 \leq n_i < p$ *for all* i. *Let* q *be the number of* n_i *such that* $n_i \geq p/2$. *Prove that*

$$v_p\left(\binom{2n}{n}\right) \geq q.$$

Exercise 1.5.18 *Let $b, c \in \mathbb{N}$ and suppose $(b, c) = 1$. Prove,*
a) For all $a \in \mathbb{Z}$: $(a, bc) = (a, b)(a, c)$.
b) For all $x, y \in \mathbb{Z}$: $(bx + cy, bc) = (c, x)(b, y)$.

Exercise 1.5.19 *(**) Let $a, b, c \in \mathbb{Z}$ not all zero such that $\gcd(a, b, c) = 1$. Prove that there exists $k \in \mathbb{Z}$ such that $\gcd(a - kc, b) = 1$.*

Exercise 1.5.20 *Prove or disprove: There are infinitely many primes p such that $p + 2$ and $p + 4$ are also prime.*

Chapter 2

Arithmetic functions

2.1 Definitions, examples

In number theory we very often encounter functions which assume certain values on $\mathbb{N}$. Well-known examples are,

i. The *unit function* e defined by $e(1) = 1$ and $e(n) = 0$ for all $n > 1$.

ii. The *identity function* E defined by $E(n) = 1$ for all $n \in \mathbb{N}$.

iii. The *power functions* I_k defined by $I_k(n) = n^k$ for all $n \in \mathbb{N}$. In particular, $E = I_0$.

iv. The number of prime divisors of n, denoted by $\Omega(n)$.

v. The number of *distinct* prime divisors of n, denoted by $\omega(n)$.

vi. The *divisor sums* σ_l defined by

$$\sigma_l(n) = \sum_{d|n} d^l.$$

In particular we write $\sigma = \sigma_1$, the sum of divisor and $d = \sigma_0$, the number of divisors.

vii. The Euler ϕ-function or totient function

$$\phi(n) = \#\{d \in \mathbb{N} | \gcd(d, n) = 1 \text{ and } d \leq n\}.$$

viii. Ramanujan's τ-function $\tau(n)$ defined by

$$\sum_{n=1}^{\infty} \tau(n) x^n = x \prod_{k=1}^{\infty} (1 - x^k)^{24}.$$

ix. The "sums of squares" function $r_d(n)$ given by the number of solutions $x_1, \ldots, x_d$ to $n = x_1^2 + \cdots + x_d^2$.

In general,

Definition 2.1.1 *An arithmetic function is a function $f : \mathbb{N} \to \mathbb{C}$.*

Of course this is a very broad concept. Many arithmetic functions which occur naturally have interesting additional properties. One of them is the multiplicative property.

Definition 2.1.2 *Let f be an arithmetic function with $f(1) = 1$. Then f is called multiplicative if $f(mn) = f(m)f(n)$ for all m, n with $(m, n) = 1$ and strongly multiplicative if $f(mn) = f(m)f(n)$ for all m, n.*

It is trivial to see that examples $e, E, I_l, 2^\Omega$ are strongly multiplicative and that 2^ω is multiplicative. In this chapter we will show that σ_l and ϕ are multiplicative. The multiplicative property of Ramanujan's τ is a deep fact based on properties of so-called *modular forms*. It was first proved by Mordell in 1917. As an aside we also mention the remarkable congruence $\tau(n) \equiv \sigma_{11}(n) (\mathrm{mod}\ 691)$ for all $n \in \mathbb{N}$. The multiplicative property of $r_2(n)/4$ will be proved in the chapter on sums of squares.

Theorem 2.1.3 *i. $\sigma_l(n)$ is a multiplicative function.*

ii. Let $n = p_1^{k_1} \cdots p_r^{k_r}$. Then

$$\sigma_l(n) = \prod_i \frac{p_i^{l(k_i+1)} - 1}{p^l - 1}.$$

Proof. Part i. The proof is based on the fact that if $d|mn$ and $(m, n) = 1$ then d can be written uniquely in the form $d = d_1 d_2$ where $d_1|m, d_2|n$. In particular $d_1 = (m, d), d_2 = (n, d)$. We have

$$\begin{aligned} \sigma_l(mn) = \sum_{d|mn} d^l &= \sum_{d_1|m, d_2|n} (d_1 d_2)^l \\ &= \left(\sum_{d_1|m} d_1^l \right) \left(\sum_{d_2|n} d_2^l \right) \\ &= \sigma_l(m)\sigma_l(n) \end{aligned}$$

Part ii. It suffices to show that $\sigma_l(p^k) = (p^{l(k+1)} - 1)/(p^l - 1)$ for any prime power p^k. The statement then follows from the multiplicative property of σ_l. Note that,

$$\sigma_l(p^k) = 1 + p^l + p^{2l} + \cdots + p^{kl} = \frac{p^{l(k+1)} - 1}{p^l - 1}.$$

□

A very ancient problem is that of perfect numbers.

Definition 2.1.4 *A perfect number is a number $n \in \mathbb{N}$ which is equal to the sum of its divisors less than n. Stated alternatively, n is perfect if $\sigma(n) = 2n$.*

Examples of perfect numbers are 6, 28, 496, 8128, 33550336, ... It is not known whether there are infinitely many. It is also not known if there exist odd perfect numbers. If they do, they must be at least 10^{300}. There is an internet search for the first odd perfect number (if it exists), see `/www.oddperfect.org`.
For even perfect numbers there exists a characterisation given by Euclid and Euler.

Theorem 2.1.5 *Let n be even. Then n is perfect if and only if it has the form $n = 2^{k-1}(2^k - 1)$ with $2^k - 1$ prime.*

Proof. Suppose $n = 2^{p-1}(2^p - 1)$ with $2^p - 1$ prime. Then it is straightforward to check that $\sigma(n) = 2n$.
Suppose that n is perfect. Write $n = 2^{k-1}m$, where m is odd and $k \geq 2$. Then,

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

On the other hand, n is perfect, so $\sigma(n) = 2n$, which implies that $2^k m = (2^k - 1)\sigma(m)$. Hence

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

Since $\sigma(m)$ is integral, $2^k - 1$ must divide m. Since $k \geq 2$ we see that m and $m/(2^k - 1)$ are distinct divisors of m. Moreover, they must be the only divisors since their sum is already $\sigma(m)$. This implies that m is prime and $m/(2^k - 1) = 1$, i.e $m = 2^k - 1$ is prime. □

Numbers of the form $2^m - 1$ are called *Mersenne numbers* . If $2^m - 1$ is prime we call it a *Mersenne prime*. It is an easy excercise to show that $2^m - 1$ prime $\Rightarrow m$ is prime. Presumably there exist infinitely many Mersenne primes but this is not proved yet. The known values of m for which $2^m - 1$ is prime, are

$$\begin{aligned} n = \quad & 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, \\ & 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, \\ & 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, \\ & 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, \\ & 20996011, 24036583, 25964951, 30402457, 32582657, \\ & 37156667, 42643801, 42643801, 43112609 \end{aligned}$$

At the moment (August 2008) $2^{43112609} - 1$ is the largest known prime. For the latest news on search activities see: `www.mersenne.org`.
An equally classical subject is that of *amicable numbers* that is, pairs of numbers m, n such that n is the sum of all divisors of m less than m and vice versa. In

other words, $m+n = \sigma(n)$ and $n+m = \sigma(m)$. The pair $220, 284$ was known to the ancient Greeks. Euler discovered some 60 pairs (for example $11498355, 12024045$) and later computer searches yielded several thousands of new pairs, some of which are extremely large.

2.2 Convolution, Möbius inversion

Definition 2.2.1 *Let f and g be two arithmetic functions. Their convolution product $f * g$ is defined by*

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

It is an easy excercise to verify that the convolution product is commutative and associative. Moreover, $f = e * f$ for any f. Hence arithmetic functions form a semigroup under convolution.

Theorem 2.2.2 *The convolution product of two multiplicative functions is again multiplicative.*

Proof. Let f, g be two multiplicative functions. We have trivially that $(f * g)(1) = f(1)g(1)$. For any $m, n \in \mathbb{N}$ with $(m, n) = 1$ we have

$$\begin{aligned}
(f * g)(mn) &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) \\
&= \sum_{d_1|m}\sum_{d_2|n} f(d_1 d_2)g\left(\frac{m}{d_1}\frac{n}{d_2}\right) \\
&= \left(\sum_{d_1|m} f(d_1)g\left(\frac{m}{d_1}\right)\right)\left(\sum_{d_2|n} f(d_2)g\left(\frac{n}{d_2}\right)\right) \\
&= (f * g)(m)(f * g)(n).
\end{aligned}$$

□

Notice that for example $\sigma_l = E * I_l$. The multiplicative property of σ_l follows directly from the mulitiplicativity of E and I_l. We now introduce an important multiplicative function.

Definition 2.2.3 *The Möbius function $\mu(n)$ is defined by $\mu(1) = 1$, $\mu(n) = 0$ if n is divisible by a square > 1 and $\mu(p_1 \cdots p_t) = (-1)^t$ for any product of distinct primes $p_1, \ldots, p_t$.*

Notice that μ is a multiplicative function. Its importance lies in the following theorem.

Theorem 2.2.4 (Möbius inversion) *Let f be an arithmetic function and let F be defined by*

$$F(n) = \sum_{d|n} f(d).$$

Then, for any $n \in \mathbb{N}$,

$$f(n) = \sum_{d|n} F(d)\mu\left(\frac{n}{d}\right).$$

Proof. More cryptically we have $F = E * f$ and we must prove that $f = \mu * F$. It suffices to show that $e = E * \mu$ since this implies $\mu * F = \mu * E * f = e * f = f$. The function $E * \mu$ is again multiplicative, hence it suffices to compute $E * \mu$ at prime powers p^k and show that it is zero there. Observe,

$$\begin{aligned}(E * \mu)(p^k) = \sum_{d|p^k} \mu(d) &= \mu(1) + \mu(p) + \cdots + \mu(p^k) \\ &= 1 - 1 + 0 + \cdots + 0 = 0.\end{aligned}$$

□

Theorem 2.2.5 *Let ϕ be the Euler ϕ-function. Then,*

i.

$$n = \sum_{d|n} \phi(d), \qquad \forall n \geq 1.$$

ii. ϕ is multiplicative.

iii.

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

Proof. Part i). Fix $n \in \mathbb{N}$. Let $d|n$ and let V_d be the set of all $m \leq n$ such that $(m, n) = d$. After dividing everything by d we see that $|V_d| = \phi(n/d)$. Since $\{1, \ldots, n\} = \cup_{d|n} V_d$ is a disjoint union we find that $n = \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d)$, as asserted.
Part ii). We have seen in part i) that $I_1 = E * \phi$. Hence, by Möbius inversion, $\phi = \mu * I_1$. Multiplicativity of ϕ automatically follows from the multiplicativity of μ and I_1.
Part iii). Because of the multiplicativity of ϕ it suffices to show that $\phi(p^k) = p^k(1 - 1/p)$. This follows from $\phi(p^k) = (I_1 * \mu)(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$. □

2.3 Exercises

Exercise 2.3.1 *Prove that the sum of the inverses of all divisors of a perfect number is two.*

Exercise 2.3.2 *Prove that an odd perfect number must contain at least three distinct primes.*
(It is known that there must be at least six distinct primes).

Exercise 2.3.3 *Describe the multiplicative functions which arise from the following convolution products (the symbol 2^ω stands for the multiplicative function $2^{\omega(n)}$).*

$$I_k * I_k \qquad \mu * I_1 \qquad \mu * \mu$$
$$\mu * 2^\omega \qquad 2^\omega * 2^\omega \qquad \mu * \phi.$$

Exercise 2.3.4 *Prove that there exist infinitely many n such that $\mu(n) + \mu(n+1) = 0$.*

Exercise 2.3.5 *Prove that there exist infinitely many n such that $\mu(n) + \mu(n+1) = -1$.*

Exercise 2.3.6 *Let F be the multiplicative function such that $F(n) = 1$ if n is a square, and 0 otherwise. Determine a multiplicative function f such that $f * E = F$.*

Exercise 2.3.7 *Let f be a multiplicative function. Prove that there exists a multiplicative function g such that $f * g = e$ (hence the multiplicative functions form a group with respect to the convolution product).*

Exercise 2.3.8 *Prove that for every $n \in \mathbb{N}$*

$$\sum_{k|n} \sigma_0(k)^3 = \left(\sum_{k|n} \sigma_0(k) \right)^2.$$

Exercise 2.3.9 *(**) Show that there exist infinitely many n such that $\phi(n)$ is a square.*

Chapter 3

Residue classes

3.1 Basic properties

Definition 3.1.1 *Let $m \in \mathbb{N}$. Two integers a and b are called congruent modulo m if $m|a-b$.*

Notation: $a \equiv b(\text{mod } m)$

Definition 3.1.2 *The residue class $a \bmod m$ is defined to be the set $\{b \in \mathbb{Z} \mid b \equiv a(\text{mod } m)\}$. The set of residue classes modulo m is denoted by $\mathbb{Z}/m\mathbb{Z}$.*

The following properties are more or less straightforward,

Remark 3.1.3 *Let $a, b, c, d \in \mathbb{Z}$ and $m, n \in \mathbb{N}$.*

i. $a \equiv a + rm(\text{mod } m)$ $\forall r \in \mathbb{Z}$.

ii. *There are m residue classes modulo m.*

iii. $a \equiv b(\text{mod } m)$ *and* $n|m \Rightarrow a \equiv b(\text{mod } n)$.

iv. $a \equiv b(\text{mod } m)$ *and* $c \equiv d(\text{mod } m) \Rightarrow a + c \equiv b + d(\text{mod } m)$, $ac \equiv bd(\text{mod } m)$.

v. *Let $P(x) \in \mathbb{Z}[x]$. Then* $a \equiv b(\text{mod } m) \Rightarrow P(a) \equiv P(b)(\text{mod } m)$.

vi. *The residue classes modulo m form a commutative ring with 1-element. Its additive group is cyclic and generated by* $1 \bmod m$. *If m is prime then $\mathbb{Z}/m\mathbb{Z}$ is a finite field. If m is composite then $\mathbb{Z}/m\mathbb{Z}$ has divisors of zero.*

Definition 3.1.4 *Let $m \in \mathbb{N}$. A residue class $a \bmod m$ is called invertible if $\exists$ $x \bmod m$ such that $ax \equiv 1(\text{mod } m)$. The set of invertible residue classes is denoted by $(\mathbb{Z}/m\mathbb{Z})^*$.*

Notice that $(\mathbb{Z}/m\mathbb{Z})^*$ is nothing but the unit group of $\mathbb{Z}/m\mathbb{Z}$. In particular the inverse $x \bmod m$ of $a \bmod m$ is uniquely determined modulo m.

Theorem 3.1.5 *Let $a \in \mathbb{Z}$ en $m \in \mathbb{N}$. Then,*

$$a \bmod m \text{ is invertble} \Longleftrightarrow (a, m) = 1.$$

Proof. The residue class $a \bmod m$ is invertible $\Longleftrightarrow \exists x : \ ax \equiv 1 (\bmod m) \Longleftrightarrow \exists x, y : \ ax + my = 1 \Longleftrightarrow (a, m) = 1.$ □

Notice that the proof of the latter theorem also shows that we can compute the inverse of a residue class via the euclidean algorithm. For example, solve $331x \equiv 15 (\bmod 782)$. The euclidean algorithm shows that the g.c.d. of 331 and 782 is 1 and $1 = -189 \cdot 331 + 80 \cdot 782$. Hence $-189 \bmod 782$ is the inverse of 331 mod 782. To solve our question, multiply on both sides with -189 to obtain $x \equiv 293 (\bmod 782)$.

3.2 Chinese remainder theorem

Theorem 3.2.1 *Let $m, n \in \mathbb{Z}$ and $(m, n) = 1$. Then the natural map $\psi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ given by $\psi : a \bmod mn \mapsto (a \bmod m, a \bmod n)$ yields an isomorphism of the rings $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Proof. It is clear that ψ is a ringhomomorphism. Furthermore ψ is injective, for if we assume $\psi(a) = \psi(b)$ this means that a and b are equal modulo m and n. So m and n both divide $a - b$ and since $(m, n) = 1$, mn divides $a - b$, i.e $a \equiv b \bmod mn$. Also, $\mathbb{Z}/mn\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ have the same cardinality, mn. Since an injective map between finite sets of the same cardinality is automatically bijective, our theorem follows. □

Via almost the same proof we obtain the following generalisation.

Theorem 3.2.2 *Let $m_1, \ldots, m_r \in \mathbb{Z}$ and $(m_i, m_j) = 1 \ \forall i \neq j$. Let $m = m_1 \cdots m_r$. Then the map*

$$\psi : \ \mathbb{Z}/m\mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_r\mathbb{Z})$$

given by

$$\psi : \ a \bmod m \mapsto a \bmod m_1, \ldots, a \bmod m_r$$

yields a ring isomorphism.

A direct consequence of Theorem 3.2.2 is as follows

Corollary 3.2.3 (Chinese remainder theorem) *Let notations be the same as in Theorem* 3.2.2. *To any r-tuple of residue classes* $c_1 \bmod m_1, \ldots, c_r \bmod m_r$ *there exists precisely one residue class* $a \bmod m$ *such that* $a \equiv c_i (\bmod\ m_i)$ $(i = 1, \ldots, r)$.

Let us give a slightly different reformulation and another proof.

Theorem 3.2.4 (Chinese remainder theorem) *Let* $m_1, \ldots, m_r \in \mathbb{Z}$ *and* $(m_i, m_j) = 1\ \forall i \neq j$. *Let* $m = m_1 \cdots m_r$. *Then the system of equations*

$$x \equiv c_j (\bmod\ m_j), \quad 1 \leq j \leq r$$

has exactly one residue class modulo m *as solution set.*

Proof. Define $M_j = m/m_j$ for $j = 1, \ldots, r$. Then clearly $(M_j, m_j) = 1,\ \forall j$. Choose for each j a number n_j such that $M_j n_j \equiv 1 (\bmod\ m_j)$. Let

$$x_0 = \sum_{j=1}^{r} c_j n_j M_j.$$

Using $m_i | M_j$ if $i \neq j$ and $n_i M_i \equiv 1 (\bmod\ m_i)$ we can observe that $x_0 \equiv c_i (\bmod\ m_i)$ for any i. Clearly, any number congruent to x_0 modulo m is also a solution of our system.
Conversely, let x_1 be a solution of our system. Then $x_1 \equiv x_0 \bmod m_j$ and hence $m_j | (x_1 - x_0)$ for all j. Since $(m_i, m_j) = 1$ for all $i \neq j$, this implies $m | (x_1 - x_0)$ and hence $x_1 \equiv x_0 \bmod m$, as desired. □

Notice that the latter proof of the Chinese remainder theorem gives us an algorithm to construct solutions. However, in most cases it is better to use straightforward calculation as in the following example.

Example. Solve the system of congruence equations

$$x \equiv 1 (\bmod\ 5), \qquad x \equiv 2 (\bmod\ 6), \qquad x \equiv 3 (\bmod\ 7).$$

First of all notice that 5, 6 and 7 are pairwise relatively prime and so, according to the chinese remainder theorem there is a unique residue class modulo $5 \cdot 6 \cdot 7 = 210$ as solution. However, in the following derivation this will follow automatically. The first equation tells us that $x = 1 + 5y$ for some $y \in \mathbb{Z}$. Substitute this into the second equation, $1 + 5y \equiv 2 (\bmod\ 6)$. Solution of this equation yields $y \equiv 5 (\bmod\ 6)$. Hence y must be of the form $y = 5 + 6z$ for some $z \in \mathbb{Z}$. For x this implies that $x = 26 + 30z$. Substitute this into the third equation, $26 + 30z \equiv 3 (\bmod\ 7)$. Solution yields $z \equiv 6 (\bmod\ 7)$. Hence $z = 6 + 7u,\ u \in \mathbb{Z}$ which implies $x = 206 + 210u$. So the residueclass 206 mod 210 is the solution to our problem. Notice by the way that $206 \equiv -4 (\bmod\ 210)$. If we would have been clever we would have seen the solution $x = -4$ and the solution to our problem without calculation.

3.3 Invertible residue classes

In this section we shall give a description of the group $(\mathbb{Z}/m\mathbb{Z})^*$ and a number of properties. With the notations of Theorem 3.2.2 we know that $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$. This automatically implies the following corollary.

Corollary 3.3.1 *Let notations be the same as in Theorem* 3.2.2. *Then,*

$$(\mathbb{Z}/m\mathbb{Z})^* \simeq (\mathbb{Z}/m_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/m_r\mathbb{Z})^*.$$

Definition 3.3.2 *Let $m \in \mathbb{N}$. The number of natural numbers $\leq m$ relatively prime with m is denoted by $\phi(m)$, Euler's totient function.*

Notice that if $m \geq 2$ then $\phi(m)$ is precisely the cardinality of $(\mathbb{Z}/m\mathbb{Z})^*$. We recall the following theorem which was already proved in the chapter on arithmetic functions. However, the multiplicative property follows also directly from the chinese remainder theorem. So we can give a separate proof here.

Theorem 3.3.3 *Let $m, n \in \mathbb{N}$.*

a) If $(m,n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$.

b) $\phi(n) = n\prod(1 - \frac{1}{p})$, where the product is over all primes p dividing n.

c) $\sum_{d|n} \phi(d) = n$.

Proof. Part a) follows directly from Corollary 3.3.1 which implies that $(\mathbb{Z}/mn\mathbb{Z})^* \simeq (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$. Hence $|(\mathbb{Z}/mm\mathbb{Z})^*| \simeq |(\mathbb{Z}/m\mathbb{Z})^*| \times |(\mathbb{Z}/n\mathbb{Z})^*|$ and thus $\phi(mn) = \phi(m)\phi(n)$.
Part b) First note that $\phi(p^k) = p^k - p^{k-1}$ for any prime p and any $k \in \mathbb{N}$. It is simply the number of integers in $[1, p^k]$ minus the number of multiples of p in the same interval. Then, for any $n = p_1^{k_1} \cdots p_r^{k_r}$ we find, using property (a),

$$\phi(n) = \prod_{i=1}^{r} \phi(p_i^{k_i}) = \prod_{i=1}^{r} (p_i^{k_i} - p_i^{k_i - 1}) = n \prod_i (1 - \frac{1}{p_i}).$$

Part c) Notice that

$$\begin{aligned} n &= \#\{k | 1 \leq k \leq n\} \\ &= \sum_{d|n} \#\{k | 1 \leq k \leq n,\ (k,n) = d\} \\ &= \sum_{d|n} \#\{l | 1 \leq l \leq n/d,\ (l, n/d) = 1\} \\ &= \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d) \end{aligned}$$

Theorem 3.3.4 (Euler) *Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$. Suppose $(a,m) = 1$. Then*

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

Proof. Since $(a,m) = 1$, the class $a \bmod m$ is an element of $(\mathbb{Z}/m\mathbb{Z})^*$, a finite abelian group. Since $\phi(m) = \#(\mathbb{Z}/m\mathbb{Z})^*$, our statement follows from Lemma 13.1.1 □

When m is a prime, which we denote by p, we have $\phi(p) = p-1$ and thus the following corollary.

Corollary 3.3.5 (Fermat's little theorem) *Let $a \in \mathbb{Z}$ and let p be a prime. Suppose $p \not| a$. Then*

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

Corollary 3.3.5 tells us that $2^{p-1} \equiv 1 (\text{mod } p)$ or equivalently, $2^p \equiv 2 (\text{mod } p)$, for any odd prime p. Almost nothing is known about the primes for which $2^p \equiv 2 (\text{mod } p^2)$. Examples are given by $p = 1093$ and 3511. No other such primes are known below 3×10^9. It is not even known whether there exist finitely or infinitely many of them. And to add an even more remarkable token of our ignorance, neither do we know if there infinitely many primes p with $2^p \not\equiv 2 (\text{mod } p^2)$.

Theorem 3.3.6 (Wilson,1770) *If p is a prime then $(p-1)! \equiv -1 (\text{mod } p)$.*

Proof. Notice that this theorem is just a special case of Lemma 13.1.12, when we take $R = (\mathbb{Z}/p\mathbb{Z})^*$. □

Theorem 3.3.7 (Gauss) *Let p be a prime. Then the group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.*

Proof. Since p is prime, $(\mathbb{Z}/p\mathbb{Z})^*$ is the unit group of the field $\mathbb{Z}/p\mathbb{Z}$. From Lemma 13.1.11 our statement follows. □

Definition 3.3.8 *Let $m \in \mathbb{N}$. An integer g such that $g \bmod m$ generates the group $(\mathbb{Z}/m\mathbb{Z})^*$ is called a primitive root modulo m.*

As an illustration consider $(\mathbb{Z}/17\mathbb{Z})^*$ and the powers of 3 modulo 17,

$$\begin{array}{llllll} 3^1 \equiv 3 & 3^2 \equiv 9 & 3^3 \equiv 10 & 3^4 \equiv 13 & 3^5 \equiv 5 & 3^6 \equiv 15 \\ 3^7 \equiv 11 & 3^8 \equiv 16 & 3^9 \equiv 14 & 3^{10} \equiv 8 & 3^{11} \equiv 7 & 3^{12} \equiv 4 \\ 3^{13} \equiv 12 & 3^{14} \equiv 2 & 3^{15} \equiv 6 & 3^{16} \equiv 1 & & \end{array}$$

Observe that the set $\{3^1, \ldots, 3^{16}\}$ equals the set $\{1, 2, \ldots, 16\}$ modulo 17. So 3 is a prinitive root modulo 17. Notice also that $2^4 \equiv 16 \equiv -1 (\text{mod } 17)$. Hence $2^8 \equiv (-1)^2 \equiv 1 (\text{mod } 17)$ and 2 is not a primitive root modulo 17.

Not all values of m allow a primitive root. For example, the order of each elements in $(\mathbb{Z}/24\mathbb{Z})^*$ is 1 or 2, whereas this group contains 8 elements. To get a good impression of $(\mathbb{Z}/m\mathbb{Z})^*$ one should take the prime decomposition $m = p_1^{k_1} \cdots p_r^{k_r}$ of m and notice that according to Corollary 3.3.1

$$(\mathbb{Z}/m\mathbb{Z})^* \simeq (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_r^{k_r}\mathbb{Z})^*.$$

The structure for the groups $(\mathbb{Z}/p^k\mathbb{Z})^*$ with p prime and $k \in \mathbb{N}$ is then given in the following two theorems.

Theorem 3.3.9 *Let p be an odd prime and $k \in \mathbb{N}$. Then $(\mathbb{Z}/p^k\mathbb{Z})^*$ is a cyclic group.*

Proof. For $k = 1$ the theorem is just Theorem 3.3.7. So let us assume $k > 1$. Let g be a primitive root modulo p and let $\mathrm{ord}(g)$ be its order in $(\mathbb{Z}/p^k\mathbb{Z})^*$. Since $g^{\mathrm{ord}(g)} \equiv 1 (\mathrm{mod}\ p^k)$ we have $g^{\mathrm{ord}(g)} \equiv 1 (\mathrm{mod}\ p)$. Moreover, g is a primitive root modulo p and thus $(p-1)|\mathrm{ord}(g)$. So $h = g^{\mathrm{ord}(g)/(p-1)}$ has order $p-1$ in $(\mathbb{Z}/p^k\mathbb{Z})^*$. From Lemma 3.3.11(i) with $r = k$ it follows that $(1+p)^{p^{k-1}} \equiv 1 (\mathrm{mod}\ p^k)$ and the same lemma with $r = k-1$ implies $(1+p)^{p^{k-2}} \equiv 1 + p^{k-1} \not\equiv 1 (\mathrm{mod}\ p^k)$. Hence $\mathrm{ord}(1+p) = p^{k-1}$. Lemma 13.1.6 now implies that $(p+1)h$ has order $(p-1)p^{k-1}$ and so $(\mathbb{Z}/p^k\mathbb{Z})^*$ is cyclic. □

Theorem 3.3.10 *Let $k \in \mathbb{Z}_{\geq 3}$. Any element of $(\mathbb{Z}/2^k\mathbb{Z})^*$ can be written uniquely in the form $(-1)^m 5^t \bmod 2^k$ with $m \in \{0, 1\},\ 0 \leq t < 2^{k-2}$.*

Note that this theorem implies that $(\mathbb{Z}/2^k\mathbb{Z})^*$ is isomorphic to the product of a cyclic group of order 2 and a cyclic group of order 2^{k-2} when $k \geq 3$. Of course $(\mathbb{Z}/4\mathbb{Z})^*$ and $(\mathbb{Z}/2\mathbb{Z})^*$ are cyclic.

Proof. From Lemma 3.3.11(ii) with $r = k$ we find $5^{2^{k-2}} \equiv 1 (\mathrm{mod}\ 2^k)$ and with $r = k-1$ we find $5^{2^{k-3}} \equiv 1 + 2^{k-1} \not\equiv 1 (\mathrm{mod}\ 2^k)$. So, $\mathrm{ord}(5) = 2^{k-2}$. Notice that all elements $5^t,\ 0 \leq t < 2^{k-2}$ are distinct and $\equiv 1 (\mathrm{mod}\ 4)$. Hence the remaining elements of $(\mathbb{Z}/2^k\mathbb{Z})^*$ are given by $-5^t,\ 0 \leq t < 2^{k-2}$. □

Lemma 3.3.11 *Let p be an odd prime and $r \in \mathbb{N}$.*

i. $(1+p)^{p^{r-1}} \equiv 1 + p^r (\mathrm{mod}\ p^{r+1})$.

ii. $5^{2^{r-2}} \equiv 1 + 2^r (\mathrm{mod}\ 2^{r+1})$ *for all* $r \geq 2$.

Proof. i. We use induction on r. For $r = 1$ our statement is trivial. Let $r > 1$ and assume we proved

$$(1+p)^{p^{r-2}} \equiv 1 + p^{r-1} (\mathrm{mod}\ p^r).$$

In other words, $(1+p)^{p^{r-2}} = 1 + Ap^{r-1}$ with $A \equiv 1 (\text{mod } p)$. Take the p-th power on both sides,

$$\begin{aligned}(1+p)^{p^{r-1}} &= 1 + \sum_{t=1}^{p} \binom{p}{t} (Ap^{r-1})^t \\ &\equiv 1 + pAp^{r-1} + \binom{p}{2} (Ap^{r-1})^2 (\text{mod } p^{r+1}).\end{aligned}$$

Because p is odd we have $\binom{p}{2} \equiv 0 (\text{mod } p)$ and we are left with

$$(1+p)^{p^{r-1}} \equiv 1 + Ap^r \equiv 1 + p^r (\text{mod } p^{r+1})$$

as asserted.
ii. Use induction on r. For $r = 2$ our statement is trivial. Let $r > 2$ and assume we proved

$$5^{2^{r-3}} \equiv 1 + 2^{r-1} (\text{mod } 2^r).$$

In other words, $5^{2^{r-3}} = 1 + A2^{r-1}$ with A odd. Take squares on both sides,

$$5^{2^{r-2}} = 1 + A2^r + A^2 2^{2r-2} \equiv 1 + 2^r (\text{mod } 2^{r+1}).$$

The latter congruence follows because A is odd and $2r - 2 \geq r + 1$ if $r > 2$. This concludes the induction step. □

3.4 Periodic decimal expansions

A very nice application of the properties of residue classes is that in writing decimal expansions of rational numbers. For example, when we write out the decimal expansion of $1/7$ we very soon find that

$$\frac{1}{7} = 0.142857142857142857142857\ldots,$$

in short hand notation

$$\frac{1}{7} = 0.\overline{142857}.$$

Using Euler's Theorem 3.3.4 this is easy to see. Note that $10^6 - 1$ is divisible by 7 and $10^6 - 1 = 7 \cdot 142857$. Then,

$$\frac{1}{7} = \frac{142857}{10^6 - 1} = 142857 \cdot 10^{-6} + 142857 \cdot 10^{-12} + \cdots$$

The second equality is obtained by expanding $1/(10^6 - 1) = 10^{-6}/(1 - 10^{-6})$ in a geometrical series.

Definition 3.4.1 *A decimal expansion is called periodic if it is periodic from a certain decimal onward, and purely periodic if it is periodic starting from the decimal point.*

For any periodic decimal expansion there is a *minimal period* and it is clear that the minimal period divides any other period.

Theorem 3.4.2 *Let α be a real number then,*

i. The decimal expansion of α is periodic $\Leftrightarrow \alpha \in \mathbb{Q}$.

ii. The decimal expansion of α is purely periodic $\Leftrightarrow \alpha \in \mathbb{Q}$ and the denominator of α is relatively prime with 10.

Suppose $\alpha \in \mathbb{Q}$ has a denominator of the form $2^k 5^l q$, where $(q, 10) = 1$. Then the minimal period length of the decimal expansion of α equals the order of 10 in $(\mathbb{Z}/q\mathbb{Z})^*$.

Proof. Suppose that the decimal expansion of α is periodic. By multiplication with a sufficiently large power 10^k we can see to it that $10^k\alpha$ is purely periodic. Suppose the minimal period length is l. Then there exist integers A, N such that $0 \leq N < 10^l - 1$ and $10^k\alpha = A + N \cdot 10^{-l} + N \cdot 10^{-2l} + \cdots$. The latter sum equals $A + N/(10^l - 1)$, hence α is rational. In case the decimal expansion is purely periodic we can take $k = 0$ and we have $\alpha = A + N/(10^l - 1)$. Thus it is clear that the denominator q of α is relatively prime with 10.
Suppose conversely that $\alpha \in \mathbb{Q}$. After multiplication by a sufficiently high power 10^k we can see to it that the denominator q of $10^k\alpha$ is relatively prime with 10. Then we can write $10^k\alpha = A + a/q$, where $A, a \in \mathbb{Z}$ and $0 \leq a < q$. Let r be the order of 10 in $(\mathbb{Z}/q\mathbb{Z})^*$ and write $N = a \cdot (10^r - 1)/q$. Then $0 \leq N < 10^r - 1$ and

$$10^k\alpha = A + \frac{N}{10^r - 1}.$$

After expansion into a geometrical series we see that $10^k\alpha$ has a purely periodic decimal expansion and that α has a periodic expansion. In particular, when the denominator of α is relatively prime with 10 we can take $k = 0$ and the expansion of α is purely periodic in this case.
To prove the last part of the theorem we make two observations. Let again r be the order of 10 in $(\mathbb{Z}/q\mathbb{Z})^*$ and let l be the minimal period of the decimal expansion. From the first part of the above proof it follows that q divides $10^l - 1$. In other words, $10^l \equiv 1 (\mathrm{mod}\ q)$ and hence $r|l$. From the second part of the proof it follows that r is a period of the decimal expansion, hence $l|r$. Thus it follows that $r = l$. □

The above theorem is stated only for numbers written in base 10. It should be clear by now how to formulate the theorem for numbers written in any base.

3.5 Exercises

Exercise 3.5.1 *Let $n \in \mathbb{N}$ be composite and $n > 4$. Prove that $(n-1)! \equiv 0 (\mathrm{mod}\ n)$.*

Exercise 3.5.2 *Prove that a natural number is modulo 9 equal to the sum of its digits.*

Exercise 3.5.3 *Prove that any palindromic number of even length is divisible by 11. (A palindromic number is a number that looks the same whether you read from right to left or from left to right).*

Exercise 3.5.4 *Determine the inverse of the following three residue classes:* $5 (\mathrm{mod}\ 7)$, $11 (\mathrm{mod}\ 71)$, $86 (\mathrm{mod}\ 183)$.

Exercise 3.5.5 *A flea jumps back and forth between the numerals on the face of a clock. It is only able to make jumps of length 7. At a certain moment the flea is located at the numeral I. What is the smallest number of jumps required to reach XII?*

Exercise 3.5.6 *Determine all $x, y, z \in \mathbb{Z}$ such that*

a) $x \equiv 3 (\mathrm{mod}\ 4) \qquad x \equiv 5 (\mathrm{mod}\ 21) \qquad x \equiv 7 (\mathrm{mod}\ 25)$

b) $3y \equiv 9 (\mathrm{mod}\ 12) \qquad 4y \equiv 5 (\mathrm{mod}\ 35) \qquad 6y \equiv 2 (\mathrm{mod}\ 11)$

c) $z \equiv 1 (\mathrm{mod}\ 12) \qquad z \equiv 4 (\mathrm{mod}\ 21) \qquad z \equiv 18 (\mathrm{mod}\ 35)$.

Exercise 3.5.7 *Determine all integral multiples of 7 which, after division by 2,3,4,5 and 6 yield the remainders 1,2,3,4 and 5 respectively.*

Exercise 3.5.8 *Prove that there exist a million consecutive positive integers, each of which is divisible by a square larger than* 1.

Exercise 3.5.9 *Notice that* $376^2 \equiv 376 (\mathrm{mod}\ 10^3)$, $90625^2 \equiv 90625 (\mathrm{mod}\ 10^5)$.
a) Let $k \in \mathbb{N}$. How many solutions $a \in \mathbb{Z}$ with $1 < a < 10^k$ does $a^2 \equiv a (\mathrm{mod}\ 10^k)$ have?
b) Solve the equation in a) for $k = 12$.

Exercise 3.5.10 *For which $n \in \mathbb{N}$ does the number n^n end with* 3 *in its decimal expansion?*

Exercise 3.5.11 *(XXI^{st} International Mathematics Olympiad 1979). Let $N, M \in \mathbb{N}$ be such that $(N, M) = 1$ and*

$$\frac{N}{M} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{1}{1317} - \frac{1}{1318} + \frac{1}{1319}.$$

Show that 1979 divides N. Generalise this.

Exercise 3.5.12 *Write the explicit isomorphism between* $\mathbb{Z}/10\mathbb{Z}$ *and* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Exercise 3.5.13 *a) Prove that* $13|(4^{2^{2n+1}} - 3) \quad \forall n \in \mathbb{N}$.
b) Prove that $37 \not| x^{9^9} + 4 \quad \forall x \in \mathbb{N}$.

Exercise 3.5.14 *Suppose* $m = p_1^{k_1} \cdots p_r^{k_r}$ *with* p_i *distinct primes and* $k_i \geq 1$ $\forall i$. *Put*

$$\lambda(m) = \text{lcm}[p_1^{k_1-1}(p_1 - 1), \ldots, p_r^{k_r-1}(p_r - 1)].$$

Show that $a^{\lambda(n)} \equiv 1 (\text{mod } n)$ *for all* a *such that* $(a, n) = 1$.

Exercise 3.5.15 *Show that* $n^{13} \equiv n (\text{mod } 2730)$ *for all* $n \in \mathbb{Z}$.

Exercise 3.5.16 *For which odd primes* p *is* $(2^{p-1} - 1)/p$ *a square ?*

Exercise 3.5.17 *Let* p *be a prime such that* $p \equiv 1 (\text{mod } 4)$. *Prove, using Wilson's theorem, that* $((p-1)/2)!)^2 \equiv -1 (\text{mod } p)$.

Exercise 3.5.18 *Is the following statement true: every positive integer, written out decimally, is either prime or can be made into a prime by changing one digit.*

Exercise 3.5.19 *Find a prime divisor of* 1111111111111 *and of* $111\ldots111$ *(79 ones).*

Exercise 3.5.20 *Prove that for all* $a, n \in \mathbb{N}$ *with* $a \neq 1$ *we have* $n|\phi(a^n - 1)$.

Exercise 3.5.21 *Prove that* $\phi(n) \to \infty$ *as* $n \to \infty$.

Exercise 3.5.22 *(H.W.Lenstra jr.) Let* $N = 16842752$.
a) Find an even $n \in \mathbb{N}$ *such that* $\phi(n) = N$.
b) Prove that there is no odd number $n \in \mathbb{N}$ *such that* $\phi(n) = N$.
c) Let $1 \leq k \leq 31$. *Construct an odd* $m \in \mathbb{N}$ *such that* $\phi(m) = 2^k$.

Exercise 3.5.23 *Prove that for all* $n \geq 2$,

$$\sum_{\substack{m=1 \\ (m,n)=1}}^{n-1} m = \frac{1}{2} n\phi(n).$$

Exercise 3.5.24 *Prove that*

$$\sum_{d|n} (-1)^{n/d} \phi(d) = \begin{cases} 0 \text{ if } n \in \mathbb{N} \text{ is even} \\ -n \text{ if } n \in \mathbb{N} \text{ is odd} \end{cases}$$

Exercise 3.5.25 *a) Determine all solutions to* $\phi(n) = 24$.
b) Show that there are no solutions to $\phi(n) = 14$.

Exercise 3.5.26 *Given* $a \in \mathbb{N}$ *characterise all* $n \in \mathbb{N}$ *such that* $\phi(n)/n = \phi(a)/a$.

Exercise 3.5.27 *Determine all* $n \in \mathbb{N}$ *such that* $\phi(n)|n$.

Exercise 3.5.28 *Compute the orders of* $5 \pmod 7$, $3 \pmod{46}$, $26 \pmod{17}$ *in the multiplicative groups mod* m.

Exercise 3.5.29 *Determine all primes such that thet period of the decimal expansion of* $1/p$ *is*

a) at most 6

b) precisely 7

c) precisely 8.

Exercise 3.5.30 *Let* p *be an odd prime and* q *a prime divisor of* $2^p - 1$. *Prove that* $q = 2mp + 1$ *for some* $m \in \mathbb{N}$.

Exercise 3.5.31 *Let* $n \in \mathbb{N}$, $a \in \mathbb{Z}$ *and* q *an odd prime divisor of* $a^{2^n} + 1$.
a) Prove that $q = m \cdot 2^{n+1} + 1$ *for some* $m \in \mathbb{N}$.
b) Prove that for any $n \in \mathbb{N}$ *there exist infinitely many primes of the form* $p \equiv 1 \pmod{2^n}$.

Exercise 3.5.32 *Let* q *be an odd prime and* $n \in \mathbb{N}$. *Show that any prime divisor* p *of* $n^{q-1} + \cdots + n + 1$ *satisfies either* $p \equiv 1 \pmod q$ *or* $p = q$. *Using this fact show that there exist infinitely many primes which are* 1 *modulo* q.

Exercise 3.5.33 *Determine all primitive roots modulo 11. Determine all primitive roots modulo 121.*

Exercise 3.5.34 *a) Determine all primitive roots modulo 13, 14 and 15 respectively.*
b) Solve the following equations: $x^5 \equiv 7 \pmod{13}$, $x^5 \equiv 11 \pmod{14}$, $x^5 \equiv 2 \pmod{15}$.

Exercise 3.5.35 *Suppose that* $(\mathbb{Z}/m\mathbb{Z})^*$ *is cyclic. Prove that* $m = 2, 4, p^k$ or $2p^k$, *where* p *is an odd prime and* $k \in \mathbb{N}$. *(Hint: use Exercise 3.5.14)*

Exercise 3.5.36 *Suppose that* p *and* $q = 2p + 1$ *are odd primes. Prove that* $(-1)^{\frac{p-1}{2}} 2$ *is a primitive root modulo* q.

Exercise 3.5.37 *Show that* $2^{2^t} - 1$ *is divisible by at least* t *distinct primes.*

Exercise 3.5.38 *In the decimal expansion of* $1/5681$ *the* 99*-th digit after the decimal point is a* 0*. Prove this.*

Exercise 3.5.39 *What is the* 840*-th digit after the decimal point in the decimal expansion of* $1/30073$*?*

Exercise 3.5.40 *What is the* 165*-th digit after the decimal point in the decimal expansion of* $1/161$*?*

Exercise 3.5.41 *(Lehmer's prime test). Let* $a, n \in \mathbb{N}$ *be such that*

$$a^{n-1} \equiv 1 (\text{mod } n) \quad \text{and} \quad a^{\frac{n-1}{p}} \not\equiv 1 (\text{mod } n) \quad \forall \text{primes } p | (n-1).$$

Prove that n *is prime.*

Exercise 3.5.42 *Use Lehmer's test to prove that* $3 \cdot 2^8 + 1$ *is prime. (Hint:use* $a = 11$*). Notice that Lehmer's test is very suitable for numbers such as* $h \cdot 2^k + 1$ *when* h *is small.*

Chapter 4

Primality and factorisation

4.1 Prime tests and compositeness tests

It is well known that one can find the prime factorisation of a numbers N by the naive method of trying all numbers below $\sqrt{N}$ as divisor. It is also known that it is extremely time-consuming to factor any number with more than 10 digits in this way. As an example, try to factor $N = 204906161249$ in this way by hand! When the number of digits of N exceeds 20 digits this naive method consumes hours of computer time, even on a fast PC. During the last 20 years powerful new methods have been developed to factorise large numbers more efficiently. A recent success has been the factorisation of the Fermat number $2^{512} + 1$, which is now, and probably for a long time to be, the largest Fermat number of which we know the complete prime factorisation. Nowadays (around 2012) numbers of about 200 digits can be factored fairly routinely. Before one tries to factor a number however, it makes sense to check first whether it is prime. Such primality tests have been developed as well and using routine methods on a supercomputer one can test primality of numbers up to 1000 digits. In this section we describe a few simple tests which are in practice very efficient and can be programmed easily on a PC.
Consider our number N again. We would like to know whether it is prime or not. Again, the naive method of trying all numbers below $\sqrt{N}$ as divisor becomes impossible if N contains more than 20 digits. The new idea is to use the following contrapositive to Fermat's little theorem.

Theorem 4.1.1 *Let $N \in \mathbb{N}$ and let $a \in \mathbb{Z}$ be such that N does not divide a. Then,*

$$a^{N-1} \not\equiv 1 (\text{mod } N) \Longrightarrow N \text{ is composite.}$$

So, given N, pick any a not divisible by N and perform the above test. However, before trying to apply this test, it is sensible to check whether $(a, N) = 1$. If not, N is of course composite and we have also found a divisor. In that case there is

no need to test N any further. As an example of the evaluation of $a^{N-1} (\mathrm{mod}\ N)$, take $a = 2$ and $N = 204906161249$. The computation of $2^{N-1} \bmod N$ may seem formidable at first sight, but with a little thought it can be done very efficiently. To do this write $N - 1$ in base 2,

$$N - 1 = 10111110110101010111110010001100000.$$

We perform a number of squaring operations and multiplications by 2 in such a way, that we try to form the binary expansion of $N - 1$ in the exponent of 2 as we go along,

$$\begin{aligned} 2^1 &\equiv 2 (\mathrm{mod}\ N) \\ 2^{10} &\equiv 2^2 \equiv 4 (\mathrm{mod}\ N) \\ 2^{101} &\equiv 2 \cdot 4^2 \equiv 32 (\mathrm{mod}\ N) \\ 2^{1011} &\equiv 2 \cdot 32^2 \equiv 2048 (\mathrm{mod}\ N) \\ &\cdots \\ 2^{N-1} &\equiv 201135347146 (\mathrm{mod}\ N). \end{aligned}$$

The number of steps required by this method is precisely the number of binary digits of $N - 1$ which is proportional to $\log N$. For large N this is extremely small compared to the $\sqrt{N}$ steps required by the naive method. By the way, we see that $2^{N-1} \not\equiv 1 (\mathrm{mod}\ N)$, hence N is composite (it will turn out that $N = 369181 \times 555029$). So Theorem 4.1.1 can be considered as a compositeness test. What to do if we had found $2^{N-1} \equiv 1 (\mathrm{mod}\ N)$ instead? We cannot conclude that N is prime. We have for example $2^{560} \equiv 1 (\mathrm{mod}\ 561)$, whereas $561 = 3 \cdot 11 \cdot 17$. But we can always choose other a and repeat the test. If $a^{N-1} \equiv 1 (\mathrm{mod}\ N)$ for several a, we still cannot conclude that N is prime. It is becoming more likely, but not 100% certain. In fact there exist N such that $a^{N-1} \equiv 1 (\mathrm{mod}\ N)$ for all a with $(a, N) = 1$. These are the so-called *Carmichael numbers*. Examples are $561, 1729, 294409, \ldots$. There exist 2163 Carmichael numbers below $25 \cdot 10^9$. It was an exciting surprise when Granville, Pomerance and Red Alford showed around 1991 that there exist infinitely many of them.
A criterion which gives better chances (but not certainty) in recognising primes is based on the following refinement of Fermat's little theorem.

Theorem 4.1.2 *Let p be an odd number and $a \in \mathbb{Z}$ such that $p \not| a$. Write $p - 1 = 2^k \cdot m$ with m odd and $k \geq 0$. Suppose p is prime. Then,*

$$\textit{either } a^m \equiv 1 (\mathrm{mod}\ p)$$

$$\textit{or } \exists i \textit{ such that } a^{2^i \cdot m} \equiv -1 (\mathrm{mod}\ p) \textit{ and } 0 \leq i \leq k - 1.$$

Proof. Since p is prime we know that

$$a^{p-1} \equiv a^{2^k \cdot m} \equiv 1 (\mathrm{mod}\ p).$$

Suppose that $a^m \not\equiv 1 (\mathrm{mod}\ p)$. Let r be the smallest non-negative integer such that $a^{2^r \cdot m} \equiv 1 (\mathrm{mod}\ p)$. Notice that $1 \leq r \leq k$. Then $a^{2^{r-1} \cdot m} \equiv \pm 1 (\mathrm{mod}\ p)$. By the minimality of r we cannot have $a^{2^{r-1} \cdot m} \equiv 1 (\mathrm{mod}\ p)$. Hence $a^{2^{r-1} \cdot m} \equiv -1 (\mathrm{mod}\ p)$ and since $0 \leq r-1 \leq k-1$ our assertion follows. □

The contrapositive statement can be formulated as follows.

Theorem 4.1.3 (Rabin test) *Let $N \in \mathbb{N}$ be odd and $a \in \mathbb{Z}$ such that $N \not| a$. Write $N - 1 = 2^k \cdot m$ with $k \geq 0$ and m odd. If*

$$a^m \not\equiv 1 (\mathrm{mod}\ N) \quad \textit{and} \quad \forall_{0 \leq i \leq k-1} : a^{2^i \cdot m} \not\equiv -1 (\mathrm{mod}\ N) \tag{4.1}$$

then N is composite.

If a satisfies property (4.1) we shall call a a *witness* to the compositeness of N. Unlike the converse to Fermat's little theorem the Rabin test allows no Carmichael-like numbers N. This is garantueed by the following theorem

Theorem 4.1.4 *Let $N \in \mathbb{N}$ be odd and composite. Among the integers between 1 and N at least 75% is a witness to the compositeness of N.*

Proof. It suffices to prove that at least 75% of the numbers in $(\mathbb{Z}/N\mathbb{Z})^*$ is a witness. We shall do this for all $N \neq 9$. For $N = 9$ the theorem is directly verified by hand. Let S be the union of the solution sets of the equations $x^m \equiv 1 (\mathrm{mod}\ N)$ and $x^{2^i \cdot m} \equiv -1 (\mathrm{mod}\ N) (i = 0, \ldots, k-1)$ respectively. It suffices to show that $|S|$ is at most $\phi(N)/4$.
Let j be the largest number with $0 \leq j \leq k-1$ such that $x^{2^j \cdot m} \equiv -1 (\mathrm{mod}\ N)$ has a solution. Such a j exists since we have trivially $(-1)^m \equiv -1 (\mathrm{mod}\ N)$. Notice that S is contained in the set of solutions of $x^{2^j \cdot m} \equiv \pm 1 (\mathrm{mod}\ N)$. Now apply Lemma 4.1.5 to see that there are at most $\phi(N)/4$ such solutions. □

Lemma 4.1.5 *Let N be an odd composite positive integer, not equal to 9. Let $M | (N-1)/2$. Suppose that $x^M \equiv -1 (\mathrm{mod}\ N)$ has a solution x_0. Then the number of solutions to $x^M \equiv \pm 1 (\mathrm{mod}\ N)$ in $x \in (\mathbb{Z}/N\mathbb{Z})^*$ is less than or equal to $\phi(N)/4$.*

Proof. Let $N = p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorisation of N. Notice that the number of solutions to $x^M \equiv 1 (\mathrm{mod}\ N)$ equals the numbers of solutions to $x^M \equiv -1 (\mathrm{mod}\ N)$, a bijection being given by $x \mapsto x x_0 (\mathrm{mod}\ N)$. The total number of solutions is equal to

$$2 \prod_i (M, p_i^{k_i - 1}(p_i - 1)) = 2 \prod_i (M, p_i - 1).$$

The equality follows from the fact that, since $M | (N-1)$, prime factors of N cannot divide M. For every prime p dividing N we know that $x^M \equiv -1 (\mathrm{mod}\ p)$

has a solution, hence $\mathrm{ord}(x)$ divides $2M$ but not M. This implies $(M, p-1) = \mathrm{ord}(x)/2 \leq (p-1)/2$.
Suppose that N has at least three distinct prime factors. Then,

$$2\prod_i (M, p_i - 1) \leq 2\prod_i \frac{p_i - 1}{2} \leq \frac{1}{4}\prod_i (p_i - 1) \leq \frac{\phi(N)}{4}.$$

Suppose that N has precisely two distinct prime factors, p and q say. First suppose that $N = pq$. There exist $e, f \in \mathbb{N}$ such that $p - 1 = 2e(M, p-1)$ and $q - 1 = 2f(M, q-1)$. Suppose $e = f = 1$. From $e = 1$ follows that $(p-1)/2$ divides M which in its turn divides $(N-1)/2 = (pq-1)/2$. Hence $(p-1)/2$ divides $(q-1)/2$. Similarly it follows from $f = 1$ that $(q-1)/2$ divides $(p-1)/2$. Hence $p = q$, which is impossible. So we must assume $ef \geq 2$. But then,

$$2(M, p-1)(M, q-1) = 2\frac{(p-1)(q-1)}{4ef} \leq \frac{(p-1)(q-1)}{4} = \frac{\phi(N)}{4}.$$

Now suppose that N has two primes p, q and is divisible by p^2, say. Then,

$$2(M, p-1)(M, q-1) \leq \frac{2(p-1)(q-1)}{4} \leq \frac{\phi(N)}{2p} \leq \frac{\phi(N)}{4}.$$

Finally suppose that N is a prime power, $p^k,\ k \geq 2$. Then, since $p^{k-1} \geq 4$,

$$2(M, p-1) \leq (p-1) \leq \frac{\phi(N)}{p^{k-1}} \leq \frac{\phi(N)}{4}.$$

□

In practice we choose a arbitrarily and apply Rabin's test. Suppose that N is composite. Let us assume that the witnesses to the compositeness of a are distributed more or less randomly, which does not seem to be unreasonable. Then, according to Theorem 4.1.3 the chance that N will not be recognised as composite is less than $1/4$. This means that after a 100, say, of such trials the chance that N is not recognised as composite is less than $(1/4)^{100}$, very small indeed. So, alternatively, if a number N is not recognised as composite after a 100 trials, the likelyhood that it is prime is practically 1!
Under the assumption of a certain conjecture Rabin's test can be made into a fullfledged primality test.

Theorem 4.1.6 *Let N be a composite number. If the Generalised Riemann Hypothesis (GRH) is true, then there is witness to the compositeness of N which is smaller than $2(\log N)^2$.*

In other words, under the assumption of GRH, if N has no witness below $2(\log N)^2$ then it is prime. This is known as the Rabin-Miller test and its run-time has the pleasant property of being polynomial in the length of the input (i.e. polynomial in $\log N$). Unfortunately, there is not much hope of proving the GRH yet.
A nice primality test is the following.

Theorem 4.1.7 (Lehmer) *Let $N \in \mathbb{N}$. Suppose that we have a number a such that*

- $a^{N-1} \equiv 1 (\text{mod } N)$
- $a^{(N-1)/q} \not\equiv 1 (\text{mod } N)$ *for every prime q dividing $N-1$.*

Then N is prime.

Proof. Let k be the order of $a (\text{mod } N)$. From the first property it follows that k divides $N-1$. Suppose that k equals $N-1$. Then we conclude that $\phi(N) \geq N-1$ and this is only possible if N is prime. So we are done when $k = N-1$.
Now suppose $k < N-1$. Then there exists a prime divisor p of $N-1$ such that $a^{(N-1)/p} \equiv 1 (\text{mod } N)$. But this contradicts our second assumption on a. So $k < N-1$ cannot occur. □

For numbers of a very special form there may exist very powerful primality tests tailored to the special circumstances. We mention here the *Fermat numbers* $2^{2^n}+1$ and the *Mersenne numbers* $2^n - 1$. The following theorem can be seen as a very special case of Lehmer's test where $N-1$ has only prime factors 2. It turns out that $a = 3$ has the desired properties.

Theorem 4.1.8 (Pepin, 1877) *Let $n \in \mathbb{N}$ and $F_n = 2^{2^n}+1$. Then,*

$$F_n \text{ is prime} \Leftrightarrow 3^{\frac{F_n-1}{2}} \equiv -1 (\text{mod } F_n).$$

Theorem 4.1.9 (Lucas, 1876) *Let $M_n = 2^n - 1$. Consider the sequence $S_1, S_2, S_3, \ldots$ given by $S_1 = 4$ and $S_k = S_{k-1}^2 - 2$ for all $k \geq 2$. Then,*

$$M_n \text{ is prime} \Leftrightarrow S_{n-1} \equiv 0 (\text{mod } M_n).$$

The proofs of these theorems are given in the chapter on quadratic reciprocity.
It turns out that F_1, F_2, F_3, F_4 are prime. This led Fermat to believe that all numbers F_n are prime. Ironically it turns out that F_n is composite for $n = 5, 6, \ldots, 22$ and many other n. It is not even known whether F_n is prime for any $n > 4$. Here is a list of factorisations of F_n for $5 \leq n \leq 9$,

$$\begin{aligned}
F_5 &= 641 \cdot 6700417 \text{ (Euler, 1732)} \\
F_6 &= 274177 \cdot 67280421310721 \text{ (Landry, Le Lasseur, 1880)} \\
F_7 &= 59649589127497217 \cdot \\
&\quad \cdot 5704689200685129054721 \text{ (Morrison, Brillhart, 1974)} \\
F_8 &= 1238926361552897 \cdot \\
&\quad \cdot (93461639715357977769163558199606896584051237541638188580280321) \text{ (Brent, Pollard, 1980)}
\end{aligned}$$

$$\begin{aligned} F_9 &= 2424833 \cdot \\ &\cdot 7455602825647884208337395736200454918783366342657 \cdot \\ &\cdot (741640062675308015247871419019374740599407810975 1 \\ &\ 9023905821316144415759504705008092818711693940737) \\ &(\text{Lenstra, Manasse, 1990}) \end{aligned}$$

In 1644 The French monk Marin Mersenne stated that $2^n - 1$ is prime for the values

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

and composite for all other $n < 257$. It was clear that Mersenne had not tested all these numbers. It was only in 1750 when Euler verified that $2^{31} - 1$ is prime. It also turned out that Mersenne was wrong about $n = 67, 257$ and that he had forgotten to add $n = 61, 89, 107$ to his list. The number $2^{127} - 1$ was proven to be prime in 1876 by Lucas and until 1952 this remained the largest known prime. For further details and more on prime numbers see the Web page `primes.utm.edu`. For the following values of n the number M_n is now (2013) known to be prime:

$$\begin{aligned} n = \quad & 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, \\ & 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, \\ & 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, \\ & 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, \\ & 20996011, 24036583, 25964951, 30402457, 32582657, \\ & 37156667, 42643801, 43112609, 57885161 \end{aligned}$$

At the moment (2013) $2^{57885161} - 1$ is the largest known prime.
For the latest news on search activities see: `primes.utm.edu/mersenne/` or `www.mersenne.org`.

4.2 A polynomial time primality test

In recent years, starting from the 1980's, several powerful primality tests have been invented. We mention the test of Adleman,Rumely,Lenstra and Cohen, which uses Gauss sums (see the chapter on Gauss sums) and tests which use the addition structure on elliptic curves and abelian varieties. These methods are still used in practice.
Despite all these ingeneous developments it still was not clear whether there exists a primality test whose runtime is polynomial in the number of digits of the number to be tested. This changed in July 2002. An Indian computer scientist, M.Agrawal and two of his students, N.Kayal and N.Saxena, had discovered a polynomial time primality test. This was a historical breakthrough in the theory of factorisation and primality proving. Another remarkable feature of their

discovery was its elementary nature. The original ingredients were some modular arithmetic with polynomials and a deep theorem in analytic number theory. However, through the efforts of H.W.Lenstra jr, the analytic number theory part has been replaced by a property of prime numbers which will actually be proved in these course notes.
To show that the algorithm is quite simple we give it here is pseudo-code.
Input: integer $n > 1$

1. If $n = a^b$ for $a \in \mathbb{N}$ and $b > 1$:
   output *Composite*

2. Find the smallest $r \in \mathbb{N}$ such that $\text{ord}_r(n) > 4(\log n)^2$.

3. If $1 < \gcd(a, n) < n$ for some $a \leq r$:
   output *Composite*

4. If $n \leq r$, output *Prime*

5. For $a = 1$ to $[2\sqrt{\phi(r)}\log n]$ do
   If $(X + a)^n \neq X^n + a (\text{mod } X^r - 1, n)$:
   output *Composite*

6. output *Prime*

Here is a *proof* for the correctness of the algorithm. In Step 1. it is clear that if $n = a^b$ with $b > 1$, then n is composite. Furthermore, in Step 3 it is clear that if $\gcd(a, n)$ is not 1 or n, the number n is composite. For Step 5 we remark that if n is prime, then $(X + a)^n \equiv X^n + a (\text{mod } n)$ for all integers a. So, a fortiori, $(X + a)^n \equiv X^n + a (\text{mod } X^r - 1, n)$ for all r and a. If this condition is violated for some a, r, then of course n cannot be prime.
The main point is now to show that if $(X + a)^n \equiv X^n + a (\text{mod } X^r - 1, n)$ for our chosen r and all a between 1 and $[2\sqrt{\phi(r)}\log n]$, then n is prime.

4.3 Factorisation methods

The test of Rabin, described in the previous section, enables one to decide compositeness of a number N without knowing anything about the prime decomposition of N. In this section we make a few remarks about the problem of factoring numbers. First of all, factoring a number is much harder than proving its compositeness. Another feature of factorisation algorithms is that they mostly give a positive chance of success, but not certainty. Factorisation methods with 100% of success are the naive method and the algorithm of Sherman-Lehman. However they are both very slow with runtimes $O(N^{1/2})$ and $O(N^{1/3})$ respectively. One therefore prefers the probabilistic methods with the filosophy that if you happen

to find a factorisation of a large number you don't complain about how it was found. As an example of such a factorisation method we sketch the *Pollard rho algorithm*. It works very well on a PC for numbers up to 25 digits.
The Pollard rho method. Choose $b \in \mathbb{Z}$ and $b \neq 0, -2$. Compute the numbers $x_0, x_1, x_2, \ldots$ by

$$x_0 = 1 \text{ and } x_{k+1} \equiv x_k^2 + b (\text{mod } N) \text{ for } k \geq 0 \tag{4.2}$$

For each k check whether

$$N > \gcd(x_k - x_l, N) > 1 \tag{4.3}$$

for some $l < k$. If condition (4.3) is fulfilled we have actually found a factor of N. Let p be a prime divisor of N. We assert that *the probability to find p using this algorithm with $k < \sqrt{2p}$ is larger than* $1/2$. Since a composite number N always has a prime divisor $< \sqrt{N}$, the expected run-time of our algorithm is therefore $O(N^{1/4})$.
Here is a heuristic argument which supports our assertion. Consider the sequence $x_0, x_1, x_2, \ldots$ modulo p. Then practical experience suggests that if $b \neq 0, -2$, this sequence behaves randomly modulo p. People are unable to prove this but it seems like a good principle. Let $q \in \mathbb{N}$. Being a random sequence, the probability that the elements $x_0, x_1, \ldots, x_q \bmod p$ are all distinct is

$$(1 - \frac{1}{p})(1 - \frac{2}{p}) \cdots (1 - \frac{q}{p}).$$

Suppose that $q > \sqrt{2p}$. Then

$$\begin{aligned} \log(1 - \frac{1}{p})(1 - \frac{2}{p}) \cdots (1 - \frac{q}{p}) &= \sum_{r=1}^{q} \log(1 - \frac{r}{p}) \\ &\simeq -\sum_{r=1}^{q} \frac{r}{p} \\ &= -\frac{1}{2}\frac{q(q+1)}{p} < -1 \end{aligned}$$

and the probability that $x_0, \ldots, x_q \bmod p$ are distinct is less than $e^{-1} < 1/2$. So, when $q > \sqrt{2p}$ the probality that two elements in $x_0, \ldots, x_q \bmod p$ are equal is larger than $1/2$. In other words, if we are moderately lucky we will find $0 \leq l < k \leq \sqrt{2p}$ such that $x_k \equiv x_l (\text{mod } p)$. Note by the way, that the above argument is an example of the so-called birthday paradox.
If we carry out the algorithm as described above, we would have to store the elements x_i of our sequence to verify (4.3). Moreover, testing all $l < k$ with

respect to $(N, x_k - x_l)$ would considerably slow down the algorithm. In practice there are two ways to overcome this problem.

The first is to compute x_i and x_{2i} simultaneously at every step. Suppose there exist $l < k < \sqrt{2p}$ satisfying $x_k \equiv x_l (\mathrm{mod}\ p)$. By its very construction, the sequence $\{x_i \bmod p\}_{i=0}^{\infty}$ will be periodic from the index l onward with period $k-l$. In particular, choose $M \in \mathbb{N}$ such that $k > M(k-l) \geq l$. Then we have by the periodicity, $x_{2M(k-l)} \equiv x_{M(k-l)} (\mathrm{mod}\ p)$ and we find that $p|(x_{2i} - x_i, N)$ for $i = M(k-l)$. Notice that $i = M(k-l) < k < \sqrt{2p}$.

A second option is to compute the sequence of $x_i (\mathrm{mod}\ N)$ and whenever we hit upon i being a power of 2 we save it as the number A. At every iteration we check whether $1 < \gcd(x_i - A) < N$. Suppose that from the index l onward the sequence $x_i (\mathrm{mod}\ p)$ becomes periodic with period $k-l$. Choose r minimal such that $2^r \geq \max l, k-l$, then there exists i with $i < 2^{r+1}$ such that $x_i - x_{2^r} \equiv x_i - A \equiv 0 (\mathrm{mod}\ p)$.

It should also be noted that instead of $x_{k+1} = x_k^2 + b$ we could have chosen any other recurrence which has a chance of producing random sequences modulo N. Our choice is simply the simplest we could think of.

In many large factorisation programs one factors out small prime factors by native trial division for primes up to 10^9, say. As a second step one often uses the Pollard rho method to find moderately small prime factors up to, say 10^{14}.

The factorisation algorithms which are the most powerful at the moment (2006) are the quadratic sieve of Pomerance (1984, to be discussed in the next section), the elliptic curve method of Lenstra (1984), the Number Field Sieve (1990) by the Lenstra's, Manasse and Pollard and variations on these methods. Typically, these methods do not garantuee 100% success in factoring a number, and their run-time analysis is again based on probability arguments. But most of the time they are very successful.

4.4 The quadratic sieve

From time to time even Fermat was forced to factor large numbers during his calculations. Of course he also stumbled upon the near impossibility of fcatoring large numbers. However, Fermat did make a few observations which enabled his to factor certain large numbers quickly. One such example is $N = 8051$. Fermat noticed that this is the difference of two squares, $8051 = 90^2 - 7^2$ and he got $8051 = (90-7)(90+7) = 83 \cdot 97$.

This idea can be formalised as follows, which we call the *method of Fermat*. Choose $r = [\sqrt{N}]$ and test if one of the numbers $(r+1)^2 - N, (r+2)^2 - N, (r+3)^2 - N, \ldots$ is a square. If this is the case, say $(r+k)^2 - N = m^2$ then we have $N = (r+k)^2 - m^2 = (r+k-m)(r+k+m)$ and thus a factorisation. The difference between the factors is $2m$. This means that if $N = ab$ with $a < b$, then

$m = (b-a)/2$. Hence

$$k = b - m - r = b - (b-a)/2 - [\sqrt{N}] < (a+b)/2 - \sqrt{ab} + 1 = 1 + (\sqrt{b} - \sqrt{a})^2/2.$$

From this we see that Fermat's method cannot only work well if the difference between a and b is small. If one is lucky this occurs and in this way Fermat managed to factor numbers successfully. For example, the fcatorisation

$$2027651281 = 46061 \cdot 44021$$

was found in only 12 steps. Unfortunately, for large differences Fermat's method fails completely. It may even be worse than naive factorisation.
In the history of number factoring there are many variations on Fermat's method. They all come down to the construction, in one way or another, of two integers x and y such that $x^2 \equiv y^2 (\text{mod } N)$. From the fact that

$$N = \gcd(N, x^2 - y^2) = \gcd(N, x-y)\gcd(N, x+y)$$

follows a possible non-trivial factorisation. The best method in this respect in C.Pomerance's *quadratic sieve* (1984). This method starts in the same way as Fermat's method. We choose $r = [\sqrt{N}] + 1$ and consider the numbers

$$(r+k)^2 - N \qquad k = 0, 1, 2, 3, \ldots$$

We cannot assume that N is the product of two numbers of comparable size, so we cannot expect to into a square very quickly. The idea however is that for small k the numbers $(r+k)^2 - N$ are small relative to N. More precisely,

$$(r+k)^2 - N < (\sqrt{N} + k)^2 - N = 2k\sqrt{N} + k^2.$$

For small k the order of magnitude is $k\sqrt{N}$. The philosophy is that smaller numbers have a better chance of containing small prime factors.
We choose a bound B and search for numbers $(r+k)^2 - N$ all of whose prime factors are $\leq B$. To improve our chances we also allow negative values of k. Here is an example. Take $N = 123889$. Then $r = [\sqrt{N}] + 1 = 352$ and $(r+k)^2 - N = 15 + 704k + k^2$. We choose $B = 13$ and try all $-20 \leq k \leq 20$. We find the following values of k for which $k^2 + 704k + 15$ consists of prime factors ≤ 13,

k	$k^2 + 704k + 15$
-19	$-2^3 \cdot 5^3 \cdot 13$
-17	$-2^4 \cdot 3^6$
-9	$-2^5 \cdot 3 \cdot 5 \cdot 13$
0	$3 \cdot 5$
1	$2^4 \cdot 3^2 \cdot 5$
7	$2^7 \cdot 3 \cdot 13$
15	$2^4 \cdot 3^3 \cdot 13$

The idea is now to choose factorisation on the right hand side such their product is a square. For example the products corresponding to $k = -19, -9, 15$ multiplied yield a square. Explicitly,

$$\begin{aligned}(r-19)^2 &\equiv -2^3 \cdot 5^3 \cdot 13 (\text{mod } N)\\ (r-9)^2 &\equiv -2^5 \cdot 3 \cdot 5 \cdot 13 (\text{mod } N)\\ (r+15)^2 &\equiv 2^4 \cdot 3^3 \cdot 5^2 (\text{mod } N)\end{aligned}$$

Multiplication of these congruences yields

$$(r-19)^2(r-9)^2(r+15)^2 \equiv (2^6 \cdot 3^2 \cdot 5^3 \cdot 13)^2 (\text{mod } N)$$

We have two different squares, equal modulo N. Let us see if this gives a factor of N,

$$\gcd(N, (r-19)(r-9)(r+15) - 2^6 \cdot 3^2 \cdot 5^3 \cdot 13) = \gcd(123889, 40982373) = 541$$

We were lucky and found $N = 541 \cdot 229$.
From this example the principle of the method can be deduced. We first find sufficiently many k so that $(r+k)^2 - N$ consists of prime factors $\leq B$. By sufficient we mean: at least two more values than the number of primes $\leq B$, preferably more. Linear algebra over $\mathbb{Z}/2\mathbb{Z}$ tells us that we can choose from these numbers a set whose product is a square. By taking this product modulo N we find a relation of the form $X^2 \equiv Y^2 (\text{mod } N)$, from which we hope to deduce a factorisation. The relationship with linear algebra can be seen from our example. The factorisation table we gave before can be depicted schematically as follows.

k	-1	2	3	5	7	11	13
-19	1	1	0	1	0	0	1
-17	1	0	0	0	0	0	0
-9	1	1	1	1	0	0	1
0	0	0	1	1	0	0	0
1	0	0	0	1	0	0	0
7	0	1	1	0	0	0	1
15	0	0	1	0	0	0	0

Notice that 7 and 11 do not occur in our factorisations. Finding factorsiations whose product is a square comes down to finding rows in our table whose sum is the zero-vector modulo 2. In other words, we must solve a system of linear equations over $\mathbb{Z}/2\mathbb{Z}$.
It has not been explained yet why this method is fast. A careful analysis, using deep heuristics from analytic number theory, shows that the expected runtime of the algorithm is $L(N)^c$ where

$$L(N) = \exp\left(\sqrt{\log(N)\log\log(N)}\right)$$

and $c = 2$. The reader can verify that $\lim_{N\to\infty} L(N)/N^\epsilon = 0$ for every $\epsilon > 0$. So the runtime is not exponential, we call this a sub-exponential algorithm.
One of the bottle-necks of the algorithm is that for each $(r+k)^2 - N$ it must be decided if it consists of prime factors $\leq B$. It was Pomerance's idea to replace this by a sieving process, hence the name quadratic sieve. We work with a sequence of number a_k which we initially choose to be $(r+k)^2 - N$. For every prime $p \leq B$ we do the following. Solve $(r+x)^2 \equiv N (\text{mod } p)$ and let x_1, x_2 be two solutions with $x_1 \not\equiv x_2 (\text{mod } p)$. For every k with with $k \equiv x_1, x_2 (\text{mod } p)$ we replace a_k by a_k/p. Having done all this, we pick those k fro which $a_k = \pm 1$. For these k the number $(r+k)^2 - N$ consists only of primes $\leq B$. Strictly speaking we must also sieve for higher powers of p, but we leave this aside for the sake of simplicity. The saving in runtime is tremendous, the runtime is now $L(N)$ instead of $L(N)^2$. As a rule of thumb we choose $B < L(N)^b$ and $|k| < L(N)^a$ for suitable $0.1 < a, b < 1$, depending on the implementation. A big advantage of the sieving technique is that it can be distributed easily over different machines. To give an idea, A.K.Lenstra's factorisation of RSA-129 (129 decimals) was distributed over 1600 computers, mostly workstations and PC's. The number of primes for which there was sieved was 524339, about half a million. The lienar algebra part was the solution of a system of linear equations modulo 2 in half a million variables. This work must be done on a central computer.

4.5 Cryptosystems, zero-knowledge proofs

An important recent application of large primes is the cryptosystem of Rivest, Shamir and Adleman (RSA-cryptosystem). This system consists of a *public encryption key*, by which anyone can encrypt messages or other information, and a *secret key* which one uses to decrypt these messages again. The important principle of the RSA-system is that one cannot deduce the secret key from the public key. Let us give a short description and explanation.
Choose two prime numbers p, q and let $N = pq$. Let $\lambda = \phi(N) = (p-1)(q-1)$. Destroy the prime numbers. Notice that

$$a^\lambda \equiv 1 (\text{mod } N) \qquad \forall a \; with \; (a, N) = 1.$$

Choose a $k, l \in \mathbb{N}$ such that $kl \equiv 1 (\text{mod } \lambda)$.
The public key consists of the numbers k and N, which may be advertised anywhere. The secret key consists of the numbers l and N, of which l is known only to the owner. Write $kl = 1 + m\lambda$. The *encryption* goes as follows. Transform the message into blocks of digits and consider them as numbers, of which we assume that they are smaller than N. Let T be such a block. The encoded form of T will be C determined by $C \equiv T^k (\text{mod } N)$. The *decryption* simply consists of determining C^l mod N, because $C^l \equiv T^{kl} \equiv T^{m\lambda+1} \equiv T (\text{mod } N)$.

Suppose we want to deduce the secret key l from the public key k. This could be done as follows. Factorise $N = pq$, determine $\lambda = (p-1)(q-1)$ and determine l by solving $kl \equiv 1 (\text{mod } \lambda)$. Notice that in order to determine λ we need the factorisation of N. No other methods are known. If however the secret primes p, q contain about 100 digits, factorisation of N with the known methods is practically impossible within a human or even universal lifetime. So the success of the RSA-cryptosystem is based on the apparent inability of mathematicians to factor large numbers.
Of course the above idea can be applied in the opposite direction. We then have the possibility of electronic signatures. Let us sketch a very simplified application. An individual, say Peter, makes or buys his own secret/public key pair. The public key is known to, say, a savings bank and the private key is securely guarded by Peter. Suppose Peter wants to transfer $10,000.- from the bank to a furniture shop electronically. He might write an electronic message saying "My name is Peter, please transfer $10,000.- to the account of furniture shop so and so". Unfortunately anyone could do this in Peter's name with undesirable consequences for Peter. The solution is that Peter encrypts his message with his private code and appends it to the message written in plain text. The bank then decodes the scrambled message with the public key and observes that the result corresponds with Peter's plain text. Since no one else but Peter could have encrypted the message succesfully, the bank is convinced of the validity of Peter's message and carries out his order.
Other applications of modular arithmetic and the near impossibility to factor large numbers are protocols by which one can prove that one possesses certain information, a password for example, without revealing that information. Such protocols are known as *zero-knowledge proofs*. . One such procedure, known as identity proof, has been devised by Goldwasser,Micali and Rackoff in 1985.
Suppose Vincent calls Vera over the telephone and Vincent wants to convince Vera that it is really him, which Vera must then verify. Of course Vincent can mention a password, only known to him and Vera, to identify himself. However, there is always the possibility of eavesdroppers. Another problem might be that Vincent considers Vera too sloppy to confide his password to. Both these problems are solved by using a zero-knowledge proof.
Just as above we let N be the product of two very large primes p and q. The secret password of Vincent, only known to him, is a number a between 1 and N. The name by which Vincent is known publicly is A, determined by $A \equiv a^2 (\text{mod } N)$ and $1 < A < N$. The identification protocol runs as follows. Vincent takes a random number x and sends the square $X \equiv x^2 (\text{mod } N)$ to Vera. Then Vera can ask either of two questions,

i. send x

ii. send ax

If Vincent is really Vincent he can of course do that and Vera can check that $x^2 \equiv X (\mathrm{mod}\ N)$ in case i) and that $(ax)^2 \equiv AX (\mathrm{mod}\ N)$ in case ii).
What if an impostor tries to pass himself as Vincent? Before sending anything he may try to guess Vera's question. If he guesses i) then he can take any x send X mod N and answer Vera's question with x. If he guesses ii) he can take any x, send $A^{-1}X$ mod N and answer Vera's question with x. In any case the chance for the imposter to make the right guess is 1/2. However, if this question and answer game is repeated a hundred times, say, the chance that the impostor is not exposed as a fraud is $(1/2)^{100}$. This is small enough for Vera to be convinced of Vincent's identity if all questions are answered correctly. Notice that in the process the value of a has not been revealed by Vincent.
Another possibility for the imposter is to infer Vincent's password a from A. He would have to solve $x^2 \equiv A (\mathrm{mod}\ N)$ and the only known way to do this is to solve the equivalent system $x^2 \equiv A (\mathrm{mod}\ p)$, $\quad x^2 \equiv A (\mathrm{mod}\ q)$. Taking square roots modulo a prime is doable in practice (see chapter on quadratic reciprocity) so it seems we are done. Unfortunately we need the factorisation of N again and this turns out to be the bottleneck in solving $x^2 \equiv A (\mathrm{mod}\ N)$. Again the safety of Vincent's password relies on our inability to factor very large numbers.

Chapter 5

Quadratic reciprocity

5.1 The Legendre symbol

In this chapter we shall consider quadratic equations in $\mathbb{Z}/m\mathbb{Z}$ and study an important criterion for the solubility of $x^2 \equiv a \bmod p$, where p is an odd prime (quadratic reciprocity).

Definition 5.1.1 *Let p be an odd prime and $a \in \mathbb{Z}$ not divisible by p. Then a is called a quadratic residue mod p if $x^2 \equiv a (\bmod\ p)$ has a solution and a quadratic nonresidue modulo p if $x^2 \equiv a (\bmod\ p)$ has no solution.*

Example. The quadratic residues modulo 13 read: 1,4,9,3,12,10 and the quadratic nonresidues : 2,5,6,7,8,11.

Definition 5.1.2 *Let p be an odd prime. The Legendre symbol is defined by*

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

Theorem 5.1.3 *Let p be an odd prime and $a, b \in \mathbb{Z}$. Then*

a) There are exactly $\frac{p-1}{2}$ quadratic residues mod p and $\frac{p-1}{2}$ quadratic nonresidues mod p.

b) (Euler)

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

c)

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

d)

$$\left(\frac{1}{p}\right) = 1, \qquad \left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 (\text{mod } 4) \\ -1 & \text{if } p \equiv -1 (\text{mod } 4) \end{cases}$$

Proof. Part a). Consider the residue classes $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ mod p. Since $a^2 \equiv (-a)^2 (\text{mod } p)$ these are all quadratic residues modulo p. They are also distinct, from $a^2 \equiv b^2 (\text{mod } p)$ would follow $a \equiv \pm b (\text{mod } p)$ and when $1 \leq a, b \leq \frac{p-1}{2}$ this implies $a = b$. So there are exactly $\frac{p-1}{2}$ quadratic residues modulo p. The remaining $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ residu classes are of course quadratic nonresidues . Part b) Clear if $a \equiv 0 (\text{mod } p)$. So assume $a \not\equiv 0 (\text{mod } p)$. Since $(a^{(p-1)/2})^2 \equiv a^{p-1} \equiv 1 (\text{mod } p)$ by Fermat's little theorem we see that $a^{(p-1)/2} \equiv \pm 1 (\text{mod } p)$. Suppose that a is a quadratic residue , i.e. $\exists x$ such that $x^2 \equiv a (\text{mod } p)$. Then $1 \equiv x^{p-1} \equiv (x^2)^{(p-1)/2} \equiv a^{(p-1)/2} (\text{mod } p)$, which proves half of our assertion. Since we work in the field $\mathbb{Z}/p\mathbb{Z}$, the equation $x^{(p-1)/2} \equiv 1 (\text{mod } p)$ has at most $\frac{p-1}{2}$ solutions. We know these solutions to be the $\frac{p-1}{2}$ quadratic residues . Hence $a^{(p-1)/2} \equiv -1 (\text{mod } p)$ for any quadratic nonresidue a mod p.
Part c)

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

Because Legendre symbols can only be $0, \pm 1$ and $p \geq 3$, the strict equality $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ follows.
Part d) Of course $\left(\frac{1}{p}\right) = 1$ is trivial. From part b) follows that $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} (\text{mod } p)$. Since $p \geq 3$ strict equality follows. □

5.2 Quadratic reciprocity

One might wonder for which prime numbers the numbers 3 and 5 ,say, are quadratic residue . Euler, Legendre and Gauss have occupied themselves with this question. For example it turns out that

$$\left(\frac{3}{p}\right) = 1 \text{ if } p \equiv \pm 1 (\text{mod } 12) \qquad \left(\frac{3}{p}\right) = -1 \text{ if } p \equiv \pm 5 (\text{mod } 12)$$

and

$$\left(\frac{5}{p}\right) = 1 \text{ if } p \equiv \pm 1 (\text{mod } 5) \qquad \left(\frac{5}{p}\right) = -1 \text{ if } p \equiv \pm 2 (\text{mod } 5).$$

Starting from such observations Euler conjectured the *quadratic reciprocity law* (see Theorem 5.2.6). Legendre gave an incomplete proof of it and later Gauss managed to give several complete proofs. In this chapter we give a proof which is basically a version given by Eisenstein. In the chapter on Gauss sums we shall give another proof.

Definition 5.2.1 *The residue classes* $1, 2, \ldots, \frac{p-1}{2} \bmod p$ *are called positive, the residue classes* $-1, -2, \ldots, -\frac{p-1}{2} \bmod p$ *are called negative.*

Theorem 5.2.2 (Gauss' Lemma) *Let* p *be an odd prime and* $a \in \mathbb{Z}$ *not divisible by* p*. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\mu}$$

where μ *is the number of negative residue classes from* $a, 2a, \ldots, \frac{p-1}{2}a \bmod p$*.*

Proof. Consider the $p-1$ residue classes $\pm a, \pm 2a, \ldots, \pm\frac{p-1}{2}a \bmod p$. They are non-zero and mutually distinct. So, the sets $\{\pm a, \pm 2a, \ldots, \pm\frac{p-1}{2}a\}$ and $\{\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\}$ are equal modulo p. Of each pair $\pm 1, \pm 2, \ldots, \pm\frac{p-1}{2} \bmod p$ exactly one element occurs in the sequence $a, 2a, \ldots, \frac{p-1}{2}a \bmod p$. Thus we find that

$$a \cdot 2a \cdots \frac{p-1}{2}a \equiv (-1)^{\mu} 1 \cdot 2 \cdots \frac{p-1}{2} (\text{mod } p)$$

and hence

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

After division by $(\frac{p-1}{2})!$ we obtain $a^{\frac{p-1}{2}} \equiv (-1)^{\mu} \bmod p$ and after using Theorem 5.1.3(b) we conclude that $\left(\frac{a}{p}\right) = (-1)^{\mu}$. □

Theorem 5.2.3 *Let* p *be an odd prime. Then*

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

Proof. We apply Gauss' lemma. To do so we must count μ, the number of negative residue classes among $2, 4, \ldots, p-1 \bmod p$. So,

$$\begin{aligned} \mu &= \#\{n \text{ even} | \ \frac{p+1}{2} \leq n \leq p-1\} \\ &= \#\{n | \ \frac{p+1}{4} \leq \ n \leq \frac{p-1}{2}\} \end{aligned}$$

Replace n by $\frac{p+1}{2} - n$ to obtain

$$\begin{aligned} \mu &= \#\{n \mid 1 \leq n \leq \frac{p+1}{4}\} \\ &= \left[\frac{p+1}{4}\right] \end{aligned}$$

This implies that μ is even if $p \equiv \pm 1 (\text{mod } 8)$ and μ is odd if $p \equiv \pm 3 (\text{mod } 8)$. Gauss' lemma now yields our assertion. □

Remark 5.2.4 *Notice that*

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

Another consequence of Gauss' lemma is the following lemma which will be needed in the proof of the quadratic reciprocity law.

Lemma 5.2.5 *Let p be an odd prime and $a \in \mathbb{Z}$ odd and not divisible by p. Define*

$$S(a,p) = \sum_{s=1}^{\frac{p-1}{2}} \left[\frac{as}{p}\right].$$

Then

$$\left(\frac{a}{p}\right) = (-1)^{S(a,p)}.$$

Proof. According to Gauss' lemma we have $\left(\frac{a}{p}\right) = (-1)^{\mu}$ where μ is the number of negative residue classes among $a, 2a, \ldots, \frac{p-1}{2}a \bmod p$. Let $1 \leq s \leq \frac{p-1}{2}$. If $sa \bmod p$ is a positive residue class we write $sa = [\frac{sa}{p}]p + u_s$ with $1 \leq u_s \leq \frac{p-1}{2}$. If $sa \bmod p$ is a negative residue class we write $sa = [\frac{sa}{p}]p + p - u_s$ with $1 \leq u_s \leq \frac{p-1}{2}$. A straightforward check shows that $\{u_1, u_2, \ldots, u_{\frac{p-1}{2}}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$. Addition of these equalities yields

$$\sum_{s=1}^{\frac{p-1}{2}} sa = p\sum_{s=1}^{\frac{p-1}{2}} \left[\frac{sa}{p}\right] + \mu p + \sum_{s=1}^{\frac{p-1}{2}} (\pm u_s).$$

Take both sides modulo 2,

$$\begin{aligned} \sum_{s=1}^{\frac{p-1}{2}} s &\equiv S(a,p) + \mu + \sum_{s=1}^{\frac{p-1}{2}} u_s \pmod 2 \\ &\equiv S(a,p) + \mu + \sum_{s=1}^{\frac{p-1}{2}} s \pmod 2. \end{aligned}$$

The summations on both sides cancel and we are left with $S(a,p) \equiv \mu \pmod 2$ hence $\left(\frac{a}{p}\right) = (-1)^{\mu} = (-1)^{S(a,p)}$. □

Theorem 5.2.6 (Quadratic reciprocity law) *Let p, q be two odd prime numbers. Then*

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

Alternatively $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ unless $p \equiv q \equiv -1 \pmod 4$, in which case we have $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Proof. Let $S(a,p)$ be as in Lemma 5.2.5. Then we assert

$$S(q,p)+S(p,q)=\frac{p-1}{2}\frac{q-1}{2}.$$

To see this, picture the rectangle $[0,p/2]\times[0,q/2]$ and the lattice points $(m,n)\in\mathbb{N}^2$ with $1\leq m\leq\frac{p-1}{2}$, $1\leq n\leq\frac{q-1}{2}$ inside it. The diagonal connecting $(0,0)$ and $(p/2,q/2)$ does not pass through any of the lattice points. Notice that the number of lattice points below the diagonal is precisely $S(q,p)$ and above the diagonal $S(p,q)$. In total there are $\frac{p-1}{2}\frac{q-1}{2}$ lattice points, hence our assertion follows.
We can now combine our assertion with Lemma 5.2.5 to obtain

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

□

5.3 A group theoretic proof

It is known that Gauss gave six (more or less) different proofs of the quadratic reciprocity law. Since then the number of proofs has increased dramatically to an estimated 200. The proof we have given above is essentially due to Eisenstein. In P.Bachmann, *Die Lehre von der Kreistheilung*, de Gruyter, Berlin, Leipzig, 1921 we find several classical proofs and we can find another 25 in O.Baumgart, *Über das quadratische Reciprocitätsgesetz*, Teubner, Berlin, 1885. In the article "On the quadratic reciprocity law" in J.Australian Math. Soc. 51(1991), 423-425 by G.Rousseau we find a proof of the reciprocity law which is surprisingly simple if one is acquainted with elementary group theory. It turns out to be an application of the chinese remainder theorem and we like to present it here.

Another proof of Theorem 5.2.6**.** Let notations be as in the theorem. We work in the group $G=((\mathbb{Z}/p\mathbb{Z})^*\times(\mathbb{Z}/q\mathbb{Z})^*)/U$ where $U=\{(1,1),(-1,-1)\}$. Clearly $\{(i,j)\mid i=1,2,\ldots,p-1;\ j=1,2,\ldots,(q-1)/2\}$ is a full set of representatives of G. Their product π equals

$$\pi\equiv((p-1)!^{(q-1)/2},((q-1)/2)!^{p-1}).$$

Since $((q-1)/2)!^2\equiv(-1)^{(q-1)/2}(q-1)!(\mathrm{mod}\ q)$ we get

$$\pi\equiv((p-1)!^{(q-1)/2},(-1)^{\frac{q-1}{2}\frac{p-1}{2}}(q-1)!^{(p-1)/2}).$$

Another full set of representatives of G is given by $\{(k(\mathrm{mod}\ p),k(\mathrm{mod}\ q))\mid k=1,2,\ldots,(pq-1)/2;\ (k,pq)=1\}$. This is a consequence of $(\mathbb{Z}/pq\mathbb{Z})^*\simeq(\mathbb{Z}/p\mathbb{Z})^*\times(\mathbb{Z}/q\mathbb{Z})^*$ (chinese remainder theorem). The product of these elements modulo p equals

$$\frac{\left(\prod_{i=1}^{p-1}i(p+i)(2p+i)\cdots(\frac{q-3}{2}p+i)\right)\prod_{i=1}^{(p-1)/2}(\frac{q-1}{2}p+i)}{1\cdot q\cdot 2q\cdots\frac{p-1}{2}q}$$

which equals

$$(p-1)!^{(q-1)/2}/q^{(p-1)/2} \equiv (p-1)!^{(q-1)/2} \left(\frac{q}{p}\right) (\text{mod } p).$$

Similarly we compute the product modulo q and we obtain

$$\pi \equiv \left((p-1)!^{(q-1)/2} \left(\frac{q}{p}\right),\ (q-1)!^{(p-1)/2} \left(\frac{p}{q}\right) \right).$$

Comparison of the two expressions for π yields

$$\left(1, (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right) \equiv \left(\left(\frac{q}{p}\right), \left(\frac{p}{q}\right) \right) \equiv \left(1, \left(\frac{q}{p}\right)\left(\frac{p}{q}\right)\right)$$

and hence the reciprocity law. □

5.4 Applications

Example 1. Is $x^2 \equiv 84 (\text{mod } 97)$ solvable? Notice that

$$\left(\frac{84}{97}\right) = \left(\frac{4}{97}\right)\left(\frac{3}{97}\right)\left(\frac{7}{97}\right) = \left(\frac{97}{3}\right)\left(\frac{97}{7}\right) = \left(\frac{1}{3}\right)\left(\frac{-1}{7}\right) = 1 \cdot -1 = -1.$$

Hence our congruence equation is not solvable.

Example 2. Is $3x^2 + 4x + 5 \equiv 0 \bmod 76$ solvable? According to the Chinese remainder theorem this congruence is equivalent to

$$3x^2 + 4x + 5 \equiv 0 (\text{mod } 4) \qquad 3x^2 + 4x + 5 \equiv 0 (\text{mod } 19).$$

The first equation is equivalent to $x^2 \equiv 1 (\text{mod } 4)$, which is solvable. Multiply the second by 13 on both sides to obtain $x^2 + 14x + 8 \equiv 0 (\text{mod } 19)$. After splitting off squares, $(x+7)^2 \equiv 3 (\text{mod } 19)$. Since $\left(\frac{3}{19}\right) = -\left(\frac{19}{3}\right) = -1$, the second congruence equation, and hence the original one, is not solvable.

Example 3. Let p be an odd prime. Then,

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

This follows from

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).$$

Since 1 is a quadratic residue modulo 3 and -1 a quadratic nonresidue our assertion follows.

Example 4. Let E_n be the integer whose digits in base 10 consist of n ones, e.g. $E_{13} = 1111111111111$. These numbers are known as *repunits*. Alternatively $E_n = (10^n - 1)/9$. As an example we like to show here that E_{33} is divisible by 67. We easily verify that $\left(\frac{10}{67}\right) = \left(\frac{2}{67}\right)\left(\frac{5}{67}\right) = -\left(\frac{67}{5}\right) = -\left(\frac{2}{5}\right) = 1$. Hence, by Theorem 5.1.3(b), $10^{33} \equiv 1 \bmod 67$ and hence $67|E_{33}$.
Extensive calculations show that among the numbers E_n with $n < 50000$ only

$$E_2, E_{19}, E_{23}, E_{317}, E_{1031}$$

are prime and E_{49081} is probably prime (H.Dubner, 1999). Here are some factorisations,

$$\begin{aligned} E_3 &= 111 = 3 \cdot 37 \\ E_5 &= 41 \cdot 271 \\ E_7 &= 239 \cdot 4649 \\ E_{11} &= 21649 \cdot 513239 \\ E_{13} &= 53 \cdot 79 \cdot 265371653 \\ E_{17} &= 2071723 \cdot 5363222357 \end{aligned}$$

Theorem 5.4.1 *Let p be a prime such that $p \equiv -1 (\mathrm{mod}\ 4)$ and $2p+1$ prime. Then $2p+1$ divides $2^p - 1$.*

Proof. Note that $2p+1$ is a prime which is $7 (\mathrm{mod}\ 8)$. Hence, $\left(\frac{2}{2p+1}\right) = 1$. Theorem 5.1.3(b) now implies $2^p \equiv \left(\frac{2}{2p+1}\right) \equiv 1 (\mathrm{mod}\ 2p+1)$. □

As a corollary we see that the Mersenne numbers

$$2^{23} - 1, 2^{83} - 1, 2^{131} - 1$$

are not prime. For $p < 10000$ there are 100 values for which Theorem 5.4.1 applies. (See also Theorem 5.4.3 below and the chapter on applications of residues for Mersenne numbers). We also note that if p is prime, then any prime divisor q of $2^p - 1$ has the form $q = 2pk + 1$. So, when looking for prime divisors of $2^p - 1$ it makes sense to start by trying $2p + 1$.

Theorem 5.4.2 (Pépin, 1877) *For any $n \in \mathbb{N}$ let $F_n = 2^{2^n} + 1$. Then,*

$$F_n \text{ is prime} \Longleftrightarrow 3^{\frac{1}{2}(F_n - 1)} \equiv -1 (\mathrm{mod}\ F_n).$$

Proof. '⇒' Because F_n is an odd prime we have

$$3^{\frac{1}{2}(F_n-1)} \equiv \left(\frac{3}{F_n}\right) \equiv \left(\frac{F_n}{3}\right) \equiv \left(\frac{-1}{3}\right) \equiv -1 (\mathrm{mod}\ F_n).$$

The second to last congruence follows from $2^{2^n}+1 \equiv (-1)^{2^n}+1 \equiv 1+1 \equiv -1 (\mathrm{mod}\ 3)$.
'$\Leftarrow$' Notice that $F_n - 1 = 2^{2^n}$ and $3^{F_n-1} \equiv 1 (\mathrm{mod}\ F_n)$. Hence ord(3) divides 2^{2^n} and equals 2^r for some $0 \leq r \leq 2^n$. Suppose $r < 2^n$ then we would have $3^{(F_n-1)/2} \equiv 1 (\mathrm{mod}\ F_n)$, contradicting our assumption. Hence $r = 2^n$ and ord(3) $= F_n - 1$. In general, if we have $a \in \mathbb{Z}$ such that ord(a) in $(\mathbb{Z}/m\mathbb{Z})^*$ is $m-1$ then m must be prime. In particular, F_n is prime. □

The numbers F_n are known as the *Fermat numbers*, see the chapter on applications of congruences for more on the primality of F_n.

Theorem 5.4.3 (Lucas, Lehmer) *For any $n \in \mathbb{N}$ let $M_n = 2^n - 1$. Define $S_1, S_2, \ldots$ by the recursion*

$$S_1 = 4 \qquad S_{k+1} = S_k^2 - 2, \quad \forall k \geq 0.$$

If $n \geq 3$ and odd then,

$$M_n \text{ is prime } \iff M_n \text{ divides } S_{n-1}.$$

In the proof of Lucas' criterion we shall work in rings of the form $R_m := \{a + b\sqrt{3} |\ a, b \in \mathbb{Z}/m\mathbb{Z}\}$ where $m \in \mathbb{N}$. More strictly speaking, $R_m := \mathbb{Z}[X]/(m, X^2 - 3)$ or $\mathbb{Z}[\sqrt{3}]/(m)$. We state one result in R_m separately.

Lemma 5.4.4 *Let p be a prime larger than 3. Let $a, b \in \mathbb{Z}$. Then, $(a+b\sqrt{3})^p \equiv a + \left(\frac{3}{p}\right) b\sqrt{3} (\mathrm{mod}\ p)$.*

Proof. Since p is a prime we have, using Fermat's little Theorem 3.3.5,

$$\begin{aligned}(a+b\sqrt{3})^p &\equiv a^p + b^p(\sqrt{3})^p (\mathrm{mod}\ p) \\ &\equiv a + b \cdot 3^{\frac{p-1}{2}}\sqrt{3} (\mathrm{mod}\ p).\end{aligned}$$

Our lemma now follows if we use Euler's Theorem 5.1.3(b). □

Proof of Theorem 5.4.3**.** By induction on k it is not hard to show that

$$S_k = (2+\sqrt{3})^{2^{k-1}} + (2-\sqrt{3})^{2^{k-1}} \quad \forall k \geq 1.$$

The condition $M_n | S_{n-1}$ can be rewritten as follow,

$$\begin{aligned}S_{n-1} \equiv 0 (\mathrm{mod}\ M_n) &\iff (2+\sqrt{3})^{2^{n-2}} + (2-\sqrt{3})^{2^{n-2}} \equiv 0 (\mathrm{mod}\ M_n) \\ &\iff (2+\sqrt{3})^{2^{n-1}} + 1 \equiv 0 (\mathrm{mod}\ M_n) \\ &\iff (2+\sqrt{3})^{2^{n-1}} \equiv -1 \pmod{M_n}.\end{aligned}$$

The second equivalence follows by multiplication with $(2+\sqrt{3})^{2^{n-2}}$ and using the fact that $(2+\sqrt{3})(2-\sqrt{3})=1$. The proof of our theorem now comes down to proving that

$$M_n \text{ is prime } \iff (2+\sqrt{3})^{2^{n-1}} \equiv -1 (\text{mod } M_n).$$

The latter congruence can also be written as $(2+\sqrt{3})^{(M_n+1)/2} \equiv -1 (\text{mod } M_n)$ and we can now note the similarity with Pepin's test.
'$\Rightarrow$'. First notice that, n being odd and ≥ 3, we have $M_n \equiv 7 (\text{mod } 24)$. Hence if M_n is prime then 3 is a quadratic nonresidue mod M_n and 2 is a quadratic residue mod M_n. Since M_n is assumed prime we have according to Lemma 5.4.4,

$$(1+\sqrt{3})^{M_n} \equiv 1 + \left(\frac{3}{M_n}\right)\sqrt{3} \equiv 1-\sqrt{3} (\text{mod } M_n).$$

Thus we find,

$$(1+\sqrt{3})^{2^n} \equiv (1+\sqrt{3})^{M_n}(1+\sqrt{3}) \equiv (1-\sqrt{3})(1+\sqrt{3}) \equiv -2 (\text{mod } M_n). \quad (5.1)$$

On the other hand,

$$(1+\sqrt{3})^{2^n} \equiv (1+\sqrt{3})^{2\cdot 2^{n-1}} \equiv (4+2\sqrt{3})^{2^{n-1}} \equiv 2^{2^{n-1}}(2+\sqrt{3})^{2^{n-1}} (\text{mod } M_n). \quad (5.2)$$

Since 2 is a quadratic residue modulo M_n, we have

$$2^{2^{n-1}} \equiv 2 \cdot 2^{(M_n-1)/2} \equiv 2 (\text{mod } M_n). \quad (5.3)$$

Combination of (5.1), (5.2), (5.3) finally yields

$$(2+\sqrt{3})^{2^{n-1}} \equiv -1 (\text{mod } M_n)$$

as asserted.
'$\Leftarrow$'. Let p be a prime divisor of M_n such that $p \not\equiv \pm 1 (\text{mod } 12)$. Since $M_n \equiv 7 (\text{mod } 12)$ such a p exists. In particular we have that 3 is a quadratic nonresidue mod p. Hence Lemma 5.4.4 yields $(2+\sqrt{3})^p \equiv 2-\sqrt{3} (\text{mod } p)$. After multiplication by $2+\sqrt{3}$ we find $(2+\sqrt{3})^{p+1} \equiv 1 (\text{mod } p)$. On the other hand, by assumption we have that $(2+\sqrt{3})^{2^{n-1}} \equiv -1 (\text{mod } p)$. This implies that $2+\sqrt{3}$ has order 2^n in the unit group of $\mathbb{Z}[\sqrt{3}]/(p)$. Hence 2^n divides $p+1$. But p divides $M_n = 2^n - 1$. Thus we conclude that $p = M_n$ and M_n is prime. □

5.5 Jacobi symbols, computing square roots

To determine the Legendre symbol $\left(\frac{111}{137}\right)$ say, we must first factor 111 before being able to apply quadratic reciprocity. This is all right for small numbers like 111, but what to do if we want to compute $\left(\frac{11111111111}{197002597249}\right)$? (197002597249 is prime)

or Legendre symbols with even larger numbers? In the chapter on applications of congruences we pointed out that factorisation of large numbers is a major computational problem. Luckily this does not mean that the computation of Legendre symbols becomes difficult. The solution is to use the slightly more general *Jacobi symbol*.

Definition 5.5.1 *Let $n \in \mathbb{N}$ be odd and $m \in \mathbb{Z}$ such that $(m,n) = 1$. Let $n = p_1 p_2 \cdots p_r$ be the prime factorisation of n. The Jacobi symbol $\left(\frac{m}{n}\right)$ is defined by*

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)\left(\frac{m}{p_2}\right)\cdots\left(\frac{m}{p_r}\right)$$

where the symbols $\left(\frac{m}{p_i}\right)$ are the Legendre symbols.

Remark 5.5.2 *Note that if $\left(\frac{m}{n}\right) = -1$ then $x^2 \equiv m (\mathrm{mod}\ n)$ is not solvable simply because $x^2 \equiv m (\mathrm{mod}\ p_i)$ is not solvable for some i. On the other hand, if $\left(\frac{m}{n}\right) = 1$ we cannot say anything about the solubility of $x^2 \equiv m (\mathrm{mod}\ n)$. For example, $\left(\frac{-1}{21}\right) = 1$ but $x^2 \equiv -1 (\mathrm{mod}\ 21)$ is certainly not solvable.*

However, we do have the following theorem.

Theorem 5.5.3 *Let n, m be odd positive integers. Then,*

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

ii)
$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$

iii)
$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$$

Proof. These statements can be proved by using the corresponding theorems for the Legendre symbol and the observation that for any r-tuple of odd numbers $u_1, \ldots, u_r$ we have

$$\frac{u_1 - 1}{2} + \cdots + \frac{u_r - 1}{2} \equiv \frac{u_1 \cdots u_r - 1}{2} (\mathrm{mod}\ 2). \tag{5.4}$$

To be more precise, the sum on the left of (5.4) is modulo 2 equal to the number k of u_i which are $-1 (\mathrm{mod}\ 4)$. If k is even, the product $u_1 \cdots u_r$ is $1 (\mathrm{mod}\ 4)$ and the term on the right of (5.4) is also even. If k is odd, we have $u_1 \cdots u_r \equiv -1 (\mathrm{mod}\ 4)$, hence the term on the right of (5.4) is also odd.

Let $n = p_1 \cdots p_r$ be the prime factorisation of n. Then i) follows from

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1}\right) \cdots \left(\frac{-1}{p_r}\right) = (-1)^{\frac{p_1-1}{2}+\cdots+\frac{p_r-1}{2}}$$

and

$$\frac{p_1-1}{2} + \cdots + \frac{p_r-1}{2} \equiv \frac{p_1 \cdots p_r - 1}{2} \equiv \frac{n-1}{2} (\text{mod } 2).$$

Similarly, ii) follows from

$$\left(\frac{2}{n}\right) = \left(\frac{2}{p_1}\right) \cdots \left(\frac{2}{p_r}\right) = (-1)^{\frac{p_1^2-1}{8}+\cdots+\frac{p_r^2-1}{8}}$$

and

$$\frac{p_1^2-1}{8} + \cdots + \frac{p_r^2-1}{8} \equiv \frac{(p_1 \cdots p_r)^2 - 1}{8} \equiv \frac{n^2-1}{8} (\text{mod } 2).$$

Let $m = q_1 \cdots q_s$ be the prime factorisation of m. Then iii) follows from

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i,j} \left(\frac{q_i}{p_j}\right)\left(\frac{p_j}{q_i}\right) = (-1)^{\sum_{i,j} \frac{p_j-1}{2}\frac{q_i-1}{2}}$$

and

$$\sum_{i,j} \frac{p_j-1}{2}\frac{q_i-1}{2} \equiv \sum_i \frac{q_i-1}{2} \sum_j \frac{p_j-1}{2} \equiv \frac{m-1}{2}\frac{n-1}{2} (\text{mod } 2).$$

□

The computation of $\left(\frac{11111111111}{197002597249}\right)$ can now be done using a euclidean-like algorithm and Theorem 5.5.3. Notice that

$$\begin{aligned} 197002597249 &= 17 \cdot 11111111111 + 8113708362 \\ 8113708362 &= 2 \cdot 4056854181 \\ 11111111111 &= 2 \cdot 4056854181 + 2997402749 \\ \cdots &\quad \cdots \end{aligned}$$

Hence,

$$\begin{aligned} & \left(\frac{11111111111}{197002597249}\right) = \left(\frac{197002597249}{11111111111}\right) \\ = & \left(\frac{8113708362}{11111111111}\right) = \left(\frac{2}{11111111111}\right)\left(\frac{4056854181}{11111111111}\right) \\ = & \left(\frac{11111111111}{4056854181}\right) = \cdots \end{aligned}$$

We keep repeating these steps of inversion and extraction of factors 2 until we find the value of the Jacobi symbol to be 1. From this algorithm we see that

computation of Jacobi symbols, and hence Legendre symbols, is polynomial in the length of the input.
Let p be a prime and $a \in \mathbb{Z}$. Suppose that by compution of the Legendre symbol $\left(\frac{a}{p}\right)$ we know that $x^2 \equiv a (\text{mod } p)$ is solvable. How do we find a solution? The following algorithm is very fast, provided we have a quadratic nonresidue mod p at our disposal. Assuming the truth of the so-called Generalised Riemann Hypothesis there exists a quadratic nonresidue between 1 and $2(\log p)^2$ and the algorithm we describe is then polynomial in the length of the input. Although we do not know for sure that there exist small quadratic nonresidues , the Riemann hypothesis is still unproved, experience seems to confirm their existence. So in practice the algorithm described here is quite fast.

Solution of $x^2 \equiv a (\text{mod } p)$, Tonelli's algorithm. Let $p - 1 = 2^s \cdot m$, with m odd. Since $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group the group G of elements whose order divides 2^s is also cyclic. To find a generator of this group we must determine a quadratic nonresidue modulo p. This can be done by just trying $2, 3, 5, 7, \ldots$. One very soon hits upon a quadratic nonresidue . Call it x_0. We assert that $b \equiv x_0^m (\text{mod } p)$ is a generator of G. First of all note that $b^{2^s} \equiv x_0^{m \cdot 2^s} \equiv x_0^{p-1} \equiv 1 (\text{mod } p)$, hence the order of b divides 2^s. On the other hand, if the order of b is less than 2^s, then b is an even power of the generator of G, hence $\left(\frac{b}{p}\right) = 1$. This contradicts $\left(\frac{b}{p}\right) = \left(\frac{x_0}{p}\right)^m = (-1)^m = -1$. Hence b generates G.
Let x be a solution of $x^2 \equiv a (\text{mod } p)$. Raise both sides to the power $(m+1)/2$, $x \cdot x^m \equiv a^{(m+1)/2} (\text{mod } p)$. Note that $x^m \in G$. Hence, up to an element of G, the solution x equals $a^{(m+1)/2} (\text{mod } p)$. So we simply try $a^{(m+1)/2} b^j$ as a solution for $j = 0, 1, \ldots, 2^{s-1} - 1$. So, if 2^s is small we find a solution very soon by just trying $j = 0, 1, \ldots, 2^{s-1} - 1$. If 2^s is large we can use an additional trick, due to D.Shanks, which is described below.

As an example we solve $x^2 \equiv 11111111111 (\text{mod } 197002597249)$. Write $p = 197002597249$. It turns out that 7 is the least quadratic nonresidue mod p. We have $p - 1 = 2^7 \cdot 1539082791$. Let $m = 1539082791$. Then,

$$b \equiv 7^m \equiv 59255134607 (\text{mod } p)$$

$$r \equiv 11111111111^{(m+1)/2} \equiv 68821647300 (\text{mod } p).$$

All we have to do now is try the numbers $b^j r (\text{mod } p)$ with $j = 0, 1, 2, \ldots, 63$ as solution of $x^2 \equiv 11111111111 (\text{mod } p)$. It turns out that $j = 37$ does the job and we find

$$57455391308^2 \equiv 11111111111 (\text{mod } 197002597249).$$

If, in Tonelli's algorithm the value of 2^s is large, we can speed up the last part of the algorithm as follows (Shanks),
Let G be a cyclic group of order 2^s with generator b. Let $g \in G$. Then the output e of the following algorithm is precisely the number such that $g = b^e$.

$e := 0$

loop:

Choose $t \in \mathbb{Z}_{\geq 0}$ minimal such that $g^{2^t} = 1$.

If $(t > 0)$ $g := gb^{-2^{s-t}}$, $e := e + 2^{s-t}$, goto **loop**

If $(t == 0)$ **stop**

By using this algorithm with $g = x^2 a^{-m-1}$ we can determine the value of $2j$ in Tonelli's algorithm quickly.

5.6 Class numbers

Take an odd prime $p > 3$ and consider the sum of quadratic residues

$$R = \sum_{1 \leq a \leq p-1, a \text{ residue mod } p} a.$$

Let N be the analogous sum of quadratic non-residues. Notice that

$$R \equiv \sum_{k=1}^{(p-1)/2} k^2 \equiv \frac{1}{6} p(p-1)(2p-1) \equiv 0 (\text{mod } p).$$

Also,

$$R + N \equiv \sum_{a=1}^{p-1} a \equiv \frac{1}{2} p(p-1) \equiv 0 (\text{mod } p).$$

Hence both R and N are divisible by p. Let us make a table of $(N-R)/p$.

p	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
$(N-R)/p$	0	1	1	0	0	1	3	0	3	0	0	1	5	0	3

This table suggests that $(N-R)/p$ is always ≥ 0 and 0 if and only if $p \equiv 1 (\text{mod } 4)$. Suppose first that $p \equiv 1 (\text{mod } 4)$. If a is a residue modulo p, the same holds for $p - a$. So the quadratic residues mod p come in pairs and there are $(p-1)/4$ such pairs. Moreover, the sum of each pair is p, hence $R = p(p-1)/4$. The same argument shows that $N = p(p-1)/4$. This confirms our expectation that $N - R = 0$ if $p \equiv 1 (\text{mod } 4)$. Proving that $(N-R)/p > 0$ if $p \equiv 3 (\text{mod } 4)$ is far more difficult however. A well-known proof by Dirichlet uses arguments from complex function theory. Here is a table of values when $p \equiv 3 (\text{mod } 4)$ and $p < 200$.

p	7	11	19	23	31	43	47	59	67	71	79	83	103
$(N-R)/p$	1	1	1	3	3	1	5	3	1	7	5	3	5

p	107	127	131	139	151	163	167	179	191	199
$(N-R)/p$	3	5	5	3	7	1	11	5	9	9

When $p \equiv 3 (\mathrm{mod}\ 4)$ we call $(N-R)/p$ the class-number of the ring $\mathcal{O} = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$. Notation: $h(-p)$. These class numbers form the tip of an iceberg, which is the field of quadratic forms, arithmetic in quadratic fields and Dirichlet L-series. For example, the interest of this class number lies in the fact that $h(-p) = 1$ if and only if we have unique factorisation in irreducibles in $\mathcal{O}$. It was already suspected by Gauss that the biggest p for which $h(-p) = 1$ is $p = 163$. This was only proved in the 1950's by Heegner, Stark and later, in the 1960's via other methods, by A.Baker.

5.7 Exercises

Exercise 5.7.1 *Determine the quadratic residues modulo 17 and 19.*

Exercise 5.7.2 *Fermat observed that if $a, b \in \mathbb{N}$ and $(a,b) = 1$ and p is an odd prime divisor of $a^2 + b^2$, then $p \equiv 1 (\mathrm{mod}\ 4)$. Prove this.*

Exercise 5.7.3 *Let p be an odd prime and $a \in \mathbb{Z}$ not divisible by p. Prove by induction on k,*

$$x^2 \equiv a (\mathrm{mod}\ p) \text{ has a solution} \Rightarrow x^2 \equiv a (\mathrm{mod}\ p^k) \text{has a solution.}$$

Exercise 5.7.4 *Let p be a prime and suppose $p \equiv 1 (\mathrm{mod}\ 8)$.*
a) Prove that $x^4 \equiv -1 (\mathrm{mod}\ p)$ has a solution.
b) Choose a solution x of $x^4 \equiv -1 (\mathrm{mod}\ p)$ and compute the residue class $(x + x^{-1})^2 (\mathrm{mod}\ p)$. Conclude that $\left(\frac{2}{p}\right) = 1$ if $p \equiv 1 (\mathrm{mod}\ 8)$.

Exercise 5.7.5 *Let p be a prime and suppose $p \equiv 1 (\mathrm{mod}\ 3)$.*

1. *Prove that $x^2 + x + 1 \equiv 0 (\mathrm{mod}\ p)$ has a solution.*
2. *Prove, using a), that $\left(\frac{-3}{p}\right) = 1$ if $p \equiv 1 (\mathrm{mod}\ 3)$.*
3. *Determine the discriminant of $x^2 + x + 1$.*
4. *Prove,using considerations such as in a) and b) that $\left(\frac{-3}{p}\right) = -1$ if $p \equiv -1 (\mathrm{mod}\ 3)$.*

Exercise 5.7.6 *Show that $\left(\frac{105}{131}\right) = 1$ and solve $x^2 \equiv 105 (\mathrm{mod}\ 131)$.*

Exercise 5.7.7 *Verify which of the following equations are solvable,*

$$\begin{aligned} x^2 &\equiv 114 (\text{mod } 127) \\ x^2 &\equiv 61 (\text{mod } 93) \\ x^2 &\equiv 47 (\text{mod } 101) \\ x^2 &\equiv 47 (\text{mod } 143) \\ x^2 &\equiv 837 (\text{mod } 2996) \\ 9x^2 + 12x + 15 &\equiv 0 (\text{mod } 58) \\ 8x^2 &\equiv 2x + 3 (\text{mod } 175). \end{aligned}$$

Exercise 5.7.8 *For which prime numbers is* 5 *a quadratic residue ? Same question for* -3 *and* 3.

Exercise 5.7.9 *Let* $a \in \mathbb{Z}$ *and* p, q *two odd primes not dividing* a. *Prove,*
a) If $a \equiv 1 (\text{mod } 4)$ *then:* $p \equiv q (\text{mod } |a|) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.
b) If $a \equiv -1 (\text{mod } 4)$ *then:* $p \equiv q (\text{mod } 4|a|) \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

Exercise 5.7.10 *Let* p *be a prime which is* -1 *modulo* 4. *Let* a *be a quadratic residue modulo* p. *Prove that a solution of* $x^2 \equiv a (\text{mod } p)$ *is given by* $x = a^{(p+1)/4}$.

Exercise 5.7.11 *Let* p *be a prime which is* 5 *modulo* 8. *Let* r *be an element of* $(\mathbb{Z}/p\mathbb{Z})^*$ *of order* 4 *and let* a *be a quadratic residue modulo* p. *Prove that a solution of* $x^2 \equiv a (\text{mod } p)$ *is given by either* $x = a^{(p+3)/8}$ *or* $x = ra^{(p+3)/8}$.

Exercise 5.7.12 *Prove that there exist infinitely many primes* p *such that* $p \equiv 1 (\text{mod } 4)$. *Prove that there exist infinitely many primes* p *such that* $p \equiv -1 (\text{mod } 4)$.

Exercise 5.7.13 *Let* p *be an odd prime. Let* a *be the smallest positive integer such that* a *is a quadratic nonresidue modulo* p. *Show that* $a < 1 + \sqrt{p}$.

Exercise 5.7.14 *a) Let* $p = 4k + 1$ *be prime. Prove,*

$$[\sqrt{p}] + [\sqrt{2p}] + \cdots + [\sqrt{kp}] = \frac{p^2 - 1}{12}.$$

b) Let $p = 4k + 3$ *be prime. Prove,*

$$[\sqrt{p}] + [\sqrt{2p}] + \cdots + [\sqrt{kp}] \leq \frac{(p-1)(p-2)}{12}.$$

(Hint: count the number of lattice points below the parabola $y = \sqrt{px}$ *with* $x < p/4$ *and use in b) that* $N \geq K$.*)*

Chapter 6

Dirichlet characters and Gauss sums

6.1 Characters

In this chapter we study an important tool in number theory, namely characters on $(\mathbb{Z}/m\mathbb{Z})^*$.

Definition 6.1.1 *Let G be a finite abelian group. A homomorphism $\chi : G \to \mathbb{C}^*$ is called a character of G.*

Since any element g of a finite group has finite order, $\chi(g)$ must have finite order in $\mathbb{C}^*$, hence be a root of unity. In particular, $\chi(e) = 1$ for all χ. Moreover if G is cyclic and g is a generator of G, then χ is determined by its value $\chi(g)$. Any other $a \in G$ is of the form $a = g^k$ and so we must have $\chi(a) = \chi(g^k) = (\chi(g))^k$.

Definition 6.1.2 *The trivial character or principal character on a finite abelian group G is the character given by $\chi(g) = 1\ \forall g \in G$. Notation: χ_0.*

Suppose we have two characters χ_1 and χ_2 on G. Then one easily verifies that the new function $\chi_1\chi_2$ given by $(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g)\ \forall g \in G$ is again a character on G. In fact, the characters on G form a group with the trivial character as identity element. We denote this group by $\hat{G}$. Correspondingly we can speak about the order of a character as being its order in $\hat{G}$.

Lemma 6.1.3 *Let G be a finite abelian group and χ a non-trivial character on G. Then,*

$$\sum_{g \in G} \chi(g) = 0.$$

Proof. Since χ is non-trivial, there exists $h \in G$ such that $\chi(h) \neq 1$. We now use the fact that if g runs through G then so does gh,

$$\sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(hg) = \chi(h) \sum_{g\in G} \chi(g).$$

Because $\chi(h) \neq 1$ our assertion follows. □

To get a good grasp on the characters of an abelian group we consider the vectorspace $V = \mathbb{C}^{|G|}$ consisting of $|G|$-tuples of complex numbers $(c_{g_1}, c_{g_2}, \ldots)$ indexed by the elements $g_1, g_2, \ldots$ of G. On V we define a complex inner product by

$$(\vec{x}, \vec{y}) = \sum_{g\in G} x_g \overline{y_g}$$

for any $\vec{x} = (x_{g_1}, x_{g_2}, \ldots)$, $\vec{y} = (y_{g_1}, y_{g_2}, \ldots)$ in V. The bar denotes complex conjugation. We let any $h \in G$ act on V by

$$h\vec{x} = (x_{hg_1}, x_{hg_2}, \ldots).$$

So we see that any h simply permutes the coordinates of $\vec{x}$ in a way prescribed by the groupstructure. In particular, the elements of G act as unitary (=length preserving) linear maps on V. Let χ be a character on G. We define the corresponding charactervector $\vec{v}_\chi$ by

$$\vec{v}_\chi = (\chi(g_1), \chi(g_2), \ldots)$$

in other words, $\vec{v}_\chi$ is just the sequence of values of χ. Notice that for any $h \in G$,

$$h\vec{v}_\chi = (\chi(hg_1), \chi(hg_2), \ldots) = \chi(h)(\chi(g_1), \chi(g_2), \ldots) = \chi(h)\vec{v}_\chi.$$

Hence $\vec{v}_\chi$ is a common eigenvector for all $h \in G$ with eigenvalues $\chi(h)$. Conversely, any common eigenvector $\vec{v}$ of all $h \in G$ defines a character on G by taking the eigenvalue of each h as charactervalue. Let $h\vec{v} = \lambda(h)\vec{v}$ and suppose we had taken $g_1 = e$. Then $h(v_e, \ldots) = (v_h, \ldots)$ and, on the other hand, $h(v_e, \ldots) = \lambda(h)(v_e, \ldots) = (\lambda(h)v_e, \ldots)$. Hence $v_h = \lambda(h)v_e$ for all $h \in G$. So $\vec{v} = v_e(\lambda(g_1), \lambda(g_2), \ldots)$. In particular, $\vec{v}$ is uniquely defined up to a scalar factor. Finally, let χ_1, χ_2 be two distinct characters. In particular, $\chi_1\overline{\chi_2} = \chi_1\chi_2^{-1}$ is not the trivial character. Then, using Lemma 6.1.3,

$$(\vec{v}_{\chi_1}, \vec{v}_{\chi_2}) = \sum_{g\in G} \chi_1(g)\overline{\chi_2(g)} = \sum_{g\in G} (\chi_1\overline{\chi}_2)(g) = 0,$$

hence $\vec{v}_{\chi_1}$ and $\vec{v}_{\chi_2}$ are orthogonal.

Lemma 6.1.4 $|\hat{G}| = |G|$.

Proof. Since, by the above remarks, character vectors belonging to distinct characters are orthogonal, there cannot be more than $|G|$ characters. Suppose that we have k distinct characters and that $k < |G|$. Then the orthogonal complement U in V of the character vectors has dimension $|G| - k > 0$. Moreover, every element $h \in G$ is unitary and hence maps U into itself. From linear algebra we know that any set of commuting unitary operators has a common eigenvector, which in its turn defines a character of G, distinct from the ones we already had. So we now have $k+1$ distinct characters. We continu this procedure untill we have $|G|$ distinct characters. □

Lemma 6.1.5 *Let G be a finite abelian group and $g \in G$ not the identity element. Then,*

$$\sum_{\chi \in \hat{G}} \chi(g) = 0.$$

Proof. Let $G = \{g_1, g_2, \ldots\}$ and $\hat{G} = \{\chi_1, \chi_2, \ldots\}$. Consider the $|G|$ by $|G|$ matrix $M = (\chi_i(g_j))_{i,j=1,\ldots,|G|}$. We have seen in the remarks above that the rows (letting j run) of this matrix are orthogonal. Moreover, all rows have lengths $\sqrt{|G|}$. Hence M is $\sqrt{|G|}$ times a unitary matrix. In such a matrix the columns are orthogonal as well, in other words for any distinct $g, h \in G$ we have

$$\sum_{\chi} \chi(g)\overline{\chi(h)} = 0.$$

Our Lemma follows by taking $h = e$. □

Definition 6.1.6 *A Dirichlet character is a character on $(\mathbb{Z}/m\mathbb{Z})^*$.*

Remark 6.1.7 *Let χ be a Dirichlet character on $(\mathbb{Z}/m\mathbb{Z})^*$. Often one extends χ to a function on $\mathbb{Z}$ by taking the value $\chi(n)$ for all n with $(n,m) = 1$ and $\chi(n) = 0$ whenever $(n,m) > 1$. By abuse of language we then still speak of a Dirichlet character.*

Examples

i. The Legendre symbol $\left(\frac{\cdot}{p}\right)$ on $(\mathbb{Z}/p\mathbb{Z})^*$ for odd primes p and the Jacobi symbol on $(\mathbb{Z}/m\mathbb{Z})^*$ for odd m. Both examples are real characters of order two.

ii. The character of order four on $(\mathbb{Z}/13\mathbb{Z})^*$ given by

a:	1	2	3	4	5	6	7	8	9	10	11	12	(mod 13)
$\chi(a)$:	1	i	1	-1	i	i	$-i$	$-i$	1	-1	$-i$	-1	

One easily verifies that $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in (\mathbb{Z}/13\mathbb{Z})^*$. We have constructed this character by assigning $\chi(2) = i$. Since 2 is a primitive root modulo 13, the powers of 2 run through $(\mathbb{Z}/13\mathbb{Z})^*$ and we can determine the character values correspondingly.

iii. The non-trivial characters χ_1, χ_2, χ_3 on $(\mathbb{Z}/8\mathbb{Z})^*$ given by

$$\begin{array}{rrrrr} a: & 1 & 3 & 5 & 7 \\ \chi_1(a): & 1 & -1 & 1 & -1 \\ \chi_2(a): & 1 & -1 & -1 & 1 \\ \chi_3(a): & 1 & 1 & -1 & -1 \end{array}$$

Definition 6.1.8 *A Dirichlet character χ is called even if $\chi(-1) = 1$ and odd if $\chi(-1) = -1$.*

6.2 Gauss sums, Jacobi sums

Although it is possible to consider more general Gauss sums, we shall restrict ourselves here to $(\mathbb{Z}/p\mathbb{Z})^*$ where p is an odd prime. For the p-th roots of unity we mention the following Lemma. In the sequel we let ζ_p denote $e^{2\pi i/p}$.

Lemma 6.2.1 *Let $n \in \mathbb{Z}$ and p an odd prime. Then,*

$$\sum_{x=1}^{p-1} \zeta_p^{nx} = \begin{cases} -1 & \text{if } p \not| n \\ p-1 & \text{if } p|n \end{cases}$$

Proof. Clearly, when $p|n$ all terms in the summation are 1, so the second case follows immediately. In the first case we use the summation formula for geometric sequences to obtain

$$(\zeta_p^{pn} - \zeta_p^n)/(\zeta_p^n - 1) = -1.$$

Definition 6.2.2 *Let p be an odd prime and χ a Dirichlet character on $(\mathbb{Z}/p\mathbb{Z})^*$. The Gauss sum S_χ is defined by*

$$S_\chi = \sum_{x=1}^{p-1} \chi(x)\zeta_p^x.$$

Theorem 6.2.3 *Let χ be a non-trivial Dirichlet character on $(\mathbb{Z}/p\mathbb{Z})^*$. Then,*

a) $S_\chi S_{\chi^{-1}} = \chi(-1)p$,

b) $|S_\chi|^2 = p$,

c) if χ is the Legendre symbol then $S_\chi^2 = (-1)^{\frac{p-1}{2}} p$.

Proof. Part a) We have

$$S_\chi S_{\chi^{-1}} = \sum_{x,y=1}^{p-1} \chi(x)\chi(y)^{-1}\zeta_p^{x+y}.$$

Replace x by zy and notice that if z runs through $(\mathbb{Z}/p\mathbb{Z})^*$ then so does $x = zy$ for any fixed $y \in (\mathbb{Z}/p\mathbb{Z})^*$. Hence

$$S_\chi S_{\chi^{-1}} = \sum_{z,y=1}^{p-1} \chi(z)\chi(y)\chi(y)^{-1}\zeta_p^{y(z+1)}.$$

The factors $\chi(y)$ cancel. According to Lemma 6.2.1 summation over y now yields -1 if $z \not\equiv -1 (\text{mod } p)$ and $p-1$ if $z \equiv -1 (\text{mod } p)$. Hence,

$$S_\chi S_{\chi^{-1}} = \chi(-1)p - \sum_{x=1}^{p-1} \chi(x).$$

The summation on the right vanishes according to Lemma 6.1.3 and we have proved assertion a).
Part b) First of all, notice that

$$\begin{aligned} S_{\chi^{-1}} &= \sum_{x=1}^{p-1} \chi(x)^{-1}\zeta_p^x \\ &= \sum_{x=1}^{p-1} \overline{\chi(x)\zeta_p^{(-x)}} \\ &= \chi(-1)\sum_{x=1}^{p-1} \overline{\chi(-x)\zeta_p^{(-x)}} \\ &= \chi(-1)\overline{S_\chi}. \end{aligned}$$

Hence $|S_\chi|^2 = S_\chi\overline{S_\chi} = \chi(-1)S_\chi S_{\chi^{-1}}$ and assertion b) follows by using assertion a).
c) If χ is the Legendre symbol we have $\chi = \chi^{-1}$ and hence, via assertion a), $S_\chi^2 = \chi(-1)p = (-1)^{(p-1)/2}p$. □

Definition 6.2.4 *Let χ_1, χ_2 be Dirichlet characters modulo p, where p is an odd prime. The Jacobi sum $J(\chi_1, \chi_2)$ is defined by*

$$J(\chi_1, \chi_2) = \sum_{x=2}^{p-1} \chi_1(x)\chi_2(1-x).$$

Theorem 6.2.5 *Let notations be as in Definition* 6.2.4. *Suppose that* χ_1 *and* χ_2 *are not each other's inverse. Then,*

$$S_{\chi_1}S_{\chi_2} = J(\chi_1,\chi_2)S_{\chi_1\chi_2}.$$

Proof. Write

$$S_{\chi_1}S_{\chi_2} = \sum_{x,y=1}^{p-1} \chi_1(x)\chi_2(y)\zeta_p^{x+y}.$$

We introduce the new summation variables u, v via $x = uv,\ y = u(1-v)$. Conversely, $u = x+y,\ v = x/(x+y)$. One easily verifies that this gives us a bijection between the sets $\{(x,y) \in (\mathbb{Z}/p\mathbb{Z})^{*2} |\ x+y \not\equiv 0 (\text{mod } p)\}$ and $\{(u,v) \in (\mathbb{Z}/p\mathbb{Z})^{*2} |\ v \not\equiv 1 (\text{mod } p)\}$. Hence,

$$\begin{aligned} S_{\chi_1}S_{\chi_2} &= \sum_{x\equiv -y} \chi_1(x)\chi_2(y)\zeta_p^{(x+y)} + \sum_{u=1}^{p-1}\sum_{v=2}^{p-1} \chi_1(uv)\chi_2(u(1-v))\zeta_p^u \\ &= \sum_{x=1}^{p-1} \chi_1(-1)\chi_1(x)\chi_2(x) + \sum_{u=1}^{p-1}\sum_{v=2}^{p-1} \chi_1(v)\chi_2(1-v)\chi_1(u)\chi_2(u)\zeta_p^u. \end{aligned}$$

The first summation vanishes because of Lemma 6.1.3 and the fact that $\chi_1\chi_2 \neq \chi_0$. In the second summation the sum over u yields $S_{\chi_1\chi_2}$ and summing over v yields $J(\chi_1,\chi_2)$. Hence $S_{\chi_1}S_{\chi_2} = J(\chi_1,\chi_2)S_{\chi_1\chi_2}$. □

Corollary 6.2.6 *Let notations be as in Definition* 6.2.4. *Suppose that the characters are not each other's inverse. Then* $|J(\chi_1,\chi_2)| = \sqrt{p}$.

Proof. This follows from Theorem 6.2.5 and Theorem 6.2.3(b). □

6.3 Applications

A nice application of Gauss sums is a *short proof of the quadratic reciprocity law.*

Let p, q be two odd primes. Write $\tau_p = S_\chi$ where χ is the Legendre symbol on $(\mathbb{Z}/p\mathbb{Z})^*$. The following calculations will be performed in $\mathbb{Z}[\zeta_p]$ considered modulo q. Using Theorem 6.2.3(c) and Euler's Theorem 5.1.3(b) we find that

$$\tau_p^q \equiv \tau_p^{q-1}\tau_p \equiv ((-1)^{\frac{p-1}{2}}p)^{\frac{q-1}{2}}\tau_p \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)\tau_p (\text{mod } q).$$

On the other hand,

$$\tau_p^q \equiv \left(\sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\zeta_p^x\right)^q$$

$$\begin{aligned} &\equiv \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \zeta_p^{qx} \equiv \left(\frac{q}{p}\right) \sum_{x=1}^{p-1} \left(\frac{qx}{p}\right) \zeta_p^{qx} \\ &\equiv \left(\frac{q}{p}\right) \tau_p (\text{mod } q). \end{aligned}$$

Comparison of the above two equalities yields

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \tau_p \equiv \left(\frac{q}{p}\right) \tau_p (\text{mod } q).$$

Multiply on both sides by τ_p and cancel the resulting $\tau_p^2 = (-1)^{\frac{p-1}{2}} p$. We then obtain

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

and since $q \geq 3$, strict equality follows.

Using the above idea we can also compute $\left(\frac{2}{p}\right)$. The following calculation will be performed in $\mathbb{Z}[i]$ modulo p. We consider $(1+i)^p (\text{mod } p)$ and compute it in two ways. First of all

$$(1+i)^p \equiv 1 + i^p \equiv 1 + (-1)^{\frac{p-1}{2}} i \equiv \begin{cases} 1+i (\text{mod } p) & \text{if } p \equiv 1 (\text{mod } 4) \\ -i(1+i) (\text{mod } p) & \text{if } p \equiv 3 (\text{mod } 4) \end{cases}$$

On the other hand, since $(1+i)^2 = 2i$,

$$(1+i)^p \equiv (2i)^{\frac{p-1}{2}} (i+1) \equiv \left(\frac{2}{p}\right) i^{\frac{p-1}{2}} (1+i) (\text{mod } p).$$

Comparison of these two results shows that

$$\left(\frac{2}{p}\right) \equiv \begin{cases} i^{-\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} & \text{if } p \equiv 1 (\text{mod } 4) \\ -i \cdot i^{-\frac{p-1}{2}} \equiv (-1)^{\frac{p+1}{4}} & \text{if } p \equiv 3 (\text{mod } 4) \end{cases}$$

One now easily checks that $\left(\frac{2}{p}\right) = 1$ if $p \equiv \pm 1 (\text{mod } 8)$ and $\left(\frac{2}{p}\right) = -1$ if $p \equiv \pm 3 (\text{mod } 8)$.

Theorem 6.3.1 *Let p be a prime with $p \equiv 1 (\text{mod } 4)$. Then p can be written as the sum of two squares. More precisely, $p = a^2 + b^2$ with*

$$a = \sum_{x=1}^{\frac{p-1}{2}} \left(\frac{x(x^2-1)}{p}\right), \qquad b = \sum_{x=1}^{\frac{p-1}{2}} \left(\frac{x(x^2-\nu)}{p}\right)$$

where ν is any quadratic nonresidue .

Remark 6.3.2 *The sum* $\sum_{x=0}^{p-1}\left(\frac{x(x^2-1)}{p}\right)$*, which equals* $2a$*, is known as the Jacobsthal sum.*

Proof. Since $p \equiv 1 (\mathrm{mod}\ 4)$ we have a character of order 4 on $(\mathbb{Z}/p\mathbb{Z})^*$ which we call χ_4. This can be constructed by taking $\chi(g) = i$ for a primitive root g. Any other element of $a \in (\mathbb{Z}/p\mathbb{Z})^*$ has the form $a \equiv g^k (\mathrm{mod}\ p)$ and so $\chi(a)$ is fixed by $\chi(a) = \chi(g^k) = \chi(g)^k = i^k$. Consider the Jacobi sum $J = J(\chi_4, \left(\frac{\div}{p}\right))$, where $\left(\frac{\div}{p}\right)$ is the Legendre symbol. Notice that $J \in \mathbb{Z}[i]$, i.e. $J = a + bi,\ a, b \in \mathbb{Z}$. Moreover, by Corollary 6.2.6, $p = |J|^2 = a^2 + b^2$. Hence our first assertion is proved.
Notice that in the summation

$$J = \sum_{x=1}^{p-1} \chi_4(x) \left(\frac{1-x}{p}\right)$$

a term is real if x is a quadratic residue and purely imaginary if x is a quadratic nonresidue . Hence

$$\begin{aligned} a = \Re J &= \sum_{y=1}^{\frac{p-1}{2}} \chi_4(y^2) \left(\frac{1-y^2}{p}\right) \\ &= \sum_{y=1}^{\frac{p-1}{2}} \left(\frac{y}{p}\right)\left(\frac{1-y^2}{p}\right) = \sum_{y=1}^{\frac{p-1}{2}} \left(\frac{y(y^2-1)}{p}\right). \end{aligned}$$

Taking ν to be any quadratic nonresidue we get

$$\begin{aligned} ib = i\Im J &= \sum_{y=1}^{\frac{p-1}{2}} \chi_4(\nu y^2) \left(\frac{1-\nu y^2}{p}\right) \\ &= \chi_4(\nu) \sum_{y=1}^{\frac{p-1}{2}} \left(\frac{y}{p}\right)\left(\frac{1-\nu y^2}{p}\right) = -\chi_4(\nu) \sum_{y=1}^{\frac{p-1}{2}} \left(\frac{y(y^2-\nu)}{p}\right). \end{aligned}$$

Since $\chi_4(\nu) = \pm i$ our asserted value of follows up to $\pm$ sign, which is sufficient. □

Another amusing application is the following theorem discovered by Gauss,

Theorem 6.3.3 *Let* p *be an odd prime for which* $p \equiv 1 (\mathrm{mod}\ 3)$*. Then,*

$$\exists x \in \mathbb{Z}:\ x^3 \equiv 2 (\mathrm{mod}\ p) \iff \exists A, B \in \mathbb{Z}:\ p = A^2 + 27B^2.$$

When $p \equiv -1 (\mathrm{mod}\ 3)$*, the congruence* $x^3 \equiv 2 (\mathrm{mod}\ p)$ *always has a solution.*

Proof. When $p \equiv 2 (\mathrm{mod}\ 3)$ we simply take $x = 2^{(2-p)/3}$ as solution (verify!). So we suppose that $p \equiv 1 (\mathrm{mod}\ 3)$. Then there exists a character χ mod p of order 3. First of all we notice that

$$\exists x \in \mathbb{Z} : \ x^3 \equiv 2 (\mathrm{mod}\ p) \iff \chi(2) = 1.$$

Notice that the third roots of unity are all distinct modulo 2. Hence it follows from Lemma 6.3.4 that

$$\exists x \in \mathbb{Z} : \ x^3 \equiv 2 (\mathrm{mod}\ p) \iff J(\chi, \chi) \equiv 1 (\mathrm{mod}\ 2).$$

We know that $J(\chi, \chi)$ is an element of $\mathbb{Z}[\omega]$, the ring of Eisenstein integers, where ω is a cube root of unity. Thus we have $J(\chi, \chi) = a + b\omega$ for some $a, b \in \mathbb{Z}$. From Lemma 6.3.4 it follows that $a \equiv -1 (\mathrm{mod}\ 3)$ and $b \equiv 0 (\mathrm{mod}\ 3)$. Similarly, if $\chi(2) = 1$ we find that $b \equiv 0 (\mathrm{mod}\ 2)$. When b is even we can rewrite $a + b\omega$ as $a - b/2 + (b/2)\sqrt{-3}$ hence it is an element of $\mathbb{Z}[\sqrt{-3}]$. So we now find

$$\exists x \in \mathbb{Z} : \ x^3 \equiv 2 (\mathrm{mod}\ p) \iff \exists A, B \in \mathbb{Z} : \ J(\chi, \chi) = A + 3B\sqrt{-3}$$

where we have put $A = a - b/2, \ B = b/6$.
Suppose that $x^3 \equiv 2 (\mathrm{mod}\ p)$ has a solution. Then$J(\chi, \chi) = A + 3B\sqrt{-3}$ and since $|J(\chi, \chi)|^2 = p$, we find that $p = A^2 + 27B^2$.
Suppose conversely that p can be written as $p = A^2 + 27B^2$. Then we have in $\mathbb{Z}[\omega]$ the factorisation $p = \pi\overline{\pi}$ where $\pi = A \pm 3B\sqrt{-3}$. Choosing the proper sign, we know, by unique factorisation, that π equals $J(\chi, \chi)$ up to a unit. Since $\pi \equiv \pm 1 (\mathrm{mod}\ 3)$ and $J(\chi, \chi) \equiv -1 (\mathrm{mod}\ 3)$ this unit must be ± 1 and hence $J(\chi, \chi)$ is of the form $A' + 3B'\sqrt{-3}$. This implies that $x^3 \equiv 2 (\mathrm{mod}\ p)$ is solvable.

Lemma 6.3.4 *Let p be an odd prime satisfying $p \equiv 1 (\mathrm{mod}\ 3)$. Let χ be a Dirichlet character mod p of order 3. Then,*

$$J(\chi, \chi) \equiv -1 (\mathrm{mod}\ 3) \qquad J(\chi, \chi) \equiv \chi(2) (\mathrm{mod}\ 2).$$

Proof. According to Theorem 6.2.5 we have

$$S_\chi^3 = S_\chi S_{\chi^2} J(\chi, \chi) = pJ(\chi, \chi).$$

Notice that modulo 3 we have

$$\begin{aligned} S_\chi^3 &\equiv \sum_{x=1}^{p-1} \chi(x)^3 \zeta_p^{3x} (\mathrm{mod}\ 3) \\ &\equiv \sum_{x=1}^{p-1} \zeta_p^{3x} \equiv -1 (\mathrm{mod}\ 3) \end{aligned}$$

where the last equality follows from Lemma 6.2.1.

Notice that modulo 2 we have

$$\begin{aligned} S_\chi^4 &\equiv \sum_{x=1}^{p-1} \chi(x)^4 \zeta_p^{4x} (\text{mod } 2) \\ &\equiv \chi(4)^{-1} \sum_{x=1}^{p-1} \chi(4x) \zeta_p^{4x} (\text{mod } 2) \\ &\equiv \chi(2) S_\chi (\text{mod } 2) \end{aligned}$$

Our congruence mod 2 follows after multiplication by $S_{\bar{\chi}}$, Theorem 6.2.3(a) and $p \equiv 1 (\text{mod } 2)$. □

6.4 Exercises

Exercise 6.4.1 *Determine all Dirichlet characters modulo* 7 *and modulo* 12.

Exercise 6.4.2 *Choose a character* χ_4 *of order* 4 *and a character* χ_2 *of order 2 on* $(\mathbb{Z}/13\mathbb{Z})^*$. *Give a table in which* $x, \chi_2(x), \chi_4(x)$ *and* $\chi_2(x)\chi_4(1-x)$ *are listed for* $x = 1, \ldots, 12$. *Compute the Jacobi sum* $J(\chi_2, \chi_4)$. *Note that it is a number in* $\mathbb{Z}[i]$ *and that its norm is* 13.

Exercise 6.4.3 *Proof that a cyclic group of order* N *has precisely* N *characters, which again form a cyclic group.*

Exercise 6.4.4 *Let* p *be an odd prime. Prove that there exists a Dirichlet character of order* 4 *if and only if* $p \equiv 1 (\text{mod } 4)$.

Exercise 6.4.5 *Let* p *be a prime and* $a \in \mathbb{Z}$, *not divisible by* p. *Suppose* $p \equiv 2 (\text{mod } 3)$. *Prove that* $x^3 \equiv a (\text{mod } p)$ *has precisely one solution modulo* p.

Exercise 6.4.6 *Determine all solutions of* $x^3 \equiv 2 (\text{mod } p)$ *for* $p = 19, 31$. *Check also if* p *can be written in the form* $p = a^2 + 27b^2$.

Chapter 7

Sums of squares, Waring's problem

7.1 Sums of two squares

In previous chapters we have already seen that if an odd prime divides the sum of two relatively prime squares, it is 1(mod 4). Moreover, Fermat showed that any prime $\equiv 1(\text{mod } 4)$ can be written as a sum of two squares. Furthermore it was observed since antiquity that any positive integer can be written as the sum of four squares. This was proved by Lagrange for the first time in 1770. Problems such as these form the subject of this section. It should be noted explicitly here that *by a square we mean the square of a number in* $\mathbb{Z}$. So, 0^2 is also considered to be a square.
The quickest and most elegant way to deal with the above mentioned problems is to work in the rings of Gaussian integers and quaternionic integers where we rely heavily on the fact that they are euclidean domains. There exist also presentations of this subject which work entirely in $\mathbb{Z}$. However, they are in fact a disguised form of application of the euclidean algorithm.

Theorem 7.1.1 (Fermat) *Let p be an odd prime. Then p is a sum of two squares if and only if $p \equiv 1(\text{mod } 4)$.*

Proof. Suppose $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. Since squares are either 0 or 1 mod 4, p, being odd, can only be 1(mod 4).
Now suppose that $p \equiv 1(\text{mod } 4)$. Then the congruence equation $x^2 \equiv -1(\text{mod } p)$ has a solution, x_0 say. Let us now work in $\mathbb{Z}[i]$ and use unique factorisation. We have $p|(x_0^2 + 1)$ hence $p|(x_0 + i)(x_0 - i)$. If p were prime in $\mathbb{Z}[i]$ we would have $p|(x - i)$ and, via complex conjugation, $p|(x + i)$. Hence $p|2i$, which is impossible. Hence $p = \alpha\beta$ in $\mathbb{Z}[i]$ with $N\alpha, N\beta > 1$. Take norms on both sides, $p^2 = N\alpha N\beta$. Since $N\alpha, N\beta > 1$ this implies $p = N\alpha$, hence p can be written as a sum of two squares. □

Theorem 7.1.2 *Let $r_2(n)$ be the number of solutions $x, y \in \mathbb{Z}$ to $n = x^2 + y^2$.*

i. The function $r_2(n)/4$ is multiplicative.

ii. Let p be a prime. Then

$$\frac{r_2(p^k)}{4} = \begin{cases} k+1 & \text{if } p \equiv 1 (\text{mod } 4) \\ 0 & \text{if } p \equiv 3 (\text{mod } 4),\ k \text{ odd} \\ 1 & \text{if } p \equiv 3 (\text{mod } 4),\ k \text{ even} \\ 1 & \text{if } p = 2 \end{cases}$$

Proof. Part i). We note that there is a 1-1-correspondence between solutions of $n = x^2 + y^2$ and factorisations $n = \alpha\overline{\alpha}$ in $\mathbb{Z}[i]$, simply by taking $\alpha = x + yi$. Also note that $r_2(n)/4$ is precisely the number of factorisations $n = \alpha\overline{\alpha}$ where we count $\alpha\overline{\alpha}$, $i\alpha \cdot -i\overline{\alpha}$, $-\alpha \cdot -\overline{\alpha}$, $-i\alpha \cdot i\overline{\alpha}$ as being the same., i.e. we count factorisations modulo units.
Let $m, n \in \mathbb{N}$ and $(m, n) = 1$. Let $mn = \lambda\overline{\lambda}$, $\lambda \in \mathbb{Z}[i]$. Let $\mu = \gcd(\lambda, m)$, $\nu = \gcd(\lambda, n)$. Note that μ, ν are unique up to units. Then $\lambda = \mu\nu$ (up to units) and $mn = \mu\nu\overline{\mu\nu} = \mu\overline{\mu}\nu\overline{\nu}$. Hence every representation of mn as sum of two squares corresponds to a pair of representations of $m = \mu\overline{\mu}$ and $n = \nu\overline{\nu}$. Conversely, every such pair gives rise to representation $mn = \mu\overline{\mu}\nu\overline{\nu}$. Hence

$$r_2(mn)/4 = (r_2(m)/4)(r_2(n)/4).$$

Part ii). Let $p = 2$. Since 2 has only one prime divisor, $1 + i$, in $\mathbb{Z}[i]$ we have, up to units, the unique factorisation

$$2^k = (1 + i)^k (1 - i)^k.$$

Hence $r_2(2^k)/4 = 1$.
Let $p \equiv 3 (\text{mod } 4)$. Then p itself is prime in $\mathbb{Z}[i]$. For k odd there is no factorisation of the form $p^k = \lambda\overline{\lambda}$, when k is even we have only $p^k = p^{k/2}p^{k/2}$.
Let $p \equiv 1 (\text{mod } 4)$. Then $p = \pi\overline{\pi}$, where $\pi, \overline{\pi}$ are distinct primes in $\mathbb{Z}[i]$. For the factorisation $p^k = \lambda\overline{\lambda}$ we have, up to units, $k + 1$ choices, namely $\lambda = \pi^k,\ \pi^{k-1}\overline{\pi}, \ldots, \overline{\pi}^k$. Hence $r_2(p^k)/4 = k + 1$, as asserted. □

In order to solve $n = x^2 + y^2$ for given n there exist several possibilities. When n is small it is best to solve it by trial and error. When n is larger, there are two possibilities. For medium sized numbers with several prime factors we suggest the following method. Let $n = p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorisation of n. Write each factor $p_j^{k_j}$ as a sum of two squares $a_j^2 + b_j^2$. Let α_j be one the complex numbers $a_j \pm b_j i$. Let $\prod_{j=1}^r \alpha_i = \alpha = a + bi$. Notice that $n = \prod_{j=1}^r p_j^{k_j} = \prod_{j=1}^r N(\alpha_j) = N(\alpha) = a^2 + b^2$. Since we have different choices for each α_j we will get different solutions to $n = x^2 + y^2$. We have seen that we get essentially all solutions in this way. As an example we write 65 as sum of two squares. Notice that $65 = 5 \times 13$

and $5 = 1^2 + 2^2$ and $13 = 2^2 + 3^2$. The multiplications $(1+2i)(2+3i) = -4+7i$ and $(1-2i)(2+3i) = 8-i$ produce the solutions $65 = 4^2 + 7^2$ and $65 = 8^2 + 1^2$. According to Theorem 7.1.2 there are 16 solutions and they can be obtained from the two solutions we found by interchanging x, y and the substitutions $x \to -x$, $y \to -y$.
When n is a large prime we use a more sophisticated method. Via the techniques described in the chapter on quadratic reciprocity we first solve $l^2 \equiv -1 (\mathrm{mod}\ n)$ and then determine $a + bi = \gcd(n, l+i)$ via the euclidean algorithm in $\mathbb{Z}[i]$. We assert that $n = a^2 + b^2$.

7.2 Sums of more than two squares

Theorem 7.2.1 (Lagrange 1770) *Every positive integer can be written as a sum of four squares.*

Proof. First of all notice the equivalenc of the statements

i. 'n is sum of four squares'

ii. 'n is the norm of a quaternionic integer'.

Going from i. to ii. is trivial. Suppose conversely that $n = N\alpha$ for some quaternionic integer α. According to Theorem 13.4.2 there exists a unit ϵ such that $\alpha\epsilon = p + qi + rj + sk$ for some $p, q, r, s \in \mathbb{Z}$. Hence $n = N\alpha = N\alpha\epsilon = p^2 + q^2 + r^2 + s^2$.
Secondly, if n, m can be written as a sum of four squares then so can nm. This follows from $N\alpha N\beta = N\alpha\beta$. Thus it suffices to prove that any prime p can be written as a sum of four squares. We assume that $p \geq 5$ and proceed as follows. First we show that there exist $x, y \in \mathbb{Z}$ such that $x^2 + y^2 + 1 \equiv 0 (\mathrm{mod}\ p)$. Consider the sets $\{i^2 \in \mathbb{Z}/p\mathbb{Z} |\ 0 \leq i \leq \frac{p-1}{2}\}$ and $\{-1 - i^2 \in \mathbb{Z}/p\mathbb{Z} |\ 0 \leq i \leq \frac{p-1}{2}\}$. Each set consists of $\frac{p+1}{2}$ distinct elements in $\mathbb{Z}/p\mathbb{Z}$. Hence these sets overlap, and there exist x, y such that $x^2 \equiv -1 - y^2 (\mathrm{mod}\ p)$, as desired.
By shifting mod p we can see to it that we have $x, y \in \mathbb{Z}$ such that $x^2 + y^2 + 1 \equiv 0 (\mathrm{mod}\ p)$ and $|x|, |y| < p/2$. Application of Theorem 13.2.3 to the numbers p and $1 + xi + yj$ yields a common right-divisor $\delta \in \mathbf{q}$ (the right-'gcd') and $\alpha, \beta \in \mathbf{q}$ such that

$$\delta = \alpha p + \beta(1 + xi + yj). \tag{7.1}$$

In the remainder of the proof $b|a$ means: $\exists c \in \mathbf{q}$ such that $a = cb$. First of all, $\delta | p \Rightarrow N\delta | p^2 \Rightarrow N\delta = 1, p$ or p^2. Secondly, $\delta | (1 + xi + yj) \Rightarrow N\delta | (1 + x^2 + y^2) \Rightarrow N\delta < 2 \cdot (p/2)^2 + 1 < p^2$. Hence $N\delta = 1$ or p. Suppose $N\delta = 1$. Then, according to Theorem 13.4.4 δ is a unit. Multiply Eq.(7.1) on both sides from the right by $(1 - xi - yj)$ to obtain $\delta(1 - xi - yj) = \alpha(1 - xi - yj)p + \beta(1 + x^2 + y^2)$. Since

$p|(1+x^2+y^2)$ we infer $p|\delta(1-xi-yj)$ and hence $p|(1-xi-yj)$, which is clearly impossible. Thus we conclude that $N\delta = p$ and p is a sum of four squares. □

Not everyone may be charmed by quaternions and for this reason we give Lagrange's original proof of Theorem 7.2.1 as well.

Proof. Just as in the previous proof we note that it suffices to prove that every prime p can be written as the sum of four squares. This is a consequence of Euler's identity,

$$\begin{aligned}&(a^2+b^2+c^2+d^2)(a'^2+b'^2+c'^2+d'^2) = \\ &= (aa'+bb'+cc'+dd')^2 \\ &+(ab'-ba'+cd'-dc')^2 \\ &+(ac'-bd'-ca'+db')^2 \\ &+(ad'+bc'-cb'-da')^2.\end{aligned}$$

Just as above, we can find x, y such that $x^2+y^2+1 \equiv 0 (\text{mod } p)$ and $|x|, |y| \leq p/2$. We then have $x^2+y^2+1 = m_0 p$ and $m_0 \leq ((p/2)^2+(p/2)^2+1)/p < p$.
Let m be the smallest positive integer such that mp can be written as the sum of four squares. We will show that $m > 1$ leads to a contradiction. Suppose

$$mp = a^2+b^2+c^2+d^2 \quad \text{and} \quad m > 1. \tag{7.2}$$

Choose A, B, C, D in the interval $(-m/2, m/2]$ such that

$$a \equiv A (\text{mod } m),\ b \equiv B (\text{mod } m),\ c \equiv C (\text{mod } m)\ d \equiv D (\text{mod } m).$$

Then,

$$A^2+B^2+C^2+D^2 \equiv a^2+b^2+c^2+d^2 \equiv mp \equiv 0 (\text{mod } m).$$

Hence,

$$mr = A^2+B^2+C^2+D^2, \quad r \geq 0, \tag{7.3}$$

where $r = (A^2+B^2+C^2+D^2)/m \leq (4 \cdot (m/2)^2)/m = m$. First we show that $r \neq 0, m$. If $r = 0$, then $A = B = C = D = 0$ and hence $m^2|a^2+b^2+c^2+d^2 = mp$ from which follows $m|p$, contradicting $1 < m < p$. If $r = m$ then $A = B = C = D = m/2$ and hence $a \equiv b \equiv c \equiv d \equiv m/2 (\text{mod } m)$. Notice that if $x \equiv \frac{m}{2} (\text{mod } m)$ then $x^2 \equiv (\frac{m}{2})^2 (\text{mod } m^2)$. And so, $mp = a^2+b^2+c^2+d^2 \equiv 4(m/2)^2 \equiv 0 (\text{mod } m^2)$, which implies that $m^2|mp$ and thus $m|p$, again a contradiction. We conclude,

$$0 < r < m. \tag{7.4}$$

Notice that in the proof of (7.4) we have used the assumption $m > 1$. Now multiply (7.2) and (7.3) and use Euler's identity to obtain

$$mp \cdot mr = (a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2) = \alpha^2+\beta^2+\gamma^2+\delta^2$$

where

$$\begin{aligned}
\alpha &= aA + bB + cC + dD \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 (\text{mod } m) \\
\beta &= aB - bA + cD - dC \equiv ab - ab + cd - cd \equiv 0 (\text{mod } m) \\
\gamma &= aC - Ac + dB - bD \equiv ac - ac + bd - bd \equiv 0 (\text{mod } m) \\
\delta &= aD - dA + bC - cB \equiv ad - ad + bc - bc \equiv 0 (\text{mod } m)
\end{aligned}$$

So m divides $\alpha, \beta, \gamma, \delta$ and we find $rp = (\alpha/m)^2 + (\beta/m)^2 + (\gamma/m)^2 + (\delta/m)^2$. We conclude that rp is a sum of four squares and $0 < r < m$. This contradicts the minimality of m. Hence we have $m = 1$, as desired. □

For completeness we like to mention the following theorem,

Theorem 7.2.2 (Jacobi) *Let $n \in \mathbb{N}$. Then the number of solutions to*

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2, \qquad x_1, x_2, x_3, x_4 \in \mathbb{Z}$$

equals

$$8 \sum{}' d$$

where the $'$ denotes summation over all d with $d | n, 4 \not| d$.

As to the question whether positive integers can be written as a sum of three squares, we can easily give infinitely many counterexamples.

Theorem 7.2.3 *A positive integer of the form $4^l(8k+7)$ cannot be written as a sum of three squares.*

Proof. We proceed by induction on a. First of all, a number which is 7(mod 8) cannot be the sum of three squares, simply because the sum of three squares can never be 7(mod 8). This can easily be verified using the fact that a square can only be $0, 1$ or 4(mod 8).
Suppose $l \geq 0$ and suppose we proved our theorem for numbers of the form $4^l(8k+7)$. Let $n = 4^{l+1}(8k+7)$ and suppose $n = a^2+b^2+c^2$. Since $n \equiv 0 (\text{mod } 4)$ we have necessarily that a, b, c are all even. Hence $n/4 = (a/2)^2 + (b/2)^2 + (c/2)^2$, contradicting our induction hypothesis. □

The converse statement is much harder to prove.

Theorem 7.2.4 (Gauss) *Any positive integer not of the form $4^l(8k+7)$ can be written as the sum of three squares.*

Corollary 7.2.5 *Any positive integer can be written as the sum of three triangular numbers.*

A triangular number is a number of the form $\binom{n}{2}$.

Proof. Let $n \in \mathbb{N}$. Write $8n+3$ as the sum of three squares, $8n+3 = a^2+b^2+c^2$. Notice that a, b, c all have to be odd. Write $a = 2p-1, b = 2q-1, c = 2r-1$. Then $8n+3 = 4(p^2-p)+4(q^2-q)+4(r^2-r)+3$ and this amounts to

$$n = \binom{p}{2} + \binom{q}{2} + \binom{r}{2}.$$

(Quoting Gauss: $EUREKA: \ num = \Delta + \Delta + \Delta$!!) □

Gauss also proved results on the number of representations of a number as sum of three squares. As a curiosity we mention

Theorem 7.2.6 *Let p be a prime with $p \equiv 3 (\mathrm{mod}\ 8)$. Then the number of solutions to $p = x^2+y^2+z^2, \quad x, y, z \in \mathbb{Z}$ equals*

$$\frac{-24}{p} \sum_{a=1}^{p-1} a \left(\frac{a}{p}\right).$$

You might recognize the class number $h(-p)$ (see subsection 5.6) in this theorem. So the number of ways in which a prime $p \equiv 3 (\mathrm{mod}\ 8)$ can be written as sum of three squares equals $24h(-p)$.
Notice that squares can be considered as quadrangular numbers and Theorem 7.2.1 can be described cryptically as $n = \square + \square + \square + \square$. Of course we can generalise this and speak of pentagonal, hexagonal,... numbers. The general form of the k-gonal numbers is $(k-2)\binom{n}{2}+n$. We mention the following theorem, conjectured by Fermat and proven by Cauchy.

Theorem 7.2.7 (Cauchy) *Any positive integer can be written as the sum of k k-gonal numbers.*

7.3 The 15-theorem

Recently Conway and Schneeberger found a remarkable theorem on the representation of integer by quadratic form. An integral *quadratic form* $F(x_1, \ldots, x_r)$ in r variables is a homogeneous polynomial of degree 2 with integer coefficients. It is called *even* if the coefficients of the terms $x_i x_j$ with $i \neq j$ are all even. The form F is called *positive definite* if $F(x_1, \ldots, x_r) > 0$ for all choices of $(x_1, \ldots, x_r) \neq (0, \ldots, 0)$.
We say that a quadratic form F represents an integer if there exist integers $x_1, \ldots, x_r$ such that $n = F(x_1, \ldots, x_r)$. For example, the form $x_1^2+x_2^2+x_3^2+x_4^2$ represents all positive integers. In 1993 Conway and Schneeberger announced the following remarkable theorem.

Theorem 7.3.1 (Conway, Schneeberger, 1993) *An integral, even positive definite quadratic form represents all positive integers if and only if it represents* $1, 2, 3, 5, 6, 7, 10, 14, 15$.

So, if we want to show that every positive integer can be written in the form $2x^2+2xy+y^2+z^2+u^2$ with x, y, z, u integers, all we have to do is check whether each of the numbers $1, 2, 3, 5, 6, 7, 10, 14, 15$ can be written in this way. A simple check shows that this is indeed the case.
The proof of this theorem was quite complicated and never published. However, in 2000 Manjul Bhargava found a simpler proof and a generalisation to all positive quadratic forms known as the 290-theorem.

Theorem 7.3.2 (Bhargava, Hanke, 2005) *An integral, positive definite quadratic form represents all positive integers if and only if it represents*

$$1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22,$$

$$23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110,$$

$$145, 203, 290.$$

7.4 Waring's problem

Around 1770 Waring put forward the following question . Let $k \in \mathbb{N}$ and $k \geq 2$. Is there a number $g(k)$ such that any positive integer is the sum of at most $g(k)$ non-negative k-th powers? About 140 years later, in 1909, Hilbert proved that the answer is 'yes' for any $k \geq 2$. His method is quite complicated and we shall not reproduce it here. Somewhat later Hardy and Littlewood developed a more conceptual approach to the problem and showed, among other things, that there exists $g(k) \leq 3 \cdot 2^k$. From now on we shall denote by $g(k)$ the *smallest* number for which Waring's problem is solvable. The method of Hardy and Littlewood, and further modifications and improvements of it, are known as *circle methods*, which have now become a standard tool in number theory (see R.C.Vaughan, *The circle method*). It is now known that $g(2) = 4$ (Lagrange,1770), $g(3) = 9$ (Wieferich,Kempner,1912), $g(4) = 19$ (Balusabramanian, Deshouillers, Dress, 1986), $g(5) = 37$ (Chen-Jingrun, 1964). For $k \geq 6$ we have, if $(3/2)^k - [(3/2)^k] > 1 - (3/4)^k$ then $g(k) = [(3/2)^k] + 2^k - 2$. It is very likely, but not quite proved yet, that the inequality always holds.
Although $g(3) = 9$ it turns out that only 23 and 239 require 9 cubes, all other numbers can be written as the sum of at most 8 positive cubes. In connection with this we can define $G(k)$, the smallest integer such that any *sufficiently large* integer can be written as the sum of at most $G(k)$ k-th powers. Since infinitely many numbers are not the sum of three or less squares we have $G(2) = 4$. It is also known that $4 \leq G(3) \leq 7$. It is generally suspected that $G(3) = 4$ but no

one has any idea how to prove this. By a refined version of the circle method I.M.Vinogradov was able to show that $G(k) \leq 6k(\log k + 4 + \log 216)$ and Wooley, in 1992 improved this to $G(k) \leq k \log k(1 + o(1))$. Special results are $G(4) = 16$, $G(5) \leq 17$ (conjectured: 6), $G(6) \leq 24$ (conjectured: 9), $G(7) \leq 33$ (conjectured: 8), $G(8) \leq 42$ (conjectured: 32), $G(9) \leq 50$ (conjectured: 13), $G(10) \leq 59$ (conjectured: 12) (see Vaughan and Wooley, Number Theory for the Milennium III p301-340 A.K.Peters, 2000).
A variation on Waring's problem is the following easier problem. Let $k \in \mathbb{N},\ k \geq 2$. Does there exist a number s such that any $n \in \mathbb{N}$ can be written in the form

$$n = \pm x_1^k \pm x_2^k \pm \cdots \pm x_s^k \ ?$$

If such an s exists we denote its minimal value by $v(k)$. Notice that when k is odd this question comes down to Waring's problem for k-th powers of numbers in $\mathbb{Z}$.

Theorem 7.4.1 *We have* $v(k) \leq 2^{k-1} + (k!)/2$.

Proof. We introduce the difference operator Δ which acts on polynomials $f(x)$ by $(\Delta f)(x) = f(x+1) - f(x)$. Notice that Δ decreases the degree of a polynomial by one. Furthermore,

$$\Delta \binom{x}{k} = \binom{x+1}{k} - \binom{x}{k} = \binom{x}{k-1}.$$

Notice also that

$$\binom{x}{k} + \frac{k-1}{2}\binom{x}{k-1} = \frac{x^k}{k!} + r(x)$$

where $r(x)$ has degree $\leq k-2$. Application of the operator Δ^{k-1} yields

$$x + \frac{k-1}{2} = \Delta^{k-1}\left(\frac{x^k}{k!}\right).$$

Hence $\Delta^{k-1}x^k = k!x + \frac{k-1}{2}k!$. The expression $\Delta^{k-1}x^k$ can be considered as the sum of 2^{k-1} terms of the form $\pm m^k$. Now let $n \in \mathbb{N}$. Determine $x, l \in \mathbb{Z}$ such that

$$n = k!x + \frac{k-1}{2}k! + l, \qquad |l| \leq \frac{1}{2}k!.$$

Hence $n = \Delta^{k-1}x^k + l$. Notice that l can be written as the sum of $|l|$ terms 1^k or -1^k. Since $|l| \leq (k!)/2$ we obtain $v(k) \leq 2^{k-1} + (k!)/2$. □

The bound of Theorem 7.4.1 is much larger than the actual value of $v(k)$. If we accept the known upper bounds for $G(k)$ Theorem 7.4.2 yields a much better result. However, the advantage of Theorem 7.4.1 is that it is simple and self-contained.

Theorem 7.4.2 *We have* $v(k) \leq G(k) + 1$.

Proof. Let $n \in \mathbb{N}$. Choose y^k sufficiently large so that $n + y^k$ can be written as the sum of at most $G(k)$ positive k-th powers, $n + y^k = x_1^k + \cdots + x_{G(k)}^k$. Hence $v(k) \leq G(k) + 1$. □

Theorem 7.4.3 *We have* $v(2) = 3$ *and* $v(3) = 4$ *or* 5.

Proof. Theorem 7.4.1 gives us $v(2) \leq 2 + 1$. Notice that also $v(2) \geq 3$ because sums of the form $\pm a^2 \pm b^2$ which are positive can never be $6 (\mathrm{mod}\ 8)$. Hence $v(2) = 3$.
Let $n \in \mathbb{N}$. Notice that $n^3 - n$ is divisible by 6. Write $n^3 - n = 6x$. Notice also that $6x = (x-1)^3 + (x+1)^3 - 2x^3$. Hence $n = n^3 - (x-1)^3 - (x+1)^3 + 2x^3$ and we see that $v(3) \leq 5$. Moreover, cubes are always $0, \pm 1 (\mathrm{mod}\ 9)$, so a sum of three cubes can never be $\pm 4 (\mathrm{mod}\ 9)$. Hence $v(3) \geq 4$. □

It is generally believed, but not proved yet, that $v(3) = 4$.
Another variation on Waring's problem is the question, is there a number s such that any $n \in \mathbb{N}$ can be written as the sum of s non-negative k-th powers of rational numbers? I do not know of a simple proof for the existence of such s but of course the positive solution to Waring's problem also implies a positive answer to our question. In fact, we can take $s \leq G(k)$. For the otherwise elusive case $k = 3$ we have a particularly nice solution.

Theorem 7.4.4 (Riley, 1825) *Any* $n \in \mathbb{N}$ *can be written as the sum of three positive rational cubes in infinitely many ways.*

Proof. Let $A = 12t(t+1) - (t+1)^3$, $\quad B = (t+1)^3 - 12t(t-1)$, $\quad C = 12t(t-1)$ and consider the identity

$$A^3 + B^3 + C^3 = 72t(t+1)^6.$$

Let $n \in \mathbb{N}$. Choose $u \in \mathbb{Q}$ such that $1 < nu^3/72 < 2$ and take $t = nu^3/72$. Then $A, B, C, t, t+1$ are all positive and we get

$$\left(\frac{A}{u(t+1)^2}\right)^3 + \left(\frac{B}{u(t+1)^2}\right)^3 + \left(\frac{C}{u(t+1)^2}\right)^3 = n.$$

Moreover, u can be choosen in infinitely many ways. □

7.5 Exercises

Exercise 7.5.1 *Let $r_2(n)$ be the number of solutions $x, y \in \mathbb{Z}$ to $n = x^2 + y^2$. Let $R(X) = \sum_{n \leq X} r_2(n)$. Prove that*

$$R(X) = \pi X + O(\sqrt{X}),$$

in other words, $|R(X) - \pi X|/\sqrt{X}$ is bounded (for all $X \geq 1$). (Hint: count the number of lattice points inside the disk with radius $\sqrt{X}$).

Exercise 7.5.2 *Find all ways to write 425 as sum of two squares.*

Exercise 7.5.3 *Which numbers can be written as a difference of two squares?*

Exercise 7.5.4 *(H.W.Lenstra jr.) Notice, $12^2 + 33^2 = 1233$, $588^2 + 2353^2 = 5882353$. Can you find more of such examples?*

Exercise 7.5.5 *Let p be a prime number such that $p \equiv 1, 3 \pmod 8$. Prove that there exist $x, y \in \mathbb{Z}$ such that $p = x^2 + 2y^2$. (Hint: prove that $\mathbb{Z}[\sqrt{-2}]$ is euclidean.)*

Exercise 7.5.6 *a) Show that 7 cannot be written as a sum of three squares (i.e. $g(2) > 3$).*
b) Show that 23 and 239 cannot be written as sum of at most 8 cubes (i.e. $g(3) > 8$).
c) Find $N \in \mathbb{N}$ such that N cannot be written as a sum of at most 18 fourth powers (i.e. $g(4) > 18$).

Exercise 7.5.7 *Let $g(k)$ be the function from Waring's problem. Prove that $g(k) \geq 2^k + [(3/2)^k] - 2$. (Hint: consider $n = 2^k[(3/2)^k] - 1$.)*

Exercise 7.5.8 *We are given the identity*

$$\begin{aligned} 6(a^2+b^2+c^2+d^2)^2 &= (a+b)^4 + (a-b)^4 + (c+d)^4 \\ &\quad +(c-d)^4 + (a+c)^4 + (a-c)^4 \\ &\quad +(b+d)^4 + (b-d)^4 + (a+d)^4 \\ &\quad +(a-d)^4 + (b+c)^4 + (b-c)^4. \end{aligned}$$

Prove that $g(4) \leq 53$. (Hint: write $n = 6N + r$ and N as sum of four squares.) Refine the argument to show that $g(4) \leq 50$.

Exercise 7.5.9 *Show that 5 cannot be written as the sum of 4 fourth powers of rational numbers. (Hint: look modulo 5).*
Can you find other numbers that cannot be written as sum of 4 rational fourth powers?

Chapter 8

Continued fractions

8.1 Introduction

Let $\alpha \in \mathbb{R}$. The *continued fraction* algorithm for α runs as follows.

$x_0 = \alpha$

$a_0 = [x_0], \qquad x_1 = 1/\{x_0\}$

$a_1 = [x_1], \qquad x_2 = 1/\{x_1\}$

.....

$a_n = [x_n], \qquad x_{n+1} = 1/\{x_n\}$

.....

Notice that $x_i \geq 1$ for all $i \geq 1$. The algorithm is said to *terminate* if $\{x_n\} = 0$ for some n. Notice that

$$\alpha = a_0 + \frac{1}{x_1} = a_0 + \frac{1}{a_1 + \frac{1}{x_2}} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots}}$$

which is denoted as

$$\alpha = [a_0, x_1] = [a_0, a_1, x_2] = [a_0, a_1, a_2, \dots] .$$

Theorem 8.1.1 *The continued fraction algorithm terminates if and only if* $\alpha \in \mathbb{Q}$.

Proof. Suppose we have termination, i.e. $\{x_n\} = 0$ for some n. Then $\alpha = [a_0, a_1, \dots, a_{n-1}]$ and we see trivially that $\alpha \in \mathbb{Q}$.
If $\alpha \in \mathbb{Q}$ then the x_i are all rational numbers, say $x_i = p_i/q_i$ with $p_i, q_i \in \mathbb{N}$ and $p_i > q_i$ for all i. Notice that $q_{i+1} = p_i - [p_i/q_i]q_i$ for all i, hence $q_1 > q_2 > q_3 > \cdots > 0$. So we see that the algorithm terminates. □

In fact, when α is rational, $\alpha = p/q$ then the continued fraction algorithm is nothing but the Euclidean algorithm applied to p, q.

Theorem 8.1.2 *Let $a_0, a_1, \ldots, a_n \in \mathbb{R}$. Suppose*

$$\begin{array}{llll} p_{-2}=0 & p_{-1}=1 & p_0=a_0 & p_n = a_n p_{n-1} + p_{n-2} \quad (n \geq 0) \\ q_{-2}=1 & q_{-1}=0 & q_0=1 & q_n = a_n q_{n-1} + q_{n-2} \quad (n \geq 0) \end{array}$$

Then,

$$[a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n}.$$

Proof. By induction on n we shall show that $[a_0, \ldots, a_n] = (a_n p_{n-1} + p_{n-2})/(a_n q_{n-1} + q_{n-2})$. For $n = 0$ this is trivial. Now suppose $n \geq 0$. Notice that

$$\begin{aligned} [a_0, a_1, \ldots, a_n, a_{n+1}] &= [a_0, a_1, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}] \\ &= \frac{(a_n + 1/a_{n+1})p_{n-1} + p_{n-2}}{(a_n + 1/a_{n+1})q_{n-1} + q_{n-2}} \\ &= \frac{a_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_n q_{n-1} + q_{n-2}) + q_{n-1}} \\ &= \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}} \end{aligned}$$

which completes our induction step. □

From now on we shall adhere to the notations $\alpha = [a_0, a_1, \ldots]$, $[a_0, a_1, \ldots, a_n] = p_n/q_n$ for the continued fraction expansion of α. We call $a_0, a_1, a_2, \ldots$ the *partial fractions* of the continued fraction and the p_n/q_n the *convergents*. Why the p_n/q_n are called convergents will become clear from the following theorem.

Theorem 8.1.3 *Let notation be as above. Then, for all $n \geq 0$,*

1. $$p_{n-1}q_n - p_n q_{n-1} = (-1)^n.$$

2. $$\alpha - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(x_{n+1}q_n + q_{n-1})}.$$

Proof. Part (1) is proved by induction on n, the case $n = 0$ being trivial.

$$\begin{aligned} p_n q_{n+1} - p_{n+1}q_n &= \begin{vmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{vmatrix} = \begin{vmatrix} p_n & a_{n+1}p_n + p_{n-1} \\ q_n & a_{n+1}q_n + q_{n-1} \end{vmatrix} \\ &= \begin{vmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{vmatrix} = -\begin{vmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{vmatrix} = -(-1)^n = (-1)^{n+1} \end{aligned}$$

Part (2) follows from $\alpha = [a_0, a_1, \ldots, a_n, x_{n+1}] = \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}}$ and a straightforward computation of the difference $\alpha - \frac{p_n}{q_n}$. □

Corollary 8.1.4 *For all convergents p_n/q_n we have*

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_{n+1}q_n} < \frac{1}{a_{n+1}q_n^2}$$

We see from the previous corollary that convergents p/q of the continued fraction of an irrational number α have the property that

$$\left|\frac{p}{q} - \alpha\right| < \frac{1}{q^2} \tag{8.1}$$

In particular this means the convergent give very good rational approximations with respect to their denominator. As an example consider

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, \dots].$$

From the theory we expect that $|\pi - p/q| < 1/(292q^2)$ where $p/q = [3, 7, 15, 1]$ which equals 355/113. In fact,

$$\pi - \frac{355}{113} = -0.000000266764$$

and 355/113 approximates π up to 6 decimal places. Note that there does not seem to be any regularity in the continued fraction of π.
Here are some other examples of continued fraction expansions:

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, \dots]$$

$$e^2 = [7, 2, 1, 1, 3, 18, 5, 1, 1, 6, 30, 8, 1, 1, 9, 42, 11, 1, 1, \dots]$$

$$e^3 = [20, 11, 1, 2, 4, 3, 1, 5, 1, 2, 16, 1, 1, 16, 2, 13, 14, 4, 6, 2, 1, 1, 2, 2, \dots]$$

$$\sqrt{2} = [1, 2, 2, 2, 2, 2, 2, \dots]$$

$$\sqrt{97} = [9, 1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18, 1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18, 1, \dots]$$

$$\sqrt{47} = [6, 1, 5, 1, 12, 1, 5, 1, 12, 1, 5, 1, 12, 1, 5, 1, \dots]$$

It is interesting to note the regularity in the expansions of e, e^2 and $\sqrt{N}$, but not in e^3. We shall reurn to the periodicity of the expansion of $\sqrt{N}$ in the next section.
It also turns out that if a fraction p/q satisfies (8.1) then it is almost a convergent of the continued fraction of α.

Theorem 8.1.5 (Legendre) *Suppose $\alpha \in \mathbb{R}$ and $p, q \in \mathbb{Z}$, $q > 0$ such that*

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

Then p/q is a convergent of the continued fraction of α

Proof. Let $p_0/q_0, p_1/q_1, \ldots$ be the convergents of the continued fraction of α. Choose n such that $q_n \leq q < q_{n+1}$. Let us assume $p/q \neq p_n/q_n$, otherwise we are done. Then we have the following inequalities,

$$\frac{1}{qq_n} \leq \left|\frac{p}{q} - \frac{p_n}{q_n}\right| \leq \left|\alpha - \frac{p_n}{q_n}\right| + \left|\alpha - \frac{p}{q}\right| < \frac{1}{q_n q_{n+1}} + \frac{1}{2q^2}$$

Multiply these inequalities with qq_n to obtain $1 < \frac{q_n}{2q} + \frac{q}{q_{n+1}}$. When $q_{n+1} \geq 2q$ we find, using $q_n \leq q$ that $1 < 1/2 + 1/2$ which is a contradiction.
So let us assume $q_{n+1} < 2q$. We now repeat our estimates with a little more care. Suppose first that $\alpha - p/q$ and $\alpha - p_n/q_n$ have the same sign. Then the absolute value of their difference, which equals $|p/q - p_n/q_n|$, is bounded above by $\max(1/2q^2, 1/q_n q_{n+1})$. It is bounded below by $1/qq_n$. Multiplication by qq_n yields $1 < max(q_n/2q, q/q_{n+1}) < \max(1/2, 1) = 1$, again a contradiction.
Now suppose that $\alpha - p/q$ and $\alpha - p_n/q_n$ have opposite sign. Then $\alpha - p/q$ and $\alpha - p_{n+1}/q_{n+1}$ have the same sign. Just as above we derive $1 < \max(q_{n+1}/2q, q/q_{n+2})$. Using $q_{n+1} < 2q$ we find $1 < \max(1, 1) = 1$, again a contradiction. □

Here is a very useful lemma in all that follows.

Lemma 8.1.6 *Let* $\alpha = [a_0, a_1, a_2, \ldots, a_m, \beta]$. *Then* $-1/\beta = [a_m, \ldots, a_2, a_1, a_0, -1/\alpha]$.

Proof. This goes by induction on m. For $m = 0$ the lemma is clear,

$$\alpha = [a_0, \beta] \Rightarrow \alpha = a_0 + \frac{1}{\beta} \Rightarrow -\frac{1}{\beta} = a_0 + \frac{1}{-1/\alpha} \Rightarrow -\frac{1}{\beta} = [a_0, -\frac{1}{\alpha}].$$

Suppose $m > 0$. Then, $\alpha = [a_0, \ldots, a_{m-1}, a_m + 1/\beta]$. By the induction hypothesis we obtain

$$-\frac{1}{a_m + 1/\beta} = [a_{m-1}, \ldots, a_1, a_0, -\frac{1}{\alpha}]$$

Invert on both sides and add a_m to obtain

$$-\frac{1}{\beta} = [a_m, \ldots, a_2, a_1, a_0, -\frac{1}{\alpha}]$$

□

8.2 Continued fractions for quadratic irrationals

A real, non-rational number α which satisfies a polynomial equation of degree 2 over $\mathbb{Q}$ is called a *quadratic irrational* . Given a quadratic irrational there exist, up to common sign change, a unique triple of integers A, B, C such that $A\alpha^2 + B\alpha + C = 0$ and $\gcd(A, B, C) = 1$, $AC \neq 0$. The polynomial $AX^2 + BX + C$ is called the *minimal polynomial* of α. The number $D = B^2 - 4AC$ is called the *discrminant* of α. If $\alpha = a + b\sqrt{D}$ for some $a, b \in \mathbb{Q}$ we call $a - b\sqrt{D}$ its *conjugate* and denote it by $\overline{\alpha}$. A quadratic irrational α is called *reduced* if $\alpha > 1$ and $-1 < \overline{\alpha} < 0$.

Theorem 8.2.1 *Let α be a quadratic irrational of discriminant D. Put $x_0 = \alpha$ and define recursively $x_{n+1} = 1/(x_n - [x_n])$. Then each x_n has discriminant D and there exists n_0 such that x_n is reduced for all $n > n_0$.*

Proof. That the discrimant does not change is clear if we realise that α and $\alpha - m$ have the samen discriminant for any $m \in \mathbb{Z}$ and that α and $1/\alpha$ have the same discrminant.
Denote by $\overline{x_n}$ the conjugate of x_n. Notice that $x_n > 1$ for all $n \geq 1$. Verify also that if x_n is reduced the same holds for $x_{n+1}, x_{n+2}, \ldots$.
Let m be the smallest index such that $[x_m] \neq [\overline{x_m}]$. If such an m would not exist, both α and $\overline{\alpha}$ have the same continued fraction expansion.
Suppose that $[\overline{x_m}] < [x_m]$. Then notice that $\overline{x_{m+1}} = 1/(\overline{x_m} - [x_m]) < 0$. From $\overline{x_{m+2}} = 1/(\overline{x_{m+1}} - [x_{m+1}])$ and $\overline{x_{m+1}} < 0$ we then conclude that $-1 < \overline{x_{m+2}} < 0$, hence x_{m+2} is reduced.
Now suppose that $[\overline{x_m}] > [x_m]$. Then $\overline{x_{m+1}} = 1/(\overline{x_m} - [x_m]) < 1$. Hence $[\overline{x_{m+1}}] = 0 < [x_{m+1}]$ and we continue as in the preceding case. □

Theorem 8.2.2 *There exist finitely many reduced quadratic irrationals of given discriminant D.*

Proof. Let α be such a quadratic irrational and write $\alpha = \frac{\sqrt{D}+P}{Q}$ with $P, Q \in \mathbb{Z}$, $Q \neq 0$ (we take $\sqrt{D} > 0$.
From $\alpha > 0 > \overline{\alpha}$ it follows that $Q > 0$. From $\alpha > 1 > -\overline{\alpha}$ it follows that $\sqrt{D} + P > \sqrt{D} - P$, hence $P > 0$. From $\overline{\alpha} < 0$ it follows that $P - \sqrt{D} < 0$, hence $P < \sqrt{D}$. From $\alpha > 1$ we conclude $P + \sqrt{D} > Q$, hence $Q < 2\sqrt{D}$.
Concluding, we find that $0 < P < \sqrt{D}$ and $0 < Q < 2\sqrt{D}$, hence we have at most finitely many possibilities. □

Let $[a_0, a_1, a_2, \ldots]$ be the continued fraction expansion of a real number. We say that the expansion is *periodic* if there exist $n_0 \in \mathbb{Z}, N \in \mathbb{N}$ such that $a_{n+N} = a_n$ for all $n \geq n_0$. We call the expansion *purely periodic* if $n_0 = 0$.

Theorem 8.2.3 *Let $\alpha \in \mathbb{R}$. Then the continued fraction expansion of α is periodic if and only if α is a quadratic irrational. It is purely periodic if and only if α is reduced.*

Proof. We first prove our theorem for purely periodic expansions. Suppose α has a purely periodic continued fraction. Then there exists an r such that $\alpha = [a_0, a_1, \ldots, a_r, \alpha]$. Hence

$$\alpha = \frac{\alpha p_r + p_{r-1}}{\alpha q_r + q_{r-1}}$$

This implies $q_r\alpha^2 + (q_{r-1} - p_r)\alpha - p_{r-1} = 0$. First of all we see that α is a quadratic irrational. Since its continued fraction is purely periodic we must have $a_0 \geq 1$,

hence $\alpha > 1$. From the quadratic equation we see that $\alpha\overline{\alpha} = -p_{r-1}/q_r$. Using either $p_{r-1}/q_r = (p_{r-1}/q_{r-1})(q_{r-1}/q_r)$ or $p_{r-1}/q_r = (p_{r-1}/p_r)(p_r/q_r)$ we conclude that $p_{r-1}/q_r < \alpha$, hence $-1 < \overline{\alpha} < 0$. So α is reduced.
Suppose conversely that α is a reduced quadratic irrational. Let $x_0 = \alpha$ and recursively $x_{n+1} = 1/(x_n - [x_n])$. Since x_0 is reduced, all x_i are reduced. Moreover their discriminants are all the same, hence there exist only finitely many distinct x_i. So there exist $r < s$ such that $x_r = x_s$. Notice that the value of a_n follows uniquely from x_{n+1} by the condition that x_n is reduced, namely $a_n = [-1/\overline{x_{n+1}}]$. Hence $x_n = [-1/\overline{x_{n+1}}] + 1/x_{n+1}$. In particular it follows from $x_r = x_s$ that $x_{r-1} = x_{s-1}$, etcetera, hence $x_0 = x_{s-r}$. So the continued fraction of $x_0 = \alpha$ is purely periodic.
Now suppose that α has a periodic continued fraction. Then there exists β with a purely periodic expansion such that $\alpha = [a_0, a_1, \ldots, a_{n_0}, \beta]$. We know that β is a quadratic irrational from the above, hence the same holds for α. Suppose conversely that α is a quadratic irrational. Then we know that there is a reduced β such that $\alpha = [a_0, \ldots, a_{n_0}, \beta]$. Since β has periodic continued fraction, the same holds for α. □

For quadratic irrational numbers of the form $\sqrt{N}$, $N \in \mathbb{N}$ not a square, we obtain the following theorem.

Theorem 8.2.4 *Let $N \in \mathbb{N}$ and suppose N is not a square. Then $\sqrt{N} = [a_0, \overline{a_1, \ldots, a_r, 2a_0}]$ where $a_0 = [\sqrt{N}]$. Moreover, $(a_1, a_2, \ldots, a_r) = (a_r, \ldots, a_2, a_1)$.*

Proof. First observe that $a_0 = [\sqrt{N}]$ is the result of the first step in the continued fraction algorithm. Now note that $\sqrt{N} + a_0$ is reduced quadratic irrational, since $\sqrt{N} + a_0 > 1$ and $-1 < -\sqrt{N} + a_0 < 0$. Hence it has a purely periodic continued fraction of the form

$$\sqrt{N} + a_0 = [\overline{2a_0, a_1, a_2, \ldots, a_r}] = [2a_0, \overline{a_1, a_2, \ldots, a_r, 2a_0}].$$

After subtraction of a_0 on both sides we obtain $\sqrt{N} = [a_0, \overline{a_1, \ldots, a_r, 2a_0}]$, as asserted. Notice also that $\sqrt{N} + a_0 = [2a_0, a_1, a_2, \ldots, a_r, \sqrt{N} + a_0]$. Substract $2a_0$ on both sides to find $\sqrt{N} - a_0 = [0, a_1, a_2, \ldots, a_r, \sqrt{N} + a_0]$. Hence

$$\frac{1}{\sqrt{N} - a_0} = [a_1, a_2, \ldots, a_r, \sqrt{N} + a_0].$$

Application of Lemma 8.1.6 yields

$$-\frac{1}{\sqrt{N} + a_0} = [a_r, \ldots, a_2, a_1, a_0 - \sqrt{N}]$$

This algebraic identity remains true if we replace $\sqrt{N}$ by $-\sqrt{N}$,

$$-\frac{1}{-\sqrt{N} + a_0} = [a_r, \ldots, a_2, a_1, a_0 + \sqrt{N}].$$

Invert both sider and add $2a_0$ to obtain

$$\sqrt{N} + a_0 = [2a_0, a_r, \ldots, a_2, a - 1, \sqrt{N} + a_0].$$

So we see that the continued fraction of $\sqrt{N}+a_0$ is also given by $[\overline{2a_0, a_r, \ldots, a_2, a_1}]$. Hence $(a_1, a_2, \ldots, a_r) = (a_r, \ldots, a_2, a_1)$. □

8.3 Pell's equation

Suppose $N \in \mathbb{N}$ is not a square and consider the diophantine equation

$$x^2 - Ny^2 = 1$$

in the unknowns $x, y \in \mathbb{Z}_{\geq 0}$. Although problems related to his equation have been around since antiquity, the first general method for solving it was given by W.Brouncker in 1657. He was able to use his method to obtain the smallest solution

$$(x, y) = (32188120829134849, 1819380158564160)$$

to $x^2 - 313y^2 = 1$! Brouncker's method was described in Wallis's book on algebra and number theory. Euler mistakenly assumed from Wallis's book that the method was due to John Pell, another English mathematician. Very soon Pell's name stuck to this equation. For several values of N we list the solution with minimal x,

$$\begin{aligned} 3^2 - 2 \cdot 2^2 &= 1 \\ 649^2 - 13 \cdot 180^2 &= 1 \\ 1766319049^2 - 61 \cdot 226153980^2 &= 1 \end{aligned}$$

Looking at these examples one observes that it is quite a miracle that any non-trivial solution for $x^2 - 61y^2 = 1$ exists. Nevertheless, using continued fractions it is possible to show that there always exists a non-trivial solution.

Proposition 8.3.1 *Let $N \in \mathbb{N}$ and suppose N is not a square. Then there exist $x, y \in \mathbb{N}$ such that $x^2 - Ny^2 = 1$.*

Proof. For $N = 2, 3, 5, 6$ our theorem is true since we have $3^2 - 2 \cdot 2^2 = 1$, $2^2 - 3 \cdot 1^2 = 1$, $9^2 - 5 \cdot 4^2 = 1$, $5^2 - 6 \cdot 2^2 = 1$. So we can assume that $N \geq 7$. Consider the continued fraction expansion of $\sqrt{N}$ given by

$$\sqrt{N} = [a_0, \overline{a_1, \ldots, a_r, 2a_0}]$$

say. Let $p/q = [a_0, a_1, \ldots, a_r]$. Then, from our elementary estimates we find that

$$\left| \frac{p}{q} - \sqrt{N} \right| < \frac{1}{2a_0 q^2}.$$

Multiply on both sides by $|p/q + \sqrt{N}|$ and use the fact that $|p/q + \sqrt{N}| \leq (2\sqrt{N}+1)$. We find,

$$\left|\frac{p^2}{q^2} - N\right| < \frac{2\sqrt{N}+1}{2a_0q^2}.$$

Multiply on both sides by q^2 to find $|p^2 - Nq^2| < (2\sqrt{N}+1)/2[\sqrt{N}]$. When $N \geq 7$ we have

$$\frac{2\sqrt{N}+1}{2[\sqrt{N}]} < \frac{2\sqrt{N}+1}{2(\sqrt{N}-1)} < 2$$

Hence $|p^2-Nq^2| < 2$. So we have either $p^2-Nq^2 = -1$ or $p^2-Nq^2 = 1$. (why can't we have $p^2 - Nq^2 = 0$?). In case $p^2 - Nq^2 = 1$ we find $x = p, y = q$ as solution. In case $p^2 - Nq^2 = -1$ we notice that $(p^2 + Nq^2)^2 - N(2pq)^2 = (p^2 - Nq^2)^2 = 1$. Hence we have the solution $x = p^2 + Nq^2, y = 2pq$. □

Now that we established the existence of non-trivial solutions to Pell's equation we would like to have the full set. An important remark to this end is the following trick which we illustrate by an example. Notice that $3^2 - 2 \cdot 2^2 = 1$ is equivalent to $(3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 1$. Take the square on both sides and use the fact that

$$(3 \pm 2\sqrt{2})^2 = 17 \pm 12\sqrt{2}$$

Hence $(17 + 12\sqrt{2})(17 - 12\sqrt{2})$ which implies $17^2 - 2 \cdot 12^2 = 1$. We can also take the cube of $(3 + 2\sqrt{2})$ to obtain $99 + 70\sqrt{2}$. We then find $99^2 - 2 \cdot 70^2 = 1$. So, given one solution of Pell's equation we can construct infinitely many! If we start with the smallest positive solution we get all solutions in this way, as shown in the following theorem.

Theorem 8.3.2 *Choose the solution of Pell's equation with $x + y\sqrt{N} > 1$ and minimal. Call it (p, q). Then, to any solution $x, y \in \mathbb{N}$ of Pell's equation there exists $n \in \mathbb{N}$ such that $x + y\sqrt{N} = (p + q\sqrt{N})^n$.*

Proof. Notice that if $u, v \in \mathbb{Z}$ satisfy $u^2 - Nv^2 = 1$ and $u + v\sqrt{N} \geq 1$, then $u - v\sqrt{N}$, being equal to $(u + v\sqrt{N})^{-1}$ lies between 0 and 1. Addition of the inequalities $u + v\sqrt{N} \geq 1$ and $1 \leq u - v\sqrt{N} > 0$ implies $u \geq 0$. Substraction of these inequalities yields $v > 0$. We call $u + v\sqrt{N}$ the size of the solution u, v.
Now let $x, y \in \mathbb{N}$ be any solution of Pell's equation. Notice that $(x + y\sqrt{N})(p - q\sqrt{N}) = (px - qyN) + (py - qx)\sqrt{N}$. Let $u = px - qyN, v = py - qx$ and we have $u^2 - Nv^2 = 1$ and $u + v\sqrt{N} = (x + y\sqrt{N})/(p + q\sqrt{N})$. Observe that

$$1 \leq \frac{x + y\sqrt{N}}{p + q\sqrt{N}} < (x + y\sqrt{N})/2,$$

hence $1 <= u + v\sqrt{N} < (x + y\sqrt{N})/2$. So we have found a new solution with positive coordinates and size bounded by half the size of $x+y\sqrt{N}$. By repeatedly

performing this operation we obtain a solution whose size is less than the size of $p+q\sqrt{N}$. By the minimality of p,q this implies that this last solution should be $1,0$. Supposing the number of steps is n we thus find that $x+y\sqrt{N} = (p+q\sqrt{N})^n$. □

In the existence proof for solutions to Pell's equation we have used the continued fraction of $\sqrt{N}$. It turns out that we can use this algorithm to find the smallest solution and also all solutions of other equations of the form $x^2-Ny^2=k$ for small k.

Theorem 8.3.3 *Suppose we have $x,y \in \mathbb{N}$ such that $|x^2-Ny^2| \leq \sqrt{N}$. Then x/y is a convergent to the continued fraction of $\sqrt{N}$.*

Proof. Let $M=[\sqrt{N}]$. Since x^2-Ny^2 is integral the inequality $|x^2-Ny^2|<\sqrt{N}$ implies $|x^2-Ny^2| \leq M$. We first show that $x \geq My$. If $x<My$ we would have the following sequence of inequalities,

$$x^2-Ny^2 < x^2-M^2y^2 = (x-yM)(x+yM) < -M$$

contradicting $|x^2-Ny^2| \leq M$. So we have $x \geq My$.
Notice that $|x^2-Ny^2| \leq M$ implies

$$|x-y\sqrt{N}| \leq \frac{M}{x+y\sqrt{N}} < \frac{M}{x+yM} \leq \frac{M}{2yM} = \frac{1}{2y}$$

Divide by y on both sides and use Theorem 8.1.5 to conclude that x/y is a convergent. □

8.4 Archimedes's Cattle Problem

The following story has been taken from Albert H.Beiler, *Recreations in the Theory of Numbers*, Dover. It deals with a problem which is attributed to Archimedes. In the form of an epigram one is asked for the number of oxen of the sun. The oxen go in four colors, white, black, spotted and yellow. Let W,X,Y,Z be the number of bulls of color white, balck, spotted, yellow respectively and x,y,z,w the number of cows. It is asked that

$$\begin{array}{ll} W=\frac{5}{6}X+Z & X=\frac{9}{20}Y+Z \\ Y=\frac{13}{42}W+Z & w=\frac{7}{12}(X+x) \\ x=\frac{9}{20}(Y+y) & y=\frac{11}{30}(Z+z) \\ z=\frac{13}{42}(W+w) & \end{array}$$

and in addition $W+X$ should be a square and $Y+Z$ a triangular number (i.e. of the form $n(n+1)/2$. The first seven conditions are easy and one verifies that

there exists $k \in \mathbb{N}$ such that

$$\begin{array}{ll} W = 10366482k & w = 7206360k \\ X = 7460514k & x = 4893246k \\ Y = 7358060k & y = 3515820k \\ Z = 4149387k & z = 5439213k \end{array}$$

The condition $W + X$ a square implies that $17826996k$ must be a square. Hence $k = 4456749t^2$ for some integer t. Finally the condition $Y + Z = n(n+1)/2$ implies

$$51285802909803t^2 = n(n+1)/2$$

Multiply by 8 on both sides and add 1 to obtain

$$\begin{aligned} 4n^2 + 4n + 1 &= (2n+1)^2 = 410286423278424t^2 + 1 \\ &= 4729494(9314t)^2 + 1 \end{aligned}$$

In other words we are looking for the solutions of the pellian equation

$$u^2 - 4729494v^2 = 1$$

where v must be divisible by 9314. Finding the smallest solution has only been possible by the use of a computer and the smallest solution value of u turns out to have 206554 decimal digits.

8.5 Cornacchia's algorithm

Closely related to the previous section is the problem to write a prime number in the form $x^2 + dy^2$, where $d \in \mathbb{N}$ is given. It is known for example, that p is a sum of two squares if and only if $p \equiv 1 (\text{mod } 4)$. The question is how to find the two squares if $p \equiv 1 (\text{mod } 4)$. One approach would be as follows. Determine $z \in \mathbb{N}$ such that $z^2 \equiv -d (\text{mod } p)$ by the method of the previous section. Then consider the lattice L generated by the vectors $(z, 1)$ and $(p, 0)$. Moreover, for every $(a, b) \in L$ we have $a^2 + db^2 \equiv 0 (\text{mod } p)$. Conversely, suppose that $a^2 + db^2 = p$ is solvable in integers a, b. Then it follows from $a^2 \equiv -db^2 (\text{mod } p)$ that $a \equiv \pm zb (\text{mod } p)$. Hence either (a, b) or $(-a, b)$ is in the lattice L. Suppose $(a, b) \in L$. If we take the norm $x^2 + dy^2$ on L then (a, b) is a shortest vector in L and we can use reduction in dimension 2 to find this shortest vector.
However, the reduction algorithm with this particular application can be reformulated in an even simpler way.

Theorem 8.5.1 (G.Cornacchia,1908) *Let $d \in \mathbb{N}$ and p a given odd prime. Suppose $a^2 + db^2 = p$ is solvable in the positive integers a, b. If $d = 1$ we assume that $a > b$. Let $x_0 \in \mathbb{N}$ be such that $x_0^2 \equiv -d (\text{mod } p)$ and $x_0 < p/2$. Apply the following algorithm recursively, $x_1 = p - [p/x_0]x_0$, $x_2 = x_0 - [x_0/x_1]x_1, \ldots, x_{i+1} = x_{i-1} - [x_{i-1}/x_i]x_i, \ldots$. Choose i such that $x_i < \sqrt{p} < x_{i-1}$. Then $x_i = a$.*

Proof. Suppose $a_0, b_0 \in \mathbb{N}$ such that $a_0^2 + db_0^2 = p$ and suppose $a_0 > b_0$ if $d = 1$. Note that $(a_0, b_0), (db_0, -a_0)$ span a lattice L of determinant p. Note also that if $(x, y) = \lambda(a_0, b_0) + \mu(db_0, -a_0)$, then $x^2 + dy^2 = (\lambda^2 + d\mu^2)p$. In particular, $(x, y) \in L \Rightarrow x^2 + dy^2 \equiv 0 (\text{mod } p)$.
Let $(a_1, b_1) = (db_0, -a_0) + [a_0/b_0](a_0, b_0)$ and define recursively

$$(a_{i+1}, b_{i+1}) = (a_{i-1}, b_{i-1}) + [|b_{i-1}/b_i|](a_i, b_i), \quad i \geq 1.$$

Notice that $a_0 < a_1 < a_2 < \cdots$ and that $|b_0| > |b_1| > |b_2| > \cdots$ and that $(-1)^i b_i > 0$ as long as $b_i \neq 0$. Notice also that, given a_{i+1} and a_i, one can recover a_{i-1} by the conditions $a_{i-1} \equiv a_{i+1} (\text{mod } a_i)$ and $0 < a_{i-1} < a_i$.
Suppose that $b_k = 0$, which will indeed happen for some k. The algorithm then terminates. Since each pair $(a_i, b_i), (a_{i-1}, b_{i-1})$ forms a basis of L, we have $\begin{vmatrix} a_{i-1} & b_{i-1} \\ a_i & b_i \end{vmatrix} = \pm p$. In particular when $i = k$ we obtain $a_k b_{k-1} = \pm p$. Hence a_k divides p. On the other hand, $0 \equiv a_k^2 + db_k^2 \equiv a_k^2 (\text{mod } p)$, hence p divides a_k. So we get $a_k = p$ and $b_{k-1} = \pm 1$. Hence, from $a_{k-1} + db_{k-1}^2 \equiv 0 (\text{mod } p)$ we get $a_{k-1}^2 \equiv -d (\text{mod } p)$. Starting with the values a_k, a_{k-1} we can compute $a_{k-2}, a_{k-3}, \ldots$ recursively. If $a_{k-1} = x_0$ this will be exactly the recursion procedure of our theorem. If $a_{k-1} = p - x_0$, we note that $a_{k-2} = x_0, a_{k-3} = p - x_0 (\text{mod } x_0) = p (\text{mod } x_0)$ and the recursion again coincides with the recursion of our theorem. We have trivially $a_0 < \sqrt{p}$. If we can show that $a_1 > \sqrt{p}$ we know exactly at which point in the euclidean algorithm for p, x_0 we have hit upon the desired a_0. To show that $a_1 > \sqrt{p}$ notice that $|b_1| < b_0| < \sqrt{p/d}$. Moreover, a short computation shows that $a_1 + db_1^2 = ([a_0/b_0]^2 + d)p$. Using $b_1^2 < p/d$ this implies $a_1^2 > ([a_0/b_0]^2 + d - 1)p$. When $d > 1$ we are done. If $d = 1$ we know that $a_0 > b_0$, hence $[a_0/b_0] \geq 1$ and we are also done. □

In the case $d = 1$ the algorithm has some nice side properties. Suppose that $x_0 \equiv -1 (\text{mod } p)$ and $0 < x_0 < p/2$. Then the continued fraction algorithm of p/x_0 is symmetric of even length. Moreover, let a and b be the first two remainders less than $\sqrt{p}$ in the euclidean algorithm for p/x_0. Then $a^2 + b^2 = p$. All this, and more, is shown in the exercises below.
First we treat the example of writing the prime $p = 10^{20} + 129$ as sum of two squares. Note that $m := (p-1)/2^7$ is odd. We first determine a generator g of the group of elements modulo p whose order divides 2^7. Then, noting that any solution x of $x^2 \equiv -1 (\text{mod } p)$ has order 4, we simply take $x \equiv g^{32}$ as solution. The smallest quadratic nonresidue modulo p is 7. We easily check $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right) = \left(\frac{5}{7}\right) = -1$. Then a generator g can be found by setting $g \equiv 7^m (\text{mod } p)$, and a solution of $x^2 \equiv -1 (\text{mod } p)$ by $x \equiv 7^{32m} \equiv 44237909966037281987 (\text{mod } p)$. The continued fraction of p/x equals

$$[2, 3, 1, 5, 5, 167, 3, 14, 69, 33, 2, 2, 33, 69, 14, 3, 167, 5, 5, 1, 3, 2]$$

and Cornacchia's algorithm yields after 11 steps,

$$p = 8970878873^2 + 4418521500^2.$$

8.6 Exercises

A small point to be recalled in the following exercises is that the continued fraction of a rational number is not unique. If we would have $p/q = [a_0, \ldots, a_r, 1]$ for example, we can rewrite it as $p/q = [a_0, \ldots, a_r+1]$. This would be the result of the continued fraction algorithm. In the exercises we shall use the word *normalised continued fraction* if we want the last partial quotient larger than 1.

Exercise 8.6.1 *Let $p, q \in \mathbb{N}$ be relatively prime and such that $q < p$. Denote the continued fraction of p/q by $[a_0, \ldots, a_r]$. Let q' be such that $qq' \equiv (-1)^r \pmod{p}$. Using Lemma* 8.1.6*, show that $p/q' = [a_r, \ldots, a_0]$.*

Exercise 8.6.2 *Suppose the rational number p/q has a symmetric continued fraction, i.e. $p/q = [a_0, a_1, \ldots, a_m]$ with $(a_0, a_1, \ldots, a_m) = (a_m, \ldots, a_1, a_0)$. Using Lemma* 8.1.6*, show that $q^2 \equiv (-1)^m \pmod{p}$.*

Exercise 8.6.3 *Let $p, q \in \mathbb{N}$ such that $\gcd(p, q) = 1$, $q < p/2$ and $q^2 \equiv \pm \pmod{p}$. Show that the normalised continued fraction expansion of p/q is symmetric.*

Exercise 8.6.4 *Let $b/a = [a_0, a_1, \ldots, a_r]$ where $a_i \in \mathbb{N}$ for all i and $\gcd(a, b) = 1$. Let $p/q = [a_r, a_{r-1}, \ldots, a_0, a_0, \ldots, a_r]$. Using Lemma* 8.1.6 *show that $p = a^2 + b^2$.*

Chapter 9

Diophantine equations

9.1 General remarks

Let $F(x_1, \ldots, x_r) \in \mathbb{Z}[x_1, \ldots, x_r]$. An equation of the form

$$F(x_1, \ldots, x_r) = 0 \tag{9.1}$$

in the unknowns $x_1, \ldots, x_r$ in $\mathbb{Z}$ or $\mathbb{Q}$ is called a *diophantine equation*.
Examples are:

$$x^7 + y^7 = z^7, \qquad x^2 - 67y^2 = 1, \qquad y^2 = x^3 - 2.$$

The behaviour of the solution sets seems to be very erratic and depends very strongly on small variations of the coefficients. For example $x^3+y^3 = z^3$ and $x^3+y^3 = 4z^3$ are known to have no integral solutions with $xyz \neq 0$ whereas $x^3+y^3 = 13z^3$ and $x^3+y^3 = 22z^3$ have infinitely many with $xyz \neq 0$ and $(x, y, z) = 1$ (the 'smallest' solutions being $(x, y, z) = (2, 7, 3), (25469, 17299, 9954)$ respectively).
A famous problem on diophantine equations was *Hilbert's tenth problem* : Is there a computer program, using unlimited memory, with which one can decide whether any equation of the form (9.1) has a solution or not. We use the term 'computer program' here to avoid having to explain the definition of 'algorithm'. The answer to this question, given in 1970 by Matijasevich is *no*. The proof is based on a combination of logic and number theory and unfortunately falls outside the scope of these notes. The result of Matijasevich suggests that any diophantine equation has its own peculiarities. On the one hand it makes the solution of diophantine equations harder, but on the other hand also more interesting because of the variety of approaches which are now required. In the following sections we shall discuss a few classes of diophantine equations.

9.2 Pythagorean triplets

One of the ancient diophantine equations is the following.

Definition 9.2.1 *A triplet $a, b, c \in \mathbb{N}$ is called Pythagorean if*

$$\gcd(a, b, c) = 1 \qquad \text{and} \qquad a^2 + b^2 = c^2.$$

Notice that in a Pythagorean triplet a and b cannot be both odd. For then we would have $a^2 + b^2 \equiv 1 + 1 \equiv 2 (\text{mod } 4)$ but c^2, being a square, cannot be $\equiv 2 (\text{mod } 4)$.

Theorem 9.2.2 *Let $a, b, c \in \mathbb{N}$ and suppose that b is even. Then a, b, c is a Pythagorean triplet if and only if $\exists r, s \in \mathbb{N}: \ r > s, \ r \not\equiv s (\text{mod } 2), \ (r, s) = 1, \ a = r^2 - s^2, \ b = 2rs, \ c = r^2 + s^2$.*

Proof. Suppose we have r, s with the given properties. Clearly a, b, c satisfy $a^2 + b^2 = c^2$. Notice also that (a, c) divides $(c - a, c + a) = (2s^2, 2r^2) = 2$. But since $r \not\equiv s (\text{mod } 2)$, a and c are odd and so $(a, c) = 1$. Hence $(a, b, c) = 1$.
Suppose now that a, b, c is a pythagorean triplet. Write $b^2 = (c-a)(c+a)$. Since a, c are both odd this implies $(b/2)^2 = ((a + c)/2)((c - a)/2)$. From $(a, b, c) = 1$ and $a^2 + b^2 = c^2$ it follows that $(a, c) = 1$. Hence also $((c + a)/2, (c - a)/2) = 1$. Since the product of these numbers equals $(b/2)^2$ each of them is a square, say $(c + a)/2 = r^2$ and $(c - a)/2 = s^2$. Hence $c = r^2 + s^2, \ a = r^2 - s^2$. Moreover, $(r, s) = 1$ and $r^2 \equiv (c+a)/2 \equiv s^2 + a \equiv s^2 + 1 (\text{mod } 2) \Rightarrow r^2 \not\equiv s^2 (\text{mod } 2) \Rightarrow r \not\equiv s (\text{mod } 2)$. □

When we rewrite the equation $a^2 + b^2 = c^2$ as $(a/c)^2 + (b/c)^2 = 1$ we see that finding Pythagorean triplets is equivalent to finding rational numbers p, q such that $p^2 + q^2 = 1$, in other words, finding rational points on the unit circle. Geometrically, the solution to this problem runs as follows. For any point $(p, q) \in \mathbb{Q}^2$ we draw the line between (p, q) and $(1, 0)$ which is given by $Y = t(1 - X)$, where $t = q/(1-p)$. Conversely, any line through $(1, 0)$ is given by $Y = t(1-X)$. The second point of intersection with the unit circle is given by $\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}$. Thus we can conclude: there exists a bijection between the sets

$$\{t \in \mathbb{Q}\} \quad \text{and} \quad \{x, y \in \mathbb{Q} |\ x^2 + y^2 = 1, \ (x, y) \neq (1, 0)\}$$

given by

$$t = \frac{y}{1 - x}, \qquad (x, y) = \left(\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{t^2 + 1} \right).$$

Using Theorem 9.2.2 it is very simple to find all $\alpha, \beta, \gamma \in \mathbb{Q}$ such that $\alpha^2 + \beta^2 = \gamma^2$. They are all of the form

$$\left(\frac{r^2 - s^2}{M} \right)^2 + \left(\frac{2rs}{M} \right)^2 = \left(\frac{r^2 + s^2}{M} \right)^2, \quad r, s, M \in \mathbb{Z}.$$

A number $n \in \mathbb{N}$ is called *congruent* if n is the surface area of a right-angled triangle with rational sides. In other words

$$n \text{ is congruent} \iff \exists r, s, M \in \mathbb{Z} \text{ such that } n = \frac{1}{2} \frac{2rs}{M} \frac{r^2 - s^2}{M}.$$

The latter equation is equivalent to $M^2n = rs(r^2 - s^2)$. It is a classical problem to characterise congruent numbers. N.Koblitz used this topic in his book 'Introduction to Elliptic Curves and Modular Forms' as a leading motive. The smallest congruent number is 5. A notorious congruent number is $n = 157$. The simplest triangle corresponding to it has right angle sides

$$\frac{6803298487826435051217540}{411340519227716149383203} \qquad \frac{411340519227716149383203}{21666555693714761309610}$$

and hypothenusa

$$\frac{224403517704336969924557513090674863160948472041}{89123322689288595880255351789671635700164808 30} \text{ (D.Zagier)}$$

As an interesting curiosity we mention two results on congruent numbers

Theorem 9.2.3 (Birch, 1975) *When n is prime and equal 5 or 7 modulo 8 then n is congruent. When n is twice a prime of the form $-1 \pmod 4$ then n is also congruent.*

Theorem 9.2.4 (Tunnell, 1983) *Suppose n is a congruent number then the number of integral solutions to $2x^2 + y^2 + 8z^2 = n$ equals twice the number of solutions to $2x^2 + y^2 + 32z^2 = n$.*

It is generally expected that the converse of Tunnell's theorem also holds.

9.3 Fermat's equation

After reading about pythagorean triples it seems natural to ask the following question. Let $n \in \mathbb{N}$ and $n > 2$. Does the equation

$$x^n + y^n = z^n \tag{9.2}$$

have any solutions in $x, y, z \in \mathbb{N}$? Fermat believed the answer to be 'no' and claimed to have a 'remarkable proof'. Unfortunately the margin of the book in which he made this claim was 'too narrow to write this proof down'. In June 1993 the English mathematician Andrew Wiles came quite close and for some time it was believed that he did have a proof. However, his 200 page manuscript of highly advanced mathematics turned out to have a gap and it took about a year of suspense before this gap was repaired with the help of R.Taylor, a former student of Wiles. This happened in October 1994. Wiles's work not only resolves Fermat's last problem, it is also a major advance in the theory of elliptic curves, in particular the Shimura-Taniyama-Weil conjecture.
Before Wiles's discovery the equation (9.2) had been solved for certain special values of n. For example, Fermat did prove the following theorem.

Theorem 9.3.1 *The equation $x^4 + y^4 = z^2$ has no solution $x, y, z \in \mathbb{N}$.*

As a consequence we see that (9.2) with $n = 4$ has no solutions.

Proof. Suppose there exists a solution. Let x_0, y_0, z_0 be a solution with minimal z_0. We may assume that $(x_0, y_0) = 1$ and that y_0 is even. We shall repeatedly use Theorem 9.2.2. From $x_0^4 + y_0^4 = z_0^2$ follows,

$$\exists\ r, s \in \mathbb{Z}\ :\ (r,s) = 1,\ x_0^2 = r^2 - s^2,\ y_0^2 = 2rs,\ z_0 = r^2 + s^2.$$

From $x_0^2 + s^2 = r^2$, x_0 odd and $(r, s) = 1$ follows,

$$\exists\ \rho, \sigma \in \mathbb{Z}\ :\ (\rho,\sigma) = 1,\ x_0 = \rho^2 - \sigma^2,\ s = 2\rho\sigma,\ r = \rho^2 + \sigma^2.$$

Together with $y_0^2 = 2rs$ this yields $(y_0/2)^2 = \rho\sigma(\rho^2 + \sigma^2)$. Since the factors $\rho, \sigma, \rho^2 + \sigma^2$ are pairwise relatively prime, and their product is a square, we get

$$\exists\ u, v, w \in \mathbb{Z}\ :\ \rho = u^2,\ \sigma = v^2,\ \rho^2 + \sigma^2 = w^2.$$

After elimination of ρ, σ we get $w^2 = u^4 + v^4$. A simple check shows $|w| = \sqrt{\rho^2 + \sigma^2} = \sqrt{r} < y_0 < z_0$, contradicting the minimality of z_0. Hence there can be no solutions. □

The principle to construct a smaller solution out of a given (hypothetical) solution is known as Fermat's *descending induction* or *descent* . This principle, in disguised form with cohomology groups and all, is still often used for many diophantine equations.
The case $n = 3$ was settled by Euler (1753), Dirichlet dealt with the case $n = 5$ in 1820 and Lamé proved Fermat's conjecture for $n = 7$ in 1839. Notice that the case $n = 6$ follows from $n = 3$ because $x^6 + y^6 = z^6$ can be rewritten as $(x^2)^3 + (y^2)^3 = (z^2)^3$. In general, since any number larger than 2 is divible either by 4 or by an odd prime, it suffices to prove Fermat's conjecture for $n = 4$, which we have already done, and for n prime. The methods of solution all follow the same pattern. Let p be an odd prime and put $\zeta = e^{2\pi i/p}$. Then $x^p + y^p = z^p$ can be rewritten as

$$(x + y)(x + \zeta y) \cdots (x + \zeta^{p-1} y) = z^p.$$

The left hand side of the equation has been factored into linear factors at the price of introducing numbers from $\mathbb{Z}[\zeta]$. The right hand side of the equation is a p-th power and the principle of the proof is now to show that the linear factors on the left are essentially p-th powers in $\mathbb{Z}[\zeta]$. To reach such a conclusion we would need the property that factorisation into irreducible elements is unique in $\mathbb{Z}[\zeta]$. Assuming this one would be able to conclude a proof of Fermat's conjecture, although it is still not easy. Unfortunately there is one more complicating factor, prime factorisation in $\mathbb{Z}[\zeta]$ need not be unique. Finding a way around this problem has been one of the major stimuli to the development of *algebraic number theory.* In 1847 E.Kummer proved the following remarkable theorem.

Theorem 9.3.2 (Kummer) *Denote by $B_0, B_1, B_2 \ldots$ the sequence of Bernoulli numbers. If the odd prime number p does not divide the numerators of $B_2, B_4, B_6, \ldots, B_{p-3}$ then $x^p + y^p = z^p$ has no solution in positive integers.*

Recall that the Bernoulli numbers $B_0, B_1, B_2, \ldots$ are given by the Taylor series

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n.$$

It is not hard to see that $B_n = 0$ when n is odd and larger than 1. A small list of values,

$$\begin{array}{ll} B_2 = 1/6 & B_4 = -1/30 \\ B_6 = 1/42 & B_8 = -1/30 \\ B_{10} = 5/66 & B_{12} = -691/2730 \\ B_{14} = 7/6 & B_{16} = -3617/510 \\ B_{18} = 43867/798 & B_{20} = -174611/330 \end{array}$$

As an amusing aside we mention that the numerator of B_k with $k \leq p-3$, k even, is divisible by p if and only if $1^k + 2^k + \cdots + (p-1)^k$ is divisible by p^2. Using the computer and further refinements of Kummer's theorem one had been able to verify Fermat's conjecture for $2 < n < 4 \cdot 10^6$ (Buhler, Crandall, Sompolski) around 1990. For more details about the history and proof of Kummer's theory we refer to the books of P.Ribenboim (13 Lectures on Fermat's last theorem, Springer Verlag 1979) and H.M.Edwards (Fermat's last theorem, Springer Verlag 1977). Of course these books were pre-Wiles. For an introduction for a general audience to the techniques entering Wiles's proof I highly recommend Simon Singh's book *Fermat's Enigma: The epic quest to solve the world's greatest matehmatical problem* (1998). It reads like a novel.
As a generalisation of Fermat's conjecture Euler conjectured that for any $k \in \mathbb{N}$ there are no positive integers $x_1, x_2, \ldots, x_k$ such that $x_1^k + \cdots + x_{k-1}^k = x_k^k$. However, this was disproved by a counterexample of Lander and Parkin (1967) reading $144^5 = 27^5 + 84^5 + 110^5 + 133^5$. Only in 2004 a second example was discovered by J.Frye:

$$55^5 + 3183^5 + 28969^5 + 85282^5 = 85359^5.$$

In 1988 N.Elkies found spectacular counterexamples in the case $k = 4$, the smallest of which reads $95800^4 + 217519^4 + 414560^4 = 422481^4$. He also showed that there exist infinitely many of such examples with $k = 4$.

9.4 Mordell's equation

Let $k \in \mathbb{Z}$. The equation

$$y^2 = x^3 - k \tag{9.3}$$

in $x, y \in \mathbb{Z}$ is known as *Mordell's equation* . This equation has been the subject of many investigation by many people. In fact, a whole book has been written about it (London, Finkelnstein: *Mordell's equation* $x^3 - y^2 = k$). The main theorem is,

Theorem 9.4.1 (Mordell) *The eqation* (9.3) *has finitely many solutions.*

The proof uses algebraic number theory and is beyond the scope of these notes. Although Mordell's theorem is a finiteness theorem, one cannot deduce an algorithm from it to actually determine the solutions of any given equation. Bounds, which in principle give an effective solution became available around 1968 by A.Baker who showed that $\log|x| \leq c \cdot |k|^{10^4}$ and slightly improved by H.Stark $\log|x| \leq C_\epsilon |k|^{1+\epsilon}$ for every $\epsilon > 0$. The constants c, c_ϵ can be computed explicitly. It turns out that the solution set depends in a very erratic way on the value of k. For example a short computer search reveals the solutions

$$\begin{aligned} 3^2 &= (-2)^3 + 17 \\ 4^2 &= (-1)^3 + 17 \\ 5^2 &= 2^3 + 17 \\ 9^2 &= 4^3 + 17 \\ 23^2 &= 8^3 + 17 \\ 282^2 &= 43^3 + 17 \\ 375^2 &= 52^3 + 17 \\ 378661^2 &= 5234^3 + 17 \end{aligned}$$

It is a highly non-trivial task to show that this the complete solution set of $y^2 = x^3 + 17$. Two examples which are easier to deal with are given in the following theorem.

Theorem 9.4.2 *The equation* $y^2 = x^3 + 7$ *has no solutions in* $x, y \in \mathbb{Z}$. *The only integral solutions to the equation* $y^2 = x^3 - 2$ *are* $(x, y) = (3, \pm 5)$ *(Fermat).*

Proof. First we deal with $y^2 = x^3 + 7$. Note that x is odd, because x even would imply that $y^2 \equiv 7 (\mathrm{mod}\ 8)$, which is impossible. Now notice that

$$y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4)$$

Notice also that for any x, $x^2 - 2x + 4 = (x-1)^2 + 3 \equiv 3 (\mathrm{mod}\ 4)$. Hence $x^2 - 2x + 4$ always contains a prime divisor p which is $3 (\mathrm{mod}\ 4)$. So we get $y^2 + 1 \equiv 0 (\mathrm{mod}\ p)$ which is impossible because of $p \equiv 3 (\mathrm{mod}\ 4)$.
To deal with $y^2 = x^3 - 2$ we use arithmetic in the euclidean ring $R = \mathbb{Z}[\sqrt{-2}]$. Notice first of all that x is odd. If x were even, then $x^3 - 2 \equiv 2 (\mathrm{mod}\ 4)$, so $x^3 - 2$ cannot be a square. From $y^2 + 2 = x^3$ follows the factorisation

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$$

The gcd of $y+\sqrt{-2}$ and $y-2\sqrt{-2}$ divides their difference which is $2\sqrt{-2}$. So the gcd is either 1 or divisible by $\sqrt{-2}$. Since y is odd the first possibility holds. Thus we find that there exist $a, b \in \mathbb{Z}$ such that $y+\sqrt{-2} = (a+b\sqrt{-2})^3$. Computing the cube, $y+\sqrt{-2} = a^3 - 6ab^2 + b(3a^2-2b^2)\sqrt{-2}$. Comparison of the coefficients of $\sqrt{-2}$ on both sides yields $1 = b(3a^2-2b^2)$. Hence $b = \pm 1$ and $3a^2-2b^2 = \pm 1$. So we find $a = \pm 1$ and $b = \pm 1$. Hence $x = a^2+2b^2 = 3$. The values of y follow. □

An interesting difference between the equations $y^2 = x^3+7$ and $y^2 = x^3-2$ is that the second equation has infinitely many rational solutions. This can be seen by the so-called chord and tangent method. In the point $(3,5)$ of the algebraic curve $y^2 = x^3-2$ we draw the tangent to the curve. It is given by $y-2 = (27/10)(x-3)$. Now intersect this line with the curve $y^2 = x^3 - 2$. Elimination of y yields

$$x^3 - \frac{729}{100}x^2 + \frac{837}{50}x - \frac{1161}{100} = 0$$

Because of our tangent construction we already know that this equation has a double root in $x = 3$. So the third root must also be a rational number. And indeed we find

$$(x-3)^2(x - \frac{129}{100}) = 0$$

. So the x coordinate of the third intersection point of the tangent with the curve equals $129/100$. The corresponding y coordinate is $383/1000$. Indeed we check that $(x,y) = (129/100, 383/1000)$ is a rational solution of $y^2 = x^3-2$. Repetition of this procedure provides us with an infinite set of rational solutions. In fact it turns out that the rational points on $y^2 = x^3 - 2$ together with the point 'at infinity' have a group structure known as the Mordell-Weil group. This is the beginning of a fascinating subject of rational points on elliptic curves. Excellent introductions can be found in Silverman and Tate: *Rational points on elliptic curves.*
By checking results for a large number of k M.Hall made the following conjecture

Conjecture 9.4.3 (Hall) *There exists a constant $C > 0$ such that $|x^3 - y^2| > Cx^{1/2}$ for any $x, y \in \mathbb{N}$ with $x^3 - y^2 \neq 0$.*

It is also known that there exist infinitely many positive integers x, y such that $0 < |x^3 - y^2| < \sqrt{x}^{1/2}$ (Danilov, 1982) so in this sense Hall's conjecture is the sharpest possible.

9.5 The 'abc'-conjecture

In 1986 Masser and Oesterlé formulated a striking conjecture, the truth of which has far reaching consequences for diophantine equations. For any $a \in \mathbb{Z}$ we let $N(a)$ (the *conductor* or *radical* of a) denote the product of all distinct primes of a.

Conjecture 9.5.1 ('abc' conjecture) *Let $\epsilon > 0$. Then there exists $c(\epsilon) > 0$ such that for any triple of non-zero numbers $a, b, c \in \mathbb{Z}$ satisfying $a + b + c = 0$ and $gcd(a, b, c) = 1$ we have*

$$\max(|a|, |b|, |c|) < c(\epsilon)N(abc)^{1+\epsilon}.$$

To get a feeling for what this conjecture says it is best to consider a number of consequences.

Consequence 1. Let p, q, r be fixed numbers larger than 1 and $(p, q, r) = 1$. Then

$$p^x + q^y = r^z$$

has only finitely many solutions $x, y, z \in \mathbb{Z}_{\geq 0}$. Application of the conjecture shows that

$$r^z < c(\epsilon)N(p^x q^y r^z)^{1+\epsilon} \leq c(\epsilon)N(pqr)^{1+\epsilon}.$$

Hence r^z is a bounded number and so are p^x, q^y. In particular x, y, z are bounded. By other methods it is indeed possible to show that $p^x + q^y = r^z$ has finitely many solutions.

Consequence 2. Fermat's conjecture is true for sufficiently large n. Apply the 'abc' conjecture to $x^n + y^n = z^n$ with $x, y, z \in \mathbb{N}$ to obtain

$$z^n < c(\epsilon)N(x^n y^n z^n)^{1+\epsilon} \leq c(\epsilon)N(xyz)^{1+\epsilon} \leq c(\epsilon)z^{3(1+\epsilon)}.$$

Hence, assuming $z \geq 2$,

$$2^{n-3(1+\epsilon)} \leq z^{n-3(1+\epsilon)} \leq c(\epsilon)$$

and this implies $n \leq \log c(\epsilon)/\log 2 + 3(1 + \epsilon)$.

Consequence 3 Let $p, q, r \in \mathbb{Z}_{\geq 2}$. Suppose

$$x^p + y^q = z^r$$

has infinitely many solutions $x, y, z \in \mathbb{N}$ with $\gcd(x, y, z) = 1$. Then

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \geq 1.$$

Application of the 'abc' conjecture yields

$$\begin{aligned} z^r &\leq c(\epsilon)N(x^p y^q z^r)^{1+\epsilon} \\ &\leq c(\epsilon)(xyz)^{1+\epsilon} \\ &\leq c(\epsilon)(z^{r/p} z^{r/q} z)^{1+\epsilon}. \end{aligned}$$

Taking $z \to \infty$ this implies $r \leq (1 + r/p + r/q)(1 + \epsilon)$ for any $\epsilon > 0$. Hence $r \leq 1 + r/p + r/q$ and our assertion follows.
Considering the potential consequences of Conjecture 9.5.1 it is likely to be very difficult to prove. In fact, any weaker version with $1 + \epsilon$ replaced by another number would already be spectacular! The best that can be done by present day methods (1994) is $\max(|a|, |b|, |c|) < \gamma \exp(N(abc)^{15})$ where γ is some (large) constant.

9.6 The equation $x^p + y^q = z^r$

Motivated by consequence 3 of the previous section and the Fermat conjecture we might look at the equation

$$x^p + y^q = z^r \qquad \gcd(x,y,z) = 1, \qquad xyz \neq 0$$

where p, q, r are given integers > 1. From the 'abc'-conjecture we expect this equation to have finitely many solutions when $1/p + 1/q + 1/r < 1$. It was a very pleasant surprise when Darmon and Granville actually proved this statement in 1993. It turns out to be a consequence of Mordell's conjecture, now known as Faltings's theorem (1983), which we will describe in the next section. Until now (1997) the only known solutions to this type of equation are

$$1^k + 2^3 = 3^2 \ (k > 5)$$

$$13^2 + 7^3 = 2^9$$

$$2^7 + 17^3 = 71^2$$

$$2^5 + 7^2 = 3^4$$

$$3^5 + 11^4 = 122^2$$

$$17^7 + 76271^3 = 21063928^2$$

$$1414^3 + 2213459^2 = 65^7$$

$$33^8 + 1549034^2 = 15613^3$$

$$43^8 + 96222^3 = 30042907^2$$

$$9262^3 + 15312283^2 = 113^7.$$

Notice that in each case there occurs an exponent 2. This leads us to the following unsolved question, which can be seen as a generalisation of Fermat's conjecture.

Question 9.6.1 *Suppose p, q, r are integers ≥ 3. Do there exist solutions to*

$$x^p + y^q = z^r \qquad \gcd(x,y,z) = 1, \qquad xyz \neq 0 \ ?$$

When $1/p + 1/q + 1/r = 1$ we can show that the set $\{p, q, r\}$ equals one of the sets $\{3,3,3\}$, $\{2,4,4\}$ or $\{2,3,6\}$. The case $p = q = r = 3$ is known to have no solution since Euler, The case $p = q = 4, r = 2$ was proved in these notes. In the exercises we show that $x^4 + y^2 = z^4$ has no non-trivial solutions. As for the case $\{2,3,6\}$ we only have the solutions $2^3 + (\pm 1)^6 = (\pm 3)^2$, but this is not easy to prove.
When $1/p + 1/q + 1/r > 1$ we can show that the set $\{p, q, r\}$ equals one of the sets $\{2,2,k\}$ $(k \geq 2)$, $\{2,3,3\}$, $\{2,3,4\}$ or $\{2,3,5\}$. The case $p = q = r = 2$ corresponds of course to pythagorean triplets. We might wonder if the other

cases allow parametric solutions as well. In 1993 Don Zagier, amused by this question, showed that the following parametrisation yield all integral solutions in the cases $\{2,3,3\}$ and $\{2,3,4\}$.
The equation $x^3 + y^3 = z^2$.

$$x = s^4 + 6s^2t^2 - 3t^4$$
$$y = -s^4 + 6s^2t^2 + 3t^4$$
$$z = 6st(s^4 + 3t^4)$$

$$x = (1/4)(s^4 + 6s^2t^2 - 3t^4)$$
$$y = (1/4)(-s^4 + 6s^2t^2 + 3t^4)$$
$$z = (3/4)st(s^4 + 3t^4)$$

$$x = s^4 + 8st^3$$
$$y = -4s^3t + 4t^4$$
$$z = s^6 - 20s^3t^3 - 8t^6$$

The equation $x^4 + y^3 = z^2$.

$$x = (s^2 - 3t^2)(s^4 + 18s^2t^2 + 9t^4)$$
$$y = -(s^4 + 2s^2t^2 + 9t^4)(s^4 - 30s^2t^2 + 9t^4)$$
$$z = 4st(s^2 + 3t^2)(s^4 - 6s^2t^2 + 81t^4)(3s^4 - 2s^2t^2 + 3t^4)$$

$$x = 6st(s^4 + 12t^4)$$
$$y = s^8 - 168s^4t^4 + 144t^8$$
$$z = (s^4 - 12t^4)(s^8 + 408s^4t^4 + 144t^8)$$

$$x = 6st(3s^4 + 4t^4)$$
$$y = 9s^8 - 168s^4t^4 + 16t^8$$
$$z = (3s^4 - 4t^4)(9s^8 + 408s^4t^4 + 16t^8)$$

$$x = s^6 + 40s^3t^3 - 32t^6$$

$$y = -8st(s^3 - 16t^3)(s^3 + 2t^3)$$

$$z = s^{12} - 176s^9t^3 - 5632s^3t^9 - 1024t^{12}$$

$$x = -5s^6 + 6s^5t + 15s^4t^2 - 60s^3t^3 + 45s^2t^4 - 18st^5 + 9t^6$$

$$y = 6s^8 - 56ts^7 + 112t^2s^6 - 168t^3s^5 + 252t^4s^4 - 168t^5s^3 + 72t^7s - 18t^8$$

$$z = -29s^{12} + 156ts^{11} - 726t^2s^{10} + 2420t^3s^9 - 4059t^4s^8 + 3960t^5s^7 - 2772t^6s^6 + 2376t^7s^5 - 3267t^8s^4 + 3564t^9s^3 - 1782t^{10}s^2 + 324t^{11}s + 27t^{12}$$

$$x = s^6 + 6s^5t - 15s^4t^2 + 20s^3t^3 + 15s^2t^4 + 30st^5 - 17t^6$$

$$y = 2s^8 - 8ts^7 - 56t^3s^5 - 28t^4s^4 + 168t^5s^3 - 112t^6s^2 + 88t^7s + 42t^8$$

$$z = -3s^{12} + 12ts^{11} - 66t^2s^{10} - 44t^3s^9 + 99t^4s^8 + 792t^5s^7 - 924t^6s^6 + 2376t^7s^5 - 1485t^8s^4 - 1188t^9s^3 + 2046t^{10}s^2 - 156t^{11}s + 397t^{12}$$

The equation $x^4 + y^2 = z^3$.

$$x = (s^2 + 3t^2)(s^4 - 18s^2t^2 + 9t^4)$$

$$y = 4st(s^2 - 3t^2)(s^4 + 6s^2t^2 + 81t^4)(3s^4 + 2s^2t^2 + 3t^4)$$

$$z = (s^4 - 2s^2t^2 + 9t^4)(s^4 + 30s^2t^2 + 9t^4)$$

$$x = 6st(s^4 - 12t^4)$$

$$y = (s^4 + 12t^4)(s^8 - 408s^4t^4 + 144t^8)$$

$$z = s^8 + 168s^4t^4 + 144t^8$$

$$x = 6st(3s^4 - 4t^4)$$

$$y = (3s^4 + 4t^4)(9s^8 - 408s^4t^4 + 16t^8)$$

$$z = 9s^8 + 168s^4t^4 + 16t^8$$

$$x = (3/2)st(s^4 - 3t^4)$$

$$y = (1/8)(s^4 + 3t^4)(s^8 - 102s^4t^4 + 9t^8)$$

$$z = (1/4)(s^8 + 42s^4t^4 + 9t^8)$$

We shall deal with the case $\{2,2,k\}$ in the exercises. The only equation that remains is $x^5+y^3=z^2$. In 1995 it was proved by F.Beukers that again a finite numbers of parametrised solutions suffice to give the complete solution set. In 2001 Johnny Edwards managed to produce the full list of these parametrisations. Here is the x-coordinate of one such parametrisation,

$$\begin{aligned} x &= 185s^{12}-144s^{11}t-2046s^{10}t^2+9680s^9t^3-13365s^8t^4+15840s^7t^5 \\ &\quad -20724s^6t^6+9504s^5t^7+8415s^4t^8-16720s^3t^9+6930s^2t^{10}-1776st^{11}+701t^{12} \end{aligned}$$

9.7 Mordell's conjecture

After seeing a good many particular examples one might wonder whether anything is known about diophantine equations in general. For a long time only one result in such a direction was known.

Theorem 9.7.1 (C.L.Siegel 1929) *Let $P(X,Y)\in\mathbb{Z}[X,Y]$ be a polynomial, irreducible in $\mathbb{C}[X,Y]$. Suppose that the genus of the projective curve given by $P=0$ is at least 1. Then $P(x,y)=0$ has at most finitely many solutions in $x,y\in\mathbb{Z}$.*

The proof is quite difficult and involves ideas from diophantine approximation and arithmetic algebraic geometry. Standard examples of curves of genus ≥ 2 are the hyper-elliptic curve $y^2=q(x)$, where $q(x)$ is a polynomial of degree at least 5 and distinct zeros and the Fermat curve $x^n+y^n=1$ with $n>3$.
Already in 1922 L.J.Mordell conjectured that under the conditions of Siegel's theorem $P(x,y)=0$ has at most finitely many solutions in $x,y\in\mathbb{Q}$. This conjecture withstood attempts to solve it for a long time until in 1983 G.Faltings managed to provide a proof of it. Unfortunately this proof can only be understood by experts in arithmetic algebraic geometry. In 1988 P.Vojta found a brilliant new proof which, unfortunately, had the same drawback as Faltings' proof in that it was accessable only to a very small group of experts. In 1990 E.Bombieri considerably simplified Vojta's proof, thus making it understandable for a large audience of number theorists and algebraic geometers.
About polynomial diophantine equations in more than two variables almost nothing is known, although there exist a good many fascinating conjectures about them.

9.8 Exercises

Exercise 9.8.1 *Let a,b,c be any integral solution of $a^2+b^2=c^2$. Prove that 5 divides abc.*

Exercise 9.8.2 *Solve the equation* $x^2+y^2=z^4$ *in* $x,y,z\in\mathbb{N}$ *with* $\gcd(x,y,z)=1$.

Exercise 9.8.3 *Let* a,b,c *be any solution of* $a^2+b^2=c^4$ *with* $\gcd(a,b,c)=1$. *Prove that* 7 *divides* abc.

Exercise 9.8.4 *Solve the equation* $x^2+y^2=z^3$ *in* $x,y,z\in\mathbb{N}$ *with* $\gcd(x,y,z)=1$. *(Hint: use factorisation in* $\mathbb{Z}[i]$*).*

Exercise 9.8.5 *(*) Prove that* $x^4-y^4=z^2$ *has no solution* $x,y,z\in\mathbb{N}$.

Exercise 9.8.6 *Show that* $2^k-3^l=\pm1,\ k,l\geq 2$ *has only the solution* $k=3,l=2$. *(The conjecture that* $x^k-y^l=1,\ k,l\geq 2$ *has only* $x^k=3^2,y^l=2^3$ *as solution has long been known as Catalan's conjecture. In 2002 it was proven by Michailescu).*

Exercise 9.8.7 *Prove that there exist no rectangular triangles with integral edges whose surface area is a square.*

Exercise 9.8.8 *Solve* $4y^2=x^3+1$ *in* $x,y\in\mathbb{Z}$.

Exercise 9.8.9 *Prove that the only integer solution of*

$$x^2+y^2+z^2=2xyz$$

is $x=y=z=0$.

Exercise 9.8.10 *Prove that* $3^{2^n}-1$ *is divisible by* 2^{n+2}. *Construct triples* $a_k,b_k,c_k\in\mathbb{N}$ *for* $k=1,2,\ldots$ *such that* $a_k+b_k=c_k$, $gcd(a_k,b_k,c_k)=1$ *and* $\lim_{k\to\infty}c_k/N(a_kb_kc_k)=\infty$. *Here* $N(x)$ *is the product of the distinct prime divisors of* x.

Exercise 9.8.11 *Suppose the abc-conjecture holds. Prove that there exist at most finitely many triples* a^r,b^s,c^t *such that* $a^r+b^s=c^t$, $\gcd(a,b)=1$ *and* $1/r+1/s+1/t<1$. *(Hint: prove and make use of the following statement:* $1/r+1/s+1/t<1\Rightarrow 1/r+1/s+1/t\leq 1-1/42$.*)*

Exercise 9.8.12 *Find* $a,b,c\in\mathbb{Z}$ *such that* $7\not| abc$ *and* $a^7+b^7\equiv c^7 \pmod{7^3}$.

Exercise 9.8.13 *Show, assuming the abc-conjecture, the modified Hall conjecture which reads as follows. For every* $a<1/2$ *there exists* $c(a)>0$ *such that for any positive integers* x,y *with* $x^3\neq y^2$ *we have* $|x^3-y^2|>c(a)x^a$.

Chapter 10

Prime numbers

10.1 Introductory remarks

In previous chapters we have seen that prime numbers play a crucial role in number theory. We repeat here that by a prime number we mean an integer which cannot be written as a product of smaller numbers. In this chapter we occupy ourselves with the distribution of primes in $\mathbb{N}$.

Theorem 10.1.1 (Euclid) *There exist infinitely many primes.*

Proof. We have already seen Euclid's proof in Theorem 1.4.5. Here we present another proof due to Euler. Although slightly more complicated than Euclid's proof it uses an idea which will return repeatedly.
We shall show that

$$\prod_{p\leq N}\left(1-\frac{1}{p}\right)$$

tends to zero as $N\to\infty$. Here, the product is taken over all primes $p\leq N$. Notice that by the unique factorisation theorem in $\mathbb{Z}$,

$$\prod_{p\leq N}\left(1-\frac{1}{p}\right)^{-1}=\prod_{p\leq N}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)>\sum_{n=1}^{N}\frac{1}{n}$$

Since the latter sum tends to infinity as $N\to\infty$ we see that our product tends to zero as $N\to\infty$. Hence there are infinitely many primes. □
As a consequence of Euler's method we find the following corollary.

Corollary 10.1.2 *The sum $\sum\frac{1}{p}$, taken over all primes, diverges.*

Proof. Notice that for any $x\in(0,\frac{1}{2})$ we have $x>\frac{1}{2}\log\frac{1}{1-x}$. Hence

$$\sum_{p\leq N}\frac{1}{p}>\frac{1}{2}\log\prod_{p\leq N}\frac{1}{1-p^{-1}}$$

and since the product tends to ∞ as $N \to \infty$ we see that our sum diverges. $\square$

A more precise analysis, as performed by Mertens, reveals that there exists a real number A such that for all $X > 2$ we have

$$\sum_{p<X} \frac{1}{p} = \log\log X + A + O((\log X)^{-1})$$

where the summation is over all primes $p < X$

Definition 10.1.3

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

The local distribution of prime numbers seems to be completely erratic, and not much is known about it. Remarkably enough one can say quite a few things about the global distribution of primes as reflected by $\pi(x)$. In the following table we have counted s, the number of primes in the interval $[x - 75000, x + 75000]$ for several values of x,

x	s	$150000/\log x$
10^8	8154	8143
10^9	7242	7238
10^{10}	6511	6514
10^{11}	5974	5922
10^{12}	5433	5428
10^{13}	5065	5011
10^{14}	4643	4653
10^{15}	4251	4342

The last column of this table suggests that the density of the primes near x is about equal to $1/\log x$. This led Gauss to conjecture,

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

The sign $\sim$ must be interpreted as asymptotic equality. More precisely, $f(x) \sim g(x)$ means that $f(x)/g(x) \to 1$ as $x \to \infty$. Since $\text{li}(x) \sim x/\log x$ we might also conjecture,

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

The first *result* in this direction was obtained by Chebyshev who proved around 1852 that

$$0.92\frac{x}{\log x} < \pi(x) < 1.11\frac{x}{\log x}$$

for sufficiently large x. In 1860 Riemann, in a now historical paper, introduced the complex function

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} \qquad \text{Re}s > 1$$

in the study of prime numbers. For Re$s > 1$ it is easy to see that $\zeta(s)$ is analytic and Riemann showed that it can be continued analytically to $\mathbb{C}$ with the exception of $s = 1$, where it has a first order pole with residue 1. The relation of $\zeta(s)$ with prime numbers is made apparent by the *Euler factorisation*

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

where the product is over all primes p. It turns out that for the distribution of the primes the zeros of $\zeta(s)$ in the *critical strip* $0 \leq$ Re$s \leq 1$ are extremely important. If there would have been no zeros in this strip one could have proved some marvelous theorems on prime numbers. Unfortunately there are zeros in the strip but, and this is fortunate again, they all seem to lie on the line Re$s = 1/2$. This was posed by Riemann as a question and until now no one has been able to confirm it. This question, known as the *Riemann hypothesis* , is one of the classical problems in mathematics. It follows very easily from Riemann's work that the zeros lie symmetrical around the X-axis. So it suffices to look at zeros in the upper half plane. We order them in the order of increasing imaginary part. Then it is known that the first 1500 000 000 zeros are all simple and lie on Re$s = 1/2$ (Brent, v.d.Lune, te Riele, Winter). It was proved by Levinson (1974) that at least a third of the zeros in the critical strip is on the line Re$s = 1/2$. It should be noted that the zeros outside the critical strip are given by $s = -2, -4, -6, \ldots$ and they are called the *trivial zeros*.
Continuing Riemann's work Hadamard and De la Vallée-Poussin, independently of each other, proved the following theorem in 1896.

Theorem 10.1.4 (Prime number theorem)

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

In 1949 Selberg and Erdös, more or less independently, gave an *elementary* proof of the prime number theorem. By elementary we mean that no use is made of complex function theory. It does not imply that the proof is simple!
Later it turned out that Gauss' function li(x) is a better approximation of $\pi(x)$ than $x/\log x$. Assuming the Riemann hypothesis we have

$$\pi(x) = \mathrm{li}(x) + O(x^{1/2} \log x).$$

However, one is a long way off at proving such results. The best known estimate are of the form

$$\pi(x) = \mathrm{li}(x) + O(x \exp(-\frac{1}{15}\sqrt{\log x}).$$

Here we give a table which compares values of $\pi(x)$ and $\mathrm{li}(x)$ for several x.

x	$\pi(x)$	$\mathrm{li}(x) - \pi(x)$
10^2	25	5
10^3	168	10
10^4	1229	17
10^5	9592	38
10^6	78498	130
10^7	664579	339
10^8	5761455	754
10^9	50847534	1701
10^{10}	455052511	3104
10^{11}	4118054813	11588
10^{12}	37607912018	38263
10^{13}	346065536839	108971
10^{14}	3204941750802	314890
10^{15}	29844570422669	1052619
10^{16}	279238341033925	3214632

As a peculiarity note that the values of $\delta(x) = \mathrm{li}(x) - \pi(x)$ in our table are all positive. Since x becomes quite large in our table one might suspect that $\delta(x)$ is always positive. That one should be careful in stating such beliefs was shown by Littlewood who proved in 1914 that $\delta(x)$ changes sign infinitely often. Around 1933 Skewes showed that, assuming the Riemann hypothesis, the first sign change should be somewhere below $10^{10^{10^{34}}}$. Numbers of this size were soon called *Skewes' numbers*. We now know, without having to assume the Riemann hypothesis, that the first change of $\delta(x)$ is somewhere below 6.7×10^{370}.
Finally a few words about the local distribution of primes. Let us denote by

$$p_1, p_2, \ldots, p_n, \ldots$$

the sequence of prime numbers in increasing order. First of all, $p_{n+1} - p_n$ may become arbitrarily large, i.e. there exist arbitrarily long gaps in the sequence of prime numbers. To find a gap of length at least $N - 1$, say, we just have to write down $N! + 2, N! + 3, \ldots, N! + N$ and notice that these numbers are divisible by $2, 3, \ldots, N$. By means of elementary methods Chebyshev proved in 1852 that $p_{n+1} < 2p_n$, thereby confirming *Bertrand's postulate* . It is now known, using deep analytic methods that $p_{n+1} - p_n = O(p_n^\theta)$ with $\theta = \frac{11}{12} - \frac{1}{384}$ (Iwaniec, Pintz, Mozzochi). If Riemann's hypothesis is true then one can prove that $p_{n+1} - p_n = O(\sqrt{p_n})$. However, based on heuristic arguments, one expects more, namely $p_{n+1} - p_n = O((\log p_n)^2)$ (Cramér).
If $p_{n+1} = p_n + 2$ then we call the pair p_n, p_{n+1} a *twin prime* . Examples are $(11, 13)$ $(29, 31)$ $(41, 43)$ $(71, 73)$ .... It is not known whether there exist infinitely many

twin primes, although one generally expects the answer to be 'yes'. The first non-trivial result was by V.Brun in 1919 who showed that the series $\sum p^{-1}$, taken over all primes belonging to a twin prime, converges. This was the first example of an important tool in analytic number theory, namely *sieve methods*. The largest known twin prime in 2001 (September) was

$$318032361 \times 2^{107001} \pm 1$$

but such records usually have a short life.
For much more information we refer to P.Ribenboim's delightful 'The book of prime number records'.

10.2 Elementary methods

In this section we shall prove two theorems by elementary methods which are similar in spirit to the methods used by Chebyshev.

Theorem 10.2.1 *Let $n \in \mathbb{N}$ and $n > 10$. Then*

$$\frac{1}{3}\frac{n}{\log n} < \pi(n) < 3\frac{n}{\log n}.$$

Theorem 10.2.2 (Bertrand's postulate) *For any $n \in \mathbb{N}$ there exists a prime number p such that $n < p \leq 2n$.*

For the proof of these theorems we require a few lemmas.

Lemma 10.2.3 *Let $n \in \mathbb{N}$. Then*

a) $\forall n \geq 5$:

$$\binom{2n}{n} < 4^{n-1}$$

b) $\forall n \geq 4$:

$$\binom{2n}{n} > \frac{4^n}{n}.$$

Proof. Notice that

$$\binom{2n}{n} = \frac{2n(2n-1)}{n \cdot n}\binom{2(n-1)}{n-1}.$$

Since $4(n-1)/n < 2n(2n-1)/(n \cdot n) < 4$ this implies

$$4\frac{n-1}{n}\binom{2(n-1)}{n-1} < \binom{2n}{n} < 4\binom{2(n-1)}{n-1}. \tag{10.1}$$

To prove statement (a) notice that it is true for $n = 5$ and apply induction on n using the second inequality in (10.1). To prove (b) note that it is true for $n = 4$ and apply induction on n using the first inequality in (10.1). □

Lemma 10.2.4 *Let p be prime and $n \in \mathbb{N}$. Let k be the number of prime factors p in $\binom{2n}{n}$. Then*

(a) $p^k \leq 2n$.

(b) If $n < p \leq 2n$ then $k = 1$.

(c) If $2n/3 < p \leq n$ and $n > 2$ then $k = 0$.

Proof. For any $m \in \mathbb{N}$ we know that the number of factors p in $m!$ is equal to

$$\left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \cdots = \sum_{r=1}^{\infty} \left[\frac{m}{p^r}\right].$$

Hence

$$k = \sum_{r=1}^{\infty} \left(\left[\frac{2n}{p^r}\right] - 2\left[\frac{n}{p^r}\right] \right). \tag{10.2}$$

Notice that $0 \leq [2x] - 2[x] \leq 1$ for any $x \in \mathbb{R}$. Notice also that the terms in (10.2) vanish when $r > \log 2n / \log p$. Hence

$$k \leq \sum_{r \leq \log 2n/\log p} 1 = \left[\frac{\log 2n}{\log p}\right] \leq \frac{\log 2n}{\log p}$$

and assertion (a) follows immediately.
If $n < p \leq 2n$ all terms in (10.2) vanish except $[\frac{2n}{p}]$, which is 1. This implies (b). Suppose $2n/3 < p \leq n$. Statement (c) can be verified by hand for $2 < n < 5$. So we can assume $n \geq 5$. Then we have $p^2 > 2n$ and all terms in (10.2) with $r > 1$ vanish. Hence $k = [2n/p] - 2[n/p]$. But $2n/3 < p \leq n$ implies $1 \leq n/p < 3/2$ and thus we find that $k = 0$, as asserted in (c). □

Lemma 10.2.5 *For any $n \geq 2$ we have*

$$\prod_{\substack{p \leq n \\ p prime}} p < 4^n.$$

Proof. Let $m \in \mathbb{N}$ and $m \geq 5$. Observe that according to Lemma 10.2.4(b) $\binom{2m}{m}$ is divisible by all primes p with $m < p \leq 2m$. Hence, using Lemma 10.2.3(a),

$$\prod_{m < p \leq 2m} p < 4^{m-1}. \tag{10.3}$$

We shall prove our statement by induction on n. First of all our lemma can be verified by hand for all $n < 10$. Now suppose $n \geq 10$. If n is even we have obviously $\prod_{p\leq n} p = \prod_{p\leq n-1} p < 4^{n-1} < 4^n$ and we are done. If n is odd we write

$$\prod_{p\leq n} p = \prod_{p\leq \frac{n+1}{2}} p \prod_{\frac{n+1}{2}<p\leq n+1} p.$$

The first product on the right can be estimated using our induction hypothesis and the second by using (10.3) with $m = (n+1)/2$. We obtain $\prod_{p\leq n} p < 4^{(n+1)/2} \cdot 4^{(n+1)/2-1} = 4^n$, as desired. □

Proof of Thm 10.2.1**.** First we prove the upper bound. Choose $\alpha \in \mathbb{R}$ between 0 and 1. Notice that Lemma 10.2.5 implies that

$$\prod_{\sqrt{n}<p\leq n} p < 4^n.$$

Since each factor in the product is larger than $\sqrt{n}$ this implies that

$$n^{(1/2)(\pi(n)-\pi(\sqrt{n}))} < 4^n$$

and hence

$$\pi(n) - \pi(\sqrt{n}) < 2\log 4\frac{n}{\log n}.$$

If we estimate $\pi(\sqrt{n})$ by $\sqrt{n}/2$ we find that

$$\pi(n) < 2.8\frac{n}{\log n} + \frac{n^{0.5}}{2}.$$

When $n > 200$ this can be bounded by $3n/\log n$ as desired. For $n \leq 200$ we have to verify this upper bound case by case.
Let $m \geq 4$. By combination of Lemma 10.2.3(b) and Lemma 10.2.4(a) the lower bound is derived as follows

$$\frac{4^m}{m} \leq \binom{2m}{m} < \prod_{p\leq 2m} (2m) = (2m)^{\pi(2m)}.$$

Hence

$$\pi(2m) \geq \frac{\log(4^m/m)}{\log 2m} > \log 2\frac{2m}{\log 2m} - 1.$$

Suppose $n \geq 8$. When $n = 2m$ is even we deduce,

$$\pi(n) \geq \log 2\frac{n}{\log n} - 1$$

and when $n = 2m+1$ is odd we have

$$\pi(n) = \pi(2m+1) = \pi(2m+2) > \log 2\frac{2m+2}{\log(2m+2)} - 1 > \log 2\frac{n}{\log n} - 1.$$

When $n \geq 10$ the bound $\log 2\frac{n}{\log n} - 1$ can be bounded below by $\frac{1}{3}\frac{n}{\log n}$ as desired. □

Proof of Thm 10.2.2**.** Using Lemma 10.2.4(a)(b)(c) we see that

$$\binom{2n}{n} < \prod_{n<p\leq 2n} p \prod_{p\leq 2n/3} p \prod_{p\leq\sqrt{2n}} (2n). \tag{10.4}$$

The second product on the right can be estimated using Lemma 10.2.5 and yields the upper bound $4^{2n/3}$. The third product on the right can be estimated by $(2n)^{\sqrt{2n}}$. Elementary estimates show that this can be bounded above by $4^{n/3}/n$ as soon as $n > 512$. Hence when $n > 512$ we obtain from (10.4),

$$\binom{2n}{n} < \left(\prod_{n<p\leq 2n} p\right) \frac{4^n}{n}. \tag{10.5}$$

From Lemma 10.2.3(b) we have the lower bound $\binom{2n}{n} > 4^n/n$. Together with (10.5) this implies that the product $\prod_{n<p\leq 2n} p$ is non-empty when $n > 512$. For $n \leq 512$ observe that

$$2, 3, 5, 7, 13, 23, 43, 83, 113, 223, 443, 881$$

is a sequence of prime numbers of which each term is smaller than twice its predecessor. Hence the theorem is also true for $n \leq 512$. □

10.3 Exercises

Exercise 10.3.1 *Prove,*

a)

$$\prod_{\substack{p\leq X\\ p \text{ prime}}} (1-p^{-s})^{-1} \geq \sum_{n\leq X} n^{-s} \qquad \forall s \in \mathbb{R}_{>0},\ \forall X \geq 1$$

b)

$$\prod_{\substack{p\leq X\\ p \text{ prime}}} (1-p^{-s})^{-1} < \sum_{n=1}^{\infty} n^{-s} \qquad \forall s > 1,\ \forall X \geq 1$$

c)

$$\prod_{p \text{ prime}} (1-p^{-s})^{-1} = \sum_{n=1}^{\infty} n^{-s} \qquad \forall s > 1.$$

Exercise 10.3.2 *Prove,*

a)

$$\prod_{\substack{p\leq X\\ p \text{ prime}}} (1-p^{-s})^{-1} \geq \sum_{n\leq X} n^{-s} \qquad \forall s \in \mathbb{R}_{>0},\ \forall X \geq 1$$

b)

$$\sum_{n\leq X}\frac{1}{n} > \log X \qquad \forall X \geq 1.$$

Now choose $s = 1$ in part a), take log's on both sides and show that
c)

$$\sum_{\substack{p\leq X\\ p \text{ prime}}}\frac{1}{p} > \log\log X - \frac{1}{2}.$$

Exercise 10.3.3 *a) Prove that*

$$\int_2^x \frac{dt}{(\log t)^k} = O\left(\frac{x}{(\log x)^k}\right) \qquad \forall k \in \mathbb{N},\ x \geq 2.$$

(Hint: split the integration interval into two parts.)
b) Prove that

$$\mathrm{li}(x) = \frac{x}{\log x} + 1!\frac{x}{(\log x)^2} + \cdots + (k-1)!\frac{x}{(\log x)^k} + O\left(\frac{x}{(\log x)^{k+1}}\right) \quad \forall n \in \mathbb{N}.$$

Exercise 10.3.4 *Prove that*

$$\prod_{p \text{ prime}}\left(\frac{p^2+1}{p^2-1}\right) = \frac{5}{2}.$$

(Hint: use $\zeta(2) = \pi^2/6$ and $\zeta(4) = \pi^4/90$).

Exercise 10.3.5 *Let $p_1, p_2, p_3, \ldots$ be the sequence of consecutive prime numbers. Prove, using the prime number theorem, that $p_n/n\log n \to 1$ as $n \to \infty$.*

Exercise 10.3.6 *Let $\epsilon > 0$. Prove, using the prime number theorem, that there exists $x_0(\epsilon)$ such that for any $x > x_0$ the interval $[x, (1+\epsilon)x]$ contains a prime number. (The case $\epsilon = 1$ is known as Bertrand's postulate.)*

Exercise 10.3.7 *Verify, using the prime number theorem, whether or not the following sums converge,*

$$\sum_{p \text{ prime}}\frac{1}{p\log p}, \qquad \sum_{p \text{ prime}}\frac{\log p}{p}.$$

Exercise 10.3.8 *Prove, using the prime number theorem, that*

$$\lim_{n\to\infty}\frac{\log(\mathrm{lcm}(1,\ldots,n))}{n} = 1.$$

Exercise 10.3.9 *(*) (H.W.Lenstra jr.) Prove that for infinitely many $n \in \mathbb{N}$ we have $\pi(n)|n$. (Examples: $\pi(30) = 10|30,\ \pi(1008) = 168|1008$).*

Exercise 10.3.10 *Consider for any n the integral $I_n = \int_{t=0}^{1} t^n(1-t)^n dt$.*
a)Prove that I_n is a rational number whose denominator divides $\mathrm{lcm}[n, \ldots, 2n+1]$.
(Hint: integrate term by term).
b)Prove that $|I_n| < (1/4)^n$.
c)Prove that $\mathrm{lcm}[1, \ldots, m] \geq 2^{m-1}$ for all $m \in \mathbb{N}$.

Exercise 10.3.11 *Use the ideas of the previous exercise.*
a) Prove that $|t(1-t)(1-2t)| < 1/6\sqrt{3},\ \forall t \in [0,1]$.
b) Prove that $\mathrm{lcm}(1, 2, \ldots, 6n+1) \geq 108^n\ \forall n \in \mathbb{N}$.
c) Prove that $\mathrm{lcm}(1, 2, \ldots, m) \geq \frac{1}{108}((108)^{1/6})^m,\ \forall m \in \mathbb{N}$.

Chapter 11

Irrationality and transcendence

11.1 Irrationality

Definition 11.1.1 *Let $\alpha \in \mathbb{C}$. We call α irrational when $\alpha \notin \mathbb{Q}$.*

Proving irrationality and transcendence of numbers is now being considered as a branch of number theory, although the techniques that are used involve subjects like complex analysis, linear differential equations and algebraic geometry. In this chapter we shall restrict ourselves to examples in which only elementary methods are used.
The easiest numbers for which irrationality can be proved are the algebraic numbers.

Theorem 11.1.2 *Let α be a zero of a polynomial $x^m + c_1 x^{m-1} + \cdots + c_m \in \mathbb{Z}[x]$. Then α is either irrational or $\alpha \in \mathbb{Z}$. In the latter case we have $\alpha | c_m$.*

Proof. Suppose $x^m + c_1 x^{m-1} + \cdots + c_m$ has a rational zero p/q with $p, q \in \mathbb{Z},\ (p,q) = 1,\ q > 0$. Then $p^m + c_1 p^{m-1} q + \cdots + c_m q^m = 0$. Hence $q | p^m$ and since $(p,q) = 1$ this implies $q = 1$. Notice that $p^m + c_1 p^{m-1} + \cdots + c_m = 0$ now implies that $p | c_m$. □

Corollary 11.1.3 *Let $m \in \mathbb{N}$. If $N \in \mathbb{Z}$ is not the m-th power of an integer then $\alpha = \sqrt[m]{N}$ is irrational.*

Proof. Notice that $\alpha^m - N = 0$. If $\alpha \in \mathbb{Q}$ then $\alpha \in \mathbb{Z}$ according to Theorem 11.1.2 and hence N is the m-th power of an integer. This contradicts our assumptions, hence $\alpha \notin \mathbb{Q}$. □

Theorem 11.1.4 *Let e be the base of the natural logarithm. Then e is irrational.*

Proof. Suppose e is rational with denominator d. We use the series expansion

$$e = \sum_{k=0}^{\infty} \frac{1}{k!}.$$

The number

$$\alpha := e - 1 - \frac{1}{1!} - \frac{1}{2!} - \cdots - \frac{1}{k!}$$

is a positive rational number with a denominator dividing $d(k!)$. Hence, since α is not zero,

$$\alpha \geq \frac{1}{k!d}.$$

On the other hand,

$$\begin{aligned} \alpha &= \frac{1}{(k+1)!} + \frac{1}{(k+2)!} + \cdots \\ &= \frac{1}{k!}\left(\frac{1}{k+1} + \frac{1}{(k+1)(k+2)} + \cdots\right) \\ &< \frac{1}{k!}\left(\frac{1}{k+1} + \frac{1}{(k+1)^2} + \cdots\right) \\ &= \frac{1}{k!}\frac{1}{k} \end{aligned}$$

contradicting our lower bound for α whenever $k > d$. □

The irrationality proof of π is more complicated and we require the following lemma.

Lemma 11.1.5 *Let $m \in \mathbb{Z}_{\geq 0}$. Then*

$$\pi \int_0^1 t^m \sin \pi t dt$$

is a polynomial in $1/\pi^2$ with integral coefficients and degree $[m/2]$.

Proof. By induction on m. For $m = 0$ and $m = 1$ we have

$$\pi \int_0^1 \sin \pi t dt = 2 \qquad \pi \int_0^1 t \sin \pi t dt = 1.$$

Suppose $m > 1$. After a two-fold partial integration we obtain

$$\pi \int_0^1 t^m \sin \pi t dt = 1 - \frac{m(m-1)}{\pi^2} \pi \int_0^1 t^{m-2} \sin \pi t dt$$

from which our assertion follows. □

Theorem 11.1.6 *We have $\pi^2 \notin \mathbb{Q}$ and $\pi \notin \mathbb{Q}$.*

Proof. Define $P_m(t) = \frac{1}{m!}(\frac{d}{dt})^m t^m(1-t)^m$ and notice that $P_m(t) \in \mathbb{Z}[t]$. Consider the integral

$$I_n = \pi \int_0^1 (\sin \pi t) P_{2n}(t) dt.$$

After a 2n-fold partial integration we find

$$I_n = \pi(-1)^n \frac{\pi^{2n}}{(2n)!} \int_0^1 (\sin \pi t) t^{2n}(1-t)^{2n} dt.$$

Hence

$$0 < |I_n| < \frac{\pi^{2n+1}}{(2n)!}.$$

On the other hand we can compute I_n term by term. Lemma 11.1.5 then implies that $I_n = A_n(1/\pi^2)$, where $A_n(x) \in \mathbb{Z}[x]$ and $\deg A_n \leq n$.
Suppose that $\pi^2 = a/b$ for some $a, b \in \mathbb{N}$. Because A_n has degree $\leq n$ the number $I_n = A_n(1/\pi^2) = A_n(b/a)$ is a fraction whose denominator divides a^n. Moreover, $I_n \neq 0$. Hence

$$|I_n| \geq \frac{1}{a^n}.$$

Together with the upper bound for $|I_n|$ this implies

$$\frac{1}{a^{2n}} < \frac{\pi^{2n+1}}{(2n)!}$$

which becomes impossible when $n \to \infty$. Hence $\pi^2 \notin \mathbb{Q}$. This immediately implies $\pi \notin \mathbb{Q}$. □

Around 1740 Euler proved e to be irrational and the first proof of the irrationality of π was given by Lambert in 1761. This proof was based on the continued fraction expansion of $\mathrm{arctg}(x)$. The proof we gave can be considered as a variation of a proof given by I.Niven. On the other hand there are many 'naturally' occurring numbers for which no irrationality results are known. For example, it is not known whether Euler's constant $\gamma = \lim_{n\to\infty}(\sum_{k=1}^n (1/k) - \log n)$ or $e + \pi$ or $e\pi$ is irrational. Motivated by the standard series for e P.Erdös asked the following question. Is

$$\sum_{k=1}^{\infty} \frac{1}{k! + 1}$$

irrational? Surprisingly this seems to be difficult to answer.

11.2 Transcendence

Definition 11.2.1 *A number $\alpha \in \mathbb{C}$ is called algebraic if it is the zero of a non-trivial polynomial with coefficients in $\mathbb{Q}$. A number is called transcendental if it is not algebraic.*

Obviously, proving transcendence of a number is much harder than proving irrationality. It is therefore no surprise that in the beginning of the 19th century no examples of transcendental numbers were known. In 1844 Liouville proved the following theorem.

Theorem 11.2.2 (Liouville 1844) *Let α be an algebraic number whose minimal polynomial has degree n. Then there exists a positive constant c such that for any $p, q \in \mathbb{Z}$ and $q > 0$,*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{c}{q^n}.$$

Proof. Let $P(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α. Since P has no rational roots we have $P(p/q) \neq 0$ and, moreover, $|P(p/q)| \geq 1/q^n$. Write $P(x) = (x-\alpha)Q(x)$ and let $M = \max_{|x-\alpha|\leq 1} |Q(x)|$. Suppose $|\alpha - p/q| \leq 1$. Then, trivially, $|P(p/q)| \leq M|\alpha - p/q|$. Combined with our lower bound for $|P(p/q)|$ this yields $|\alpha - p/q| \geq 1/(Mq^n)$. This proves our theorem with $c = \min(1, 1/M)$. □

Corollary 11.2.3 *Let $\alpha \in \mathbb{R}$. Suppose that there exists a sequence of rational numbers $\{p_n/q_n\}_{n=1}^{\infty}$, with $q_n > 0$ for all n, and a sequence of numbers λ_n such that*

$$0 < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{c}{q_n^{\lambda_n}} \qquad \lim_{n\to\infty} \lambda_n = \infty$$

for some $c > 0$. Then α is transcendental.

This corollary enabled Liouville to construct infinitely many examples of transcendental numbers. We give one example here,leaving the construction of other examples to the reader.

Corollary 11.2.4 *The number*

$$\alpha = \sum_{k=0}^{\infty} \frac{1}{2^{k!}}$$

is transcendental.

Proof. We apply Corollary 11.2.3. Let $q_n = 2^{n!}$ and $p_n = 2^{n!}\sum_{k=0}^{n}(1/2^{k!})$. Then

$$\left|\alpha - \frac{p_n}{q_n}\right| = \left|\sum_{k=n+1}^{\infty} \frac{1}{2^{k!}}\right| < \frac{1}{2^{(n+1)!}} \sum_{j=0}^{\infty} \frac{1}{2^j} = \frac{2}{2^{(n+1)!}} = \frac{2}{q_n^{n+1}}.$$

Application of Corollary 11.2.3 yields our result. □

Through the pioneering work of Cantor on set theory around 1874 it also became clear that 'almost all' real numbers are transcendental. This follows from the following two theorems.

Theorem 11.2.5 *The set of algebraic numbers is countable.*

Proof. It suffices to show that the set $\mathbb{Z}[X]$ is countable. To any polynomial $P(X) = p_nX^n + p_{n-1}X^{n-1} + \cdots + p_1X + p_0 \in \mathbb{Z}[X]$ with $p_n \neq 0$ we assign the number $\mu(P) = n + |p_n| + |p_{n-1}| + \cdots + |p_0| \in \mathbb{N}$. Clearly for any $N \in \mathbb{N}$ the number of solutions to $\mu(P) = N$ is finite, because both the degree and the size of the coefficients are bounded by N. Hence $\mathbb{Z}[X]$ is countable. □

Theorem 11.2.6 (Cantor) *The set of real numbers is uncountable.*

Proof. We will show that the set of real numbers in the interval $[0, 1)$ is uncountable. Suppose that this set is countable. Choose an enumeration and denote the decimal expansion of the n-th real number by $0.a_{n1}a_{n2}a_{n3}\cdots$, where $a_{nm} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ for all n, m. Now consider the real number β whose decimal expansion reads $0.b_1b_2b_3\cdots$ where the b_i are chosen such that $b_i \neq a_{ii}$ for every i. This choice implies that β does not occur in our enumeration. Hence $[0, 1)$ is uncountable. □

The principle of the proof of Theorem 11.2.6 is known as *Cantor's diagonal procedure* and it occurs in many places in mathematics.
Almost all real numbers being transcendental, it seems ironic that until the end of the 19-th century not a single 'naturally occurring' number was known to be transcendental. Only in 1873 Hermite showed that e is transcendental and in 1882 Lindemann proved π to be transcendental. In his famous lecture of 1900 D.Hilbert asked whether numbers of the form a^b with a, b algebraic, $a \neq 0, 1$ and $b \notin \mathbb{Q}$, are transcendental. Specific examples are $2^{\sqrt{2}}$ and $i^{-2i} = e^{\pi}$. This problem was considered to be very difficult by Hilbert, but already in the 1930's A.O.Gel'fond and Th.Schneider indepently developed techniques to solve this problem. So now we know,

Theorem 11.2.7 (Gel'fond, Schneider ,1934) *Let a, b be algebraic and suppose that $a \neq 0, 1$ and $b \notin \mathbb{Q}$. Then a^b is transcendental.*

Corollary 11.2.8 *Let α, β be two positive real algebraic numbers such that $\beta \neq 1$ and $\log \alpha / \log \beta \notin \mathbb{Q}$. Then $\log \alpha / \log \beta$ is transcendental.*

Proof. Let $b = \log \alpha / \log \beta$ and suppose b is algebraic. Then, according to Theorem 9.2.7 the number $\alpha = \beta^b$ is transcental which is impossible since α is algebraic. □

Nowadays the Gel'fond-Schneider theory has grown into a field of its own in which large classes of numbers, ususally related to algebraic geometry, are known to be transcendental.

11.3 Irrationality of $\zeta(3)$

Let $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. We shall be interested in the numbers $\zeta(m)$ with $m \in \mathbb{Z}_{\geq 2}$. Euler showed that

$$\zeta(2n) = (-1)^{n-1} 2^{2n-1} \frac{B_{2n}}{(2n)!} \pi^{2n}$$

where B_{2n} is the $2n$-th Bernoulli number. Hence $\zeta(2n)$ is transcendental because π^{2n} is transcendental. Strangely enough next to nothing is known about the numbers $\zeta(2n+1)$ for $n \geq 1$. It was therefore a complete surprise when in 1978 the french mathematician R.Apéry announced a proof of $\zeta(3) \notin \mathbb{Q}$. The first reaction of his fellow mathematicians was incredulity, since the presentation of the proof was a mixture of remarkable formulae and downright impossible statements. Later this proof was patched up by H.Cohen and D.Zagier and Apéry turned out to be correct on all the crucial parts. The simple proof we present here was found by F.Beukers, but the shape of the integrals is motivated by Apéry's formulae.

Lemma 11.3.1 *Let $r, s \in \mathbb{Z}_{\geq 0}$. If $r > s$ then*

$$\int_0^1 \int_0^1 -\frac{\log xy}{1-xy} x^r y^s dxdy \in \frac{\mathbb{Z}}{[1,2,\ldots,r]^3}.$$

If $r = s$ then

$$\int_0^1 \int_0^1 -\frac{\log xy}{1-xy} x^r y^r dxdy = 2\left(\zeta(3) - \frac{1}{1^3} - \cdots - \frac{1}{r^3}\right).$$

Proof. Let $\sigma > 0$ and consider the integral

$$\int_0^1 \int_0^1 \frac{x^{r+\sigma} y^{s+\sigma}}{1-xy} dxdy.$$

Develop $(1-xy)^{-1}$ in a geometrical series and carry out the integration term by term. We find

$$\sum_{k=0}^{\infty} \frac{1}{(k+r+\sigma+1)(k+s+\sigma+1)}.$$

When $r > s$ this implies

$$\begin{aligned} \int_0^1 \int_0^1 \frac{x^{r+\sigma} y^{s+\sigma}}{1-xy} dxdy &= \sum_{k=0}^{\infty} \frac{1}{r-s}\left(\frac{1}{k+s+\sigma+1} - \frac{1}{k+r+\sigma+1}\right) \\ &= \frac{1}{r-s}\left(\frac{1}{s+1+\sigma} + \cdots + \frac{1}{r+\sigma}\right) \end{aligned}$$

Differentiate with respect to σ and put $\sigma = 0$,

$$\int_0^1 \int_0^1 \frac{\log xy}{1-xy} x^r y^s dxdy = -\frac{1}{r-s}\left(\frac{1}{(s+1)^2} + \cdots + \frac{1}{r^2}\right) \in \frac{\mathbb{Z}}{[1,2,\ldots,r]^3}.$$

When $r = s$ we find in a similar way,

$$\int_0^1 \int_0^1 \frac{\log xy}{1-xy} x^r y^r dxdy = \sum_{k=0}^{\infty} \frac{-2}{(k+r+1)^3} = -2\left(\zeta(3) - \frac{1}{1^3} - \frac{1}{r^3}\right)$$

□

Lemma 11.3.2 *When n is sufficiently large,* $\mathrm{lcm}[1,2,\ldots,n] < 3^n$.

Proof. Notice that

$$\mathrm{lcm}[1,2,\ldots,n] = \prod_{p\le n} p^{[\log n/\log p]} < \prod_{p\le n} p^{\log n/\log p} \le \prod_{p\le n} n = n^{\pi(n)}$$

where the products are taken over the primes p. According to the prime number theorem we have $\pi(n) < (\log 3)n/\log n$ for sufficiently large n. Hence $n^{\pi(n)} < 3^n$ for n sufficiently large. □

Theorem 11.3.3 (R.Apéry 1978) *The number $\zeta(3)$ is irrational.*

Proof. Consider the double integral

$$I_n = \int_0^1 \int_0^1 \frac{-\log xy}{1-xy} P_n(x)P_n(y)dxdy$$

where $P_n(x) = \frac{1}{n!}\left(\frac{d}{dx}\right)^n x^n(1-x)^n$. Notice that $P(x) \in \mathbb{Z}[x]$. From Lemma 11.3.1 it follows that

$$I_n = \frac{A_n + B_n\zeta(3)}{[1,2,\ldots,n]^3}, \qquad A_n, B_n \in \mathbb{Z}.$$

Notice that

$$\frac{-\log xy}{1-xy} = \int_0^1 \frac{1}{1-(1-xy)z} dz$$

hence

$$I_n = \int \frac{P_n(x)P_n(y)}{1-(1-xy)z} dxdydz$$

where $\int$ stands for $\int_0^1\int_0^1\int_0^1$. After an n-fold partial integration with respect to x we obtain

$$I_n = \int \frac{(xyz)^n(1-x)^n P_n(y)}{(1-(1-xy)z)^{n+1}} dxdydz.$$

Substitute $z = (1-(1-xy)w)/(1-w)$. Then

$$I_n = \int (1-x)^n (1-w)^n \frac{P_n(y)}{1-(1-xy)w} dxdydw.$$

An n-fold partial integration with respect to y yields

$$I_n = \int \frac{x^n(1-x)^n y^n (1-y)^n w^n (1-w)^n}{(1-(1-xy)w)^{n+1}} dxdydw.$$

It is an excercise to show that for all $0 \leq x, y, w \leq 1$ we have

$$\left| \frac{x(1-x)y(1-y)w(1-w)}{1-(1-xy)w} \right| \leq (\sqrt{2}-1)^4.$$

Hence

$$|I_n| < (\sqrt{2}-1)^{4n} \int \frac{dxdydw}{1-(1-xy)w} = 2(\sqrt{2}-1)^{4n}\zeta(3).$$

On the other hand, $I_n \neq 0$ and $I_n = (A_n + B_n\zeta(3))/[1,2,\ldots,n]^3$. Suppose $\zeta(3) = p/q$ with $p, q \in \mathbb{Z}$ and $q > 0$. Then, using Lemma 11.3.2,

$$\frac{1}{27^n q} < \frac{1}{[1,2,\ldots,n]^3 q} \leq |I_n| < 2(\sqrt{2}-1)^{4n}\zeta(3).$$

Hence,

$$1 < (\sqrt{2}-1)^{4n} 27^n 2\zeta(3) q.$$

Since $(\sqrt{2}-1)^{4n}27^n$ tends to 0 as $n \to \infty$, we have a contradiction. Therefore, $\zeta(3) \notin \mathbb{Q}$. □

11.4 Exercises

Exercise 11.4.1 *Prove, using the series expansions for e and e^{-1}, that e is not algebraic of degree 2.*

Exercise 11.4.2 *Show that $\frac{\log 3}{\log 2}$ is irrational.*

Exercise 11.4.3 *Prove that $e + \pi$ and $e\pi$ are not both rational.*

Exercise 11.4.4 *Prove that*

$$\sum_{n=0}^{\infty} \left(\frac{4}{5}\right)^n \frac{1}{3^{n^2}} \notin \mathbb{Q}.$$

Exercise 11.4.5 *Show that the so-called Champernowne number*

$$0.12345678910111213141516 17\ldots$$

is irrational (Actually K.Mahler proved it transcendental in the 1930's, but that is much harder).

Chapter 12

Solutions to selected problems

(1.5.3) When m is odd we have the polynomial factorisation

$$x^m + 1 = (x+1)(x^{m-1} - x^{m-2} + \cdots - x + 1).$$

Suppose that n is not a power of 2, i.e. n contains an odd divisor $m > 1$. Suppose $n = m \cdot k$. Substitute $x = 2^k$ in the above identity, then

$$2^n + 1 = 2^{mk} + 1 = (2^k + 1)(2^{k(m-1)} - 2^{k(m-2)} + \cdots - 2^k + 1).$$

So $2^k + 1$ is a divisor of $2^n + 1$. It remains to point out that it is a non-trivial divisor, i.e. $1 < 2^k + 1 < 2^n + 1$. So $2^n + 1$ is not prime, a contradiction. Therefore n cannot contain odd divisors > 1.

(1.5.2) When m is odd we have the polynomial factorisation

$$x^m - 1 = (x-1)(x^{m-1} + x^{m-2} + \cdots + x + 1).$$

Suppose that n is not a prime i.e. $n = m \cdot k$ for some integers $k, m > 1$. Substitute $x = 2^k$ in the above identity, then

$$2^n - 1 = 2^{mk} - 1 = (2^k - 1)(2^{k(m-1)} + 2^{k(m-2)} + \cdots + 2^k + 1).$$

So $2^k - 1$ is a divisor of $2^n - 1$. It remains to point out that it is a non-trivial divisor, i.e. $1 < 2^k - 1 < 2^n - 1$. So $2^n - 1$ is not prime, a contradiction. Therefore n cannot be composite.

(1.5.6) Suppose that $p+2$ is composite for only finitely many primes p. Then there is a number P_0 such that p prime and $p > P_0$ implies $p + 2$ prime. Choose a prime $p > P_0$. Then, consequently, all odd numbers larger than p are prime. This is clearly impossible since, fore example, all powers of 3 are composite. We get a contradiction.

(1.5.8) Since n is odd we can write $n = 2m + 1$. Hence

$$n^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 8\binom{m+1}{2} + 1.$$

So we see that n^2 is 1 modulo 8.

(1.5.12) For a),b) we refer to the course notes. Let $eta = (1+\sqrt{5})/2$, the golden ratio. Note that $\eta^2 = \eta + 1$.

Part c) When $n = k$ we must prove that $r_k \geq 1$ which is clearly true, since r_k is the last non-zero remainder. When $n = k-1$ we must show that $r_{k-1} \geq \eta$ which is true as well, since $r_{k_1} \geq 2$. Now we apply induction using

$$\begin{aligned} r_{n-2} &= q_{n-1}r_{n-1} + r_n \\ &\geq r_{n-1} + r_n \\ &\geq \eta^{k-n+1} + \eta^{k-n} = \eta^{k-n}(\eta+1) \\ &= \eta^{k-n}\eta^2 = \eta^{k-n+2} \end{aligned}$$

Part d) We have $a = r_{-1}$ and $r_{-1} \geq \eta^{k+1}$. Hence $\eta^{k+1} \leq a$, from which our desired inequality follows.

(1.5.14) We give a hint. Suppose $n > m$ and suppose $n = mq + r$ with $0 \leq r < m$. Notice that we have the polynomial identity

$$(x^n - 1) = (x^m - 1)(x^{n-m} + x^{n-2m} + \cdots + x^{n-qm}) + x^r - 1.$$

By application of the euclidean algorithm to $a^n - 1$ and $a^m - 1$ we see that the exponents are precisely the remainders of the euclidean algorithm applied to n, m.

(1.5.16) Let k be the number of zeros. In other words, k is the highest power such that 10^k divides 123!. Since there are more factors 2 than 5 in 123!, it suffices to count the number of factors 5. Between 1 and 123 there are 24 five-tuples and 4 twentyfive-tuples (twentyfive-tuples are also counted as five-tuples). There are no hundredtwentyfive-tuples or higher between 1 and 123. In total this gives us 24+4 factors 5. Hence $k = 28$.

(1.5.17(a)) Consider the numbers 1 to n. Among these numbers there are $[n/p]$ p-tuples, $[n/p^2]$ p^2-tuples, $[n/p^3]$ p^3-tuples, etc. Here we count p^k-tuples also as p^{k-1}-tuples. The total number of factors p in $n!$ therefore equals

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

(2.3.1) A perfect number n is characterised by $\sigma(n) = 2n$. In other words, $\sum_{d|n} d = 2n$ divide on both sides by n to obtain

$$\sum_{d|n} \frac{d}{n} = 2.$$

Notice that as d runs over the divisors of n, the number d/n runs over all inverses of the divisors of n. Hence

$$\sum_{d|n} \frac{1}{d} = 2.$$

(2.3.3) All convolution products are convolution products of multiplicative functions. Hence the convolution products are also multiplicative. To describe the products it suffices to describe their values in the prime powers. Here are the results,

1. $(I_k * I_k)(n) = \sigma_0(n)n^k$
2. $\mu * I_1 = \phi$
3. $(\mu * \mu)(p^k) = -2$ als $k = 1$, 1 als $k = 2$, 0 als $k > 2$
4. $(\mu * 2^\omega)(n) = |\mu(n)|$
5. $(2^\omega * 2^\omega)(p^k) = 4k$
6. $(\mu * \phi)(p^k) = p^k - 2p^{k-1} + p^{k-2}$ if $k \geq 2$, $p - 2$ if $k = 1$.

(2.3.7) We shall prove something more general. Let $f(n)$ be any arithmetic function with $f(1) \neq 0$. Then there exists an arithmetic function g such that $f * g = e$. In other words, we must determine numbers $g(1), g(2), g(3), \ldots$ such that $f(1)g(1) = 1$ and for all $n > 1$,

$$\sum_{d|n} f(d)g(n/d) = 0$$

Hence $g(1) = 1/f(1)$ and for $n = 2, 3, 4, \ldots$,

$$f(1)g(n) = -\sum_{d|n, d<n} g(d)f(n/d).$$

Note that the latter relation allows us to determine $g(2), g(3), g(4), \ldots$ recursively. Notice also that g is uniquely determined.

To complete our exercise, we must show that if f is multiplicative, then so is g. To that end we construct a multiplicative function h such that $f * h(p^k) = 0$ for all prime powers p^k and $f * h(1) = 1$. By the multiplicative

property of f, h it follows that $f * h = e$ and by the uniqueness of g we conclude that $g = h$. For the construction of h we use the analogue of the construction for g, but now restricted to prime powers p^k,

$$f(1)h(p^k) = h(p^k) = -\sum_{l=0}^{k-1} h(p^l)f(p^{k-l}).$$

The values of h at other integers are now defined by the requirement of multiplicativity.

(2.3.8) Notice that both lefthand side and righthand side are multiplicative functions. Thus it suffices to show equality when n is a prime power p^k. Note that

$$\sum_{d|p^k} \sigma_0(d)^3 = \sum_{l=0}^{k} \sigma_0(p^l)^3 = \sum_{l=0}^{k} (l+1)^3.$$

Also note that

$$(\sum_{d|p^k} \sigma_0(d))^2 = (\sum_{l=0}^{k} \sigma_0(p^l))^2 = (\sum_{l=0}^{k} (l+1))^2.$$

The two results are equal because we have the famous identity

$$1^3 + 2^3 + \cdots + (k+1)^3 = (1 + 2 + \cdots + (k+1))^2$$

for all positive integers k.

(3.5.1) Suppose that $n = ab$ with $1 < a < b < n$. Then the product $(n-1)!$ contains both factors a and b. Hence ab divides $(n-1)!$. Suppose n is composite and suppose it cannot be written as a product of two distinct numbers $a, b < n$. Then n must be the square of a prime p, i.e. $n = p^2$. We have assumed $n > 4$, so $p > 2$. But in that case the product $(n-1)!$ contains the factors p and $2p$. So p^2 divides $(n-1)!$.

(3.5.3) Note that a number is divisible by 11 if and only if the alternating sum of its digits is divisible by 11. The alternating sum of the digits of a palindromic number of even length is zero.

(3.5.4) Answers: $3 \pmod 7$, $13 \pmod{71}$, $83 \pmod{183}$.

(3.5.6) Answers:

a) $x \equiv 1307 \pmod{2100}$

b) $y \equiv 675 \pmod{1540}$

c) $z \equiv 193 \pmod{420}$

(3.5.8) Instead of a million consecutive numbers we can more generally ask for n consecutive numbers, where n is any integer. We choose n distinct primes $p_1, p_2, \ldots, p_n$ and solve the simultaneous system of congruences

$$x+1 \equiv 0 (\text{mod } p_1^2) \quad x+2 \equiv 0 (\text{mod } p_2^2) \quad \cdots \quad x+n \equiv 0 (\text{mod } p_n^2).$$

Since the numbers p_i^2 are pairwise relatively prime, the Chinese remainder theorem shows the existence of a solution $x \in \mathbb{N}$. Hence $x+1, x+2, \ldots, x+n$ is a sequence of n consecutive numbers all divisible by a square > 1.

(3.5.9) Notice that by the chinese remainder theorem,

$$a^2 \equiv a (\text{mod } 10^k) \iff a^2 \equiv a (\text{mod } 2^k), \quad a^2 \equiv a (\text{mod } 5^k).$$

Suppose we want to solve $a^2 \equiv a (\text{mod } p^k)$ for any prime p. Observe that the equation is equivalent to $p^k | a^2 - a$, hence $p^k | a(a-1)$. Since a and $a-1$ are relatively prime, we have either $p^k | a$ or $p^k | a-1$. In other words, $a \equiv 0 (\text{mod } p^k)$ or $a \equiv 1 (\text{mod } p^k)$. Applying this to $p = 2, 5$ we get the following possibilities

1. $a \equiv 0 (\text{mod } 2^k),\ a \equiv 0 (\text{mod } 5^k)$. But this implies that a is divisible by 10^k. This gives trivial solutions which are ruled out by the constraint $1 < a < 10^k$.
2. $a \equiv 1 (\text{mod } 2^k),\ a \equiv 1 (\text{mod } 5^k)$. In this case $a-1$ is divisible by 10^k, which is another trivial solution ruled out by the extra requirement $1 < a < 10^k$.
3. $a \equiv 0 (\text{mod } 2^k),\ a \equiv 1 (\text{mod } 5^k)$. According to the chinese remainder theorem this has a unique residue class modulo 10^k as solution. It is not 0 or 1 modulo 10^k, hence there exists a unique solution a with $1 < a < 10^k$.
4. $a \equiv 1 (\text{mod } 2^k),\ a \equiv 0 (\text{mod } 5^k)$. Again this gives a unique solution.

In all we find two solutions to our general problem.

Now let $k = 12$ according to the above we must first solve $a \equiv 0 (\text{mod } 2^{12}), a \equiv 1 (\text{mod } 5^{12})$, which gives us $a \equiv 81787109376 (\text{mod } 10^{12})$ and hence $a = 81787109376$. Secondly we must solve $a \equiv 1 (\text{mod } 2^{12}), a \equiv 0 (\text{mod } 5^{12})$, which gives us $a = 918212890625$. These are the two solutions.

Notice that the sum of the non-trivial solutions found above, add up to 1000000000001. Can you explain that?

(3.5.12) Use the map $a (\text{mod } 10) \mapsto (a (\text{mod } 2), a (\text{mod } 5)$ to find

$$0 (\text{mod } 10) \quad \mapsto \quad (0 (\text{mod } 2), 0 (\text{mod } 5))$$

$$\begin{aligned}
1(\text{mod } 10) &\mapsto (1(\text{mod } 2), 1(\text{mod } 5)) \\
2(\text{mod } 10) &\mapsto (0(\text{mod } 2), 2(\text{mod } 5)) \\
3(\text{mod } 10) &\mapsto (1(\text{mod } 2), 3(\text{mod } 5)) \\
4(\text{mod } 10) &\mapsto (0(\text{mod } 2), 4(\text{mod } 5)) \\
5(\text{mod } 10) &\mapsto (1(\text{mod } 2), 0(\text{mod } 5)) \\
6(\text{mod } 10) &\mapsto (0(\text{mod } 2), 1(\text{mod } 5)) \\
7(\text{mod } 10) &\mapsto (1(\text{mod } 2), 2(\text{mod } 5)) \\
8(\text{mod } 10) &\mapsto (0(\text{mod } 2), 3(\text{mod } 5)) \\
9(\text{mod } 10) &\mapsto (1(\text{mod } 2), 4(\text{mod } 5))
\end{aligned}$$

(3.5.13) Case a) We must show that $4^{2^{2n+1}} \equiv 3(\text{mod } 13)$. Notice that the order of $4(\text{mod } 13)$ equals 6. This means that in the determination of $4^k(\text{mod } 13)$ for any k, only the value of $k(\text{mod } 6)$ matters. So we must determine $2^{2n+1}(\text{mod } 6)$ for all n. Note that $2^{2n+1} \equiv 0(\text{mod } 2)$ and $2^{2n+1} \equiv (-1)^{2n+1} \equiv -1(\text{mod } 3)$ for all n. Hence $2^{2n+1} \equiv 2(\text{mod } 6)$. We conclude that $4^{2^{2n+1}} \equiv 4^2 \equiv 3(\text{mod } 13)$.

Case b) When 37 divides x, the statement is certainly true. Suppose now that 37 does not divide x. In that case, $x^{36} \equiv 1(\text{mod } 37)$. So we must determine $9^9(\text{mod } 36)$. Notice that $9^9 \equiv 0(\text{mod } 9)$ and $9^9 \equiv 1^9 \equiv 1(\text{mod } 4)$. Hence $9^9 \equiv 9(\text{mod } 36)$. A quick calculation shows that $x^9(\text{mod } 37)$ has in total 4 different values, $1, -1, 6, -6$. After adding 4 to these numbers we get $5, 3, 10, -2(\text{mod } 37)$ None of these numbers is $0(\text{mod } 37)$.

(3.5.14) By Euler's theorem we have

$$a^{\phi(p_i^{k_i})} \equiv a^{p_i^{k_i-1}(p_i-1)} \equiv 1(\text{mod } p_i^{k_i}) \quad \text{for } i = 1, 2, \ldots, r$$

Hence

$$a^{\lambda(n)} \equiv 1(\text{mod } p_i^{k_i}) \quad \text{for } i = 1, 2, \ldots, r$$

By the Chinese remainder theorem this implies $a^{\lambda(n)} \equiv 1(\text{mod } n)$.

(3.5.15) Notice that $2730 = 2 \times 3 \times 5 \times 7 \times 13$. By the Chinese remainder theorem it suffices to show that $n^{13} \equiv n(\text{mod } p)$ for all n and $p = 2, 3, 5, 7, 13$. We repeatedly use Fermat' little theorem.

$n^{13} \equiv n(\text{mod } 13)$ for all n (Fermat's little theorem).
$n^{13} \equiv n^7 \cdot n^6 \equiv n \cdot n^6 \equiv n^7 \equiv n \pmod 7$.
$n^{13} \equiv (n^5)^2 \cdot n^3 \equiv n^2 \cdot n^3 \equiv n^5 \equiv n(\text{mod } 5)$.
$n^{13} \equiv (n^3)^4 \cdot n \equiv n^4 \cdot n \equiv n^3 \cdot n \cdot n \equiv n^3 \equiv n(\text{mod } 3)$.
$n^{13} \equiv n(\text{mod } 2)$ because n is even $\iff$ n^{13} is even.

(3.5.16) We must solve: $2^{p-1}-1=pu^2$ in an odd prime p and an integer u. Note that u must be odd. factorisation of the left hand side yields $(2^{(p-1)/2}-1)(2^{(p-1)/2}+1)=pu^2$. The factors on the left are relatively prime (check!). This implies that there exist positive integers r,s such that either

$$2^{(p-1)/2}-1=pr^2, \qquad 2^{(p-1)/2}+1=s^2$$

or

$$2^{(p-1)/2}-1=r^2, \qquad 2^{(p-1)/2}+1=ps^2.$$

In the first case s^2-1 is a power of 2. So $s-1=2^k$ and $s+1=2^l$ for certain integers k,l met $l>k>0$. taking the difference, $2^l-2^k=2$. From this follows that $2^k|2$ and hence $k=1$. Consequently, $s=3$ and $2^{(p-1)/2}+1=8$. This gives us $p=7$. A small check, $(2^6-1)/7=9$, a square.

In the second case we see that r^2+1 is a power of 2. Since r is odd, we have $r^2\equiv 1(\text{mod } 4)$ and hence $r^2+1\equiv 2(\text{mod } 4)$. In other words, r^2+1 contains at most one factor 2. So, $r^2+1=2\Rightarrow r=1\Rightarrow 2^{(p-1)/2}-1=1$.We conclude that $p=3$. A small check, $(2^2-1)/3=1$, a square.

(3.5.17) Wilson's theorem tells us that $(p-1)!\equiv -1(\text{mod } p)$. We now rewrite the product $(p-1)!$ as

$$(p-1)!=\left(\frac{p-1}{2}\right)!\times\frac{p+1}{2}\times\cdots\times(p-1).$$

The second group of factors on the right is modulo p equal to the factors $-(p-1)/2,-(p-3)/2,\ldots,-2,-1$. Hence

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

If we now notice that $(-1)^{(p-1)/2}=1$ (because $p\equiv 1(\text{mod } 4)$) and $(p-1)!\equiv -1(\text{mod } p)$, our assertion follows.

(3.5.20) Notice that $a^n\equiv 1(\text{mod } a^n-1)$. Furthermore, $a^k\not\equiv 1(\text{mod } a^n-1)$ for all $0<k<n$ because $1<a^k-1<a^n-1$ for all such k. Hence the order of $a(\text{mod } a^n-1)$ is precisely n. The order of an element divides the order of the group, hence $n\div\phi(a^n-1)$.

(3.5.21) This is slightly tedious. Write $\phi(n)=n\prod_{p|n}(1-1/p)$. We give a lower bound for $\prod_{p|n}(1-1/p)$. Notice that

$$\prod_{p|n}(1-1/p)\geq\frac{1}{2}\prod_{p|n,\ p\text{ odd}}(1-1/p)$$

The number of distinct primes dividing n can be at most $\log_2(n)$ (the logarithm of n in base 2). Note that for each odd prime p we have $1-1/p \geq 2/3$. Hence

$$\begin{aligned}\prod_{p|n}(1-1/p) &\geq \frac{1}{2}\left(\frac{2}{3}\right)^{\log_2(n)} \\ &= \frac{1}{2}n^{-\log(2/3)/\log(2)} \\ &\geq \frac{1}{2}n^{-0.5}\end{aligned}$$

We conclude that $\phi(n) \geq \frac{1}{2}\cdot n^{1-0.5} = \frac{1}{2}\cdot n^{0.5}$. The latter goes to ∞ as $n \to \infty$.

(3.5.28) The orders are $6, 11, 8$ respectively. To shortcut the computation, notice for example that $\phi(46) = 22$. So the order of $3 (\mathrm{mod}\ 46)$ divides 22. Thus we need only check whether, $3^1, 3^2, 3^{11}$ are $1 (\mathrm{mod}\ 46)$. If not, then 22 is the order of $3 (\mathrm{mod}\ 46)$. It turns out that $3^{11} \equiv 1 (\mathrm{mod}\ 46)$.

(3.5.30) Note that $2^p \equiv 1 (\mathrm{mod}\ q)$. The order of $2 (\mathrm{mod}\ q)$ thus divides p. Since p is a prime and $2^1 \not\equiv 1 (\mathrm{mod}\ q)$ the order is precisely p. Hence p divides $\phi(q) = q-1$. So $q \equiv 1 (\mathrm{mod}\ p)$. Furthermore, since q is odd, $q \equiv 1 (\mathrm{mod}\ 2)$. Hence, because p is odd, we conclude that $q \equiv 1 (\mathrm{mod}\ 2p)$. So q is of the form $q = 2mp + 1$.

(3.5.31) To show part (a) notice that $a^{2^n} \equiv -1 (\mathrm{mod}\ q)$. Together with its square $a^{2^{n+1}} \equiv 1 (\mathrm{mod}\ q)$ we note that a has order 2^{n+1} in $(\mathbb{Z}/q\mathbb{Z})^*$. Hence 2^{n+1} divides $q-1$ which solves part (a).

We now follow a variation on Euclids proof. Suppose there are finitely many primes p with $p \equiv 1 (\mathrm{mod}\ 2^n)$. Call them $p_1, p_2, \ldots, p_r$. Let q be a prime divisor of $N = (2p_1p_2\cdots p_r)^{2^n} + 1$, which is necessarily odd. Then it follows from (a) that $q \equiv 1 (\mathrm{mod}\ 2^n)$. So there is an i such that $q = p_i$. Hence $N-1$ is divisible by q. Together with $q|N$ this gives $q|1$ which is impossible. We have a contradiction. There are infinitely many primes of the form $k\cdot 2^n + 1$.

(3.5.33) Trial and error shows that 2 is a primitive root modulo 11. All other primitive roots modulo 11 can then be obtained by computation of $2^k (\mathrm{mod}\ 11)$ for $1 \leq k < 10$ and $\gcd(k, 10) = 1$. So, $2^1 \equiv 2 (\mathrm{mod}\ 11)$, $2^3 \equiv 8 (\mathrm{mod}\ 11)$, $2^7 \equiv 7 (\mathrm{mod}\ 11)$, $2^9 \equiv 6 (\mathrm{mod}\ 11)$ are the primitive roots modulo 11.

From the theory it follows that $2 (\mathrm{mod}\ 11^2)$ has order 10 or 110. Checking that $2^{10} \equiv 56 (\mathrm{mod}\ 121)$ we conclude that $2 (\mathrm{mod}\ 121)$ has order 110 and hence is a primitive root. All other primitive roots modulo 121 can be

computed by computing $2^k \pmod{121}$ with $1 \leq k < 110$ and $\gcd(k, 110) = 1$.

(3.5.34)

1. By testing $2^d \pmod{13}$ for all divisors d of 12 we quickly see that 2 is a primitive root modulo 13. The other primitive roots are given by $2^k \pmod{13}$, where $\gcd(k, 12) = 1$. So, $2, 6, 7, 11 \pmod{13}$.

   Notice $(\mathbb{Z}/14\mathbb{Z})^* \simeq (\mathbb{Z}/7\mathbb{Z})^* \times (\mathbb{Z}/2\mathbb{Z})^* \simeq (\mathbb{Z}/7\mathbb{Z})^*$. The latter group is cyclic, so there is a primitive root modulo 14. Note $\phi(14) = 6$. A quick check shows that 3 is a primitive root modulo 14. The other primitive roots are given by $3^k \pmod{14}$, where $\gcd(k, 6) = 1$. So, $3, 5 \pmod{14}$.

   Since $x^4 \equiv 1 \pmod{5}$ and $x^2 \equiv 1 \pmod{3}$ for all x with $\gcd(x, 15) = 1$, we see that $x^4 \equiv 1 \pmod{15}$ for all such x. But $\phi(15) = 8$, so there cannot be primitive roots modulo 15.

2. Note that 5 is relatively prime with 12, the order of $(\mathbb{Z}/13\mathbb{Z})^*$. Notice that $5 \cdot 5 \equiv 1 \pmod{12}$. To solve $x^5 \equiv 7 \pmod{13}$ raise both sides to the power 5. We find, $(x^5)^5 \equiv x^{25} \equiv x \equiv 7^5 \equiv 11 \pmod{13}$. The solution is $x \equiv 11 \pmod{13}$.

   In a similar way we get $x^5 \equiv 11 \pmod{14} \Rightarrow x \equiv 9 \pmod{14}$ and $x^5 \equiv 2 \pmod{15} \Rightarrow x \equiv 2 \pmod{15}$.

(3.5.35) We use the function $\lambda(n)$ from exercise 3.5.14. If we have a primitive root modulo m then we should have $\lambda(m) = \phi(m)$. In other words

$$\text{lcm}(p_1^{k_1}(p_1 - 1), \ldots p_r^{k_r}(p_r - 1)) = (p_1^{k_1}(p_1 - 1), \cdots p_r^{k_r}(p_r - 1)).$$

This means that the numbers $p_i^{k_i}(p_i - 1)$ are all relatively prime. In particular, there can be at most one odd prime factor p_i. So m is of the form $m = 2^l p^k$. When $k = 0$ we have $m = 2^l$ and we know that $l = 1, 2$. When $l = 0$ we have $m = p^k$. Suppose that $k, l > 0$ Then 2^{l-1} and $p^{k-1}(p-1)$ are relative prime. But this is impossible if $l > 1$. Hence $l = 1$ and $m = 2p^l$.

(3.5.29) Case a) We must determine all p such that 10 has order 1,2,3,4,5 or 6 modulo 10. Hence we must determine all p that divide at least one of $10-1, 10^2-1, 10^3-1, 10^4-1, 10^5-1, 10^6-1$. This gives us $p = 3, 7, 11, 13, 37, 41, 101, 271$.

Case b) Using the idea from case a) we get $p = 239, 4649$.

Case c) $p = 73, 137$

(3.5.41) From $a^{n-1} \equiv 1 \pmod{n}$ we see that $\gcd(a, n) = 1$. Let k be the order of $a \pmod{n}$. Then $k | n-1$. Suppose that $(n-1)/k$ contains a prime divisor q. Then $a^{(n-1)/q} \equiv 1 \pmod{n}$, contradicting our assumptions. Hence $(n-1)/k$ contaisn no prime divisors, hence $(n-1)/k = 1$ from which we get $k = n-1$. We also know that k and hence $n-1$ divide $\phi(n)$. This is only possible if $\phi(n) = n - 1$, hence n is prime.

(3.5.42) Let $N = 3 \cdot 2^8 + 1$. The prime divisors of $N-1$ are $2, 3$. Notice that $11^{(N-1)/2} \equiv -1 (\text{mod } N)$ and $11^{(N-1)/2} \equiv 360 (\text{mod } N)$. Hence, by Lehmer's test, N is prime.

(5.7.1) Simply write down all squares $1^2, 2^2, \ldots, 8^2$ modulo 17. We get $1, 4, 9, 16, 8, 2, 15, 13 (\text{mod } 17)$ as quadratic residues modulo 17. Similarly we get $1, 4, 9, 16, 6, 17, 11, 7, 5 (\text{mod } 19)$ as quadratic residues modulo 19.

(5.7.2) We first show that p does not divide b. If it did, then $p|a^2 + b^2$ and $p|b$ would imply $p|a$, which contradicts $\gcd(a, b) = 1$. Hence p does not divide b.

Now it follows from $p|a^2 + b^2$ that $a^2 \equiv -b^2 (\text{mod } p)$. Multiply on both sides by $b^{-2} (\text{mod } p)$. We get $(ab^{-1})^2 \equiv -1 (\text{mod } p)$. Hence -1 is a quadratic residue modulo p which implies that $p \equiv -1 (\text{mod } 4)$.

(5.7.4) Part a) Let a be a quadratic nonresidue modulo p and let $x = a^{(p-1)/8}$. Then, $x^4 \equiv a^{(p-1)/2} \equiv -1 (\text{mod } p)$.

Part b) Notice that $x^4 \equiv -1 (\text{mod } p)$ implies that $x^2 \equiv -x^{-2} (\text{mod } p)$ and hence $x^2 + x^{-2} \equiv 0 (\text{mod } p)$. So we find that $(x + 1/x)^2 \equiv x^2 + 2 + x^{-2} \equiv 0 (\text{mod } p)$. In other words, $(x + 1/x)^2 \equiv 2 (\text{mod } p)$ and 2 is a quadratic residue modulo p.

(5.7.7) We treat two examples. First $x^2 \equiv 114 (\text{mod } 127)$. Note that 127 is prime, so it suffices to determine $\left(\frac{114}{127}\right)$. Notice,

$$\left(\frac{114}{127}\right) = \left(\frac{2}{127}\right)\left(\frac{3}{127}\right)\left(\frac{19}{127}\right)$$

The first factor is 1 because $127 \equiv -1 (\text{mod } 8)$. The second factor, by reciprocity equals $-\left(\frac{127}{3}\right) = -\left(\frac{1}{3}\right) = -1$. The third factor, again by reciprocity, equals $-\left(\frac{127}{19}\right) = -\left(\frac{13}{19}\right) = -\left(\frac{19}{13}\right) = -\left(\frac{6}{13}\right)$. The latter equals $-\left(\frac{2}{13}\right)\left(\frac{3}{13}\right) = -(-1)\left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$. So we conclude $\left(\frac{114}{127}\right) = -1$, our equation is not solvable.

We now study the solvability of $9x^2 + 12x + 15 \equiv 0 (\text{mod } 58)$. Splitting off squares gives $(3x + 2)^2 + 11 \equiv 0 (\text{mod } 58)$. So it suffices to study solvability of $y^2 \equiv -11 (\text{mod } 58)$. By the Chinese remainder theorem this is equivalent to the system $y^2 \equiv 1 (\text{mod } 2)$, $y^2 \equiv -11 (\text{mod } 29)$. The first equation is solvable, it remains to determine $\left(\frac{-11}{29}\right)$. Note that is equals

$$\left(\frac{-1}{29}\right)\left(\frac{11}{29}\right) = \left(\frac{29}{11}\right) = \left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -1.$$

Hence there are no solutions.

(5.7.8) Let p be an odd prime $\neq 5$. Note that

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$$

The latter is 1 if $p \equiv \pm 1 (\mathrm{mod}\ 5)$ and -1 if $p \equiv \pm 2 (\mathrm{mod}\ 5)$.

Now let p be an odd prime $\neq 3$. Then

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p-1)/2}\left(\frac{p}{3}\right).$$

The latter is 1 if $p \equiv 1 (\mathrm{mod}\ 3)$ and -1 if $p \equiv -1 (\mathrm{mod}\ 3)$.

Finally,

$$\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right).$$

we can now read off that the Legendre symbol is 1 if $p \equiv \pm 1 (\mathrm{mod}\ 12)$ and -1 if $p \equiv \pm 5 (\mathrm{mod}\ 12)$.

(5.7.9) Let $a = (-1)^{k_0} p_1 \cdots p_r$ be the prime factorisation of a where $k_0 \equiv 0$ or 1 and the primes p_i are not necessarily distinct. Note that the primes p_i are odd because $a \equiv \pm 1 (\mathrm{mod}\ 4)$. We now compute the Legendre symbol $\left(\frac{a}{p}\right)$ using quadratic reciprocity.

$$\begin{aligned}\left(\frac{a}{p}\right) &= \left(\frac{-1}{p}\right)^{k_0}\prod_{i=1}^{r}\left(\frac{p_i}{p}\right) \\ &= (-1)^{k_0(p-1)/2}\prod_{i=1}^{r}(-1)^{(p_i-1)(p-1)/4}\prod_{i=1}^{r}\left(\frac{p}{p_i}\right)\end{aligned}$$

Now notice the identity

$$k_0 + \sum_{i=1}^{r}(p_i - 1)/2 \equiv (a-1)/2 (\mathrm{mod}\ 2)$$

On the left we simply have modulo 2 the number of primes p_i which are $\equiv -1 (\mathrm{mod}\ 4)$ and the sign of a. When this total is odd we have $a \equiv -1 (\mathrm{mod}\ 4)$, when it is even we have $a \equiv 1 (\mathrm{mod}\ 4)$. So we get

$$\left(\frac{a}{p}\right) = (-1)^{(a-1)(p-1)/2}\prod_{i=1}^{r}\left(\frac{p}{p_i}\right).$$

The value of the product $\prod\left(\frac{p}{p_i}\right)$ only depends on the residue class $p (\mathrm{mod}\ |a|)$, the value of the sign depends on the parity of $(p-1)/2$. Hence $\left(\frac{a}{p}\right)$ depends

only on the residue class $p(\mathrm{mod}\ 4|a|)$. Moreover, if $a \equiv 1(\mathrm{mod}\ 4)$ the sign in front of the product is always $+$, so now $\left(\frac{a}{p}\right)$ depends only on the class $p(\mathrm{mod}\ |a|)$.

(5.7.10) Note that $x^2 \equiv a^{(p+1)/2} \equiv a^{(p-1)/2}a \equiv \left(\frac{a}{p}\right) a \equiv a(\mathrm{mod}\ p)$.

(5.7.13) Let a be the smallest quadratic nonresidue and let b the smallest positive number such that $ab > p$. Then, $0 < ab - p < a$. Hence, by minimality of a, the residue class $ab(\mathrm{mod}\ p)$ must be quadratic residue class. Hence b is a quadratic non-residue. We also have $ab < p + a$, hence $b < p/a + 1$. Since also $a + 1 \leq b$ it follows that $a < p/a$ and so, $a < \sqrt{p}$.

(5.7.14(a)) Notice that the sum $[\sqrt{p}] + \cdots + [\sqrt{kp}]$ equals the number of lattice point, with positive coordinates, below the graph of $\sqrt{px}$ in the interval $1 \leq x \leq k$. Notice that $[\sqrt{pk}] = [\sqrt{p(p-1)/4}] = (p-1)/2$. The graph of $\sqrt{px}$ does not contain lattice points when $1 \leq x \leq k$. To do the counting we might as well take the number of lattice points in the rectangle $1 \leq x \leq k, 1 \leq y \leq (p-1)/2$ and the subtract the number of lattice points on the right of the graph. Hence,

$$\frac{k(p-1)}{2} - \sum_{l=1}^{(p-1)/2} \left[\frac{y^2}{p}\right].$$

Note that

$$\left[\frac{y^2}{p}\right] = \frac{y^2}{p} - \left\{\frac{y^2}{p}\right\}.$$

Take the sum for $y = 1, 2, \ldots, (p-1)/2$. The first part can be summed using the formula $\sum_{l=1}^{n} n^2 = \frac{1}{6}n(n+1)(2n+1)$. The sum of the second part is precisely equal to K/p where K is the sum of the quadratic residues modulo p. In case $p \equiv 1(\mathrm{mod}\ 4)$ this equals half the sum of all residue classes, which is $p(p-1)/2$.

(7.5.1) The sum $\sum_{n \leq X} r_2(n)$ equals the number of lattice points within the disc with radius $\sqrt{X}$. To every lattice point (a, b) we associate the elementary square $\{(a + x, b + y) | 0 \leq x, y \leq 1\}$. Let S be the union of these squares. The number $R(X)$ is precisely equal to the surface area of S. Not that S lies within the circle with radius $\sqrt{X} + \sqrt{2}$. Note also that the circle with radius $\sqrt{X} - \sqrt{2}$ is entirely contained in S. Hence

$$\pi(\sqrt{X} - \sqrt{2})^2 \leq R(X) \leq (\sqrt{X} + \sqrt{2})^2.$$

from which we can derive that $|R(X) - \pi X| \leq 2\pi\sqrt{2X} + 2\pi$.

(7.5.4) Part a),b) are done simply by trying. Part c) can be done by trying, but also follows from the next exercise.

(7.5.5) We write $n = 2^k[(3/2)^k]-1$ as sum of k-th powers. Since $n < 3^k$, it can only be written as repeated sum with terms $1^k, 2^k$. The most economic way to do this is to use as many terms 2^k as possible. The remainder can then be written as a sum of ones. Note that $[n/2^k] = [(3/2)^k]-1$ and the remainder after division of n by 2^k is $2^k - 1$. So we require $[n/2^k] - 1$ terms 2^k and $2^k - 1$ terms 1^k. Hence $g(k) \geq 2^k + [(3/2)]^k - 2$.

(7.5.6) From the identity it follows that a number of the form $6m^2$ can be written as a sum of 12 fourth powers. We simply write $n = a^2+b^2+c^2+d^2$ (possible by Lagrange's theorem) and use the identity.

From the hint: $n = 6N + r$ and write N as sum of four squares, we deduce that $6N$ can be written as the sum of $4 \times 12 = 48$ squares. Now choose r such that $0 \leq r \leq 5$ and write r as sum of r terms 1^4. We conclude that $g(4) \leq 48 + 5 = 53$.

To get a refinement, note that r need not be chosen between 0 and 5. We can also choose among the remainders $0, 1, 2, 33, 16, 17$, each which is the sum of at most two fourth powers. Hence $g(4) \leq 48 + 2 = 50$.

(9.8.1) We can assume that a, b, c form a Pythagorean triple. Suppose, without loss of generality, that b is even. Then there exist r, s such that $a = r^2 - s^2, b = 2rs, c = r^2 + s^2$. Hence $abc = 2rs(r^4 - s^4)$. If r or s is divisible by 5 we are done. If r, s are not divisible by 5 we have $r^4 \equiv 1 (\mathrm{mod}\ 5)$ and $s^4 \equiv 1 (\mathrm{mod}\ 5)$. Hence $r^4 - s^4 \equiv 1 - 1 \equiv 0 (\mathrm{mod}\ 5)$. So $r^4 - s^4$ is divisible by 5.

(9.8.2) Note that x, y, z^2 is a Pythagorean triple. Assume that y is even, the case x even being similar. Then there exist $r, s \in \mathbb{N}$, with $\gcd(r, s) = 1$ and distinct parity, such that $x = r^2 - s^2, y = 2rs, z^2 = r^2 + s^2$. Note that r, s, z is again a Pythagorean triple. Now suppose r is even. Then there exist integers p, q, with $\gcd(p, q) = 1$ and distinct parity, such that $r = 2pq, s = p^2 - q^2, z = p^2 + q^2$. So we conclude that

$$x = (2pq)^2 - (p^2 - q^2)^2 = -p^4 + 6p^2q^2 - q^4, \quad y = 4pq(p^4 - q^4), \quad z = p^2 + q^2.$$

Similarly, when s is even we conclude $s = 2pq, r = p^2 - q^2, z = p^2 + q^2$ and hence

$$x = (p^2 - q^2)^2 - (2pq)^2 = p^4 - 6p^2q^2 + q^4, \quad y = 4pq(p^2 - q^2), \quad z = p^2 + q^2.$$

The remaining solutions arise from the previous ones by interchanging x and y.

(9.8.3) From the previous problem we know that there exist integers p, q such that $abc = \pm 4pq(p^2 - q^2)(p^2 + q^2)(p^4 + p^2q^2 + q^4 - 7p^2q^2)$. Modulo 7 this equals

$4pq(p^2-q^2)(p^6-q^6)$. When 7 divides p or q we are done. When 7 does not divide pq we have $p^6 \equiv q^6 \equiv 1 (\mathrm{mod}\ 7)$. Hence $p^6 - q^6 \equiv 1 - 1 \equiv 0 (\mathrm{mod}\ 7)$, and we are done again.

(9.8.4) Factorisation of $x^2 + y^2 = z^3$ yields $(x+iy)(x-iy) = z^3$. We should now find the greatest common divisor d of $x+iy$ and $x-iy$. Note that d divides the sum $2x$ and the difference $2iy$. Since x, y are relatively prime we conclude that d divides 2. Hence, up to units in $\mathbb{Z}[i]$, $d = 1, 1+i, 2$. Suppose 2 divides $x+iy$. This implies that x, y are both even, which is excluded by $\gcd(x,y) = 1$. Notice that $1+i$ divides $x+iy$ if and only if x, y have the same parity, i.e. they are both odd. But then we have $x^2 + y^2 \equiv 1 + 1 \equiv 2 (\mathrm{mod}\ 4)$. In other words, $x^2 + y^2$ contains only one factor 2, so it can never be a square.

We conclude that $x+iy$ and $x-iy$ are relatively prime and hence $x+iy$ is, up to units, a cube in $\mathbb{Z}[i]$. So there exist $a, b \in \mathbb{Z}$ such that

$$x + iy = \epsilon(a+bi)^3$$

where $\epsilon = \pm 1, \pm i$. Note that each of these units is a cube, so we can "absorb" the unit into the cube part. Hence there exist integers a, b such that $x + iy = (a+bi)^3$. After comparison of real and imaginary part we obtain

$$x = a^3 - 3ab^2, \qquad y = 3a^2b - b^3.$$

(9.8.6) We start with the equation $2^k - 3^l = 1$. Consider the equation modulo 3. We see that $2^k \equiv 1 (\mathrm{mod}\ 3)$, hence k should be even. From the equation it follows that $2^k - 1 = 3^l$, hence $(2^{k/2} - 1)(2^{k/2} + 1) = 3^l$. Hence the factors $2^{k/2} \pm 1$ are either 1 or a power of 3. Write these factors as $3^a, 3^b$ with $b < a$ and note that their difference is 2. I.e. $3^a - 3^b = 2$. In other words, $(3^{a-b} - 1) \cdot 3^b = 2$ and we conclude that $b = 0$ and $a - b = 1$. This implies that $l = a + b = 1$ and $k = 2$. So there are no solutions $k, l \geq 2$ in this case.

Now we solve $2^k - 3^l = -1$. Consider the equation modulo 4. We find that $-3^l \equiv -1 (\mathrm{mod}\ 4)$. Hence l is even and we can proceed in a similar way as above. We get $2^k = 3^l - 1 = (3^{l/2} - 1)(3^{l/2} + 1)$. The factors $3^{l/2} \pm 1$ are either 1 or a power of 2. Write the factors as $2^a, 2^b$ with $b < a$. The difference is 2, so we get $2^a - 2^b = 2$. Hence $(2^{a-b} - 1)2^b = 2$, from which we conclude that $b = 1$ and $a - b = 1$. So $k = a + b = 3$ and $l = 2$. This is the only solution.

NOTE: Catalan's conjecture has been solved in 2002 by Michailovich.

(9.8.8) Write $4y^2 = x^3 + 1$ as $4y^2 - 1 = x^3$. Factor the left hand side, $(2y-1)(2y+1) = x^3$. The numbers $2y-1, 2y+1$ are odd and have difference 2. So they are relatively prime and from $(2y+1)(2y-1) = x^3$ it follows that

$2y+1=u^3$ and $2y-1=v^3$ are cubes. Hence $u^3-v^3=2$. The difference of two cubes can only be 2 when $u=1, v=-1$. One way to see this is to note that $(u-v)(u^2+uv+v^2)=2$. Hence $u^2+uv+v^2=\pm 1, \pm 2$. The solutions are then found by trying.

So the final solution is $y=0, x=-1$.

(9.8.10) We prove the first statement by induction on n. For $n=1$ we note that 8 divides 3^2-1. For larger n we remark that $3^{2^n}-1=(3^{2^{n-1}}-1)(3^{2^{n-1}}+1)$ and use the induction hypothesis 2^{n-1} divides $3^{2^{n-1}}-1$ and the fact that the second factor is even.

We take $c_k=3^{2^k}, a=1, b=c_k-1$. From the above remark we know that 2^{k+2} divides b_k. Note that

$$N(a_kb_kc_k)\leq 3N(b_k)\leq \frac{3}{2^{k+1}}b_k<\frac{3}{2^{k+1}}c_k.$$

Hence $c_k/N(a_k,b_k,c_k)>2^{k+1}/3$. The latter tends to ∞ as $k\to\infty$.

(9.8.13) To show this we assume that $x^3>y^2$ and define $\delta=x^3-y^2$ and We then apply the *abc*-conjecture to $a=\delta/d, b=y^2/d, c=x^3/d$ where $d=\gcd(x^3,y^2)$. For every $\epsilon>0$ we get

$$x^3/d<c(\epsilon)\mathrm{rad}(x^3y^2\delta/d^3)^{1+\epsilon}.$$

Notice that $\mathrm{rad}(x^3y^2\delta/d^3)\leq xy\delta/d$. Also notice that $y<\sqrt{x^3-\delta}<x^{3/2}$. So we get

$$x^3/d<c(\epsilon)(xy\delta/d)^{1+\epsilon}<c(\epsilon)(x^{5/2}\delta/d)^{1+\epsilon}.$$

After multiplication by $d^{1+\epsilon}$ we obtain

$$x^3\leq x^3d^{\epsilon}<c(\epsilon)(x^{5/2}\delta)^{1+\epsilon}.$$

Now choose ϵ such that $-5/2+3/(1+\epsilon)=a$. Then it follows that

$$x^a<c(\epsilon)^{1/(1+\epsilon)}\delta$$

from which our assertion follows.

When $y^2>x^3$ we put $\delta=y^2-x^3$ and find, as above, that

$$y^{2a/3}<c(a)\delta.$$

Noticing that, by assumption, $x<y^{2/3}$, and our assertion follows also in this case.

(10.3.1) To show part (a) we expand each factor in the product as a geometric series

$$\frac{1}{1-p^{-s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots$$

Taking the product we see that

$$\prod_{p \leq X, p \text{ prime}} \frac{1}{1-p^{-s}}$$

equals the sum of $\frac{1}{n^s}$ over all n which consist entirely of primes $\leq X$. This is certainly larger than the sum of $\frac{1}{n^s}$ over all $n \leq X$.

We should actually have $X > 3$ in part (b). To show part (b) one uses the integral criterion

$$\sum_{n \leq X} > \int_1^{X-1} \frac{dt}{t} = \log(X-1)$$

With a bit more case we can also get the lower bound $\log(X)$:

$$\sum_{n \leq X} > 1 + \int_2^{X-1} \frac{dt}{t} = 1 - \log(2) + \log(X-1) > \log(X).$$

From (a) and (b) with $s = 1$ it follows that

$$\prod_{p \leq X, p \text{ prime}} \frac{1}{1-p^{-1}} > \log(X).$$

Take logs on both sides

$$\sum_{p \leq X, p \text{ prime}} -\log(1-p^{-1}) > \log\log(X).$$

Some calculus shows that $-\log(1-x) < x + 4x^2/5$ for all $x \in [0, 1/2]$. Hence

$$\sum_{p \leq X, p \text{ prime}} \frac{1}{p} + \frac{4}{5p^2} > \log\log(X).$$

Notice also that the sum of $1/p^2$ over all primes p can be bounded above by the sum of $1/n^2$ over all integers $n \neq 1, 4$. The latter sum equals $\pi^2/6 - 1 - 1/16 = 0.58....$ Times $4/5$ this yields a number $< 1/2$. So we get

$$\frac{1}{2} + \sum_{p \leq X, p \text{ prime}} \frac{1}{p} > \log\log(X)$$

as desired.

(10.3.4) Notice that

$$\begin{aligned}\prod_{p \text{ prime}} \frac{p^2+1}{p^2-1} &= \prod_{p \text{ prime}} \frac{p^2-1}{(p^2-1)^2} \\ &= \prod_{p \text{ prime}} \frac{1-p^{-4}}{(1-p^{-2})^2} \\ &= \frac{\zeta(2)^2}{\zeta(4)} = \frac{(\pi^2/6)^2}{\pi^4/90} = \frac{5}{2}.\end{aligned}$$

(10.3.5) Notice that, by definition, $n = \pi(p_n)$. Hence, by the prime number theorem,

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

It now remains to show that

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

This follows from the fact that for sufficiently large n we have

$$\frac{1}{2}\frac{p_n}{\log(p_n)} < n < 2\frac{p_n}{\log(p_n)},$$

which implies

$$\log(p_n) - \log\log(p_n) - \log(2) < \log(n) < \log(p_n) - \log\log(p_n) + \log(2).$$

After division by $\log(n)$ and letting $n \to \infty$ we find the desired limit.

(10.3.7) From the previous exercise we know that p_n, the n-th prime is asymptotic to $n\log(n)$. In particular, for sufficiently large n, $p_n > n\log(n)/2 > \sqrt{n}$. So we get

$$\sum_{p \text{ prime}} \frac{1}{p\log(p)} < finite\ part + \sum_{n \text{ large}} \frac{2}{n\log(n)\cdot\log(n)/2}.$$

The latter infinite series converges by the integral criterion.

Similarly we have for sufficiently large n that $p_n < 2n\log(n) < n^2$. Hence

$$\sum_{p \text{ prime}} \frac{\log(p)}{p} > finite\ part + \sum_{n \text{ large}} \frac{2\log(n)}{n\log(n)/2}.$$

The latter infinite series is the harmonic series which diverges.

(11.4.3) Suppose that $e+\pi$ and $e\pi$ are rational. Then the polynomial $(X-e)(X-\pi)$ has rational coefficients. Hence its zeros e, π would be quadratic numbers, contradicting the fact that e is transcendental.

(11.4.4) Suppose the series has a rational value, say p/q. Choose k and consider the difference

$$\delta = \frac{p}{q} - \sum n = 0^k \left(\frac{4}{5}\right)^n \frac{1}{3^{n^2}}.$$

This is a non-zero rational number with denominator dividing $q5^k3^{k^2}$. So we get that $\delta \geq \frac{1}{q}5^{-k}3^{-k^2}$. On the other hand we have

$$\delta = \sum_{n=k+1}^{\infty} \left(\frac{4}{5}\right)^n \frac{1}{3^{n^2}}.$$

Let us estimate the terms of this series by $(4/5)^n 3^{-(k+1)^2}$. Hence

$$\delta < \sum_{n=k+1}^{\infty} (4/5)^n 3^{-(k+1)^2} < 3^{-(k+1)^2} \sum_{n=0}^{\infty} (4/5)^n = 5 \cdot 3^{-(k+1)^2}.$$

Comparison of the bounds show that

$$\frac{1}{q}5^{-k}3^{-k^2} < 5 \cdot 3^{-(k+1)^2}.$$

Multiplication by 3^{k^2} gives us $\frac{1}{q}5^{-k} < 5 \cdot 3^{-2k-1}$, hence $(9/5)^k < 5q/3$. This is impossible if we choose k big enough. Hence our number is irrational.

Chapter 13

Appendix: Elementary algebra

13.1 Finite abelian groups

In this section we consider some elementary facts on finite abelian groups. The main application in this course will be to groups of the form $(\mathbb{Z}/m\mathbb{Z})^*$, the invertible residue classes modulo m. So, if one does not like to work with general groups one should simply read $(\mathbb{Z}/m\mathbb{Z})^*$ whenever the expression "finite abelian group" is used. The order of a finite group is simply the number of elements it contains.

Lemma 13.1.1 *Let G be a finite abelian group of order $|G|$. Then $a^{|G|} = e$ for any $a \in G$.*

Proof. Let $a \in G$. Consider the product $P = \prod_{g \in G} g$. Notice that if g runs through G, then so does ag. Hence

$$P = \prod_{g \in G} g = \prod_{g \in G} ag.$$

The latter product can also be written as $a^{|G|} \prod_{g \in G} g$, which equals $a^{|G|}P$. So, $P = a^{|G|}P$ and hence $e = a^{|G|}$. □

Remark 13.1.2 *Lemma* 13.1.1 *is actually true for any finite group, also the non-abelian ones. The proof we gave here, due to Lagrange, works only for abelian groups.*

Definition 13.1.3 *Let G be a finite group and $g \in G$. The smallest positive integer k such that $g^k = e$ is called the order of g. Notation:* $\mathrm{ord}(g)$.

Lemma 13.1.4 *Let G be a finite group and $g \in G$. Suppose $g^k = e$. Then* $\mathrm{ord}(g)|k$.

Proof. From $g^k = e$ follows $g^{k-q\text{ord}(g)} = e$ for any $q \in \mathbb{Z}$. Choose q such that $0 \leq k - q\text{ord}(g) < \text{ord}(g)$ and write $r = k - q\text{ord}(g)$. so $g^r = e$. Since $0 \leq r < \text{ord}(g)$ the minimality of $\text{ord}(g)$ implies that $r = 0$ and thus that $\text{ord}(g)$ divides k. □

Corollary 13.1.5 *Let G be a finite abelian group. Then* $\text{ord}(g)$ *divides* $|G|$ *for any* $g \in G$.

Lemma 13.1.6 *Let G be a finite abelian group and $g, h \in G$. If* $\text{ord}(g)$ *and* $\text{ord}(h)$ *are relatively prime then* $\text{ord}(gh) = \text{ord}(g)\text{ord}(h)$.

Proof. Let $M = \text{ord}(gh)$. From $e = (gh)^M$ it follows that $e = (gh)^{M\text{ord}(g)} = h^{M\text{ord}(g)}$. Hence $\text{ord}(h)|M\text{ord}(g)$. Since $(\text{ord}(g), \text{ord}(h)) = 1$ we conclude $\text{ord}(h)|M$. Similarly, $\text{ord}(g)|M$. Hence $\text{ord}(g)\text{ord}(h)|M$. On the other hand, $(gh)^{\text{ord}(h)\text{ord}(g)} = e$ and so $M|\text{ord}(g)\text{ord}(h)$ and thus we find that $M = \text{ord}(g)\text{ord}(h)$. □

Lemma 13.1.7 *Let G be a finite abelian group and $g, h \in G$. Let L be the lowest common multiple of the orders* $\text{ord}(g), \text{ord}(h)$. *Then there exists $k \in G$ such that* $L = \text{ord}(k)$.

Proof. Write L as a product of L_1 and L_2 such that $\gcd(L_1, L_2) = 1$ and $L_1|\text{ord}(g), L_2|\text{ord}(h)$. Notice that $g^{\text{ord}(g)/L_1}$ has order L_1. Similarly $h^{\text{ord}(h)/L_2}$ has order L_2. According to our previous Lemma the product $g^{\text{ord}(g)/L_1}h^{\text{ord}(h)/L_2}$ has order $L_1L_2 = L$.

By repeated application of this Lemma to more than two elements of G we obtain the following result.

Corollary 13.1.8 *Let G be a finite abelian group and let L be the lowest common multiple of the orders of all elements of G. Then there exists an element in G of order L.*

Definition 13.1.9 *Let G be finite group. The annihilator of G is the smallest positive integer k such that $g^k = e$ for all $g \in G$. Notation:* $\text{Ann}(G)$.

Lemma 13.1.10 *Let G be a finite abelian group. Then,* $\text{Ann}(G) = |G| \Leftrightarrow$ *G is cyclic.*

Proof. The '$\Leftarrow$' being trivial (why?) we shall assume that $\text{Ann}(G) = |G|$ and prove that G is cyclic.
Let L be the lowest common multiple of the orders of all $g \in G$. Notice that

$$\text{Ann}(G) \leq L \leq |G|.$$

The equality $\text{Ann}(G) = |G|$ implies $|G| = L$. According to Lemma 13.1.7 there exists $g \in G$ such that $\text{ord}(g) = L$. Hence, by the equality $L = |G|$, the element g generates G and thus G is cyclic. □

Lemma 13.1.11 *Let R be a commutative domain. Then any finite subgroup of R^* (the unit group of R) is cyclic.*

Proof. Suppose $G \subset R^*$ is a finite subgroup. Let $k = \text{Ann}(G)$ and suppose that $|G| > k$. Choose $g_1, \ldots, g_{k+1} \in G$ distinct. Consider the VanderMonde determinant

$$\delta = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ g_1 & g_2 & \cdots & g_{k+1} \\ \vdots & & & \vdots \\ g_1^k & g_2^k & \ldots & g_{k+1}^k \end{vmatrix}$$

On the one hand this determinant equals $\pm \prod_{i<j}(g_i - g_j)$. On the other hand, since $g_i^k = 1 \ \forall i$, we have $\delta = 0$. Since R has no zero divisors this implies that $g_i = g_j$ for some $i \neq j$, contradicting our choice of distinct elements. So we must assume that $k = |G|$ and, by Lemma 13.1.10 , G is cyclic. □

As we said before, the main application of this section is to groups of the form $(\mathbb{Z}/m\mathbb{Z})^*$. In particular, $\mathbb{Z}/p\mathbb{Z}$ is a field when p is prime. Lemma 13.1.11 implies that $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group. This can be illustrated by the following example modulo 13. We have

$$(\mathbb{Z}/13\mathbb{Z})^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

A possible generator of $(\mathbb{Z}/13\mathbb{Z})^*$ is the element 2. Indeed,

$$(2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}, 2^{11}, 2^{12}) \equiv (2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1)$$

and we see that every invertible residue class modulo 13 is a power of 2 modulo 13.

Lemma 13.1.12 *Let R be a domain and G a finite subgroup of R^*. Then,*

$$\prod_{g \in G} g = \begin{cases} 1 \ if \ \ -1 \notin G \\ -1 \ if \ \ -1 \in G \end{cases}$$

Proof. Notice that $x = 1/x \Leftrightarrow x^2 = 1$ for any $x \in R$. Since R is a domain the only solutions of $x^2 = 1$ are $x = \pm 1$. So, in the product

$$\prod_{g \in G} g$$

all elements cancel except $g = 1$ and $g = -1$ if $-1 \in G$. The product of these exceptional elements is 1 if $-1 \notin G$ and -1 if $-1 \in G$, which proves our lemma. □

This lemma, applied to $R = \mathbb{Z}/p\mathbb{Z}$ for any prime p, yields the following result, $(p-1)! \equiv -1 (\text{mod } p)$. This is known as *Wilson's theorem.*

13.2 Euclidean domains

Let R be a (not necessarily commutative) domain. The reason to consider non commutative domains as well is that we would like to include the quaternions in our considerations. It will not make our statements more difficult, except that we have to be careful to speak about 'left-' and 'right-' versions of concepts such as divisibility. For commutative domains we can drop the suffixes 'left-' and 'right-'.

Definition 13.2.1 *A domain R is called (right) euclidean if there exists a function $g: R-\{0\} \mapsto \mathbb{N}$ such that*

i. $g(ab) \geq g(b),\ \forall a, b \in R-\{0\}$

ii. To every $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that

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

Definition 13.2.2 *Let R be a domain and $a, b \in R$. Then b is called a (right) divisor of a if there exists $c \in R$ such that $a = cb$.*

Theorem 13.2.3 *Let R be a (right) euclidean domain and suppose that $a_1, \ldots, a_n \in R$ are not all zero. Then there exists a common (right) divisor $d \in R$ of $a_1 \ldots, a_n$ such that $d = t_i a_i + \cdots t_n a_n$ for suitable $t_1, \ldots, t_n \in R$.*

Proof. Choose d such that $g(d) = \min\{g(x) |\ x \in S - \{0\}\}$, where

$$S = \{x_1 a_1 + \cdots + x_n a_n |\ x_1, \ldots, x_n \in R\}.$$

Then d is a (right) divisor for any $a \in R$. To see this choose $q \in R$ such that $a - qd$ is either 0 or $g(a-qd) < g(d)$. Since $a - qd \in S$ the latter inequality would contradict the minimality of d. Hence $a - qd = 0$. In particular d is common (right) divisor of all a_i. Furthermore we know that $d \in S$, so $d = t_1 a_1 + \cdots + t_n a_n$ for suitable $t_1, \ldots, t_n$. □

As a bonus it follows from Theorem 13.2.3 that any common (right) divisor of the a_i is also a divisor of d. Moreover, by property (i) for euclidean domains we have $g(d) \geq g(d')$ for any (right) divisor d' of d. So d can truly be called a greatest common divisor of $a_1, \ldots, a_n$.

Lemma 13.2.4 *Let R be a (right) euclidean domain. Suppose $g(1) = 1$. Then,*

$$\epsilon \in R^* \Longleftrightarrow g(\epsilon) = 1.$$

Proof. '$\Rightarrow$' Choose ϵ' such that $\epsilon'\epsilon = 1$. Via property (i) of euclidean domains we see that $g(1) \geq g(\epsilon)$. Since $g(1) = 1$ and $g(\epsilon) \in \mathbb{N}$ this implies $g(\epsilon) = 1$.
'$\Leftarrow$' According to property (ii.) of euclidean domains there exists $q \in R$ such that either $1 - q\epsilon = 0$ or $g(1 - q\epsilon) < g(\epsilon)$. The latter inequality is impossible, hence we have $1 = q\epsilon$ hence $\epsilon \in R^*$. □

The simplest example of a euclidean domain, $\mathbb{Z}$, is treated in a separate chapter. In the next three sections we shall deal with three examples which are also of interest in number theory.

13.3 Gaussian integers

Definition 13.3.1 *The ring of Gaussian integers is the subring of* $\mathbb{C}$ *given by* $\{a+bi|\ a,b\in\mathbb{Z}\}$. *Notation:* $\mathbb{Z}[i]$. *The norm of an element* $\alpha=a+bi\in\mathbb{Z}[i]$ *is given by* $N\alpha:=a^2+b^2$.

Theorem 13.3.2 *We have*

a) $N\alpha\beta=N\alpha N\beta$ *for any* $\alpha,\beta\in\mathbb{Z}[i]$

b) $\mathbb{Z}[i]$ *is a euclidean domain with the function* $g(\alpha)=N\alpha$

c) The following statements are equivalent,

i. ϵ *is a unit in* $\mathbb{Z}[i]$

ii. $N\epsilon=1$

iii. $\epsilon\in\{1,-1,i,-i\}$.

Proof. a) Note that $N\alpha=|\alpha|^2$ where $|\cdot|$ is the ordinary absolute value on $\mathbb{C}$. Our assertion follows from $|\alpha\beta|=|\alpha|\cdot|\beta|$.
b) Notice that $N\alpha=0\Leftrightarrow\alpha=0$ and $N\alpha\geq 1$ for all $\alpha\neq 0$. Property (i) for euclidean domains now follows from a). To show property (ii) we work momentarily in $\mathbb{C}$. Let $\alpha/\beta=x+yi\in\mathbb{C}$. Let $\kappa=p+qi$ where p,q are the nearest integers to x and y respectively. So,

$$|(x+yi-\kappa)|^2\leq(1/2)^2+(1/2)^2=1/2.$$

Hence, after multiplication by $N\beta$, $N(\alpha-\kappa\beta)\leq N\beta/2$. This proves property (ii) for euclidean domains.
c) Equivalence of i. and ii. follows from Lemma 13.2.4 and the fact that $N1=1$. Equivalence of ii. and iii. follows from the observation

$$a^2+b^2=1\Leftrightarrow(a,b)\in\{(1,0),(-1,0),(0,1),(0,-1)\}.$$

□

13.4 Quaternion integers

First of all we recall the definition of *quaternions*.

Definition 13.4.1 *The quaternions are expressions of the form* $a+bi+cj+dk,\ a,b,c,d\in\mathbb{R}$ *with addition given by*

$$(a+bi+cj+dk)+(a'+b'i+c'j+d'k)=(a+a')+(b+b')i+(c+c')j+(d+d')k$$

and multiplication generated by the rules

$$\begin{array}{llll} i^2 & = j^2 = & k^2 & = -1, \\ ij & = k, & ji & = -k, \\ jk & = i, & kj & = -i, \\ ki & = j, & ik & = -j. \end{array}$$

Notation: $\mathbb{H}$

With the above addition and multiplication the quaternions form a (non-commutative) domain. The *conjugate* of a quaternion $\alpha = a+bi+cj+dk$ is given by $a-bi-cj-dk$ and denoted by $\overline{\alpha}$. The *norm* of a quaternion $\alpha = a + bi + cj + dk$ is given by $N\alpha = \alpha\overline{\alpha}$ and equals $a^2 + b^2 + c^2 + d^2$ (verify!). This implies that the inverse of a non-zero quaternion α exists and is given by $\overline{\alpha}/N\alpha$. Furthermore,

Theorem 13.4.2 *Let α and β be quaternions. Then $N\alpha\beta = N\alpha \cdot N\beta$.*

Proof. Write $\alpha = a + bi + cj + dk$ and $\beta = a' + b'i + c'j + d'k$. Then,

$$\begin{aligned} (a + bi + cj + dk)(a' + b'i + c'j + d'k) = \\ = (aa' - bb' - cc' - dd') \\ +(ab' + ba' + cd' - dc')i \\ +(ac' - bd' + ca' + db')j \\ +(ad' + bc' - cb' + da')k \end{aligned}$$

Our statement now follows from Euler's identity,

$$\begin{aligned} (a^2 + b^2 + c^2 + d^2)(a'^2 + b'^2 + c'^2 + d'^2) = \\ = (aa' - bb' - cc' - dd')^2 \\ +(ab' + ba' + cd' - dc')^2 \\ +(ac' - bd' + ca' + db')^2 \\ +(ad' + bc' - cb' + da')^2. \end{aligned}$$

□

An alternative way to describe quaternions is to identify $a + bi + cj + dk$ with the matrix

$$\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$$

where $i = \sqrt{-1}$. Addition and multiplication of quaternions comes down to addition and multiplication of the corresponding matrices. The matrix corresponding to the conjugate reads

$$\begin{pmatrix} a - bi & -c - di \\ c - di & a + bi \end{pmatrix}.$$

The norm is simply the determinant of the corresponding matrix. Associativity of quaternion multiplication now follows directly from associativity of matrix multiplication. Also, the relation $\alpha\overline{\alpha} = a^2 + b^2 + c^2 + d^2$ is now easy to verify.

Definition 13.4.3 *Let notations be as above. The quaternion integers are given by the set*

$$\{\frac{1}{2}(p + qi + rj + sk) |\ p, q, r, s \in \mathbb{Z},\ p \equiv q \equiv r \equiv s (\text{mod } 2)\}.$$

Notation: $\mathbf{q}$.

We leave it to the reader to verify that $\mathbf{q}$ is a subring of $\mathbb{H}$ and that $N\alpha \in \mathbb{N}$ for all $\alpha \in \mathbf{q},\ \alpha \neq 0$.

Theorem 13.4.4 *We have*

a) $\mathbf{q}$ *is a (right-)euclidean domain with the function* $g(\alpha) = N\alpha$.

b) The following statements are equivalent,

i. ϵ *is a unit in* $\mathbf{q}$

ii. $N\epsilon = 1$

iii. $\epsilon \in \{\pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k)\}$.

c) To any quaternionic integer α *there exists a unit* ϵ *such that* $\alpha\epsilon$ *is of the form* $p + qi + rj + sk,\ p, q, r, s \in \mathbb{Z}$.

Proof. a) Notice that $N\alpha = 0 \Leftrightarrow \alpha = 0$ and $N\alpha \geq 1$ for all $\alpha \neq 0$. Property (i) for euclidean domains now follows from Theorem 13.4.2. To show property (ii) we work momentarily in $\mathbb{H}$. Let $\alpha\beta^{-1} = x + yi + zj + uk \in \mathbb{H}$. Let $\kappa = p + qi + rj + sk$ where p, q, r, s are the nearest integers to x, y, z, u respectively. So, $N(x + yi + zj + uk - \kappa) \leq (1/2)^2 + (1/2)^2 + (1/2)^2 + (1/2)^2 = 1$. Hence, after multiplication by $N\beta$, $N(\alpha - \kappa\beta) \leq N\beta$. This proves property (ii) for euclidean domains when strict inequality holds. Notice that the equality sign holds if and only if all four numbers x, y, z, u are halfintegral. But then we have automatically $x + yi + zj + uk \in \mathbf{q}$. So property (ii) holds in all cases.
b) Equivalence of i. and ii. follows from Lemma 13.2.4 and the fact that $N1 = 1$. Equivalence of ii. and iii. follows by determination of all integral solutions of $a^2 + b^2 + c^2 + d^2 = 4,\ a \equiv b \equiv c \equiv d (\text{mod } 2)$.
c) If α is already of the form $p + qi + rj + sk,\ p, q, r, s \in \mathbb{Z}$ we can take $\epsilon = 1$. If α is of the form $(p + qi + rj + sk)/2,\ p, q, r, s \in \mathbb{Z}_{\text{odd}}$ we write $p = 4p_1 + p_2,\ q = 4q_1 + q_2,\ r = 4r_1 + r_2,\ s = 4s_1 + s_2$ with $p_2, q_2, r_2, s_2 \in \{\pm 1\}$. Then

$$\alpha = 2(p_1 + q_1 i + r_1 j + s_1 k) + (p_2 + q_2 i + r_2 j + s_2 k)/2.$$

Observe that we can now take $\epsilon = (p_2 - q_2 i - r_2 j - s_2 k)/2$ □
It is a nice exercise to show that the unit group in $\mathbf{q}$ modulo ± 1 is isomorphic to the alternating group A_4.

13.5 Polynomials

Let F be a field and $F[X]$ the corresponding polynomial ring in one variable. As well known, any non-zero polynomial $f \in F[X]$ has a degree, which we denote by $\deg(f)$. We have $\deg(fg) = \deg(f) + \deg(g)$ and $\deg(f+g) \leq \deg(f) + \deg(g)$.

Theorem 13.5.1 *Let $F[X]$ be a polynomial ring over a field F. Then,*

a) $F[X]$ is a euclidean domain with the function $g(f) = 2^{\deg(f)}$ if $f \not\equiv 0$.

b) $f \in F[X]^*$ if and only if f is a constant non-zero polynomial.

Proof. Property (a) follows from the well-known division algorithm for polynomials. Property (b) is a consequence of Lemma 13.2.4

Index