Lecture notes for “Number theory for beginners” (Ma 7 at Caltech, Spring 2019)

Alexander Yom Din

June 5, 2019

Contents

Chapter 1

Introduction

These notes are partially based on notes written by Zavosh Amir Khosravi (which are in their turn partially based on notes written by Serin Hong) as well as books by Davenport and Stein.

Chapter 2

Numbers, factorization, prime numbers and the simplest Diophantine equations

2.1 The numbers

The set of natural numbers $\mathbb{N} = \{1, 2, 3, \cdots\}$ is the most basic; As Kronecker said, "God made the integers, all else is the work of man". We have addition of natural numbers, multiplication, as well as the order relation (the relation $m \leq n$, which can be characterized through addition as saying: there exists ℓ s.t. $n = m + \ell$). We will not rigorously define all this, and will not make a list of properties. A very nice possible approach is to define the natural numbers as a set $\mathbb{N}$ together with an element $1 \in \mathbb{N}$ and a function $s : \mathbb{N} \to \mathbb{N}$ (thought of secretly as $s(n) = n + 1$), such that:

1. 1 is not in the image of s.
2. s is injective (i.e. if $s(m) = s(n)$ then $m = n$).
3. If a subset $S \subset \mathbb{N}$ satisfies $1 \in S$ and $s(n) \in S$ for every $n \in S$, then $S = \mathbb{N}$.

All can then be patiently constructed and proved from these axioms (in the setting of axiomatic set theory). Notice that the last axiom is a reformulation of the principle of mathematical induction:

Principle 2.1.1. *Let $P(n)$ be a statement, depending on $n \in \mathbb{N}$. Assume that:*

- *$P(1)$ is correct.*

- *For every $n \in \mathbb{N}$, if $P(n)$ is correct then $P(n+1)$ is correct.*

Then $P(n)$ is correct for every $n \in \mathbb{N}$.

It is not hard to show that this principle is equivalent to the following one, which is more convenient sometimes:

Principle 2.1.2. *Let $P(n)$ be a statement, depending on $n \in \mathbb{N}$. Assume that:*

- *$P(1)$ is correct.*
- *For every $n \in \mathbb{N}$, if $P(m)$ is correct for all $m < n$, then $P(n)$ is correct.*

Then $P(n)$ is correct for every $n \in \mathbb{N}$.

As an example of using this principle, let us show:

Proposition 2.1.3. *Let $S \subset \mathbb{N}$ be a subset. If S is non-empty, then there exists a minimal element in S, i.e. an element $m \in S$ such that for every $n \in S$ we have $m \leq n$.*

Proof. Let us consider the statement $P(n)$: If for a subset $S \subset \mathbb{N}$ one has $n \in S$, then S contains a minimal element. If we know all $P(n)$'s to be correct, the proposition will follow, since given a non-empty S, there exists $n \in S$, and then by $P(n)$ we will know that S contains a minimal element. "Base of induction": The statement $P(1)$ is correct, since if $1 \in S$ then 1 is a minimal element in S (as it is minimal in the whole $\mathbb{N}$). "Step of induction": Let now n be given and assume that $P(m)$ is correct for all $m < n$; We want to establish $P(n)$. Let then $S \subset \mathbb{N}$ be such that $n \in S$. If n itself is minimal in S, we are done. If not, there exists $m \in S$ such that $m < n$. Then by the correctness of $P(m)$ we deduce that S contains a minimal element. □

One can then consider "artificially" formal differences $m - n$ of natural numbers, with the identification of $m - n$ with $m' - n'$ whenever $m + n' = n + m'$. This gives the set of integers $\mathbb{Z}$. One can define addition, multiplication and the order relation on $\mathbb{Z}$, and prove all desired elementary properties. In particular, one has the once-avantgarde element $n - n$, which does not depend on n and denoted 0. It is common to think that once upon the time it was not clear, why one needs a symbol for "nothing".

2.2 Divisibility

Definition 2.2.1. Let $m, n \in \mathbb{Z}$. We define $m|n$ (in words: *m divides n* or *n is divisible by m*) if there exists $k \in \mathbb{Z}$ such that $n = m \cdot k$.

Lemma 2.2.2. *Let $k, m, n \in \mathbb{Z}$. One has:*

1. $1|n$, $n|n$, $-n|n$.
2. $k|m$ and $m|n \implies k|n$.

3. $m|n$ and $n|m \iff m \in \{n, -n\}$.

4. $k|m$ and $k|n \implies k|m+n$.

5. $k|m \implies k|mn$.

Proof.

1. $n = n \cdot 1$, $n = 1 \cdot n$, $n = (-1) \cdot (-n)$...

2. $m = k \cdot q_1, n = m \cdot q_2 \implies n = k \cdot (q_1 \cdot q_2)$.

3. If $m = 0$ or $n = 0$ then the statement is clear, so let's assume $m \neq 0$ and $n \neq 0$. If we have $n = m \cdot q_1, m = n \cdot q_2$ then $n = n \cdot (q_2 \cdot q_1)$. Since $n \neq 0$, we get $1 = q_2 \cdot q_1$. By Lemma 2.2.4 that follows, we obtain $q_1 \in \{1, -1\}$ and the claim follows.

4. $m = kq_1, n = kq_2 \implies m + n = k(q_1 + q_2)$.

5. $m = kq \implies mn = k(qn)$.

□

Definition 2.2.3. Let $n \in \mathbb{Z}$. We say that n is *invertible* if there exists $m \in \mathbb{Z}$ such that $1 = m \cdot n$.

Lemma 2.2.4. *The invertible elements in* $\mathbb{Z}$ *are* 1 *and* -1.

Proof. Clearly 1 and -1 are invertible $(1 = 1 \cdot 1, 1 = (-1) \cdot (-1))$. The element 0 is not invertible (because $m \cdot 0 = 0$ for all m, so there is no m for which $m \cdot 0 = 1$). If $|n| > 1$ then n is not invertible because then $|mn| > 1$ for $m \neq 0$ and $mn = 0$ for $m = 0$, so in no case can we have $mn = 1$. □

Remark 2.2.5. Let us say that $n, m \in \mathbb{Z}_{\neq 0}$ are *associate*, if $m|n$ and $n|m$. Equivalently, by Lemma 2.2.2, if $m \in \{n, -n\}$. This is an equivalence relation. In terms of divisibility, we should not distinguish associate numbers. Thus, when studying gcd's, primes and so on, it is in fact "most correct" to do so in terms of the equivalence classes of the above equivalence relation. The set of equivalence classes is in clear bijection with $\mathbb{Z}_{\geq 0}$ (each equivalence class has a unique non-negative element).

Remark 2.2.6. If n is divisible by d and $d \neq 0$, there exists a unique $m \in \mathbb{Z}$ such that $n = md$. We denote this m by $\frac{n}{d}$.

2.3 Division with remainder

Theorem 2.3.1. *Let* $m \in \mathbb{Z}_{\neq 0}$ *and* $n \in \mathbb{Z}$. *There exists a unique pair* $(q, r) \in \mathbb{Z} \times [0, |m| - 1]$ *for which*

$$n = qm + r.$$

Proof. Let us prove uniqueness first. If $(q_1, r_1), (q_2, r_2) \in \mathbb{Z} \times [0, |m| - 1]$ are two pairs such that $n = q_1 m + r_1$ and $n = q_2 m + r_2$ then we get $q_1 m + r_1 = q_2 m + r_2$ so $(q_2 - q_1)m = r_1 - r_2$. Notice that we have $r_1 - r_2 \leq (|m| - 1) - 0 = |m| - 1$ and also $r_1 - r_2 \geq 0 - (|m| - 1) = -(|m| - 1)$, in other words $|r_1 - r_2| \leq |m| - 1$. But, on the other hand, $|(q_2 - q_1)m| \geq |m|$ if $q_2 - q_1 \neq 0$, i.e. if $q_1 \neq q_2$. Therefore we must have $q_1 = q_2$. Then from the equation $q_1 m + r_1 = q_2 m + r_2$ we also get $r_1 = r_2$.

Now let us establish existence. We can assume that $n \geq 0$ because if $-n = qm + r$ then $n = (-q)m + (-r)$. We proceed by induction on n. Base case: $n = 0$. Then the pair $(0, 0)$ works. Induction step: Assume that the existence claim holds for some $n \geq 0$, and let us show it for $n + 1$. Write $n = qm + r$. If $r < m - 1$, then the pair $(q, r + 1)$ works for $n + 1$. If $r = m - 1$, then the pair $(q + 1, 0)$ works for $n + 1$. □

2.4 gcd and Euclid's algorithm

Definition 2.4.1. Let $m, n \in \mathbb{Z}$ and let $d \in \mathbb{Z}$. We say that d is the greatest common divisor of m and n (abbreviating "*gcd*") if:

1. $d|m$ and $d|n$.

2. For every $e \in \mathbb{Z}$ satisfying $e|m$ and $e|n$, one has $e|d$.

Lemma 2.4.2. *Let $m, n \in \mathbb{Z}$. Any two gcd's of m and n are associate.*

Proof. If d, e are both *gcd*'s of m and n, then by the definition we have $e|d$ because e is a divisor and d is a *gcd*, and in the same way we have $d|e$. Thus d and e are associates. □

Remark 2.4.3. One should interpret the above lemma as saying that the *gcd* is unique, by our remark above that associate numbers should not be distinguished when talking about divisibility.

Theorem 2.4.4 (Euclid)**.** *Let $m, n \in \mathbb{Z}$. Then there exists a gcd for m and n.*

Proof. The proof is via an algorithm ("Euclid's algorithm")/induction, using Lemma 2.4.5 that follows.

1. If $m = 0$, it is easy to see that n is the *gcd* of m and n.

2. If $m \neq 0$, we perform division with remainder, writing $n = qm + r$ with $r \in [0, |m| - 1]$. Then by Lemma 2.4.5 below, the *gcd* of m and n will be the same as the *gcd* of r and m, so we replace the pair (n, m) with the pair (m, r). and return to the first step.

The algorithm will end: If $m = 0$ this is clear; if $n = 0$ this is clear (after the swap of the second step we will have $m = 0$); if $|n| = |m|$ also clear because after the second step we will have $m = 0$; if $|n| < |m|$ then after the second step we will have $|n| > |m|$; and finally, if $|n| > |m|$, then $max\{|m|, |n|\}$ becomes strictly smaller after the second step. □

Lemma 2.4.5. *Let $n = qm + r$. Then if d is the gcd of r and m, it is also the gcd of m and n.*

Proof. Since $d|m$, we have $d|qm$. Then, since $d|qm$ and $d|r$, we have $d|qm + r$, i.e. $d|n$. Furthermore, if $e|m$ and $e|n$, we have $e|n - qm$, i.e. $e|r$, and therefore, since d is the *gcd* of r and m, we get $e|d$. □

Example 2.4.6. *Let us find the gcd of -1740 and 522:*

- $-1740 = (-4) \cdot 522 + 348.$
- $522 = 1 \cdot 348 + 174.$
- $348 = 2 \cdot 174 + 0.$

Therefore, the gcd of our two numbers is 174 (or -174).

We will denote the *gcd* of the numbers m and n by $gcd(m, n)$. For convenience, we will usually mean by that the non-negative representative of the set of *gcd*'s (which is an equivalence class for being associate).

2.5 Ideals and *gcd*

Definition 2.5.1. Let $I \subset \mathbb{Z}$ be a subset. We say that I is an *ideal*, if the following hold:

1. $0 \in I$.
2. If $m, n \in I$ then $m + n \in I$.
3. If $m \in I$ and $n \in \mathbb{Z}$, then $mn \in I$.

Example 2.5.2. *Let $d \in \mathbb{Z}$. Consider then*

$$(d) := \{m \in \mathbb{Z} \mid d|m\} = \{m \in \mathbb{Z} \mid \exists e \text{ s.t. } m = ed\}.$$

It is easy to see that (d) is an ideal.

Remark 2.5.3. The previous example shows that we can think of an ideal as a set of numbers which potentially can be the set of all numbers that are divisible by a given fixed number.

Example 2.5.4. *Let $d_1, \ldots, d_r \in \mathbb{Z}$. Consider then*

$$(d_1, \ldots, d_r) := \{m \in \mathbb{Z} \mid \exists e_1, \ldots, e_r \text{ s.t. } m = e_1d_1 + \ldots + e_rd_r\}.$$

It is easy to see that $(d_1, \ldots, d_r)$ is an ideal.

Proposition 2.5.5. *Let $I \subset \mathbb{Z}$ be an ideal. Then there exists $d \in \mathbb{Z}$ such that $I = (d)$. Any two such d's are associate.*

Proof. It is clear that if $(d_1) = (d_2)$ then d_1 and d_2 are associates, so we are left with proving the existence.

If I has no elements other than 0 then $I = (0)$ and we are done. Otherwise, there exists $m \in I$ such that $m \neq 0$. Since $-m = (-1) \cdot m \in I$, and either m or $-m$ is positive, we see that $I \cap \mathbb{Z}_{>0}$ is non-empty. Let d be the minimal element of $I \cap \mathbb{Z}_{>0}$. We claim now that $I = (d)$. First, notice that $d \in I$ and therefore $md \in I$ for every $m \in \mathbb{Z}$, and hence $(d) \subset I$. Conversely, let $m \in I$ (we want to show that $m \in (d)$. We perform division with remainder: $m = qd + r$ where $0 \leq r \leq d-1$. Since $m \in I$ and $d \in I$ we have $r = m - qd \in I$. By the minimality of d, we therefore must have $r = 0$. Hence $m = qd$ and so $m \in (d)$. □

Remark 2.5.6. Therefore, the ideals in $\mathbb{Z}$ are in bijection with equivalence classes of integers up to being associate. In fact, the "correct" way of thinking about divisibility issues is in terms of ideals.

Discussion 2.5.7 (*gcd* via ideals)**.** Let now $m, n \in \mathbb{Z}$. By Proposition 2.5.5, there exists $d \in \mathbb{Z}$ such that $(d) = (m, n)$. We claim that d is the *gcd* of m and n. Indeed, since $m \in (m, n) = (d)$, we have $d|m$. Similarly, $d|n$. To proceed, notice that since $d \in (d) = (m, n)$, there exist f, g such that $d = fm + gn$. Then, if some e satisfies $e|m$ and $e|n$, we obtain $e|fm + gn = d$. This concludes showing that d is the *gcd* of m and n.

Remark 2.5.8. The last discussion teaches us that the *gcd* of m and n is an integral linear combination of m and n, i.e. that there exist f, g such that $d = fm + gn$. This also follows easily from Euclids algorithm, as we demonstrate in the next example.

Example 2.5.9. *We found earlier that* 174 *is the gcd of* -1740 *and* 522*. Let us find how the former can be expressed as an integral linear combination of the latter:*

$$174 = 1 \cdot 522 + (-1) \cdot 348 = 1 \cdot 522 + (-1) \cdot (1 \cdot (-1740) + 5 \cdot 522) = (-4) \cdot 522 + (-1) \cdot (-1740).$$

2.6 Linear equations in two variables - existence of solutions

Let us apply the above to study the solutions of a linear equation $mx + ny = r$ (here $m, n, r \in \mathbb{Z}$ and we seek solutions $(x, y) \in \mathbb{Z}^2$).

Proposition 2.6.1. *The equation* $mx + ny = r$ *has a solution if and only if* $gcd(m, n)|r$.

Proof. This is clear in view of the above theory, since the existence of a solution to the equation is, by definition, equivalent to the statement $r \in (m, n)$. Denoting $d = gcd(m, n)$, we have $(m, n) = (d)$ and therefore the existence of a solution to the equation is equivalent to $r \in (d)$, i.e. to $d|r$. □

2.7 Relatively prime numbers

Definition 2.7.1. We say that m and n are *relatively prime* if $gcd(m, n) = 1$. Equivalently, if no $d > 1$ divides both m and n.

Lemma 2.7.2. *The equation $mx + ny = 1$ has a solution if and only if m and n are relatively prime.*

Proof. The equation $mx + ny = 1$ has a solution if and only if $gcd(m, n)|1$, which in turn is equivalent to $gcd(m, n) = 1$. □

Lemma 2.7.3. *Suppose that either m or n is not zero. Denote $g := gcd(m, n)$. Then $\frac{m}{g}$ and $\frac{n}{g}$ are relatively prime.*

Proof. We can write $xm + yn = g$. Then, dividing by g, we obtain $x\frac{m}{g} + y\frac{n}{g} = 1$. □

Lemma 2.7.4. *Let m and n be relatively prime. If $m|ne$ then $m|e$.*

Proof. Write $1 = fm + gn$. Then $e = 1 \cdot e = fme + gne$. Clearly $m|fme$ and $m|ne|gne$. Hence $m|fme + gne = e$. □

Lemma 2.7.5. *Let m and n be relatively prime. If $m|e$ and $n|e$ then $mn|e$.*

Proof. Since $m|e$, we can write $e = km$ for some k. Since $n|e = km$ and n is relatively prime to m, by the previous lemma we obtain $n|k$. Thus we can write $k = \ell n$ for some ℓ. Then $e = km = \ell nm$, i.e. $nm|e$. Write $1 = fm + gn$. Then $e = 1 \cdot e = fme + gne$. Clearly $m|fme$ and $m|ne|gne$. Hence $m|fme + gne = e$. □

Lemma 2.7.6. *Suppose that m and n are relatively prime, and that k and n are relatively prime. Then mk and n are relatively prime.*

Proof. Write $em + fn = 1, gk + hn = 1$. Then

$$1 = (em + fn)(gk + hn) = eg \cdot mk + (emh + fgk + fhn) \cdot n.$$

□

2.8 Linear equations in two variables - finding all solutions

Proposition 2.8.1. *Suppose that either m or n is not zero. Suppose that the equation $mx + ny = r$ has a solution (x_0, y_0). Denote $g := gcd(m, n)$. Then the general solution of the equation is:*

$$(x_0 - \frac{n}{g}t, y_0 + \frac{m}{g}t), \quad t \in \mathbb{Z}.$$

Proof. First of all, $(x_0 - \frac{n}{g}t, y_0 + \frac{m}{g}t)$ is indeed a solution for every $t \in \mathbb{Z}$:

$$m(x_0 - \frac{n}{g}t) + n(y_0 + \frac{m}{g}t) = r.$$

Next, let (x_1, y_1) be a solution. We will assume that $m \neq 0$ (the case $n \neq 0$ is dealt with analogously). We have

$$m(x_1 - x_0) + n(y_1 - y_0) = 0.$$

Therefore $m|n(y_1 - y_0)$, and thus $\frac{m}{g}|\frac{n}{g}(y_1 - y_0)$. Since $\frac{m}{g}$ and $\frac{n}{g}$ are relatively prime, we have $\frac{m}{g}|y_1 - y_0$. Therefore there exists $t \in \mathbb{Z}$ such that $\frac{m}{g}t = y_1 - y_0$, or $y_1 = y_0 + \frac{m}{g}t$. Substituting this into the equation, we obtain $m(x_1 - x_0) + \frac{mn}{g}t = 0$ and so, since $m \neq 0$, $x_1 - x_0 + \frac{n}{g}t = 0$, or $x_1 = x_0 - \frac{n}{g}t$. □

2.9 Primes

Definition 2.9.1. Let $p \in \mathbb{Z}_{\geq 1}$ be not equal to 1. We say that p is *prime* if for all $m, n \in \mathbb{Z}_{\geq 1}$ one has the implication:

$$p = mn \implies p = m \text{ or } p = n.$$

In other words, if $m \in \mathbb{Z}_{\geq 1}$ satisfies $m|p$ then $m = p$ or $m = 1$.

We have the following property:

Lemma 2.9.2. *Let p be a prime and $n \in \mathbb{Z}$. Then either $p|n$ or p and n are relatively prime.*

Proof. $gcd(p, n)$ divides p, and hence is either p or 1. If it is p then $p|n$. If it is 1, then p and n are relatively prime. □

We have the following important characterization of primes:

Claim 2.9.3. *Let $p \in \mathbb{Z}_{\geq 1}$ be not equal to 1. The following conditions are equivalent:*

1. *For all $m, n \in \mathbb{Z}$ one has the implication:*

$$p|mn \implies p|m \text{ or } p|n.$$

2. *p is prime.*

Proof. Suppose that the first condition holds. If we have $p = mn$, then in particular $p|mn$ and therefore $p|m$ or $p|n$, let's say the first. Then we have $p|m$ but also $m|p$ (because $p = mn$) and therefore p and m are associates, and therefore are equal (as both are positive).

Conversely, suppose that the second condition holds. Suppose that we have $p|mn$. Then by Lemma 2.9.2 either $p|m$, in which case we are done, or p and m are relatively prime, in which case $p|n$ by Lemma 2.7.4. □

Remark 2.9.4. Again, it is more correct to talk about primeness of equivalence classes of integers up to being associate (and thus, in fact, about prime ideals).

Theorem 2.9.5 (Euclid)**.** *There are infinitely many primes.*

Proof. If there are finitely many primes, say $p_1, p_2, \dots, p_r$, we can form the following number:

$$n := p_1 \cdot p_2 \cdot (\dots) \cdot p_r + 1.$$

By Lemma 2.9.6 that follows, there exists a prime p such that $p|n$. Then for every $1 \leq i \leq r$ we have $p \neq p_i$, since $p_i|n$ would force $p_i|1$. Hence there is a new prime p, contradicting $p_1, p_2, \dots, p_r$ being all primes. □

Lemma 2.9.6. *Let $n \in \mathbb{Z}_{\geq 1}$. Then either $n = 1$ or there exists a prime p such that $p|n$.*

Proof. We proceed by induction on n. For $n = 1$ the claim is clear. Let $n > 1$ and suppose that the claim holds for all numbers in $[1, n-1]$. If n is prime, the claim is clear for n. If not, then there exists $m \in \mathbb{Z}_{\geq 1}$ such that $m|n$ but neither $m = n$ nor $m = 1$. Thus, by the induction assumption, there exists a prime p such that $p|m$. Since $m|n$, we get $p|n$ and we are done. □

2.10 Factorization into primes

Theorem 2.10.1. *Let $n \in \mathbb{Z}_{\geq 1}$.*

1. *There exists a list of primes $p_1, \dots, p_r$ such that*

   $$n = p_1 p_2 \cdots p_r$$

   ($n = 1$ is considered to be a product of an empty list of primes).

2. *If $q_1, \dots, q_s$ is another list of primes such that*

   $$n = q_1 q_2 \cdots q_s,$$

   then the two lists are the same up to reordering; That is, for every prime p, the number of $1 \leq i \leq r$ for which $p_i = p$ is equal to the number of $1 \leq j \leq s$ for which $q_j = p$.

Proof. For existence, we proceed by induction on n. If $n = 1$, we should consider it as the product of the empty list of primes. Assume thus that $n > 1$. If n is prime, then it is the product of the list n consisting of one prime. If n is not prime, by Lemma 2.9.6 there exists a prime p such that $p|n$. Since $\frac{n}{p} < n$, we can assume by induction that $\frac{n}{p} = p_1 \cdots p_r$ for some primes $p_1, \dots, p_r$. Then $n = p_1 \cdots p_r \cdot p$.

The uniqueness claim will be clear from the following characterization: The number k of $1 \leq i \leq r$ for which $p_i = p$ is the unique number for which p^k divides

n and p^{k+1} does not divide n. Indeed, clearly p^k divides n. Showing that p^{k+1} does not divide n is equivalent to showing that p does not divide $\frac{n}{p^k}$. Notice that $\frac{n}{p^k}$ is written as a product of primes, non of which is p. Therefore p does not divide it (because if it would, it would divide on of the primes appearing in the product, and therefore would be equal to it). □

We can rephrase the unique factorization into primes as follows. Let us consider the set of primes $P \subset \mathbb{Z}_{\geq 1}$. Let us denote by Exp the set of functions $\alpha : P \to \mathbb{Z}_{\geq 0}$ for which

$$\{p \in P \mid \alpha(p) \neq 0\}$$

is finite. Thus, more concretely, ordering the primes

$$p_1 < p_2 < \dots$$

we can depict α as a sequence

$$\alpha(p_1), \alpha(p_2), \dots$$

all of whose entries are 0 after a certain point. For every $\alpha \in Exp$, we can form a well defined product

$$\prod_{p \in P} p^{\alpha(p)},$$

because almost all (i.e., all except finitely many) terms of the product are equal to 1, so we can disregard them.

Proposition 2.10.2 (Unique factorization)**.** *One has a bijection*

$$Exp \to \mathbb{Z}_{\geq 1}$$

given by

$$\alpha \mapsto \prod_p p^{\alpha(p)}.$$

Example 2.10.3. *One has*

$$819 = 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^1 \cdot 11^0 \cdot 13^1 \cdot 17^0 \cdot \ldots .$$

2.11 Another proof of Euclid's theorem

Let us sketch a different proof of the fundamental Theorem 2.9.5, which requires some knowledge of analysis (due to Euler). Consider the infinite sum of positive numbers:

$$\sum_{n \in \mathbb{Z}_{\geq 1}} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \ldots .$$

By the unique factorization into primes, one can write this as a product:

$$\sum_{n \in \mathbb{Z}_{\geq 1}} \frac{1}{n} = \prod_{p \in P} \left(\frac{1}{p^0} + \frac{1}{p^1} + \frac{1}{p^2} + \ldots \right) = \prod_{p \in P} \frac{1}{1 - p^{-1}}.$$

Therefore, would there be finitely many primes, the sum would converge. But, by basic analysis, this sum does not converge.

2.12 Statistics of primes

One can think as follows. The additive structure of $\mathbb{Z}_{\geq 1}$ is very simple. The multiplicative structure of $\mathbb{Z}_{\geq 1}$ is also very simple (as evidenced by proposition 2.10.2). What is highly complicated is the relation between the two structures. One of the basic questions one can ask about this relation is something as follows: The m-th prime number, how many times one should add 1 to itself to obtain it? Much more than m? Quite equivalently, one can ask how many primes one has in the interval $[1, n]$ for a given n.

Let us denote therefore by $\pi(n)$ the number of prime numbers in the interval $[1, n]$. Euclid's theorem gives the most basic information, that

$$\lim_{n \to \infty} \pi(n) = \infty,$$

One has the much more precise very famous theorem:

Theorem 2.12.1 (Prime number theorem)**.** *One has*

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

In other words, for every $0 < \epsilon$ there exists N such that for $n > N$ the ratio $\frac{\pi(n)}{n}$ of primes in the interval $[1, n]$ lies between $\frac{1-\epsilon}{ln(n)}$ and $\frac{1+\epsilon}{ln(n)}$.

Example 2.12.2. *The number of primes between* 1 *and* $n := 1000000$ *is* 78498. *On the other hand,* $\frac{n}{ln(n)} \approx 72382$.

Let us give a very very crude heuristic for the prime number theorem (which will be unsatisfying, but a start). First, notice that if a number m is composite, then it has a prime factor $\leq \sqrt{m}$ (this is since it has at least to prime factors, and if those two are $> \sqrt{m}$, their product, and even more so m, is $> m$). Therefore, if we want to count primes in $[\sqrt{n}, n]$, we need to remove all numbers divided by primes $< \sqrt{n}$. The proportion of numbers not divided by p is around $1 - \frac{1}{p}$. Therefore, crudely assuming that to not be divided by primes are independent events, we get that the proportion of primes in the interval $[\sqrt{n}, n]$ is around

$$\alpha = \prod_{p < \sqrt{n}} \left(1 - \frac{1}{p}\right).$$

We have:

$$\alpha^{-1} = \prod_{p \leq \sqrt{n}} \frac{1}{1 - p^{-1}} = \sum_{\substack{m \text{ which can be written} \\ \text{as a product of primes } < \sqrt{n}}} \frac{1}{m} \sim \sum_{m \leq n} \frac{1}{m} \sim ln(n)$$

and thus $\alpha \sim \frac{1}{ln(n)}$.

In fact, a better approximation to $\pi(n)$ than $n/ln(n)$ is

$$Li(n) := \int_2^n \frac{dt}{ln(t)}$$

(it kinds of aggregates all the local densities $\frac{1}{ln(t)}$ adjusting them as we travel along the line).

Example 2.12.3. *One has* $Li(1000000) \approx 78626$ *- much better!*

One has

$$\lim_{n\to\infty} \frac{Li(n)}{\frac{n}{ln(n)}} = 1$$

and therefore the prime number theorem is equivalent to

$$\lim_{n\to\infty} \frac{\pi(n)}{Li(n)} = 1.$$

The hyper-celebrated *Riemann hypothesis* is equivalent to the statement that

$$|\pi(n) - Li(n)| = O(\sqrt{n} \cdot ln(n)),$$

which means that there exists $C > 0$ such that

$$|\pi(n) - Li(n)| \leq C \cdot (\sqrt{n} \cdot ln(n)).$$

Remark 2.12.4. Gauss (around the age of 15) made tables of $Li(n)$ and conjectured that the density of primes around a given number n is around $\frac{1}{ln(n)}$.

2.13 gcd and lcm in terms of prime factorization

Given $m, n \in \mathbb{Z}_{\geq 1}$, let us write

$$m = \prod_{p\in P} p^{\alpha(p)}, \quad n = \prod_{p\in P} p^{\beta(p)}.$$

Then it is easy to see that $m|n$ if and only if $\alpha(p) \leq \beta(p)$ for all $p \in P$. It is therefore easy to see that

$$gcd(m,n) = \prod_{p\in P} p^{min\{\alpha(p),\beta(p)\}}.$$

We can also define the lowest common multiple of m, n as a number k such that $m|k$, $n|k$ and additionally if $m|\ell$ and $n|\ell$ for some ℓ, then $k|\ell$. Then it is easy to see that

$$lcm(m,n) = \prod_{p\in P} p^{max\{\alpha(p),\beta(p)\}}.$$

Remark 2.13.1. We see that

$$lcm(m,n) = \frac{mn}{gcd(m,n)}$$

(because $max\{a,b\} = a + b - min\{a,b\}$).

2.14 Pythagorean triples

Definition 2.14.1. A *Pythagorean triple* is a solution $(x, y, z) \in \mathbb{Z}^3$ to the equation

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

In other words, we are seeking right-angle triangles whose side lengths are integers.

Definition 2.14.2. A Pythagorean triple (x, y, z) is said to be *primitive*, if x, y, z are relatively prime (equivalently, some two numbers out from x, y, z are relatively prime).

Given a Pythagorean triple (x, y, z), let $g = gcd(x, y, z)$. Then the triple $(\frac{x}{g}, \frac{y}{g}, \frac{z}{g})$ is a primitive Pythagorean triple. And of course conversely, if (x, y, z) is a Pythagorean triple, then so is (dx, dy, dz). This shows that it is enough to understand primitive Pythagorean triples.

Let (x, y, z) be a primitive Pythagorean triple. We can assume that $x, y, z > 0$ (all other possibilities are easily recovered from those). Exactly one out of x, y is even; Indeed, if both x, y are odd, then writing $x = 2x_0+1, y = 2y_0+1, z = 2z_0$ we obtain $x^2 + y^2 = 4(\cdots) + 2$ and $z^2 = 4(\cdots)$ so $x^2 + y^2 - z^2 = 4(\cdots) + 2$, so it can't be 0.

Suppose then, without loss of generality, that x is even and y is odd - all other possibilities will be easily recovered from those. Write $x = 2x_0$. Then

$$4x_0^2 = z^2 - y^2 = (z - y)(z + y).$$

Notice that

$$gcd(z - y, z + y) = gcd(z - y, 2y) = 2 \cdot gcd(z - y, y) = 2 \cdot gcd(z, y) = 2.$$

Therefore, we can write $z - y = 2m, z + y = 2n$ and $gcd(m, n) = 1$. We obtain

$$x_0^2 = mn.$$

Since m and n are relatively prime, it follows easily that m and n are squares - $m = m_0^2, n = n_0^2$. We obtain

$$z = \frac{z - y}{2} + \frac{z + y}{2} = n_0^2 + m_0^2$$

and

$$y = -\frac{z - y}{2} + \frac{z + y}{2} = n_0^2 - m_0^2,$$

and thus

$$x^2 = z^2 - y^2 = 4n_0^2 m_0^2,$$

so

$$x = 2n_0 m_0.$$

Now, conversely, for integers m_0, n_0 the triple

$$\left(2n_0m_0, n_0^2 - m_0^2, n_0^2 + m_0^2\right)$$

is a Pythagorean triple, which is primitive if $gcd(n_0, m_0) = 1$ and one of n_0, m_0 is even.

Now we present a different approach to Pythagorean triples, a geometric one. A point $(x, y) \in \mathbb{R}^2$ is said to be *rational*, if $x, y \in \mathbb{Q}$. For a subset $A \subset \mathbb{R}^2$, we denote

$$A_{\mathbb{Q}} = \{(x, y) \in A \mid x, y \in \mathbb{Q}\}.$$

Imagine the unit circle in the Cartesian plane:

$$S := \{(X, Y) \in \mathbb{R}^2 \mid X^2 + Y^2 = 1\}.$$

Given $(X, Y) \in S_{\mathbb{Q}}$, we write

$$X = \frac{x}{z}, Y = \frac{y}{w}$$

where $w, z \in \mathbb{Z}_{\geq 1}$ and

$$gcd(x, z) = 1, gcd(y, w) = 1.$$

We must have $z = w$; Indeed,

$$w^2x^2 + z^2y^2 = z^2w^2$$

and this shows easily that divisors of z are also divisors of w and vice versa. Therefore,

$$(X, Y) = (\frac{x}{z}, \frac{y}{z})$$

with

$$gcd(x, z) = 1, gcd(y, z) = 1.$$

We see that (x, y, z) is a primitive Pythagorean triple. Conversely, given a primitive Pythagorean triple (x, y, z) we can form the point

$$(\frac{x}{z}, \frac{y}{z}) \in S_{\mathbb{Q}}.$$

This shows that $S_{\mathbb{Q}}$ is in bijection with the set primitive Pythagorean triples (x, y, z) with $z > 0$.

The question now is how to construct points of $S_{\mathbb{Q}}$.

We say that a line $L \subset \mathbb{R}^2$ is *rational*, if it can be written in the form

$$L = \{(x, y) \in \mathbb{R}^2 \mid ax + by = c\}$$

for some $a, b, c \in \mathbb{Q}$ (where $(a, b) \neq (0, 0)$).

Lemma 2.14.3. *1. Let $L, M \subset \mathbb{R}^2$ be two rational lines. Then all points in $L \cap M$ are rational.*

2. Let $L \subset \mathbb{R}^2$ be a rational line. Then if one of the points in $L \cap S$ is rational, so are all.

Proof.

1. This follows from the method of solving a system of two linear equations in two variables by substitution - all we do is multiply/divide/add/substract the coefficients, to obtain the solutions.

2. Writing $ax+by=c$ for the equation of L with rational coefficients, suppose $b \neq 0$ (the other case, $a \neq 0$, is dealt with analogously). Then we can rewrite
$$L = \{(x,y) \in \mathbb{R}^2 \mid y = ex + f\}$$
for some $e, f \in \mathbb{Q}$. Then the intersection points $L \cap S$ correspond to x for which
$$(1+e^2)x^2 + 2efx + (f^2-1) = 0.$$
So if there are two intersection points (the case of 0 or 1 intersection points is clear), they correspond to two roots x of the equation. But if a quadratic equation $\alpha x^2 + \beta x + \gamma = 0$ with rational coefficients has one rational root, then the other root must also be rational, since the sum of the roots is equal to $-\frac{\beta}{\alpha}$. Therefore the x-coordinate of the second intersection point will be also rational, and therefore also the y-coordinate (because $y = ex + f$).

□

Let us consider now
$$L := \{(X,Y) \in \mathbb{R}^2 \mid Y = 0\}$$
(the x-axis). It is not hard to see that there is a bijection between $L_{\mathbb{Q}}$ and $S_{\mathbb{Q}} \setminus \{(0,1)\}$, as follows: to $P \in L_{\mathbb{Q}}$ we associate the unique intersection point of S with the line passing through P and $(0,1)$. And to $P \in S_{\mathbb{Q}} \setminus \{(0,1)\}$ we associate the unique intersection point of L with the line passing through P and $(0,1)$.

Let us compute the concrete form of the bijection. Given $(t,0) \in L_{\mathbb{Q}}$, The line through $(0,1)$ and $(t,0)$ has the form
$$L' = \{(0,1) + s(t,0) \ : \ s \in \mathbb{R}\}.$$
We find the intersection points in $L' \cap S$ in terms of s, and obtain an equation
$$(1+t^2)s^2 - 2s = 0.$$

The solution $s = 0$ corresponds to the point $(0, 1)$. The othe solution is $s = \frac{2}{1+t^2}$, giving the point

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

Let us write

$$t = \frac{n}{m}$$

with $gcd(n, m) = 1$ and $m \in \mathbb{Z}_{\geq 1}$. Then our point is written

$$\left(\frac{2nm}{n^2+m^2}, \frac{n^2-m^2}{n^2+m^2} \right),$$

corresponding to the Phytagorean triple

$$(2nm, n^2 - m^2, n^2 + m^2).$$

Chapter 3

Modular arithmetic

3.1 Definitions and illustrations

Definition 3.1.1. Let us fix $d \in \mathbb{Z}_{\geq 1}$. For $m, n \in \mathbb{Z}$, we say that m *is congurent to* n *modulo* d, and write

$$m \equiv_d n$$

or

$$m \equiv n \pmod{d}$$

if $d|n - m$.

Lemma 3.1.2. *The relation* $\equiv_d$ *is an equivalence relation on* $\mathbb{Z}$. *In detail:*

1. *For all* $n \in \mathbb{Z}$, $n \equiv_d n$.

2. *For all* $n, m \in \mathbb{Z}$, *if* $n \equiv_d m$ *then* $m \equiv_d n$.

3. *For all* $n, m, k \in \mathbb{Z}$, *if* $n \equiv_d m$ *and* $m \equiv_d k$ *then* $n \equiv_d k$.

Lemma 3.1.3. *Let us perform division with remainder:*

$$n = q_1 d + r_1, \ \ m = q_2 d + r_2$$

where $r_1, r_2 \in [0, \ldots, d-1]$. *Then* $m \equiv_d n$ *if and only if* $r_1 = r_2$.

Proof. We have $m \equiv_d n$ i.f.f.

$$d|n - m = (q_1 - q_2)d + (r_1 - r_2).$$

This happens i.f.f. $d|r_1 - r_2$. Since $|r_1 - r_2| \leq d - 1$, this happens i.f.f. $r_1 - r_2 = 0$, i.e. $r_1 = r_2$. □

The congruence relation interacts well with addition and multiplication:

Lemma 3.1.4. *If $m_1 \equiv_d m_2$ and $n_1 \equiv_d n_2$, then*

$$m_1 + n_1 \equiv_d m_2 + n_2$$

and

$$m_1 n_1 \equiv_d m_2 n_2.$$

Proof. Let us prove the second claim, for example. We have

$$m_2 n_2 - m_1 n_1 = m_2(n_2 - n_1) + (m_2 - m_1)n_1.$$

Since $d|n_2 - n_1$ and $d|m_2 - m_1$, we have also $d|m_2(n_2 - n_1) + (m_2 - m_1)n_1$. □

Since congruence modulo d is an equivalence relation, we can form equivalence classes (which are in this case called *residue classes modulo d*), i.e. consider the sets of the form

$$[n]_d = \{m \mid m \equiv_d n\} \subset \mathbb{Z}.$$

One can also write a bit more explicitly

$$[n]_d = n + \mathbb{Z}d = \{n + kd \ : \ k \in \mathbb{Z}\}.$$

The set of all residue classes has d elements, and we denote it by $\mathbb{Z}_d$. Each $n' \in [n]_d$ is called a *representative* of the residue class $[n]_d$.

Example 3.1.5.

$$\begin{aligned} \mathbb{Z}_3 = \Big\{ &\{\cdots, -6, -3, 0, 3, 6, \cdots\} \\ &\{\cdots, -5, -2, 1, 4, 7, \cdots\} \\ &\{\cdots, -4, -1, 2, 5, 8, \cdots\} \Big\} \end{aligned} \tag{3.1.1}$$

From the last lemma it follows that the set $\mathbb{Z}_d$ has well-defined addition and multiplication: If we need to add/multiply to classes, we choose representatives of them, add/multiply these integers, and then take residue class of the result. The point is that the end answer does not depend on the representatives chosen, thanks to the lemma. For example:

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[0]_3$	$[1]_3$	$[2]_3$

Example 3.1.6. *Let us notice that*

$$1^2 \equiv_4 3^2 \equiv_4 1$$

and

$$0^2 \equiv_4 2^2 \equiv_4 0.$$

Thus, for example, the number 25798347 *can not be a square, because*

$$25798347 = ? \cdot 100 + 47 \equiv_4 3.$$

Exercise 3.1.7. *Let*

$$\epsilon_k \ldots \epsilon_1 \epsilon_0$$

be the decimal representation of a number $n \in \mathbb{Z}_{\geq 0}$ (so here $\epsilon_i \in \{0, 1, \ldots, 9\}$). Show that is divisible by 3 if and only if

$$\epsilon_k + \epsilon_{k-1} + \ldots + \epsilon_0$$

is divisible by 3.

Solution. Notice that $10^m \equiv_3 1$. Therefore

$$n = \sum_{0 \leq i \leq k} \epsilon_i \cdot 10^i \equiv_3 \sum_{0 \leq i \leq k} \epsilon_i.$$

□

Theorem 3.1.8. *There are infinitely many primes which are congruent to 3 modulo 4.*

Proof. Suppose, to obtain a contradiction, that there are only finitely many primes which are congruent to 3 modulo 4 - enumerate them $p_1, p_2, \ldots, p_k$. Consider

$$n := 4 \cdot p_1 \cdot \ldots \cdot p_k - 1.$$

Notice that $n \equiv_4 3$. Would all primes dividing n be congruent to 1 modulo 4, their product, n, would also be congruent to 1 modulo 4. Hence, there exists at least one prime dividing n which is congruent to 3 modulo 4. As none of $p_1, \ldots, p_k$ divide n, we obtain a new prime which is congruent to 3 modulo 4, contradicting the assumptions. □

Remark 3.1.9. In fact, there are also infinitely many primes which are congruent to 1 modulo 4, we will see this later. Anyhow, a much more general statement holds, a very famous theorem of Dirichlet: Let m be relatively prime to d. Then there exist infinitely many primes which are congruent to m modulo d. One can say that the ideas involved in the proof are highly beautiful.

3.2 The Chinese remainder theorem

Remark 3.2.1. Let $d, e \in \mathbb{Z}_{\geq 1}$ and assume that $d|e$. Then every residue class modulo e determines a well-defined residue class modulo d. Indeed, given $n \in \mathbb{Z}$, we associate to the residue class $[n]_e$ the residue class $[n]_d$. We only then need to see that this does not depend on the n chosen to represent the class. Indeed, if $[n']_e = [n]_e$, we have $e|n' - n$ and thus in particular $d|n' - n$ so $[n']_d = [n]_d$.

In other words, we have a well-defined "forgetting information" map

$$frgt_d^e : \mathbb{Z}_e \to \mathbb{Z}_d.$$

Theorem 3.2.2. *Let $d, e \in \mathbb{Z}_{\geq 1}$ be relatively prime. Let $m, n \in \mathbb{Z}$. Then there exists $k \in \mathbb{Z}$ such that*

$$k \equiv_d m, \quad k \equiv_e n.$$

Moreover, such k is unique modulo de. In other words, the map

$$frgt_d^{de} \times frgt_e^{de} : \mathbb{Z}_{de} \to \mathbb{Z}_d \times \mathbb{Z}_e$$

is a bijection.

Proof. Let us show uniqueness first. Suppose that k_1, k_2 both satisfy the demands. Then $k_1 \equiv_d k_2$ and $k_1 \equiv_e k_2$. This means that $d|k_2 - k_1$ and $e|k_2 - k_1$. Since d and e are relatively prime, this implies that $de|k_2 - k_1$, i.e. $k_1 \equiv_{de} k_2$.

Now let us show existence. It is enough to show that there exists $r \in \mathbb{Z}$ such that

$$r \equiv_d 1, \quad r \equiv_e 0.$$

Indeed, then analogously there exists s such that

$$s \equiv_d 0, \quad s \equiv_e 1,$$

and then $k = mr + ns$ will satisfy what we want. Since d and e are relatively prime, there exist f_1, f_2 such that $f_1 d + f_2 e = 1$. Then $r = f_2 e$ is a number as we desire. Indeed, $f_2 e = 1 - f_1 d \equiv_d 1$ and clearly $f_2 e \equiv_e 0$. □

We can extend this:

Theorem 3.2.3. *Let $d_1, \ldots, d_n \in \mathbb{Z}_{\geq 1}$ be pairwise relatively prime*[1]*. Let $m_1, \ldots, m_n \in \mathbb{Z}$. Then there exists $k \in \mathbb{Z}$ such that*

$$k \equiv_{d_i} m_i \quad \forall 1 \leq i \leq n.$$

Moreover, such k is unique modulo $d_1 \cdot \ldots \cdot d_n$. In other words, the map

$$\prod_{1 \leq i \leq n} frgt_{d_i}^{d_1 \cdot \ldots \cdot d_n} : \mathbb{Z}_{d_1 \cdot \ldots \cdot d_n} \to \prod_{1 \leq i \leq n} \mathbb{Z}_{d_i}$$

is a bijection.

Proof. Let us show uniqueness. Suppose that k_1, k_2 both satisfy the demand. Then $d_i | k_2 - k_1$ for all $1 \leq i \leq n$. Since the d_i's are pairwise relatively prime, we obtain that $d_1 \cdot \ldots \cdot d_n | k_2 - k_1$, as desired.

Now let us show existence. Analogously to the previous reasoning, it is enough to show that there exists $r \in \mathbb{Z}$ such that $r \equiv_{d_1} 1$ and $r \equiv_{d_i} 0$ for all $2 \leq i \leq n$. Again since $r_2, \ldots, r_n$ are pairwise relatively prime, the condition $r \equiv_{d_i} 0$ for all $2 \leq i \leq n$ is equivalent to the condition $r \equiv_{d_2 \cdot \ldots \cdot d_n} 0$. Since d_1 and $d_2 \cdot \ldots \cdot d_n$ are relatively prime, we can use the previous result, deducing the existence of r. □

[1] For example, the numbers $2, 2, 1$ are relatively prime but not pairwise relatively prime.

Exercise 3.2.4. *Which integers leave a remainder* 1 *when divided by* 2*, a reminder* 2 *when devided by* 3*, and remainder* 3 *when divided by* 11*?*

Solution. We find a solution to

$$2x + 3y = 1,$$

say $(-1, 1)$. Then

$$3 \equiv_2 1, 3 \equiv_3 0$$

and

$$-2 \equiv_2 0, -2 \equiv_3 1.$$

Therefore

$$1 \cdot 3 + 2 \cdot (-2) = -1$$

is an integer which is 1 modulo 2 and 2 modulo 3. We now find a solution to

$$6x + 11y = 1,$$

say $(2, -1)$. Then

$$-11 \equiv_6 1, -11 \equiv_{11} 0$$

and

$$12 \equiv_6 0, 12 \equiv_{11} 1.$$

Therefore

$$-1 \cdot (-11) + 3 \cdot 12 = 47$$

is a number as desired. Then the general solution is

$$47 + k \cdot (2 \cdot 3 \cdot 11),\ k \in \mathbb{Z}.$$

□

3.3 Invertibility, Wilson's theorem

Definition 3.3.1. We say that a residue class $\alpha \in \mathbb{Z}_d$ is *invertible*, if there exists a residue class $\beta \in \mathbb{Z}_d$ such that $\alpha\beta = [1]_d$. The residue class β is then called an *inverse* to α. We denote by

$$\mathbb{Z}_d^\times \subset \mathbb{Z}_d$$

the subset of invertible elements. We say that a number $n \in \mathbb{Z}$ is *invertible modulo d*, if $[n]_d$ is an invertible residue class. We say that $m \in \mathbb{Z}$ is *inverse to n modulo d* if $[m]_d$ is inverse to $[n]_d$ (i.e. if $mn \equiv_d 1$).

Example 3.3.2. *Set* $d = 10$*. Consider* $n = 3$*. Then one finds that* $3 \cdot 3 \equiv_{10} -1$ *and so* $3 \cdot (-3) \equiv_{10} 1$*, so* -3 *is inverse to* 3 *modulo* 10 *(if you wish,* 7 *is inverse to* 3 *modulo* 10*). However,* 2 *does not have an inverse modulo* 10*:* 2 *times anything is even, so can't be of the form* $10k + 1$ *(i.e.* 1 *modulo* 10*). So* $[3]_{10} \in \mathbb{Z}_{10}^\times$ *and* $[2]_{10} \notin \mathbb{Z}_{10}^\times$.

Lemma 3.3.3. *The inverse of a residue class, if exists, is unique (concretely, if $m_1 n \equiv_d 1$ and $m_2 n \equiv_d 1$ then $m_1 \equiv_d m_2$).*

Proof. Let $\alpha \in \mathbb{Z}_d$ and let $\beta_1, \beta_2 \in \mathbb{Z}_d$ be two inverses of α. Then

$$\beta_1 = \beta_1 \cdot [1]_d = \beta_1 \cdot (\alpha\beta_2) = (\beta_1\alpha) \cdot \beta_2 = [1]_d \cdot \beta_2 = \beta_2.$$

□

Definition 3.3.4. If $\alpha \in \mathbb{Z}_d$ is invertible, we will denote by $\alpha^{-1} \in \mathbb{Z}_d$ its inverse (we saw that it is unique, if it exists).

Example 3.3.5. *Thus,* $[3]_{10}^{-1} = [-3]_{10}$.

Remark 3.3.6. Notice that $[1]_d \in \mathbb{Z}_d^\times$, if $\alpha, \beta \in \mathbb{Z}_d^\times$ then $\alpha\beta \in \mathbb{Z}_d^\times$, and if $\alpha \in \mathbb{Z}_d^\times$ then $\alpha^{-1} \in \mathbb{Z}_d^\times$.

Claim 3.3.7. *n is invertible modulo d if and only if n is relatively prime to d.*

Proof. n admits an inverse modulo d i.f.f. there exists m s.t. $d|(mn-1)$. This happens i.f.f. there exist m, k s.t. $mn - 1 = kd$, i.e. $mn + (-k)d = 1$. As we saw earlier, the possibility of writing 1 as an integral linear combination of n and d is equivalent to n and d being relatively prime. □

Corollary 3.3.8. *Let p be prime.*

1. *Every $[0]_p \neq \alpha \in \mathbb{Z}_p$ is invertible. In other words, n is invertible modulo p if and only if $n \not\equiv_p 0$.*

2. *Let $\alpha, \beta \in \mathbb{Z}_p$. If $\alpha\beta = [0]_p$ then $\alpha = [0]_p$ or $\beta = [0]_p$. Equivalently, if $\alpha \neq [0]_p$ and $\beta \neq [0]_p$ then $\alpha\beta \neq [0]_p$.*

3. *Let $[0]_p \neq \alpha \in \mathbb{Z}_p$ and $\beta, \gamma \in \mathbb{Z}_p$. If $\alpha\beta = \alpha\gamma$ then $\beta = \gamma$.*

Proof.

1. This is because n is relatively prime to p if and only if p does not divide n.

2. This is simply a restatement of the property: $p|nm$ implies $p|n$ or $p|m$. But in terms of the previous item, this can be proven as follows: $\alpha\beta = [0]_p$ and $\alpha \neq [0]_p$, then $\beta = [1]_p\beta = \alpha^{-1}\alpha\beta = \alpha^{-1}[0]_p = [0]_p$.

3. If $\alpha\beta = \alpha\gamma$ then $\alpha(\beta - \gamma) = [0]_p$ and thus, by the previous item, as $\alpha \neq [0]_p$, we have $\beta - \gamma = [0]_p$, i.e. $\beta = \gamma$.

□

Remark 3.3.9. This corollary says that $\mathbb{Z}_p$ is a field. It is a finite field, sometimes called a Galois field.

Let us now prove Wilson's theorem, after a lemma.

Lemma 3.3.10. *Let p be a prime and let $n \not\equiv_p 0$. Then n is its own inverse modulo p if and only if $n \equiv_p 1$ or $n \equiv_p -1$.*

Proof. In other words, we need to show that $\alpha \in \mathbb{Z}_p$ satisfies $\alpha^2 = [1]_p$ if and only if $\alpha \in \{[1]_p, [-1]_p\}$. We have $\alpha^2 = [1]_p$ i.f.f. $\alpha^2 - [1]_p = [0]_p$, i.f.f. $(\alpha - [1]_p)(\alpha + [1]_p) = [0]_p$, and by the last lemma this implies that either $\alpha - [1]_p = [0]_p$ (in which case $\alpha = [1]_p$) or $\alpha + [1]_p = [0]_p$ (in which case $\alpha = -[1]_p$). □

Theorem 3.3.11 (Wilson's theorem)**.** *Let p be a prime. Then*

$$(p-1)! \equiv_p -1.$$

Equivalently, p divides $(p-1)! + 1$. Conversely, if $n \in \mathbb{Z}_{\geq 1} \setminus \{1\}$ satisfies $(n-1)! \equiv_n -1$ then n is prime.

Proof. For $p = 2$ we verify directly, so assume that $p > 2$. One would like to say that each term in the product

$$(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1)$$

gets canceled with its inverse modulo p, but one should be careful with elements which are their own inverses modulo p. By the previous lemma, those are 1 and $p-1$. Therefore, all terms in the product get canceled, except 1 and $p-1$, and we get:

$$(p-1)! \equiv_p 1 \cdot (p-1) \equiv_p -1.$$

Now, if n is as in the statement then, since -1 is relatively prime to n, also $(n-1)!$, which is congruent to it modulo n, is relatively prime to n. Therefore, each $1 \leq k \leq n-1$ is relatively prime to n, clearly implying that n is prime. □

Let us also discuss integer powers of an invertible element. Let $\alpha \in \mathbb{Z}_d^\times$. For $n \in \mathbb{Z}$ we define $\alpha^n \in \mathbb{Z}_d^\times$ as follows. If $n = 0$, we define $\alpha^n = [1]_d$. If $n > 0$, we define $\alpha^n = \alpha \cdot \ldots \cdot \alpha$ where we multiply n terms. When $n < 0$, we define $\alpha^n = (\alpha^{-1})^{-n}$. Note that there is no conflict of the two meanings of α^{-1} we have now.

Lemma 3.3.12. *For $n, m \in \mathbb{Z}$ one has $\alpha^{n+m} = \alpha^n \cdot \alpha^m$ and $\alpha^{nm} = (\alpha^n)^m$.*

3.4 Fermat's little theorem

Let $d \in \mathbb{Z}_{\geq 1}$. Notice that given $\alpha \in \mathbb{Z}_d^\times$, it is easy to see that there exists $k \in \mathbb{Z}_{\geq 1}$ such that $\alpha^k = [1]_d$. Indeed, we consider the elements $[1]_d, \alpha, \alpha^2, \ldots \in \mathbb{Z}_d^\times$. Those are infinitely many elements in a finite set, and therefore two of them must be equal - there exist $i < j$ such that $\alpha^i = \alpha^j$. Then $\alpha^{j-i} = [1]^\times$, and $j - i \in \mathbb{Z}_{\geq 1}$. We want now to obtain more specific information about possible k's.

Theorem 3.4.1 (Fermat's little theorem)**.** *Let $p \in \mathbb{Z}_{\geq 1}$ be a prime. Let $\alpha \in \mathbb{Z}_p^\times$ (i.e. $[0]_p \neq \alpha \in \mathbb{Z}_p$). Then $\alpha^{p-1} = [1]_p$. In other words, given $n \not\equiv_p 0$ one has*

$$n^{p-1} \equiv_p 1.$$

Proof. Let us denote $\alpha = [n]_p$. We want to see that $\alpha^{p-1} = [1]_p$.

Let us consider all the non-zero residue classes

$$\alpha_1, \dots, \alpha_{p-1}.$$

Now consider also the residue classes

$$\alpha\alpha_1, \dots, \alpha\alpha_{p-1}.$$

All of those are non-zero, and pairwise different (if $\alpha\alpha_i = \alpha\alpha_j$ then $\alpha(\alpha_i - \alpha_j) = [0]_p$ and therefore $\alpha_i - \alpha_j = [0]_p$ i.e. $\alpha_i = \alpha_j$). Hence, our second list also contains all non-zero residue classes, each appearing exactly once. Therefore we have

$$\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_{p-1} = (\alpha\alpha_1) \cdot (\alpha\alpha_2) \cdot \ldots \cdot (\alpha\alpha_{p-1}) = \alpha^{p-1} \cdot \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_{p-1}.$$

Since $\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_{p-1}$ is non-zero, we obtain $[1]_p = \alpha^{p-1}$. □

Example 3.4.2. *Let us find the last digit of 7^{2017}. This means, since we use the decimal system, to find the remainder upon division by 10. Applying Fermat's theorem for $p = 5$, we get*

$$7^{2017} = 7^{4 \cdot ? + 1} = (7^4)^? \cdot 7 \equiv_5 1^? \cdot 7 \equiv_5 2.$$

Also, clearly $7^{2017} \equiv_2 1$. We check that the only residue modulo 10 which is 2 modulo 5 and 1 modulo 2 is 7. Hence 7 is the last digit of 7^{2017}.

3.5 Euler's theorem

Definition 3.5.1. We define

$$\phi(d) := |\mathbb{Z}_d^\times|.$$

In words, $\phi(d)$ is the number of residue classes modulo d which are invertible. In other words, $\phi(d)$ is the number of numbers in the list $0, 1, \dots, d-1$ which are relatively prime to d.

Claim 3.5.2. *Let $d, e \in \mathbb{Z}_{\geq 1}$ be relatively prime. Then*

$$\phi(de) = \phi(d)\phi(e).$$

Proof. Let us recall the bijection

$$frgt^{de}_d \times frgt^{de}_e : \mathbb{Z}_{de} \to \mathbb{Z}_d \times \mathbb{Z}_e.$$

We claim that an element $\alpha \in \mathbb{Z}_{de}$ is invertible i.f.f. the elements $frgt^{de}_d(\alpha)$ and $frgt^{de}_e(\alpha)$ are invertible. Indeed, write $\alpha = [n]_{de}$. Then $frgt^{de}_d(\alpha) = [n]_d$ and $frgt^{de}_e(\alpha) = [n]_e$. Thus what we want to show is that n is relatively prime to de i.f.f. it is relatively prime to both d and e. This we saw. □

Example 3.5.3. *We have $\phi(1) = 1$. For a prime p, we have $\phi(p) = p - 1$. We also have $\phi(p^k) = p^k - p^{k-1}$. Indeed, a number is relatively prime to p^k i.f.f. it is relatively prime to p, i.f.f. it is not a multiple of p. There are p^{k-1} multiples of p in the interval $[0, p^k]$. Then, for example,*

$$\phi(45) = \phi(3^2 \cdot 5) = \phi(3^2)\phi(5) = (3^2 - 3) \cdot (5 - 1) = 24.$$

Theorem 3.5.4 (Euler)**.** *Let $d \in \mathbb{Z}_{\geq 1}$. Let $\alpha \in \mathbb{Z}^{\times}_d$. Then $\alpha^{\phi(d)} = [1]_d$. In other words, given $n \in \mathbb{Z}$ which is relatively prime to d one has*

$$n^{\phi(d)} \equiv_d 1.$$

Proof. The proof is practically identical to that of Fermat's little theorem. Namely, consider all the different residue classes

$$\alpha_1, \ldots, \alpha_{\phi(d)}$$

constituting $\mathbb{Z}^{\times}_d$. Then

$$\alpha\alpha_1, \ldots, \alpha\alpha_{\phi(d)}$$

is again a list of residue classes in $\mathbb{Z}^{\times}_d$, and they are all different: If $\alpha\alpha_i = \alpha\alpha_j$ then we get $\alpha(\alpha_j - \alpha_i) = [0]_d$ and multiplying by α^{-1} we get $\alpha_j - \alpha_i = [0]_d$, i.e. $\alpha_i = \alpha_j$. Therefore, since these are $\phi(d)$ different residue classes in $\mathbb{Z}^{\times}_d$, which has $\phi(d)$ members, we deduce that these are again exactly all the different residues classes in $\mathbb{Z}^{\times}_d$. Then

$$(\alpha\alpha_1) \cdot (\alpha\alpha_2) \cdot \ldots \cdot (\alpha\alpha_{\phi(d)}) = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_{\phi(d)}$$

and so, dividing by $\alpha_1^{-1} \cdot \alpha_2^{-1} \cdot \ldots \cdot \alpha^{-1}_{\phi(d)}$, we obtain

$$\alpha^{\phi(d)} = [1]_d.$$

□

Example 3.5.5. *Let us compute the remainder of 3^{54} after division by 35.*

We compute

$$\phi(35) = \phi(5)\phi(7) = 4 \cdot 6 = 24.$$

We thus have

$$3^{540} = 3^{2 \cdot 24 + 6} = (3^{24})^2 \cdot 3^6 \equiv_{35} 1^2 \cdot 3^6.$$

We compute then

$$3^6 = (3^3)^2 \equiv_{35} (-8)^2 \equiv_{35} 64 \equiv_{35} -6 \equiv_{35} 29.$$

Alternatively, we have

$$3^6 \equiv_5 3^4 \cdot 3^2 \equiv_5 3^2 \equiv_5 4$$

and

$$3^6 \equiv_7 1;$$

The second congruence says that 3^6 *is in the list* $1, 8, 15, 22, 29$ *modulo* 35*, while the first congruence then pins it to* 29*.*

Example 3.5.6. *there are some calculating mistakes in this example....*

Let us denote $p_0 = 3$ *and* $p_{n+1} = 3^{p_n}$ *recursively. Let us calculate* $p_{2012} \bmod 100$.

We have $\phi(100) = \phi(2^2 5^2) = 40$*. So we would like to calculate* $[p_{2011}]_{40}$*. Iterating, we have* $\phi(40) = \phi(2^3 5) = 16$*,* $\phi(16) = 8$ *,* $\phi(8) = 4$ *,* $\phi(4) = 2$*. So:*

$[p_{2007}]_2 = 1$ *and thus* $p_{2008} = 3^{p_{2007}} \equiv_4 3$*. Then* $p_{2009} = 3^{p_{2008}} \equiv_8 3^3 \equiv_8 1$*. Then* $p_{2010} = 3^{p_{2009}} \equiv_{16} 3$*. Then* $p_{2011} = 3^{p_{2012}} \equiv_{40} 3^3 = 27$*. Then* $p_{2012} = 3^{p_{2011}} \equiv_{100} 3^{27}$*. So we are left with computing* $3^{27} \bmod 100$*. We have:*

$$3^{27} \equiv_{100} 3 \cdot (3^{13})^2 \equiv_{100} 3 \cdot (3 \cdot (3^6)^2)^2 \equiv_{100} 3 \cdot (3 \cdot ((3^3)^2)^2)^2.$$

We have

$$(3^3)^2 = (20+7)^2 \equiv_{100} 49 + 80 \equiv_{100} 29.$$

Then

$$((3^3)^2)^2 \equiv_{100} 29^2 = (30-1)^2 \equiv_{100} 1 - 60 \equiv_{100} 41.$$

Then

$$3 \cdot ((3^3)^2)^2 \equiv_{100} 3 \cdot 41 \equiv_{100} 23.$$

Then

$$(3 \cdot ((3^3)^2)^2)^2 \equiv_{100} 23^2 \equiv_{100} (20+3)^2 \equiv_{100} 29.$$

Then finally

$$3 \cdot (3 \cdot ((3^3)^2)^2)^2 \equiv_{100} 3 \cdot 29 = 87.$$

Thus, $p_{2012} \equiv_{100} 87$.

Chapter 4

Polynomials etc.

4.1 Polynomials

Let $P \in \mathbb{Z}[X]$ be a polynomial. If $n \equiv_d m$, then $P(n) \equiv_d P(m)$. Therefore, for every $\alpha \in \mathbb{Z}_d$ we can define the value $P(\alpha) \in \mathbb{Z}_d$ unambiguously as $[P(n)]_d$ for any $n \in \mathbb{Z}$ for which $[n]_d = \alpha$. Thus, our polynomial defines a function

$$\mathbb{Z}_d \to \mathbb{Z}_d : \alpha \mapsto P(\alpha).$$

For polynomials $P, Q \in \mathbb{Z}[X]$, we write $P \equiv_d Q$ if for all $i \in \mathbb{Z}_{\geq 0}$ the coefficient of X^i in P is congruent modulo d to the coefficient of X^i in Q. Notice that if $P \equiv_d Q$, then these define the same function $\mathbb{Z}_d \to \mathbb{Z}_d$, i.e. $P(\alpha) = Q(\alpha)$ for all $\alpha \in \mathbb{Z}_d$, or in other words $P(n) \equiv_d Q(n)$ for all $n \in \mathbb{Z}$.

Remark 4.1.1. One should be careful - one can have two polynomials $P, Q \in \mathbb{Z}[X]$ for which $P \not\equiv_d Q$ but nevertheless $P(\alpha) = Q(\alpha)$ for all $\alpha \in \mathbb{Z}_d$. For example, take $d = p$ to be a prime, $P = X$ and $Q = X^p$ (and recall Fermat's little theorem).

4.2 Roots modulo relatively prime numbers

Let $d, e \in \mathbb{Z}_{\geq 1}$ be relatively prime, and let $P \in \mathbb{Z}[X]$. Then we see that there is a bijection

$$\{\gamma \in \mathbb{Z}_{de} \mid P(\gamma) = [0]_{de}\} \xrightarrow{\sim} \{\alpha \in \mathbb{Z}_d \mid P(\alpha) = [0]_d\} \times \{\beta \in \mathbb{Z}_e \mid P(\beta) = [0]_e\}$$

given by

$$\gamma \mapsto \left(frgt_d^{de}(\gamma), frgt_e^{de}(\gamma) \right).$$

Therefore, in order to study modular roots it is enough to do so modulo prime powers.

4.3 Roots modulo p

Throughout this section, we fix a prime $p \in \mathbb{Z}_{\geq 1}$.

Lemma 4.3.1. *Let $P \in \mathbb{Z}[X]$ be a polynomial of degree $d > 0$ and let $n \in \mathbb{Z}$ be such that $P([n]_p) = [0]_p$ (i.e. $P(n) \equiv_p 0$). Then there exists a polynomial $Q \in \mathbb{Z}[X]$ of degree $d-1$ such that $P \equiv_p Q \cdot (X-n)$.*

Proof. One can perform division with remainder, writing

$$P = Q(X-n) + P(n)$$

for some (uniquely defined) $Q \in \mathbb{Z}[X]$. Since $P(n) \equiv_p 0$, we have $P \equiv_p Q(X-n)$. □

Lemma 4.3.2. *Let $P \in \mathbb{Z}[X]$ be a polynomial of degree $d > 0$ and let $n_1, \dots, n_k \in \mathbb{Z}$ be pairwise distinct modulo p, where $k \leq d$. Assume that $P([n_i]_p) = [0]_p$ (i.e. $P(n_i) \equiv_p 0$) for all $1 \leq i \leq k$. Then there exists a polynomial $Q \in \mathbb{Z}[X]$ of degree $d-k$ such that $P \equiv_p Q \cdot (X-n_1) \cdot \ldots \cdot (X-n_k)$.*

Proof. We prove this by induction on k, where the case $k=1$ is the previous lemma. To perform the induction step, we write $P \equiv_p Q \cdot (X-n_k)$. For every $1 \leq i \leq k-1$, we have

$$0 \equiv_p P(n_i) = Q(n_i)(n_i - n_k).$$

Since $n_i - n_k \not\equiv_p 0$, we have $Q(n_i) \equiv_p 0$. Therefore, we can utilize the induction hypothesis to find Q' such that

$$Q \equiv_p Q' \cdot (X-n_1) \cdot \ldots \cdot (X-n_{k-1}).$$

Then

$$P \equiv_p Q' \cdot (X-n_1) \cdot \ldots \cdot (X-n_{k-1}) \cdot (X-n_k).$$

□

Corollary 4.3.3. *Let $P \in \mathbb{Z}[X]$ be a polynomial of degree $d > 0$ for which the coefficient of X^d is not zero modulo p. Then*

$$|\{\alpha \in \mathbb{Z}_p \mid P(\alpha) = [0]_p\}| \leq d.$$

Proof. Suppose that $\alpha_1, \dots, \alpha_d \in \mathbb{Z}_p$ are pairwise distinct, and all are roots of P. We will show then that there are no additional roots of P. Choose $n_1, \dots, n_d \in \mathbb{Z}$ such that $[n_i]_p = \alpha_i$. Then by the previous lemma we have

$$P \equiv_p Q \cdot (X-n_1) \cdot \ldots \cdot (X-n_d)$$

for some Q of degree 0, i.e. $Q = m$ for some $m \in \mathbb{Z}$. Notice that m is congruent modulo p to the coefficient of X^d in P, hence by our assumption $m \not\equiv_p 0$. Therefore if $n \in \mathbb{Z}$ satisfies $P(n) \equiv_p 0$ we get $n - n_i \equiv_p 0$ for some $1 \leq i \leq d$. This means that if $\alpha \in \mathbb{Z}_p$ satisfies $P(\alpha) = [0]_p$ then $\alpha = \alpha_i$ for some $1 \leq i \leq d$. □

Example 4.3.4. *Let $p = 3$ and consider*

$$P = X^2 + 1 \in \mathbb{Z}[X].$$

Note that P has no root modulo 3. This is similar to how $X^2 + 1$ has no real root. One then synthetically adds an imaginary root i, and gets the complex numbers as the set of formal expressions of the form $a + ib$ for $a, b \in \mathbb{R}$. One can do the same in our case, and create a new set, consisting of expressions of the form $\alpha + i\beta$ for $\alpha, \beta \in \mathbb{Z}_3$. Thus, this set has 3^2 elements. One then can define multiplication and addition on that set:

$$(\alpha + i\beta) + (\gamma + i\delta) = (\alpha + \gamma) + i(\beta + \delta),$$

$$(\alpha + i\beta) \cdot (\gamma + i\delta) = (\alpha\gamma - \beta\delta) + i(\alpha\delta + \beta\gamma).$$

One obtains a finite field with 9 elements. But, contrary to the case with real/complex numbers, where once we add i all polynomials have a root ("fundamental theorem of algebra") here, although the polynomial $X^2 + 1$ will have a root now, other polynomials will still be lacking a root. Then one can construct a field with 3^3 elements having some more roots, etc. One eventually obtains an infinite field, by enlarging in this way. It is called the algebraic closure *of $\mathbb{Z}_3$. It is quite important because it is related to number theory (of somewhat combinatorial flavor, of counting), but philosophically is similar to the field of complex numbers, so in some sense is "continuous". The famous Weil conjectures (already theorems) are one precise manifestation of that.*

4.4 Roots modulo prime powers

Let $p \in \mathbb{Z}_{\geq 1}$ be a prime. Suppose that we have a root $\beta \in \mathbb{Z}_{p^{k+1}}$ of $P \in \mathbb{Z}[X]$. Then clearly $frgt_{p^k}^{p^{k+1}}(\beta) \in \mathbb{Z}_{p^k}$ is also a root of P (i.e. for $n \in \mathbb{Z}$ one has $P(n) \equiv_{p^{k+1}} 0$ then one also has $P(n) \equiv_{p^k} 0$). We want now to ask the converse: If we have a root $\alpha \in \mathbb{Z}_{p^k}$ of P, whether we can find a root $\beta \in \mathbb{Z}_{p^{k+1}}$ of P such that $frgt_{p^k}^{p^{k+1}}(\beta) = \alpha$.

Proposition 4.4.1 (Hensel's lemma)**.** *Let $P \in \mathbb{Z}[X]$ and let $\alpha \in \mathbb{Z}_{p^k}$ be a root of P. Suppose in addition that $P'(\alpha) \in \mathbb{Z}_{p^k}^{\times}$. Then there exists a unique $\beta \in \mathbb{Z}_{p^{k+1}}$ such that $frgt_{p^k}^{p^{k+1}}(\beta) = \alpha$ and β is a root of P.*

In other words, let $P \in \mathbb{Z}[X]$ and let $n \in \mathbb{Z}$ be $P(n) \equiv_{p^k} 0$. Suppose in addition that $P'(n)$ is not divided by p. Then there exists $m \in \mathbb{Z}$ such that $m \equiv_{p^k} n$ and $P(m) \equiv_{p^{k+1}} 0$. Moreover, any two such m's are congruent modulo p^{k+1}.

Proof. In general, the elements in $\mathbb{Z}_{p^{k+1}}$ which are mapped under $frgt_{p^k}^{p^{k+1}}$ to some $[r]_{p^k}$ are exactly the following ones:

$$[r]_{p^{k+1}}, [r + p^k]_{p^{k+1}}, \ldots, [r + (p-1)p^k]_{p^{k+1}}.$$

One can state it a bit better, saying that there is a bijection

$$\mathbb{Z}_p \xrightarrow{\sim} \{\alpha \in \mathbb{Z}_{p^{k+1}} \mid frgt_{p^k}^{p^{k+1}}(\alpha) = [r]_{p^k}\}$$

given by $[m]_p \mapsto [r + m \cdot p^k]_{p^{k+1}}$ (in particular, one checks that this map is well-defined).

Let us take $n \in \mathbb{Z}$ such that $\alpha = [n]_{p^k}$. By the above, since $[P(n)]_{p^k} = [0]_{p^k}$, there exists a unique $0 \le i \le p-1$ such that $[P(n)]_{p^{k+1}} = [i \cdot p^k]_{p^{k+1}}$. Recall that we can write

$$P(n+X) = P(n) + P'(n) \cdot X + Q \cdot X^2$$

for some $Q \in \mathbb{Z}[X]$. We have therefore:

$$P(n+jp^k) = P(n) + P'(n) \cdot jp^k + (jp^k)^2 \cdot ?$$

where ? is some integer. Therefore

$$P([n+jp^k]_{p^{k+1}}) = [P(n+jp^k)]_{p^{k+1}} = [P(n)]_{p^{k+1}} + [P'(n) \cdot jp^k]_{p^{k+1}} = [(i+P'(n) \cdot j) \cdot p^k]_{p^{k+1}}.$$

Since $P'(n) \not\equiv_p 0$, there will be exactly one $0 \le j \le p-1$ such that

$$i + P'(n)j \equiv_p 0,$$

which is equivalent to

$$(i + P'(n)j) \cdot p^k \equiv_{p^{k+1}} 0.$$

(need to polish a bit the presentation) □

Example 4.4.2. *Let us consider the polynomial $P(X) = X^2 - 7$ and $p = 3$. We have a root $[1]_3$ of P. Notice that $P'(X) = 2X$ and $P'([1]_3) = [2]_3 \neq [0]_3$. Hence there exists a unique element $\alpha_2 \in \mathbb{Z}_9$ such that $\alpha_2^2 = [7]_9$ and $frgt_3^9(\alpha_2) = 1$. So the options for α_2 are $[1]_9, [4]_9, [7]_9$ and one finds that $\alpha_2 = [4]_9$. We can continue, finding the unique $\alpha_3 \in \mathbb{Z}_{27}$ such that $frgt_9^{27}(\alpha_3) = [4]_9$ and $\alpha_3^2 = [7]_{27}$. One finds $\alpha_3 = [13]_{27}$. One can continue, obtaining an infinite sequence*

$$([1]_3, [4]_9, [13]_{27}, \dots,)$$

of "better and better" solutions to $X^2 - 7 = 0$, in the sense that as we progress we find varios $n \in \mathbb{Z}$ such that $n^2 - 7$ is divided by bigger and bigger powers of 3.

4.5 p-adic integers

Let $p \in \mathbb{Z}_{\ge 1}$ be a prime. Let $P \in \mathbb{Z}[X]$ and let $\alpha_1 \in \mathbb{Z}_p$ be such that $P(\alpha_1) = [0]_p$ and $P'(\alpha_1) \neq [0]_p$. Then by Hensel's lemma, there exists a unique $\alpha_2 \in \mathbb{Z}_{p^2}$ such that $P(\alpha_2) = [0]_{p^2}$ and $frgt_p^{p^2}(\alpha_2) = \alpha_1$. Continuing in this fashion, we find recursively $\alpha_k \in \mathbb{Z}_{p^k}$ such that $P(\alpha_k) = [0]_{p^k}$ and $frgt_{p^{k-1}}^{p^k}(\alpha_k) = \alpha_{k-1}$.

Definition 4.5.1. A *p-adic integer* is a sequence

$$(\alpha_1, \alpha_2, \ldots)$$

where $\alpha_k \in \mathbb{Z}_{p^k}$ for $k \in \mathbb{Z}_{\geq 1}$, and for each $k \in \mathbb{Z}_{\geq 1}$ one has

$$frgt_{p^k}^{p^{k+1}}(\alpha^{k+1}) = \alpha^k.$$

Therefore, one can think of a p-adic integer as the information of an imaginary integer's residues modulo powers of p. In particular, an actual integer $n \in \mathbb{Z}$ determines a p-adic integer by taking $\alpha_k := [n]_{p^k}$.

Example 4.5.2. *Here is a concrete example of a* 3*-adic integer, which is not determined by an actual integer:*

$$\alpha_k = [1 + 3 + \ldots + 3^{k-1}]_{3^k}.$$

One can think that this 3*-adic integer is the sum of the series*

$$1 + 3 + 3^2 + \ldots.$$

Since

$$1 + 3 + \ldots + 3^{k-1} = \frac{3^k - 1}{2}$$

we see that our p-adic integer is in fact $-1/2$ *(in other words, if we multiply it by* 2*, we get* -1*).*

A more interesting example would be to consider the unique p-adic integer (α_k) *for which* $\alpha_1 = [1]_3$ *and* $\alpha_k^2 = [7]_{3^k}$ *for all k. This will be an element whose square is* 7*.*

The field of p-adic numbers $\mathbb{Q}_p$ is obtained by formally considering quotients of p-adic integers.

Chapter 5

Orders, primitive roots

5.1 Orders

Let us fix $d \in \mathbb{Z}_{\geq 1}$. Let $\alpha \in \mathbb{Z}_d^\times$. Let us consider the subset of the integers

$$I_\alpha = \{n \in \mathbb{Z} \mid \alpha^n = [1]_d\} \subset \mathbb{Z}.$$

Then one checks that this is an ideal. Moreover, this ideal is not $\{0\}$, since $\phi(d) \in I_\alpha$ by Euler's theorem. Therefore, by the principal ideal theorem, there exists a unique $k \in \mathbb{Z}_{\geq 1}$ such that $I_\alpha = (k)$. We call this k the *order* of α and denote it by $ord(\alpha)$. Therefore:

$$\alpha^m = [1]_p \text{ if and only if } ord(\alpha)|m.$$

Also, one can characterize the order as the smallest non-negative integer k for which $\alpha^k = [1]_p$. We have

$$ord(\alpha)|\phi(d).$$

For $n \in \mathbb{Z}$ which is relatively prime to d (and so $[n]_d \in \mathbb{Z}_d^\times$), we denote

$$ord_d(n) := ord([n]_d).$$

Lemma 5.1.1. *Let $\alpha \in \mathbb{Z}_d^\times$. Then the elements of the list*

$$[1]_p, \alpha, \ldots, \alpha^{ord(\alpha)-1}$$

are pairwise distinct, and for every $k \in \mathbb{Z}$ the element α^k is equal to one of the elements in that list. In particular, the set $\{\alpha^k \ : \ k \in \mathbb{Z}\}$ has $ord(\alpha)$ elements.

Proof. If $\alpha^i = \alpha^j$ for some $0 \leq i < j \leq ord(\alpha) - 1$, we get $\alpha^{j-i} = [1]_p$ and thus $j - i \in I_\alpha$ and $1 \leq j - i < ord(\alpha)$, contradicting $ord(\alpha)$ being the smallest.

Given $k \in \mathbb{Z}$, we perform division with remainder $k = q \cdot ord(\alpha) + r$ where $0 \leq r < ord(\alpha)$. Then $\alpha^k = (\alpha^{ord(\alpha)})^q \cdot \alpha^r = [1]_d^q \cdot \alpha^r = \alpha^r$. □

Claim 5.1.2. *Let $\alpha \in \mathbb{Z}_d^\times$ and let $k \in \mathbb{Z}$. Then*

$$ord(\alpha^k) = \frac{ord(\alpha)}{gcd(ord(\alpha), k)}.$$

In particular, if $k|ord(\alpha)$, we have

$$ord(\alpha^k) = \frac{ord(\alpha)}{k}.$$

Proof. We have $m \in I_{\alpha^k}$ i.f.f. $(\alpha^k)^m = [1]_p$ i.f.f. $\alpha^{km} = [1]_p$ i.f.f. $km \in I_\alpha$ i.f.f. $ord(\alpha)|km$ i.f.f. $\frac{ord(\alpha)}{gcd(ord(\alpha),k)}|m$. Thus:

$$I_{\alpha^k} = \left(\frac{ord(\alpha)}{gcd(ord(\alpha), k)}\right).$$

□

5.2 Primitive roots

Definition 5.2.1. We say that $\alpha \in \mathbb{Z}_d^\times$ is a *primitive root* if

$$ord(\alpha) = \phi(d).$$

We say that $n \in \mathbb{Z}$ is a *primitive root modulo d* if $[n]_d$ is a primitive root (in particular, $[n]_d \in \mathbb{Z}_d^\times$, i.e. n and d are relatively prime).

Lemma 5.2.2. *Let $\alpha \in \mathbb{Z}_d^\times$. The following are equivalent:*

1. *α is a primitive root.*
2. *$\mathbb{Z}_d^\times = \{[1]_p, \alpha, \alpha^2, \ldots, \alpha^{\phi(d)-1}\}$.*
3. *For every $\beta \in \mathbb{Z}_d^\times$ there exists $k \in \mathbb{Z}_{\geq 0}$ such that $\beta = \alpha^k$.*

Proof. (1) $\implies$ (2) follows from lemma 5.1.1. (2) $\implies$ (3) is trivial. (3) $\implies$ (1): By lemma 5.1.1 the set $\{\alpha^k \mid k \in \mathbb{Z}\}$ has $ord(\alpha)$ elements. By the current assumption, this set is equal to $\mathbb{Z}_d^\times$. Therefore we get that $ord(\alpha) = \phi(d)$. □

Example 5.2.3. 2 *is a primitive root modulo* 5*, since*

$$2^0 \equiv_5 1, 2^1 \equiv_5 2, 2^2 \equiv_5 4, 2^3 \equiv_5 3$$

are all distinct modulo 5*.*

Example 5.2.4. *There is no primitive root modulo* 8*. Indeed, we have*

$$\mathbb{Z}_8^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\}$$

so $\phi(8) = 4$, but every $\alpha \in \mathbb{Z}_8^\times$ satisfies $\alpha^2 = [1]_8$.

Claim 5.2.5.

1. *If $\alpha \in \mathbb{Z}_d^\times$ is a primitive root, then $\alpha^k \in \mathbb{Z}_d^\times$ is a primitive root if and only if $gcd(k, \phi(d)) = 1$.*

2. *If $\mathbb{Z}_d^\times$ admits a primitive root, then it admits exactly $\phi(\phi(d))$ primitive roots.*

Proof. We have that α^k is a primitive root if and only if $ord(\alpha^k) = ord(\alpha)$ (since $ord(\alpha) = \phi(d)$, and we have $ord(\alpha^k) = \frac{ord(\alpha)}{gcd(ord(\alpha),k)}$, so α^k is a primitive root if and only if $gcd(ord(\alpha), k) = 1$, i.e. $gcd(\phi(d), k) = 1$.

As for the second claim, using the first claim we see that from the elements $[1]_d, \alpha, \dots, \alpha^{\phi(d)-1}$ of $\mathbb{Z}_d^\times$, the ones which are primitive roots are α^i where $gcd(i, \phi(d)) = 1$. As i runs from 0 to $\phi(d)-1$, there are exactly $\phi(\phi(d))$ such. □

Lemma 5.2.6. *Let $e|d$. If $\alpha \in \mathbb{Z}_d^\times$ is a primitive root, then $frgt_e^d(\alpha) \in \mathbb{Z}_e^\times$ is also a primitive root. In terms of integers: If $n \in \mathbb{Z}$ is a primitive root modulo d, then n is also a primitive root modulo e.*

Proof. For every $\beta \in \mathbb{Z}_e^\times$ there exists $\gamma \in \mathbb{Z}_d^\times$ such that $frgt_e^d(\gamma) = \beta$. Next, there exists $k \in \mathbb{Z}_{\geq 0}$ such that $\gamma = \alpha^k$. Hence

$$\beta = frgt_e^d(\gamma) = frgt_e^d(\alpha^k) = frgt_e^d(\alpha)^k.$$

In other words, every element in $\mathbb{Z}_d^\times$ is a power of $frgt_e^d(\alpha)$, and thus by a criterion we saw above, $frgt_e^d(\alpha)$ is a primitive root. □

5.3 The case of a prime

Lemma 5.3.1. *Let $\alpha, \beta \in \mathbb{Z}_d^\times$. Assume that $ord(\alpha)$ and $ord(\beta)$ are relatively prime. Then*

$$ord(\alpha\beta) = ord(\alpha) \cdot ord(\beta).$$

Proof. Abbreviate $a := ord(\alpha)$ and $b := ord(\beta)$. For starters,

$$(\alpha\beta)^{ab} = (\alpha^a)^b \cdot (\beta^b)^a = [1]_d.$$

Now assume $(\alpha\beta)^k = [1]_d$ for some $k \in \mathbb{Z}$. Then $\alpha^k = \beta^{-k}$ and so, calling their common value γ, we have that

$$ord(\gamma) = ord(\alpha^k)|ord(\alpha) = a$$

and similarly $ord(\gamma)|b$ and thus, since a and b are relatively prime, $ord(\gamma) = 1$, i.e. $\gamma = [1]_d$. We obtain thus $\alpha^k = [1]_d$ so $a|k$ and $\beta^k = [1]_d$ so $b|k$. Since a and b are relatively prime, we obtain $ab|k$. This finishes showing that $ord(\alpha\beta) = ab$. □

Lemma 5.3.2. *Let $\alpha, \beta \in \mathbb{Z}_d^\times$. Then there exists an element in $\mathbb{Z}_d^\times$ of order $lcm(ord(\alpha), ord(\beta))$.*

Proof. Let us first note that given $\gamma \in \mathbb{Z}_d^\times$ and $k|ord(\gamma)$, there exists an element in $\mathbb{Z}_d^\times$ of order k. Indeed, take $\gamma^{\frac{ord(\gamma)}{k}}$.

Let us now write decompositions into primes

$$ord(\alpha) = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$$

and

$$ord(\beta) = p_1^{b_1} \cdot \ldots \cdot p_k^{a_k}.$$

Since $p_i^{a_i}|ord(\alpha)$, there exists in $\mathbb{Z}_d^\times$ an element of order $p_i^{a_i}$. Similarly, there exists in $\mathbb{Z}_d^\times$ an element of order $p_i^{b_i}$. Therefore there exists an element γ_i of order $p_i^{max\{a_i,b_i\}}$. Using the previous lemma, we obtain that

$$ord(\gamma_1 \cdot \ldots \cdot \gamma_k) = ord(\gamma_1) \cdot \ldots \cdot ord(\gamma_k) =$$

$$= p_1^{max\{a_1,b_1\}} \cdot \ldots \cdot p_k^{max\{a_k,b_k\}} = lcm(ord(\alpha), ord(\beta)).$$

□

Theorem 5.3.3. *Let p be a prime. Then there exists a primitive root in $\mathbb{Z}_p^\times$.*

Proof. Let $\alpha \in \mathbb{Z}_p^\times$ with maximal possible order w.r.t. multiplication. In other words, we assume that $ord(\alpha)$ does not strictly divide $ord(\beta)$ for all $\beta \in \mathbb{Z}_p^\times$. Because $\mathbb{Z}_p^\times$ is finite, we can find such α. Let now $\beta \in \mathbb{Z}_p^\times$. If $ord(\beta) \not| ord(\alpha)$ then $ord(\alpha)$ strictly divides $lcm(ord(\alpha), ord(\alpha))$; Since by the previous lemma there exists an element of $\mathbb{Z}_p^\times$ of order $lcm(ord(\alpha), ord(\beta))$, we obtain a contradiction to the choice of α. Therefore, we see that for every $\beta \in \mathbb{Z}_p^\times$ we have $ord(\beta)|ord(\alpha)$. Therefore, abbreviating $k := ord(\alpha)$, we see that every $\beta \in \mathbb{Z}_p^\times$ satisfies $\beta^k = [1]_p$. Therefore the polynomial $x^k - 1$ has $p - 1$ different roots modulo p, and thus $k \geq p - 1$. Since $k|p - 1$, we deduce $k = p - 1$ and so α is a primitive root. □

5.4 The case of a prime power

Notice that in $\mathbb{Z}_4^\times$ we have a primitive root by observation. Notice that in $\mathbb{Z}_8^\times$ we don't have a primitive root (since for every $\alpha \in \mathbb{Z}_8^\times$ one has $\alpha^2 = [1]_8$). Therefore, there is also no primitive root in $\mathbb{Z}_{2^k}^\times$ for every $k \geq 3$. Settled this, we will now deal with powers of an odd prime.

Claim 5.4.1. *Let p be an odd prime. If n is a primitive root modulo p, then either n or $n + p$ is a primitive root modulo p^2.*

Proof. Consider $k := ord_{p^2}(n)$. We know that $k|\phi(p^2) = p^2 - p = p(p - 1)$. On the other hand, clearly $p-1 = ord_p(n)|ord_{p^2}(n) = k$. Therefore either $k = p-1$ or $k = p(p - 1)$. In the latter case, n is a primitive root modulo p^2, so suppose the former. Then $n^p \equiv_{p^2} n \cdot n^{p-1} \equiv_{p^2} n$. Notice that since $n + p \equiv_p n$, we argue as above replacing n by $n + p$ and also see that $ord_{p^2}(n + p)$ is either $p - 1$ or

$p(p-1)$. We want to rule out the former possibility, i.e. we want to show that $(n+p)^{p-1} \not\equiv_{p^2} 1$ or, equivalently, that $(n+p)^p \not\equiv_{p^2} n+p$. And indeed, we have:

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

□

Claim 5.4.2. *Let p be an odd prime, and let $k \geq 2$. If n is a primitive root modulo p^k then n is also a primitive root modulo p^{k+1}.*

Proof. Let us consider $r := ord_{p^{k+1}}(n)$. We have $r|\phi(p^{k+1}) = p^k(p-1)$. On the other hand, $ord_{p^k}(n)|r$, so since n is a primitive root modulo p^k we have $p^{k-1}(p-1)|n$. Therefore either $r = p^{k-1}(p-1)$ or $r = p^k(p-1)$. We want to rule out the former, i.e. we want to show that $n^{p^{k-1}(p-1)} \not\equiv_{p^{k+1}} 1$.

Since n is a primitive root modulo p^{k-1}, we have $n^{p^{k-2}(p-1)} \equiv_{p^{k-1}} 1$ and so we can write $n = 1 + p^{k-1}a$ for some $a \in \mathbb{Z}$. Notice that $a \not\equiv_p 0$, because otherwise we would have $n^{p^{k-2}(p-1)} \equiv_{p^k} 1$, but n is a primitive root modulo p^k, so its order is $p^{k-1}(p-1)$. Now, we have:

$$n^{p^{k-1}(p-1)} = (1 + p^{k-1}a)^p \equiv_{p^{k+1}} 1 + p^k a.$$

Since, as we said, $a \not\equiv_p 0$, we obtain that $n^{p^{k-1}(p-1)} \not\equiv_{p^{k+1}} 1$, as desired. □

Corollary 5.4.3 (of the last two claims)**.** *Let p be an odd prime. Then for every $k \in \mathbb{Z}_{\geq 1}$, there exist in $\mathbb{Z}_{p^k}^\times$ primitive roots.*

5.5 The rest of cases

Claim 5.5.1. *Let p be an odd prime, let $k \in \mathbb{Z}_{\geq 1}$ and let n be a primitive root modulo p^k. Then either n or $n + p^k$ is a primitive root modulo $2p^k$.*

Proof. Exactly one of n and $n + p^k$ is odd - let us by abuse of notation and without loss of generality assume therefore that n is odd. Thus, n is a primitive root modulo p^k and is odd, and we want to show that n is a primitive root modulo $2p^k$. For starters, notice that n is indeed relatively prime to $2p^k$.

Notice that $\phi(2p^k) = \phi(p^k)$. Now, $n^{\phi(2p^k)} = n^{\phi(p^k)}$ is congruent to 1 modulo p^k and also modulo 2, therefore by the Chinese remainder theorem it is congruent to 1 modulo $2p^k$. Conversely, if $n^r \equiv_{2p^k} 1$, then also $n^r \equiv_{p^k} 1$ and therefore $\phi(2p^k) = \phi(p^k)|r$. These two observations shows that n is a primitive root modulo $2p^k$. □

Proposition 5.5.2. *The numbers $d \in \mathbb{Z}_{\geq 1}$ for which there exists a primitive root modulo d are exactly ones of the following: $2, 4, p^k, 2p^k$ (here p is an odd prime and $k \in \mathbb{Z}_{\geq 1}$.*

Proof. We already saw that for d in the list, there exists a primitive root modulo d. We now want to rule out the other d's.

Suppose that d, e are relatively prime. By the Chinese reminder theorem, if for some $\alpha \in \mathbb{Z}_{de}^{\times}$ we have $frgt_d^{de}(\alpha)^k = [1]_d$ and $frgt_e^{de}(\alpha)^k = [1]_e$, then $\alpha^k = [1]_{de}$, and therefore $ord(\alpha)|k$. Clearly $k = lcm(\phi(d), \phi(e))$ satisfies these conditions, and so we get

$$ord(\alpha)|lcm(\phi(d), \phi(e)).$$

Since $lcm(\phi(d), \phi(e)) = \frac{\phi(d)\phi(e)}{gcd(\phi(d),\phi(e))}$, we see that if $gcd(\phi(d), \phi(e)) > 1$ then every element $\alpha \in \mathbb{Z}_{de}^{\times}$ has order strictly less than $\phi(d)\phi(e) = \phi(de)$, and therefore there are no primitive roots modulo de.

In particular, if (continuing to assume that d and e are relatively prime) each of d and e is divisible by an odd prime or 4, we see that there are no primitive roots modulo de, because both $\phi(d)$ and $\phi(e)$ are even, so not relatively prime.

Therefore, we rule out numbers which are divisible by more than one odd prime, and numbers which are divisible by some odd prime and by 4. We have already seen that numbers divisible by 8 are also ruled out. This finishes the claim.

5.6 A Theorem of Gauss-Wilson

Theorem 5.6.1 (Gauss-Wilson)**.** *Let $d \in \mathbb{Z}_{\geq 2}$. Then*

$$\prod_{\alpha \in \mathbb{Z}_d^{\times}} \alpha \in \mathbb{Z}_d^{\times}$$

is equal to $[-1]_d$ if $\mathbb{Z}_d^{\times}$ admits primitive roots, and to $[1]_d$ if $\mathbb{Z}_d^{\times}$ admits no primitive roots.

Proof. We will prove only the first claim. If $d = 2$ then it is verified directly. Hence, assume $d \neq 2$. Notice that then $\phi(d)$ is even.

Let $\gamma \in \mathbb{Z}_d^{\times}$ be a primitive root. Notice that $(\gamma^s)^2 = [1]_p$ if and only if $\phi(d)|2s$, i.e. if and only if $\frac{\phi(d)}{2}|s$. Therefore, γ^0 and $\gamma^{\frac{\phi(d)}{2}}$ are exactly all the elements α of $\mathbb{Z}_d^{\times}$ which satisfy $\alpha^2 = [1]_d$. Therefore, since $[1]_d$ and $[-1]_d$ are such elements, we must have $\gamma^{\frac{\phi(d)}{2}} = [-1]_d$. So, as in the proof of Wilson's theorem, when computing the product we want to compute, pairs of elements which are mutually inverse will cancel out, except for when an element is its own inverse, which happens for $[1]_d$ and $[-1]_d$. Therefore the product is equal to the product of $[1]_d$ and $[-1]_d$, i.e the product is equal to $[-1]_d$.

□

□

Chapter 6

Cryptography

6.1 Substitution ciphers

The most basic encryption is by a substitution cipher, or a dictionary, i.e. if we want to encrypt messages drawn from a set X, we construct a bijection $E : X \to Y$ with some other set and tell E the person with whom we are communicating. Here E^{-1} should be also easily calculated.

In practice, if we have a long message, we break it down to smaller parcels which can be encoded in terms of X, and send them one by one.

For example, we can choose a number $d \in \mathbb{Z}_{\geq 1}$, have $X = Y = \mathbb{Z}_d$, and $E(\mu) := \sigma\mu$ where $\sigma \in \mathbb{Z}_d^\times$ is some invertible residue class. It is relatively easy to compute σ^{-1}, by using Euclids algorithm (picking $m \in \mathbb{Z}$ for which $[m]_d = \sigma$, we compute $fm + gd = 1$ and then $\sigma^{-1} = [f]_d$) or by using $\sigma^{-1} = \sigma^{\phi(d)-1}$ (by Euler's theorem).

Notice that to compute σ^k we only need about $log_2(k)$ multiplication modulo d operations, and not k as the most naive way of computing would yield. Indeed, if k is even we have $\sigma^k = (\sigma^2)^{k/2}$ and if k is odd we have $s^k = (\sigma^2)^{\frac{k-1}{2}} \cdot s$ so the number of operations $N(k)$ needed satisfies

$$N(k) \leq N(\lfloor \frac{k}{2} \rfloor) + 2, \quad N(1) = 0.$$

Thus we can show that

$$N(k) \leq log_2(k)$$

by induction.

One of the possible problems with the substitution cipher is that, in texts, letters have various frequencies (for example, "e" is the most commonly appearing letter in an English text), so that a person reading the encrypted message can start to guess what is the dictionary E based on frequencies.

Another possible problem is that the two communicating sides should somehow agree on E, so need to be physically close, or communicate E via a non-safe medium, etc. This can be even more annoying if they want to change E frequently, to alleviate the previous problem.

6.2 Sharing a secret (Diffie-Hellman key agreement)

We will now see how both sides can share a secret σ (σ has a meaning as above) across a non-safe medium (i.e. all they send to each other is seen by others). This is called the *Diffie-Hellman key exchange.*

We assume that $d = p$ is a prime (which is large). We next choose a primitive root $\alpha \in \mathbb{Z}_p^\times$ (this root does not have to be big). The information of p and α is accessible to all.

Recall that there is a bijection

$$\mathbb{Z}_{p-1} \to \mathbb{Z}_p^\times : k \mapsto \alpha^k.$$

The critical property of this bijection is the following: From a computational point of view, it is easy to compute α^k given k but very hard to compute k given α^k. The general property of that kind is known as that of a *one-way function*, while in this specific case this is known as the *discrete logarithm problem.*

Let now Alice choose $a \in \mathbb{Z}_{p-1}$ and Bob choose $b \in \mathbb{Z}_{p-1}$ (their *"private keys"*). Those are their personal secrets, they keep them to themselves. However, Alice makes α^a public, and Bob makes α^b public (their *"public keys"*). Now, Alice knows her a and the public α^b, so she can compute $(\alpha^b)^a$. Bob knows his b and the public α^a, so he can compute $(\alpha^a)^b$. But, of course,

$$(\alpha^b)^a = \alpha^{ba} = \alpha^{ab} = (\alpha^a)^b.$$

This value is the secret σ that Alice and Bob both now know. The public knows, except the general p and α of the setting, also α^a and α^b. From this, it is not clear how to compute α^{ab}.

If a third person, Carol, wants now be part of the secretive group, she can choose her $c \in \mathbb{Z}_{p-1}$, and then proceed as follows. Alice and Bob make α^{ab} public, and thus Carol can compute α^{abc}. As α^a and α^b are already public, Carol can also compute α^{ac} and α^{bc} and make them public. Then Alice and Bob can compute α^{abc} as well, and it becomes the new secret (the public knows $\alpha^a, \alpha^b, \alpha^{ab}, \alpha^{ac}, \alpha^{bc}$).

6.3 Combining the two last sections

Let us retain the setting of the previous subsection - of p and α, Alices (resp. Bobs) private key a (resp. b) and Alices (resp. Bobs) public key α^a (resp. α^b).

Then Alice and Bob both know the secret

$$\sigma = \alpha^{ab} \in \mathbb{Z}_p^\times.$$

If now Bob wants to send an encryption of a message

$$\mu \in \mathbb{Z}_p^\times$$

to Alice, he sends

$$\sigma\mu \in \mathbb{Z}_p^\times.$$

Alice can compute

$$\mu = \sigma^{-1}(\sigma\mu).$$

Thus, we use an asymmetric setting (Alice and Bob have private and public keys) in order to create a common secret key which is then used in a symmetric cipher (one uses the same key for encoding and decoding).

6.4 Al-Gamal encryption

When we do as before, but Bob each time changes his private key, we obtain the Al-Gamal encryption, which can be now regarded as an asymmetric cipher. Notice that this seems to eliminate the problem of guessing the key σ based on letter frequencies, as this key changes with every step. Let us describe it explicitly again.

Alice choses $a \in \mathbb{Z}_{p-1}$ and shares publicly α^a. Then a is called the *private key* and α^a is called the *public key.*

If Bob wants to communicate a message $\mu \in \mathbb{Z}_p^\times$ to Alice, he peeks randomly some $b \in \mathbb{Z}_{p-1}$ and sends the pair

$$(\alpha^b, \alpha^{ab}\mu) \in \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$$

to Alice (notice that Bob knows how to compute $\alpha^{ab} = (\alpha^a)^b$ since Alice's public key α^a is, well, public). Alice can decode the message by first computing the shared secret $\alpha^{ab} = (\alpha^b)^a$, then computing its inverse, thus being able to compute

$$\mu = (\alpha^{ab})^{-1} \cdot (\alpha^{ab}\mu).$$

Thus, basically, each time Bob wants to send a message, he fulfills his part in creating the common secret, so that now Alice and Bob share a secret $\sigma \in \mathbb{Z}_p^\times$, and then Bob sends to Alice $\sigma\mu$, and Alice deciphers it, as we explained in the first subsection.

6.5 RSA encryption

In the previous sections, we have used, for a prime $p \in \mathbb{Z}_{\geq 1}$, the bijection

$$\mathbb{Z}_{p-1} \to \mathbb{Z}_p^\times : k \mapsto \alpha^k,$$

where $\alpha \in \mathbb{Z}_p^\times$ is a fixed primitive root. The property of this bijection is that (if p and α are known) it is easy to calculate it on a given value, but hard to calculate the inverse bijection on a given value.

We will now use a different bijection with a similar, but different property. Namely, given some knowns it will be easy to calculate the bijection on a given value. However, the inverse bijection will also be easy to calculate given some other knowns. Therefore, the inverse bijection is not universally hard to compute (as in the previous case) - it is easy to compute for those having some extra information.

Let

$$d \in \mathbb{Z}_{\geq 1}$$

and let $e \in \mathbb{Z}$ be such that $gcd(e, \phi(d)) = 1$. Then the function

$$\mathbb{Z}_d^\times \to \mathbb{Z}_d^\times : \alpha \mapsto \alpha^e$$

is, by Euler's theorem, a bijection with inverse

$$\mathbb{Z}_d^\times \to \mathbb{Z}_d^\times : \alpha \mapsto \alpha^f$$

where f is inverse to e modulo $\phi(d)$.

In fact, if d is square-free (i.e. a product of distinct primes) then we can replace $\mathbb{Z}_d^\times$ above with $\mathbb{Z}_d$, i.e. we claim that with e and f as above the maps

$$\mathbb{Z}_d \to \mathbb{Z}_d : \alpha \mapsto \alpha^e$$

and

$$\mathbb{Z}_d \to \mathbb{Z}_d : \alpha \mapsto \alpha^f$$

are mutually inverse bijections. In other words, we want to check that $\alpha^{ef} = \alpha$ for all $\alpha \in \mathbb{Z}_d$. By the Chinese remainder theorem, this is the same as checking $frgt_p^d(\alpha)^{ef} = frgt_p^d(\alpha)$ for all primes $p|d$. If $frgt_p^d(\alpha) = [0]_p$, then the equality is clear. If $frgt_p^d(\alpha) \neq [0]_p$, notice that $ef \equiv_{\phi(d)} 1$ and $\phi(p)|\phi(d)$ and hence $ef \equiv_{\phi(p)} 1$ and so by Fermat's little theorem we obtain

$$frgt_p^d(\alpha)^{ef} = frgt_p^d(\alpha) \cdot frgt_p^d(\alpha)^{?\cdot\phi(p)} = frgt_p^d(\alpha).$$

Assume that d is square-free. The bijection

$$\mathbb{Z}_d \to \mathbb{Z}_d : \alpha \mapsto \alpha^e$$

has the property that when d and e known it is easy to compute it on a given value, but it is only easy to compute its inverse on a given value if one knows $\phi(d)$, because it is necessary in order to find f as above.

Is it easy to find $\phi(d)$? In order to compute it, we write $d = p_1 \cdot \ldots \cdot p_k$ as a product of distinct primes. Then $\phi(d) = (p_1 - 1) \cdot \ldots \cdot (p_k - 1)$. Therefore, it is easy to compute $\phi(d)$ if we know the decomposition of d as a product of primes. Is it easy to find the decomposition of d into primes? No! This is the basic problem, the factorization of a number into a product of primes is a hard thing computationally (I think that modern encryption is based on having computational problems which are easy theoretically but hard computationally).

We thus obtain the following asymmetric encryption/decryption scheme. We generate two huge prime numbers p and q and set $d = pq$. We also choose $e \in \mathbb{Z}$ which is relatively prime to $\phi(d)$. We let d and e be publicly known. Thus, the public can compute easily

$$\mathbb{Z}_d \to \mathbb{Z}_d : \alpha \mapsto \alpha^e.$$

We can also compute easily the inverse, because we can compute $\phi(d) = (p - 1)(q - 1)$ and then compute $f \in \mathbb{Z}$ which is inverse to e modulo $\phi(d)$. Then as explained above

$$\mathbb{Z}_d \to \mathbb{Z}_d : \alpha \mapsto \alpha^f$$

is inverse to E. Hence, if someone wants to encode a message $\mu : \mathbb{Z}_d$ for us, he sends us μ^e. We can decode it: $\mu = (\mu^e)^f$.

Chapter 7

Quadratic residue classes

7.1 The Legendre symbol

Let p be an odd prime. We are interested in deciding whether an equation

$$x^2 + mx + n \equiv_p 0$$

has a solution or not.

Lemma 7.1.1. *The equation*

$$x^2 + mx + n \equiv_p 0$$

has a solution if and only if the equation

$$x^2 \equiv_p m^2 - 4n$$

has a solution.

Proof. Let us denote by c an inverse to 2 modulo p. Since 2 is invertible modulo p, the equation

$$x^2 + mx + n \equiv_p 0$$

has the same solutions as the equation

$$4x^2 + 4mx + 4n \equiv_p 0.$$

We have

$$4x^2 + 4mx + 4n = (2x)^2 + 2 \cdot m \cdot 2x + m^2 + (4n - m^2) = (2x + m)^2 + (4n - m^2)$$

and therefore, performing the invertible modulo p substitution $y = 2x + m$, we see that our equation has a solution if and only if the equation

$$y^2 + (4n - m^2) \equiv_p 0$$

has a solution. □

Therefore, our general question is reduced to the question of determining which residue classes modulo p admit a square root, i.e. are squares modulo p.

Definition 7.1.2 (Legendre symbol)**.** Let $\alpha \in \mathbb{Z}_p$. If $\alpha \neq [0]_p$ and there exists $\beta \in \mathbb{Z}_p$ such that $\beta^2 = \alpha$, we write $\left(\frac{\alpha}{p}\right) = 1$. If $\alpha \neq [0]_p$ and there does not exist $\beta \in \mathbb{Z}_p$ such that $\beta^2 = \alpha$, we write $\left(\frac{\alpha}{p}\right) = -1$. If $\alpha = [0]_p$, we write $\left(\frac{\alpha}{p}\right) = 0$.

For $n \in \mathbb{Z}$, we write $\left(\frac{n}{p}\right)$ for $\left(\frac{[n]_p}{p}\right)$.

Claim 7.1.3 (Euler's criterion)**.** *Let $\alpha \in \mathbb{Z}_p$. Then*

$$[\left(\frac{\alpha}{p}\right)]_p = \alpha^{\frac{p-1}{2}}.$$

In other words: let $n \in \mathbb{Z}$. Then

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

Proof. For $\alpha = [0]_p$ the claim is clear, so we assume that $\alpha \neq [0]_p$, i.e. $\alpha \in \mathbb{Z}_p^\times$.

Notice that $(\alpha^{\frac{p-1}{2}})^2 = \alpha^{p-1} = [1]_p$ by Fermat's little theorem. As we saw before, one therefore has $\alpha^{\frac{p-1}{2}} \in \{[1]_p, [-1]_p\}$. Therefore, we want to show that $\alpha^{\frac{p-1}{2}}$ is equal to $[1]_p$ if and only if α is a square.

If α is a square, so $\alpha = \beta^2$ for some $\beta \in \mathbb{Z}_p^\times$., then

$$\alpha^{\frac{p-1}{2}} = (\beta^2)^{\frac{p-1}{2}} = \beta^{p-1} = [1]_p$$

by Fermat's little theorem again.

Now assume conversely that $\alpha^{\frac{p-1}{2}} = [1]_p$. We use the existence of a primitive root $\gamma \in \mathbb{Z}_p^\times$. Recall that $\gamma^r = [1]_p$ if and only if $p-1|r$. Write $\alpha = \gamma^k$ for some $k \in \mathbb{Z}$. Then $[1]_p = \alpha^{\frac{p-1}{2}} = \gamma^{k\cdot\frac{p-1}{2}}$ and therefore $p-1|k\cdot\frac{p-1}{2}$. This gives $2|k$. Therefore, we can consider $\beta = \alpha^{\frac{k}{2}}$, which will be an element fo which $\beta^2 = \alpha$. □

Remark 7.1.4. Since p is an odd prime, so in particular $p > 2$, the map $\{-1, 0, 1\} \hookrightarrow \mathbb{Z} \to \mathbb{Z}_p$ is injective. Therefore, $[\left(\frac{\alpha}{p}\right)]_p$ determines $\left(\frac{\alpha}{p}\right)$.

Corollary 7.1.5. *Let $n, m \in \mathbb{Z}$. One has*

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \cdot \left(\frac{n}{p}\right).$$

Proof. One has

$$\left(\frac{mn}{p}\right) \equiv_p (mn)^{\frac{p-1}{2}} = m^{\frac{p-1}{2}} \cdot n^{\frac{p-1}{2}} \equiv_p \left(\frac{m}{p}\right) \cdot \left(\frac{n}{p}\right)$$

and hence the equality. □

Corollary 7.1.6. *One has*

$$\left(\frac{-1}{p}\right) \equiv_p (-1)^{\frac{p-1}{2}}$$

and so -1 is a square modulo p if $p \equiv_4 1$ and a non-square modulo p if $p \equiv_4 3$.

We can now prove:

Theorem 7.1.7. *There are infinitely many primes which are congruent to 1 modulo 4.*

Proof. Again, suppose that there are only finitely many such, denote then $p_1, \ldots, p_k$. Consider then

$$n := 4(p_1 \cdots p_k)^2 + 1.$$

Let p be a prime factor of n. As p can not be any of the p_i's, it is enough to show that $p \equiv_4 1$ to obtain a contradiction. And indeed, we have:

$$-1 \equiv_p 4(p_1 \cdots p_k)^2$$

so -1 is a square modulo p, and therefore by the previous corollary we have $p \equiv_4 1$. □

7.2 Statement of the quadratic reciprocity law and examples

Theorem 7.2.1 (Gauss's quadratic reciprocity law)**.** *Let p, q be two distinct odd primes. One has:*

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

And we also have:

Theorem 7.2.2 (The supplementary law)**.**

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv_8 \pm 1 \\ -1 & \text{if } p \equiv_8 \pm 3 \end{cases}.$$

For the proof, we will need a few preliminaries. Let us first see some examples of applying this.

Example 7.2.3. *Fix an odd prime $p \in \mathbb{Z}_{\geq 1}$, and vary an odd prime $q \in \mathbb{Z}_{\geq 1}$ (with q different than p). We see that the answer to the question of whether p is a square modulo q depends only on $[q]_{4p}$! This is one possible "essence" of this law.*

Example 7.2.4. *For a prime $p \in \mathbb{Z}_{\geq 1}$ distinct from 2 and 5, one has*

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right).$$

Notice that in $\mathbb{Z}_5$, the non-zero squares are $[1]_5$ and $[4]_5$. Therefore, 5 is a square modulo p if and only if p is congruent to 1 or 4 modulo 5.

Example 7.2.5.

$$\left(\frac{12}{23}\right) = (\left(\frac{2}{23}\right))^2 \cdot \left(\frac{3}{23}\right) = \left(\frac{3}{23}\right) = -\left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1.$$

Alternatively, one can compute:

$$\left(\frac{12}{23}\right) = \left(\frac{-11}{23}\right) = \left(\frac{-1}{23}\right)\left(\frac{11}{23}\right) = (-1) \cdot -\left(\frac{23}{11}\right) = (-1) \cdot -\left(\frac{1}{11}\right) = 1.$$

Thus, 12 is a square modulo 23. One can indeed find that $9^2 - 12 = 3 \cdot 23$ so $9^2 \equiv_{23} 12$.

Example 7.2.6.

$$\left(\frac{30}{59}\right) = \left(\frac{2}{59}\right) \cdot \left(\frac{3}{59}\right) \cdot \left(\frac{5}{59}\right) = (-1) \cdot (-\left(\frac{59}{3}\right)) \cdot \left(\frac{59}{5}\right) = (-1) \cdot (-\left(\frac{2}{3}\right)) \cdot (\left(\frac{4}{5}\right)) = (-1) \cdot 1 \cdot 1 = -1.$$

Thus, 30 is not a square modulo 59.

7.3 The discrete Fourier transform

Throughout, fix $d \in \mathbb{Z}_{\geq 1}$. We denote

$$\mu_d = \{\zeta \in \mathbb{C}^\times \mid \zeta^d = 1\}.$$

Elements $\zeta \in \mu_d$ are called *d-th roots of unity*. Denoting

$$\zeta_1 = e^{\frac{2\pi i}{d}} = cos(\frac{2\pi i}{d}) + i \cdot sin(\frac{2\pi i}{d}),$$

we have

$$\mu_d = \{1, \zeta_1, \ldots, \zeta_1^{d-1}\}$$

(and all the listed elements are different, i.e. μ_d contains d elements). Notice that if $n \equiv_d m$, then $\zeta^n = \zeta^m$. Hence for $\alpha \in \mathbb{Z}_d$ we can define unambiguously ζ^α as ζ^n for any n for which $[n]_d = \alpha$.

Let $f : \mathbb{Z}_d \to \mathbb{C}$ be a function. The *(discrete) Fourier transform* of f is the function $F_f : \mu_d \to \mathbb{C}$ given by

$$F_f(\zeta) = \sum_{\alpha \in \mathbb{Z}_d} f(\alpha) \cdot \zeta^\alpha.$$

Remark 7.3.1. By identifying $\{0, \ldots, d-1\}$ with μ_d via $k \mapsto \zeta_1^k$ and also writing $f(n) = f([n]_d)$ we obtain the perhaps more recognizable to some formula:

$$F_f(k) = \sum_{0 \le j \le d-1} f(j) \cdot e^{\frac{2\pi i \cdot jk}{d}}.$$

Theorem 7.3.2 (Parseval's identity)**.**

1. *Let $f, g : \mathbb{Z}_d \to \mathbb{C}$. Then we have*

$$\sum_{\alpha \in \mathbb{Z}_d} f(\alpha)\overline{g(\alpha)} = \frac{1}{d} \cdot \sum_{\zeta \in \mu_d} F_f(\zeta)\overline{F_g(\zeta)}.$$

2. *Let $f \in \mathbb{Z}_d \to \mathbb{C}$. Then we have*

$$\sum_{\alpha \in \mathbb{Z}_d} |f(\alpha)|^2 = \frac{1}{d} \cdot \sum_{\zeta \in \mu_d} |F_f(\zeta)|^2.$$

Proof. The second part follows from the first by substituting $g := f$, so let us prove the first part. Notice that if we fix g, both sides are linear in f. Similarly, if we fix f both sides are conjugate-linear in g. Therefore, we reduce to the case

$$f = \delta_\alpha, g = \delta_\beta.$$

We calculate

$$F_{\delta_\alpha}(\zeta) = \sum_{\gamma \in \mathbb{Z}_d} \delta_\alpha(\gamma) \cdot \zeta^\gamma = \zeta^\alpha.$$

The left hand sides of the equation to be established is equal to $\delta_{\alpha,\beta}$. The right hand side is equal to

$$\frac{1}{d} \sum_{\zeta \in \mu_d} \zeta^\alpha \cdot \overline{\zeta^\beta} = \frac{1}{d} \sum_{\zeta \in \mu_d} \zeta^{\alpha - \beta} = \delta_{\alpha,\beta},$$

where the last equality is by the Lemma that follows. □

We have used the following lemma:

Lemma 7.3.3. *Let $\alpha \in \mathbb{Z}_d$. Then*

$$\sum_{\zeta \in \mu_d} \zeta^\alpha = \delta_{\alpha,[0]_d} \cdot d.$$

Proof. If $\alpha = [0]_d$, the the sum is a sum of d ones, so the claim is clear. Suppose then that $\alpha \neq [0]_d$. We have:

$$\sum_{\zeta \in \mu_d} \zeta^\alpha = \sum_{\zeta \in \mu_d} (\zeta_1 \cdot \zeta)^\alpha = \zeta_1^\alpha \sum_{\zeta \in \mu_d} \zeta^\alpha.$$

Since $\zeta_1^\alpha \neq 1$, we obtain that our sum must be equal to zero. □

7.4 Algebraic numbers and integers

Definition 7.4.1. Let $c \in \mathbb{C}$. The number c is called *algebraic* if there exists a non-zero polynomial $P \in \mathbb{Q}[X]$ such that $P(c) = 0$. Thus, concretely, c is algebraic if there exists $n \geq 1$ and $a_0, \ldots, a_{n-1} \in \mathbb{Q}$ such that

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

If c is not algebraic, it is called *transcendental*.

Example 7.4.2. *Every rational number is algebraic. The number $\sqrt{2}$ is algebraic, since it is a root of the polynomial $Z^2 - 2$. For $q \in \mathbb{Q}$, the number $e^{2\pi i \cdot q}$ is algebraic.*

Example 7.4.3. *It was proven that the numbers π and e are transcendental.*

Definition 7.4.4. Let $c \in \mathbb{C}$. The number c is called an *algebraic integer* if there exists $n \geq 1$ and $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ such that

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

Lemma 7.4.5. *A number $q \in \mathbb{Q}$ is an algebraic integer if and only if it is an integer (i.e. lies in $\mathbb{Z}$).*

Proof. Clearly, if $q \in \mathbb{Q}$ is an integer then since q is a root of $X - q$, we obtain that q is an algebraic integer. Conversely, assume that $q \in \mathbb{Q}$ is an algebraic integer. So, there exist $n \in \mathbb{Z}_{\geq 1}$ and $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ such that

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

Write $q = \frac{r}{s}$ in reduced terms, so $r, s \in \mathbb{Z}$ and $s > 0$ and $gcd(r, s) = 1$. Then we have

$$r^n + a_{n-1}r^{n-1}s + \ldots + a_1 r s^{n-1} + a_0 s^n = 0.$$

If a prime p divides s, we obtain from this equation that it also divides r. Since r and s are relatively prime, this is not possible, so no prime divides s, which implies that $s = 1$. Hence $q = r \in \mathbb{Z}$, i.e. q is an integer. □

Lemma 7.4.6. *Let $c \in \mathbb{C}$ be algebraic. Then there exists $d \in \mathbb{Z}_{\geq 1}$ such that dc is an algebraic integer.*

Proof. There exists $n \in \mathbb{Z}_{\geq 1}$ and $a_0, \ldots, a_{n-1} \in \mathbb{Q}$ such that

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

There exists $e \in \mathbb{Z}_{\geq 1}$ such that $ea_i \in \mathbb{Z}$ for all $0 \leq i \leq n-1$. Then, setting $d := e^n$, we have:

$$(dc)^n + (a_{n-1}d)d^{n-1} + \ldots + (a_1 d^{n-1})c + a_0 d^n = 0$$

which shows that dc is an algebraic integer. □

Proposition 7.4.7. *Let $c, d \in \mathbb{C}$. If both c and d are algebraic (resp. algebraic integers) then $c + d$ and cd are algebraic (resp. algebraic integers).*

Proof. Omitted. □

Remark 7.4.8. Let $c_1, c_2 \in \mathbb{C}$ be algebraic integers. We say that $c_1 | c_2$ if there exists an algebraic integer $e \in \mathbb{C}$ such that $c_2 = ec_1$. Let $d \in \mathbb{Z}_{\geq 1}$. For algebraic integers $c_1, c_2 \in \mathbb{C}$, we say that $c_1 \equiv_d c_2$ if $d | c_2 - c_1$. Then (we will need this observation in the proof of the quadratic reciprocity law using Gauss sums) if $c_1, c_2 \in \mathbb{Z}$ and $c_1 \equiv_d c_2$ using that definition, we in fact have $c_1 \equiv_d c_2$ using our standard definition. Indeed, The former says that there exists an algebraic integer e such that $c_2 - c_1 = ed$, while the latter says that there exists an integer e such that $c_2 - c_1 = ed$. But, if e is an algebraic integer satisfying $c_2 - c_1 = ed$, we have that e is rational, and then, by lemma 7.4.5, we have that in fact $e \in \mathbb{Z}$.

7.5 Gauss sums

Throughout, we fix an odd prime p.

We define $G : \mu_p \to \mathbb{C}$ as

$$G := F_{\left(\frac{\cdot}{p}\right)},$$

the Fourier transform of the Legendre symbol. Thus, concretely:

$$G(\zeta) = \sum_{\alpha \in \mathbb{Z}_p} \left(\frac{\alpha}{p}\right) \cdot \zeta^{\alpha}.$$

The expression/number $G(\zeta)$ is called a *Gauss sum*.

Lemma 7.5.1. *Let $\zeta \in \mu_p$ and let $[0]_p \neq \alpha \in \mathbb{Z}_p$. Then*

$$G(\zeta^{\alpha}) = \left(\frac{\alpha}{p}\right) G(\zeta).$$

Proof. We have

$$G(\zeta^{\alpha}) = \sum_{\beta \in \mathbb{Z}_p} \left(\frac{\beta}{p}\right) \zeta^{\alpha\beta} = \sum_{\beta \in \mathbb{Z}_p} \left(\frac{\alpha^{-1}\beta}{p}\right) \zeta^{\alpha(\alpha^{-1}\beta)} = \left(\frac{\alpha^{-1}}{p}\right) \sum_{\beta \in \mathbb{Z}_p} \left(\frac{\beta}{p}\right) \zeta^{\beta} = \left(\frac{\alpha}{p}\right) G(\zeta).$$

□

Corollary 7.5.2. $G(1) = 0$.

Proof. Let $\alpha \in \mathbb{Z}_p^{\times}$ be a non-square. We have then

$$G(1) = G(1^{\alpha}) = \left(\frac{\alpha}{p}\right) G(1) = -G(1)$$

so $2G(1) = 0$, and thus $G(1) = 0$. □

Lemma 7.5.3. *Let $1 \neq \zeta \in \mu_p$. Then*

$$|G(\zeta)|^2 = p.$$

Proof. Notice that by Lemma 7.5.1 one has $|G(\zeta)|^2 = |G(\zeta')|^2$ for all $\zeta, \zeta' \in \mu_p$ which are not 1 (and by Corollary 7.5.2, $|G(1)|^2 = 0$). Denote by a the common value of $|G(\zeta)|^2$ for $1 \neq \zeta \in \mu_p$ (we want to show that $a = p$). By Parseval's identity we have :

$$(p-1)a = \sum_{\zeta \in \mu_p} |G(\zeta)|^2 = p \cdot \sum_{\alpha \in \mathbb{Z}_p} |\left(\frac{\alpha}{p}\right)|^2 = p(p-1)$$

and hence $a = p$. □

Claim 7.5.4. *Let $1 \neq \zeta \in \mu_p$. one has*

$$G(\zeta)^2 = (-1)^{\frac{p-1}{2}} p.$$

Proof. We have

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

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

□

Finally, we can prove Gauss's quadratic reciprocity theorem and the supplementary law.

Proof (of Gauss's quadratic reciprocity theorem). We study now $G(\zeta)^q$ modulo q. One one hand, we have

$$G(\zeta)^q = \left(\sum_{\alpha \in \mathbb{Z}_p} \left(\frac{\alpha}{p}\right) \zeta^\alpha \right)^q \equiv_q \sum_{\alpha \in \mathbb{Z}_p} \left(\left(\frac{\alpha}{p}\right) \zeta^\alpha \right)^q = \sum_{\alpha \in \mathbb{Z}_p} \left(\frac{\alpha}{p}\right) (\zeta^q)^\alpha = G(\zeta^q) = \left(\frac{q}{p}\right) \cdot G(\zeta).$$

On the other hand, we have:

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

Comparing the two expressions, we deduce

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

We now argue that we can cancel $G(\zeta)$ from both sides. Indeed, $G(\zeta)^2$ is an integer which is prime to q, hence it admits an inverse m modulo q, so multiplying by $G(\zeta) \cdot m$ the two sides of the equation has the effect of canceling $G(\zeta)$. Thus, we get

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

From this follows

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

□

Proof (of the supplementary law). Let $\zeta \in \mu_8$ be primitive; For concretenss, say $\zeta = e^{\frac{2\pi i}{8}}$. Notice that $\zeta^2 = i$ and therefore $\zeta^{-2} = -i$ and so $\zeta^2 + \zeta^{-2} = 0$. Denoting

$$g := \zeta + \zeta^{-1}$$

(some version of Gauss sums) we obtain

$$g^2 = (\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2 = 2.$$

Now we calculate, quite similarly to previously:

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

On the other hand, we have:

$$g^p = (\zeta + \zeta^{-1})^p \equiv_p \zeta^p + \zeta^{-p}.$$

If $p \equiv_8 \pm 1$ this last expression is equal to g. If $p \equiv_8 \pm 3$, the last expression is equal to

$$\zeta^3 + \zeta^{-3} = \zeta^4 \cdot \zeta^{-1} + \zeta^{-4} \cdot \zeta = -\zeta^{-1} - \zeta = -g.$$

Thus, overall, we obtain

$$g \cdot \left(\frac{2}{p}\right) \equiv_p g \cdot \epsilon_p$$

where for convenience we denote

$$\epsilon_p = \begin{cases} 1 & \text{if } p \equiv_8 \pm 1 \\ -1 & \text{if } p \equiv_8 \pm 3 \end{cases}.$$

Now, since $g^2 = 2$ as in the previous proof we can cancel g and obtain

$$\left(\frac{2}{p}\right) \equiv_p \epsilon_p$$

and thus

$$\left(\frac{2}{p}\right) = \epsilon_p,$$

as desired. □

7.6 Another proof of Gauss's quadratic reciprocity theorem

It seems that the following proof is due to G. Rousseau, and then independently due to D. Kunisky.

Fix distinct odd primes $p, q \in \mathbb{Z}_{\geq 1}$.

Recall the Chinese remainder theorem bijection, applied to invertible residue classes:

$$crt^{\times}_{p,q} : \mathbb{Z}^{\times}_{pq} \xrightarrow{\sim} \mathbb{Z}^{\times}_{p} \times \mathbb{Z}^{\times}_{q}$$

given by $\alpha \mapsto (frgt^{pq}_p(\alpha), frgt^{pq}_q(\alpha))$ or more concretely $[n]_{pq} \mapsto ([n]_p, [n]_q)$. In what follows, to simplify notation, we will abuse notation and identify $\mathbb{Z}^{\times}_{pq}$ with $\mathbb{Z}^{\times}_{p} \times \mathbb{Z}^{\times}_{q}$ (in other words, instead of writing $(crt^{\times}_{p,q})^{-1}(\beta, \gamma)$, we will simply write (β, γ)).

For an odd integere $d \in \mathbb{Z}_{\geq 3}$, we define an equivalence relation on $\mathbb{Z}^{\times}_{d}$ given by $\alpha \sim \beta$ if $\alpha = \beta$ or $\alpha = -\beta$. We will be interested in sets of representatives for the equivalence classes. One such set we define as follows:

$$H_d := \big\{[k]_d \ : \ k \in \{1, \dots, \frac{d-1}{2}\}, \ gcd(k, d) = 1\big\}.$$

We will now describe three sets of representatives for the equivalence classes in the case $d := pq$:

1. We take H_{pq}.
2. We take $H^p_{pq} := (crt^{\times}_{p,q})^{-1}\big(H_p \times \mathbb{Z}^{\times}_{q}\big)$.
3. We take $H^q_{pq} := (crt^{\times}_{p,q})^{-1}\big(\mathbb{Z}^{\times}_{p} \times H_q\big)$.

We will now compute, for each such set H,

$$crt^{\times}_{p,q}\big(\prod_{\alpha \in H} \alpha\big) \in \mathbb{Z}^{\times}_{p} \times \mathbb{Z}^{\times}_{q}.$$

It is clear that these will differ by ±, i.e. for two such (α_1, β_1) and (α_2, β_2), one has either $\alpha_1 = \alpha_2$ and $\beta_1 = \beta_2$, or $\alpha_1 = -\alpha_2$ and $\beta_1 = -\beta_2$. By observing the signs, we will obtain Gauss's quadratic reciprocity law. For simplicity of notation, denote $P := \frac{p-1}{2}$ and $Q := \frac{q-1}{2}$.

(1) The result for H_{pq} we calculate as follows. We need to calculate the product of numbers between 1 and $\frac{pq-1}{2}$ which are relatively prime to pq, modulo p (and analogously modulo q). First, those which are relatively prime to p, but not to q, are (notice that $\frac{pq-1}{2} = Pq + Q$):

$$q, 2q, \dots, Pq.$$

Those which are relatively prime to p are (notice that we have $\frac{pq-1}{2} = Qp + P$):

$$1, \ldots, p-1; p+1, \ldots, p+(p-1); \ldots; Qp+1, \ldots, Qp+P.$$

Thus, the desired residue class modulo p is

$$[P! \cdot q^P]_p^{-1} \cdot [(p-1)!^{Q-1} \cdot P!]_p = [-\left(\frac{-1}{q}\right)\left(\frac{q}{p}\right)]_p$$

(the equality by Wilson's theorem and Euler's criterion). Thus, the thing to be computed is equal to

$$\left([-\left(\frac{-1}{q}\right)\left(\frac{q}{p}\right)]_p, [-\left(\frac{-1}{p}\right)\left(\frac{p}{q}\right)]_q\right).$$

(2) The result for H_{pq}^p is

$$\left([(P!)^{q-1}]_p, [((q-1)!)^P]_q\right) = \left([(-1)^{PQ}\left(\frac{-1}{q}\right)]_p, [\left(\frac{-1}{p}\right)]_q\right)$$

(the equality in the q-coordinate is by Wilson's theorem and Euler's criterion, while the equality in the first coordinate is by noticing that since $(P!)^{q-1} = ((P!)^2)^Q \equiv_p ((-1)^P \cdot (p-1)!)^Q$ and thus by Wilson's theorem and Euler's criterion $\equiv_p (-1)^{PQ}\left(\frac{-1}{q}\right)$).

(3) The result for H_{pq}^q is, analogously to the previous case,

$$\left([\left(\frac{-1}{q}\right)]_p, [(-1)^{PQ}\left(\frac{-1}{p}\right)]_q\right).$$

Notice that the p-coordinate of (3) differs from that of (1) by $-\left(\frac{q}{p}\right)$. The q-coordinate of (2) differs from that of (1) by $-\left(\frac{p}{q}\right)$. Finally, (3) differs from (2) by $(-1)^{PQ}$. Therefore, we obtain:

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

or

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

which is Gauss's quadratic reciprocity law.

Chapter 8

Gaussian integers

8.1 Gaussian integers

Similalry to the case of integers, we have the following definitions:

Definition 8.1.1.

1. $a \in \mathbb{Z}[i]$ is said to be *invertible* (or a *unit*) if there exists a $b \in \mathbb{Z}[i]$ such that $ab = 1$. Such a b is unique if exists, and written then a^{-1}.

2. $a \in \mathbb{Z}[i]$ is said to *divide* $b \in \mathbb{Z}[i]$ if there exists $c \in \mathbb{Z}[i]$ such that $b = ac$. We write $a|b$ if a divides b.

3. $a, b \in \mathbb{Z}[i]$ are said to be *associate* if there exists an invertible $u \in \mathbb{Z}[i]$ such that $a = bu$. We will write $a \sim b$ for a and b being associate. Equivalently, a and b are associate if $a|b$ and $b|a$. Being associate is an equivalence relation. An element is associate to 1 if and only if it is invertible.

4. $a \in \mathbb{Z}[i]$ is said to be *prime* if a is not invertible and all divisors of a are either associate to a or invertible.

Definition 8.1.2.

1. The *norm* of $a \in \mathbb{Z}[i]$ is defined to be $N(a) := |a|^2 \in \mathbb{Z}_{\geq 0}$. Explicitly, writting $a = n + mi$, we have $N(a) = n^2 + m^2$.

2. The *conjugate* of $a \in \mathbb{Z}[i]$ is defined to be, writing $a = n + mi$, $\overline{a} := n - mi \in \mathbb{Z}[i]$.

Lemma 8.1.3.

1. *Let $a \in \mathbb{Z}[i]$. Then $a = 0$ if and only if $N(a) = 0$.*

2. *One has $N(1) = 1$.*

3. *Let $a, b \in \mathbb{Z}[i]$. One has $N(ab) = N(a)N(b)$.*

4. *Let $a \in \mathbb{Z}[i]$. One has $a \cdot \overline{a} = N(a)$.*

5. *Let $a \in \mathbb{Z}[i]$.Then a is invertible if and only if $N(a) = 1$.*

Proof.

1. Easy.

2. Easy.

3. Easy.

4. Easy.

5. Suppose that a is invertible. Then $1 = N(1) = N(aa^{-1}) = N(a)N(a^{-1})$. Since the norms are elements of $\mathbb{Z}_{\geq 1}$, this implies $N(a) = 1$. Conversely, suppose that $N(a) = 1$. Then $a \cdot \overline{a} = N(a) = 1$ and hence a is invertible, with inverse $\overline{a}$.

□

Proposition 8.1.4. *The units of $\mathbb{Z}[i]$ are $1, -1, i, -i$.*

Proof. Clearly those are units. Conversely, given $n + mi \in \mathbb{Z}[i]$ a unit, one has $1 = N(n + mi) = n^2 + m^2$. But this can only happen if $n^2 = 0, m^2 = 1$ or $n^2 1, m^2 = 0$, or put differently $n = 0, m \in \{1, -1\}$ or $n \in \{1, -1\}, m = 0$, from which the claim is clear. □

8.2 Division with remainder

Proposition 8.2.1. *Let $a, b \in \mathbb{Z}[i]$, and $b \neq 0$. Then there exists a pair $(q, r) \in \mathbb{Z}[i]^2$ such that $N(r) < N(b)$ and $a = qb + r$. Given this, one has $b|a$ if and only if $r = 0$.*

Proof. First, given such (q, r), if $r = 0$ then clearly $b|a$. Conversely, if $b|a$, then $b|(a - qb) = r$ and so $N(b)|N(r)$. Since $N(r) < N(b)$, this can happen only if $N(r) = 0$, so $r = 0$.

Now let us proof the existence of such (q, r). We consider the complex number $\frac{a}{b} \in \mathbb{C}$. It is easy to see that there exists $q \in \mathbb{Z}[i]$ such that $\left|\frac{a}{b} - q\right| < 1$. Then setting $r := a - qb \in \mathbb{Z}[i]$, we have

$$N(r) = |r|^2 = |a - qb|^2 = \left|b\left(\frac{a}{b} - q\right)\right|^2 = |b|^2 \cdot \left|\frac{a}{b} - q\right|^2 < |b|^2 = N(b).$$

□

8.3 Ideals

We define ideals as in the case of $\mathbb{Z}$:

Definition 8.3.1. An *ideal* $I \subset \mathbb{Z}[i]$ is a subset such that:

1. $0 \in I$.

2. Let $a, b \in I$. Then $a + b \in I$.

3. Let $a \in I$ and $b \in \mathbb{Z}[i]$. Then $ab \in I$.

As for $\mathbb{Z}$, given $a_1, \ldots, a_n \in \mathbb{Z}[i]$ we define an ideal

$$(a_1, \ldots, a_n) := \{b_1 a_1 + \ldots + b_n a_n \ : \ b_1, \ldots, b_n \in \mathbb{Z}[i]\}.$$

We have a claim similar to the one we had for $\mathbb{Z}$:

Theorem 8.3.2 (Principal ideal theorem)**.** *Let $I \subset \mathbb{Z}[i]$ be an ideal. Then there exists $a \in \mathbb{Z}[i]$ such that $I = (a)$. Also, one has $(a) = (b)$ if and only if $a \sim b$.*

Proof. The uniqueness claim: For an element $a \in \mathbb{Z}[i]$ and an ideal $I \subset \mathbb{Z}[i]$, one checks easily that one has $a \in I$ if and only if $(a) \subset I$. Therefore, for $a, b \in \mathbb{Z}[i]$ one has $a|b$ if and only if $(b) \subset (a)$. Therefore $a \sim b$, i.e. $a|b$ and $b|a$, if and only if $(a) \subset (b)$ and $(b) \subset (a)$, i.e. if and only if $(a) = (b)$.

Now we proceed to the existence claim. Let $I \subset \mathbb{Z}[i]$ be an ideal. If $I = \{0\}$ then $I = (0)$ and we are done. So suppose that $I \neq \{0\}$.Consider an element $0 \neq a \in I$ with minimal possible $N(a)$. Clearly $(a) \subset I$ and we will show that $I \subset (a)$, so then $I = (a)$ and we will be done. Thus, let $b \in I$ (we want to deduce that $b \in (a)$). We perform division with remainder and obtain $b = qa + r$ with $N(r) < N(a)$. We have $r = b - qa \in I$. Then by the minimality assumption, we must have $r = 0$. Therefore $b = qa$, i.e. $b \in (a)$. □

8.4 *gcd*

We define the *gcd* as for $\mathbb{Z}$:

Definition 8.4.1. Let $a, b \in \mathbb{Z}[i]$. Then $c \in \mathbb{Z}[i]$ is said to be a *gcd* of a and b if $c|a$ and $c|b$, and for every $d \in \mathbb{Z}[i]$ such that $d|a$ and $d|b$ one has $d|c$.

Then it is easy to see that if c is a *gcd* of a and b, then an arbitrary element d is a *gcd* of a and b if and only $c \sim d$. We show the existence of a *gcd*'s by using ideals (an approach using the Euclidean algorithm is also possible).

Claim 8.4.2. *Let $a, b \in \mathbb{Z}[i]$. By the principal ideal theorem, we can write $(a, b) = (c)$ for some $c \in \mathbb{Z}[i]$. Then $c = gcd(a, b)$. In particular, the gcd of a and b can be expressed as $da + eb$ for some $d, e \in \mathbb{Z}[i]$.*

Proof. $a \in (c)$ and therefore $c|a$. Analogously, $c|b$. If $f|a$ and $f|b$, we want to show that $f|c$. But notice that we can write $c = da + eb$ for some d and e by the definition of the ideal (a, b). Then clearly $f|da + eb = c$. □

For $a, b \in \mathbb{Z}[i]$, we write $gcd(a, b) = c$ in case c is a gcd of a and b. As before, we define:

Definition 8.4.3. Let $a, b \in \mathbb{Z}[i]$. We say that a and b are *relatively prime* if $gcd(a, b) = 1$.

For example, it is easy to see that a prime element $a \in \mathbb{Z}[i]$ is not relatively prime to an element $b \in \mathbb{Z}[i]$ if and only if $a|b$.

8.5 Unique factorization

To not make a confusion with the primes in $\mathbb{Z}$, which can be interpreted as elements of $\mathbb{Z}[i]$ but about whose primeness as such we have not yet meditated, we will denote primes in $\mathbb{Z}[i]$ in the style $\mathfrak{p}, \mathfrak{q}$ etc.

Proposition 8.5.1.

1. *For every $a \in \mathbb{Z}[i]$ there exists a (possibly empty) list of prime elements $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathbb{Z}[i]$ such that*

$$a \sim \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n.$$

2. *If for two lists of primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ one has*

$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n \sim \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_m,$$

then for every prime elemetn $\mathfrak{p} \in \mathbb{Z}[i]$, the number of $1 \leq i \leq n$ such that $\mathfrak{p} \sim \mathfrak{p}_i$ is equal to the number of $1 \leq j \leq m$ such that $\mathfrak{p} \sim \mathfrak{q}_j$.

Proof. (complete) □

8.6 Splitting

Let $p \in \mathbb{Z}_{\geq 1}$ be a prime. We consider now p as an element of $\mathbb{Z}[i]$, and study whether it is prime as an element of that ring. We have $N(p) = p^2$. Therefore, in the prime decomposition of p in $\mathbb{Z}[i]$ there are either 1 or 2 primes. There are therefore three possibilities:

1. *p stays prime in $\mathbb{Z}[i]$*: p is a prime in $\mathbb{Z}[i]$.

2. *p splits in $\mathbb{Z}[i]$* and more specifically *splits completely*: p is associate to a product of two non-associate primes.

3. *p splits in $\mathbb{Z}[i]$* and more specifically *ramifies*: p is associate to the square of a prime.

Theorem 8.6.1. *Let $p \in \mathbb{Z}_{\geq 1}$ be a prime. The following are equivalent:*

1. *p splits in $\mathbb{Z}[i]$.*
2. *p is the sum of two squares in $\mathbb{Z}$.*
3. *Either $p = 2$ or $p \equiv_4 1$.*
4. *$[-1]_p$ is a square.*

Proof. (1) $\implies$ (2): Let $a + bi$ be a prime factor of p. Then, since $N(p) = p^2$, we must have $a^2 + b^2 = N(a + bi) = p$.

(2) $\implies$ (3): The only square in $\mathbb{Z}_4$ are $[0]_4$ and $[1]_4$, so the implication is easy to check.

(3) $\implies$ (4): We studied this.

(4) $\implies$ (1): There exists $n \in \mathbb{Z}$ such that $n^2 \equiv_p -1$. Now we have two elements in $\mathbb{Z}[i]$ whose square modulo p is -1, and which do not differ by ± 1: n and i. We have $n^2 - i^2 \equiv_p 0$ and so $(n - i)(n + i) \equiv_p 0$, i.e. $p|(n - i)(n + i)$, but: neither $p|n - i$ nor $p|n + i$ (since $n \not\equiv_p \pm i$). This implies that p is not prime in $\mathbb{Z}[i]$, by definition, and so splits in $\mathbb{Z}[i]$, by definition. □

For completeness, we also want to see:

Claim 8.6.2. *Among the primes in $\mathbb{Z}$, 2 is the only one which ramifies in $\mathbb{Z}[i]$.*

Proof. First, we have $2 = (1 + i)(1 - i)$ and notice that $(1 - i) = (-i) \cdot (1 + i)$, so $1 - i \sim 1 + i$, therefore 2 ramifies in $\mathbb{Z}[i]$.

Now, if conversely $p \in \mathbb{Z}_{\geq 1}$ is a prime which ramifies in $\mathbb{Z}[i]$, we write $a + bi$ for a prime factor of p. Then as we said above, we have $p = N(a + bi) = a^2 + b^2$. Therefore $p = (a + bi)(a - bi)$, and this is the prime decomposition of p in $\mathbb{Z}[i]$. Clearly both $a \neq 0$ and $b \neq 0$. We want now to see that if $a - bi \sim a + bi$ then $p = 2$. Indeed, one easily sees that this implies that $b \in \{a, -a\}$. But then ia divides $a + bi$, and since $a + bi$ is prime this is only possible if $a \in \{1, -1\}$, which implies that $a + bi \in \{1 + i, 1 - i\}$, and then $p = 2$. □

8.7 Sum's of two squares

Let us reiterate what we got in Theorem 8.6.1.

Corollary 8.7.1 (Fermat's theorem). *Let $p \in \mathbb{Z}_{\geq 1}$ be a prime. Then p is a sum of two integer squares if and onyl if $p = 2$ or $p \equiv_4 1$.*

We want now to characterize all integers $n \in \mathbb{Z}_{\geq 1}$ which are sums of two integer squares.

Lemma 8.7.2. *Let $p \in \mathbb{Z}_{\geq 1}$ be a prime, and assume that $p \equiv_4 3$. If, for $a, b \in \mathbb{Z}$, one has $p|a^2 + b^2$, then $p|a$ and $p|b$.*

Proof. We say in Theorem 8.6.1 that p stays prime in $\mathbb{Z}[i]$. Therefore, $p|a^2+b^2$, which can be rewritten as $p|(a+bi)(a-bi)$, implies that $p|a+bi$ or $p|a-bi$. Both are equivalent to $p|a$ and $p|b$. □

Theorem 8.7.3. *Let $n \in \mathbb{Z}_{\geq 1}$. Denoting by $ord_p(n)$ the exponent of p in the prime decomposition of n, we have that n can be written as the sum of two squares if and only if every prime $p \in \mathbb{Z}_{\geq 1}$ such that $p \equiv_4 3$, satisfies $2|ord_p(n)$.*

Proof. If the condition $2|ord_p(n)$ is satisfied for all primes congruent to 3 modulo 4, then n is the product of numbers which are either squares or primes congruent to 2 or 1 modulo 4. We already know that each such is a sum of two integer squares, and since the product of sums of two squares is again a sum of two squares, the desired conclusion is clear.

Let us assume conversely that n can be written as the sum of two squares. We proceed by induction on n.If $n = 1$ or n is a prime, we already know the claim. If all the prime factors of n are congruent to 2 or 1 modulo 4, the claim is clear. Suppose therefore that there exists a prime factor p of n which is congruent to 3 modulo 4. Write $n = a^2 + b^2$ for $a, b \in \mathbb{Z}$. Then $p|n = a^2 + b^2$ and by the previous lemma we have $p|a$ and $p|b$. Therefore $p^2|a^2+b^2 = n$. Hence we can write $\frac{n}{p^2} = (\frac{a}{p})^2 + (\frac{b}{p})^2$. Therefore, by induction, all the exponents of primes congruent to 3 modulo 4 in the prime decomposition of $\frac{n}{p^2}$ are even, and thus this also holds for n. □

Chapter 9

Continued fractions

9.1 Continued fractions

Definition 9.1.1. A *real continued fraction* is a sequence $(n_0; n_1, n_2, \ldots)$ where there can appear either finitely many terms after the semi-colon, or infinitely many, and where $n_0 \in \mathbb{R}$ and $n_1, \ldots, n_k \in \mathbb{R}_{\geq 1}$. We will say that the real continued fraction is simply a *continued fraction* if all the n_i are integers. The associated value of a finite real continued fraction $(n_0; n_1, \ldots, n_k)$ (by abuse of language, also called a finite real continued fraction) is

$$\langle n_0; n_1, \ldots, n_k \rangle := n_0 + \cfrac{1}{n_1 + \frac{1}{n_2 + \frac{1}{n_3 + \ddots \frac{1}{n_{k-1} + \frac{1}{n_k}}}}}.$$

In other words, we define recursively

$$\langle n_0; \rangle := n_0$$

and

$$\langle n_0; n_1, \ldots, n_{k+1} \rangle := n_0 + \frac{1}{\langle n_1; n_2, \ldots, n_k \rangle}.$$

9.2 The continued fraction associated to a real number

Let us describe how to associate a continued fraction to a real number. For a $0 \neq x \in \mathbb{R}$ we denote by $\lfloor x \rfloor$ the biggest integer not bigger than x.

Let $a \in \mathbb{R}$. Set $a_0 := a$. Suppose that we have already constructed $n_0, n_1, \ldots, n_{k-1} \in \mathbb{Z}$ and $a_0, \ldots, a_k \in \mathbb{R}$ with $n_i \geq 1$ and $a_i > 1$ whenever $i > 0$, such that:

$$a = \langle n_0; n_1, \ldots, n_{\ell-1}, a_\ell \rangle$$

for all $0 \leq \ell \leq k$ (clearly we have just done so for $k := 0$). Then we define $n_k := \lfloor a_k \rfloor$. If a_k is an integer (so $n_k = a_k$), we stop here. In particular, in that case a is rational, as

$$a = \langle n_0; n_1, \ldots, n_k \rangle.$$

Otherwise, we set $a_{k+1} := \frac{1}{a_k - n_k} \in \mathbb{R}_{>1}$ and continue recursively.

Suppose that a is rational. We write a in reduced form $a = \frac{m_{-2}}{m_{-1}}$ (so $m_{-2}, m_{-1} \in \mathbb{Z}$ and $m_{-1} \geq 1$). Apply the Euclidean algorithm: Define m_i recursively, for $i \geq 0$:

$$m_{i-2} = q_i m_{i-1} + m_i \quad (q_i, n_i \in \mathbb{Z}, 0 \leq m_i < m_{i-1})$$

stopping when $m_i = 0$. Set $k \in \mathbb{Z}_{\geq 0}$ to be the number at which we stop, so $m_k = 0$. Notice that $q_i = \lfloor \frac{m_{i-2}}{m_{i-1}} \rfloor$ for all $0 \leq i \leq k$. Therefore, we verify recursively that n_i defined above is equal to q_i, for $0 \leq i \leq k$ and that a_i defined above is equal to $\frac{m_{i-2}}{m_{i-1}}$ for $0 \leq i \leq k$. Indeed, for $i = 0$ this is clear, and we have established that for some $i < k$, then

$$a_{i+1} = \frac{1}{a_i - n_i} = \frac{1}{(\frac{m_i}{m_{i-1}})} = \frac{m_{i-1}}{m_i}$$

and

$$n_i = \lfloor a_i \rfloor = \lfloor \frac{m_{i-1}}{m_i} \rfloor = q_i.$$

We deduce that the continued fraction associated to a real number a is finite if and only if a is rational.

Example 9.2.1. *write down example of golden section*

9.3 Partial convergents

Let $(n_0; n_1, \ldots)$ be a real continued fraction (finite or not - if not, we will denote by $k \in \mathbb{Z}_{\geq 0}$ the last integer for which n_k is still defined). We will define r_i and s_i recursively. Namely, set

$$r_{-2} = 0, r_{-1} = 1$$

and

$$r_i = n_i r_{i-1} + r_{i-2}$$

for $0 \leq i$ recursively (if the real continued fraction is finite, we only continue till $i = k$). Also, set

$$s_{-2} = 1, s_{-1} = 0$$

and

$$s_i = n_i s_{i-1} + s_{i-2}$$

for $0 \leq i \leq k$ rescursively (if the real continued fraction is finite, we only continue till $i = k$). Note that $s_0 = 1$, $s_1 = n_1$ and $s_i \geq s_{i-1} + 1$ for $i \geq 2$, so we see in particular that $s_i \geq i$ for all $0 \leq i$. Also, note that if we are dealing with a continued fraction (i.e. all the n_i are integers) then all r_i and s_i are integers as well.

Claim 9.3.1. *For $0 \leq \ell$ (if the real continued fraction is finite, then we also assume $\ell \leq k$) one has*

$$\langle n_0; n_1, \ldots, n_\ell \rangle = \frac{r_\ell}{s_\ell}.$$

Proof. For $\ell = 0$ this is immediately checked. Recursively, assume that we are given $\ell \geq 1$ and we know this claim for $\ell - 1$ (for all real continued fractions). We then calculate:

$$\langle n_0; n_1, \ldots, n_\ell \rangle = \langle n_0; n_1, \ldots, n_{\ell-2}, n_{\ell-1} + \frac{1}{n_\ell} \rangle = \frac{\left(n_{\ell-1} + \frac{1}{n_\ell}\right) \cdot r_{\ell-2} + r_{\ell-3}}{\left(n_{\ell-1} + \frac{1}{n_\ell}\right) \cdot s_{\ell-2} + s_{\ell-3}} =$$

$$= \frac{(n_{\ell-1}n_\ell + 1)r_{\ell-2} + n_\ell r_{\ell-3}}{(n_{\ell-1}n_\ell + 1)s_{\ell-2} + n_\ell s_{\ell-3}} = \frac{n_\ell(n_{\ell-1}r_{\ell-2} + r_{\ell-3}) + r_{\ell-2}}{n_\ell(n_{\ell-1}s_{\ell-2} + s_{\ell-3}) + s_{\ell-2}} = \frac{n_\ell r_{\ell-1} + r_{\ell-2}}{n_\ell s_{\ell-1} + s_{\ell-2}} = \frac{r_\ell}{s_\ell}.$$

□

Claim 9.3.2. *For $0 \leq \ell$ (if the real continued fraction is finite, then we also assume $\ell \leq k$) one has*

$$r_\ell s_{\ell-1} - s_\ell r_{\ell-1} = (-1)^{\ell+1}.$$

Proof. For $\ell = 0$ this is immediately checked. Then, assuming this holds for some ℓ, we perform the induction step:

$$r_{\ell+1}s_\ell - s_{\ell+1}r_\ell = (n_\ell r_\ell + r_{\ell-1})s_\ell - (n_\ell s_\ell + s_{\ell-1})r_\ell = r_{\ell-1}s_\ell - s_{\ell-1}r_\ell = -(-1)^{\ell+1} = (-1)^{\ell+2}.$$

□

Corollary 9.3.3. *Suppose that our real continued fraction is a continued fraction (i.e. all n_i are integers). For $0 \leq \ell$ (if the real continued fraction is finite, then we also assume $\ell \leq k$) one has $s_\ell > 0$ and $gcd(r_\ell, s_\ell) = 1$. Thus,*

$$\langle n_0; n_1, \ldots, n_\ell \rangle = \frac{r_\ell}{s_\ell}$$

is a reduced expression.

Proof. We have already noted above that s_ℓ that $s_\ell > 0$. From the formula in Claim 9.3.2 it is clear that $gcd(r_\ell, s_\ell) = 1$. □

Corollary 9.3.4. *For $0 \leq \ell$ (if the real continued fraction is finite, then we also assume $\ell \leq k$) one has*

$$\frac{r_\ell}{s_\ell} - \frac{r_{\ell-1}}{s_{\ell-1}} = \frac{(-1)^{\ell+1}}{s_\ell s_{\ell-1}}.$$

In particular we have, for $2 \leq \ell$:

$$\left|\frac{r_\ell}{s_\ell} - \frac{r_{\ell-1}}{s_{\ell-1}}\right| \leq \frac{1}{\ell(\ell-1)}.$$

Corollary 9.3.5. *Suppose that our $(n_0; n_1, \ldots)$ is the continued fraction associated to an $a \in \mathbb{R}$ (which might be finite or infinite, depending on whether a is rational or not). For $1 \leq \ell$ (if the real continued fraction is finite, then we also assume $\ell \leq k$) one has*

$$\big|a - \frac{r_\ell}{s_\ell}\big| \leq \frac{1}{(\ell+1)\ell}.$$

Proof. If ℓ is the last integer for which n_ℓ is still defined, then $a = \frac{r_\ell}{s_\ell}$ and the claim is clear. Otherwise, consider the real continued fraction $(n_0; n_1, \ldots, n_\ell, a_{\ell+1}$ and the corresponding sequences

$$r_0, \ldots, r_\ell, r'_{\ell+1}$$

and

$$s_0, \ldots, s_\ell, s'_{\ell+1}.$$

We then have

$$\big|a - \frac{r_\ell}{s_\ell}\big| = \big|\frac{r'_{\ell+1}}{s'_{\ell+1}} - \frac{r_\ell}{s_\ell}\big| \leq \frac{1}{(\ell+1)\ell}.$$

□

9.4 Convergence

Definition 9.4.1 (Convergence of a sequence)**.**

Theorem 9.4.2. *Let $a \in \mathbb{R}$ be irrational, and let $(n_0; n_1, \ldots)$ be the associated continued fraction. Then*

$$a = \lim_{k\to\infty} \langle n_0; n_1, \ldots, n_k \rangle.$$

Proof. By the above, we have

$$\big|a - \langle n_0; n_1, \ldots, n_k \rangle\big| = \big|a - \frac{r_k}{s_k}\big| \leq \frac{1}{(k+1)k}$$

and so the claim is clear. □

9.5 Periodicity

9.6 Good approximation

Proposition 9.6.1. *Let $a \in \mathbb{R}$ and $d \in \mathbb{Z}_{\geq 1}$. Then there exists a reduced fraction $\frac{n}{m}$ such that $0 < m \leq d$ and*

$$\left|a - \frac{n}{m}\right| \leq \frac{1}{m(d+1)}.$$

Proof. Denote by $(n_0; n_1, \ldots)$ the continued fraction associated to a (which might be finite or infinite) and by $r_0, \ldots$ and $s_0, \ldots$ the corresponding sequences. If there does not exists $\ell \geq 0$ for which s_ℓ is defined and $s_\ell > d$, then we must have that the continued fraction is finite (and so a is rational) so, if it is $(n_0; n_1, \ldots, n_k)$, we have

$$a = \langle n_0; n_1, \ldots, n_k \rangle = \frac{r_k}{s_k}$$

and so

$$\left| a - \frac{r_k}{s_k} \right| = 0$$

and $s_k \leq d$, and thus we are done.

We therefore now assume that there exists $\ell \geq 0$ for which s_ℓ is defined and $s_\ell > d$. Let us understand now by ℓ the minimal such ℓ. Notice that $\ell > 0$ (as $s_0 = 1$) and $s_{\ell-1} \leq d, s_\ell \geq d+1$. We have:

$$\left| a - \frac{r_\ell}{s_\ell} \right| \leq \left| \frac{r_{\ell-1}}{s_{\ell-1}} - \frac{r_\ell}{s_\ell} \right| = \frac{1}{s_{\ell-1} s_\ell} \leq \frac{1}{s_{\ell-1}(d+1)}$$

so $m := s_{\ell-1}$ is as we want.

□

9.7 Sums of two squares

We want to show that a prime $p \in \mathbb{Z}_{\geq 1}$ which is congruent to 1 modulo 4 can be written as a sum of two integer squares. We learned that $[-1]_p$ is a square, so there exists an integer $0 < n < p$ such that $n^2 \equiv_p -1$. Then for all $m, k \in \mathbb{Z}$ we have $m^2 + (nm + pk)^2 \equiv_p m^2 + (nm)^2 = m^2(n^2 + 1) \equiv_p 0$. Therefore, if we can find $m, k \in \mathbb{Z}$ such that $0 < m < \sqrt{p}$ and $0 < nm + pk < \sqrt{p}$, the number $m^2 + (nm + pk)^2$ will be both divisible by p and lying in $(0, 2p)$, so will must be equal to p, showing that p can be written as the sum of two integer squares.

We can rewrite the inequalities as searching for $m, k \in \mathbb{Z}$ such that $0 < m < \sqrt{p}$ and $0 < |\frac{n}{p} + \frac{k}{m}| < \frac{1}{m\sqrt{p}}$. By the above Proposition, setting $a := \frac{n}{p}$ and $d := \lfloor \sqrt{p} \rfloor$, we can find $k, m \in \mathbb{Z}$ with $0 < m \leq \lfloor \sqrt{p} \rfloor$ such that

$$\left| \frac{n}{p} + \frac{k}{m} \right| \leq \frac{1}{m(\lfloor \sqrt{p} \rfloor + 1)}.$$

The first inequality implies $0 < m < \sqrt{p}$ and the second inequality implies

$$\left| \frac{n}{p} + \frac{k}{m} \right| < \frac{1}{m\sqrt{p}}$$

so we get what we wanted.

Chapter 10

Some amusements

10.1 Perfect nubmers and Mersenne primes

Definition 10.1.1. A number $n \in \mathbb{Z}_{\geq 1}$ is said to be *perfect* if it is equal to the sum of its positive divisors, except itself:

$$n = \sum_{\substack{1 \leq d < n \\ d \mid n}} d.$$

Example 10.1.2. *The number* 6 *is perfect:*

$$6 = 1 + 2 + 3.$$

Definition 10.1.3. A number $n \in \mathbb{Z}_{\geq 1}$ is said to be *triangular*, if it is of the form $1 + 2 + \ldots + k = \frac{k(k+1)}{2}$ for some $k \in \mathbb{Z}_{\geq 1}$.

Definition 10.1.4. A prime p is said to be a *Mersenne prime*, if it is equal to $2^n - 1$ for some $n \in \mathbb{Z}_{\geq 1}$.

Theorem 10.1.5 (Euclid-Euler)**.** *The even perfect number are exactly the triangular numbers $1 + 2 + \ldots + p$ where p is a Mersenne prime. Equivalently, but less juicy, of the form*

$$2^{n-1}(2^n - 1)$$

where $n > 1$ and $2^n - 1$ is prime.

Remark 10.1.6. It is not known whether there are infinitely many Mersenne primes or not (there are 51 known Mersenne primes, as of December 2018); Thus, it is not known whether there are infinitely many even perfect number or not. In addition, it is not known if there are any odd perfect numbers.

To prove the theorem, we would like to study some important multiplicative functions.

Definition 10.1.7. A function $f : \mathbb{Z}_{\geq 1} \to \mathbb{Z}_{\geq 1}$ is said to be *multiplicative* if

$$f(nm) = f(n)f(m)$$

whenever $m, n \in \mathbb{Z}_{\geq 1}$ are relatively prime.

Definition 10.1.8. Define

$$\sigma_k(n) = \sum_{\substack{d \in \mathbb{Z}_{\geq 1} \\ d|n}} d^k.$$

Remark 10.1.9. For example, $\sigma_0(n)$ is equal to the number of divisors of n, while $\sigma_1(n)$ is equal to the sum of divisors of n.

Claim 10.1.10. *The functions σ_k are multiplicative.*

Proof. For $n \in \mathbb{Z}_{\geq 1}$, denote by $D_n \subset \mathbb{Z}_{\geq 1}$ the set of divisors of n. Let $m, n \in \mathbb{Z}_{\geq 1}$ be relatively prime. It is easy to see that one has a bijection

$$D_m \times D_n \to D_{mn}$$

given by $(a, b) \mapsto ab$. Therefore:

$$\sigma_k(mn) = \sum_{d \in D_{mn}} d^k = \sum_{a \in D_m, b \in D_n} (ab)^k = \left(\sum_{a \in D_m} a^k \right) \cdot \left(\sum_{b \in D_m} b^k \right) = \sigma_k(m) \cdot \sigma_k(n).$$

□

Proof (of Theorem 10.1.5). Assume first that n is such that $2^n - 1$ is prime. We want to show that $m := 2^{n-1}(2^n - 1)$ is perfect. We need to show that $\sigma_1(m) = 2m$. Indeed:

$$\sigma_1(m) = \sigma_1(2^{n-1})\sigma_1(2^n - 1) = (1+2+\ldots+2^{n-1}) \cdot (1+(2^n-1)) = (2^n-1) \cdot 2^n = 2m.$$

Conversely, let m be an even perfect number. We can write $m = 2^k \ell$ with odd ℓ. We easily see that $\ell \neq 1$. We have

$$2^{k+1}\ell = 2m = \sigma_1(m) = (2^{k+1} - 1) \cdot \sigma_1(\ell).$$

Therefore $2^{k+1} - 1 | \ell$. If $2^{k+1} - 1 \neq \ell$ we have

$$\sigma_1(\ell) \geq \ell + 1 + \frac{\ell}{2^{k+1} - 1}$$

so

$$(2^{k+1} - 1)\sigma_1(\ell) \geq (2^{k+1} - 1)(\ell + 1 + \frac{\ell}{2^{k+1} - 1}) = 2^{k+1}\ell + 2^{k+1} - 1 > 2^{k+1}\ell.$$

This is a contradiction, therefore we must have $2^{k+1} - 1 = \ell$. Thus we obtain

$$(\ell + 1)\ell = \ell \cdot \sigma_1(\ell)$$

so $\sigma_1(\ell) = \ell + 1$. Therefore ℓ is prime. □

10.2 Uncategorized amusements

Proposition 10.2.1. *Let $n \in \mathbb{Z}_{\geq 1}$. Then n is a square if and only if $\sigma_0(n)$ is odd.*

Proof. Write $n = p_1^{e_1} \dots p_r^{e_r}$. Then

$$\sigma_0(n) = (e_1 + 1) \dots (e_r + 1).$$

Therefore, $\sigma_0(n)$ is odd if and only if all e_i's are even, which clearly happens if and only if n is a square. □