Contents

1 Introduction: What is Number Theory? 3
   1.1 Diophantine equations ........................................... 3
   1.2 Questions about prime numbers ............................... 4
   1.3 Topics covered in the course ................................ 5
   1.4 The integers and the well-ordering principle ............... 5

2 Divisibility theory 5
   2.1 Divisibility .................................................. 5
   2.2 Euclidean division .............................................. 6
   2.3 GCD and Euclid’s algorithm .................................. 7
   2.4 The least common multiple .................................. 9
   2.5 The Diophantine equation $ax + by = c$ ..................... 10

3 Prime numbers 11
   3.1 The fundamental theorem of Arithmetic .................... 11
   3.2 Irrationality of $\sqrt{2}$ ...................................... 12
   3.3 $p$-adic valuation .............................................. 13
   3.4 Infiniteness of primes ....................................... 13

4 Pythagorean triples 14
   4.1 Primitive triples .............................................. 14
   4.2 Complete characterization of Pythagorean triples .......... 15
   4.3 A geometric application ..................................... 15
   4.4 Pythagorean triples and the unit circle .................... 15

5 Congruences 15
   5.1 Definition and basic properties .............................. 15
   5.2 Complete systems of residues ................................ 16
   5.3 Invertible integers modulo $n$ ............................... 17
   5.4 Linear congruences .......................................... 18
   5.5 The Chinese remainder theorem ............................ 19
   5.6 Fermat’s little theorem ...................................... 20
   5.7 Wilson’s theorem ............................................. 20

6 Euler’s theorem 21
   6.1 Euler’s phi function ........................................... 21
   6.2 Euler’s theorem .............................................. 22
   6.3 RSA cryptosystem ............................................. 23
1 Introduction: What is Number Theory?

Number theory is the study of properties of the integers

\[ \ldots, -3, -2, -1, 0, 1, 2, \ldots \]

or, more particularly, of the positive integers (or natural numbers)

\[ 1, 2, 3, \ldots \]

It is a very old science, it has been studied since Antiquity, in particular in ancient Greece.

In what follows, we are going to give a few example of typical number-theoretic problems.

1.1 Diophantine equations

A Diophantine equation is a polynomial equation in several unknowns for which we want to find the integral solutions. For example, a typical Diophantine problem would be to find all integers satisfying the equation

\[ 2x + 5y = 7. \]

Such an equation is called a linear Diophantine equation (because we don’t have terms of degree two or higher). A well-known example of a Diophantine equation is

\[ x^2 + y^2 = z^2. \]

Triples of integers \((x, y, z)\) satisfying this are called Pythagorean triples. By the Pythagorean theorem, if the lengths of the sides of a right triangle are integers, then they form a
Pythagorean triple. For example, \((3, 4, 5)\) and \((5, 12, 13)\) are Pythagorean triples. In this course, we will show there is an infinite number of such triples, and we will completely characterize them.

On the other hand, there are no positive integral solutions to the equation

\[ x^3 + y^3 = z^3. \]

This is a special case of Fermat’s last theorem, which states that for any \(n \geq 3\), there is no triple \((x, y, z)\) of positive integers satisfying the equation

\[ x^n + y^n = z^n. \]

Another important type of Diophantine equations are Pell’s equations, which are of the form

\[ x^2 - ny^2 = 1 \]

for some integer \(n\).

### 1.2 Questions about prime numbers

A positive integer \(n\) is said to be prime if its only positive divisors are 1 and \(n\). The smallest prime numbers are

\[ 2, 3, 5, 7, 11, 13, 17 \ldots \]

We are going to show that there is an infinite number of prime numbers, and, moreover, that there is an infinite number of prime numbers of the form \(4k + 1\) where \(k\) is an integer. For example, 5 is such a prime number, but 7 is not.

Two primes are called twin primes if they differ by 2. For example 3 and 5, 5 and 7, 11 and 13 are twin primes. It is not known whether there are infinitely many pairs of twin primes. Two primes are called cousin primes if they differ by 4. For example, 3 and 7, 7 and 11, 13 and 17, are cousin primes. Two primes are called sexy primes if they differ by 6. For example, 5 and 11, 7 and 13, 11 and 17 are sexy primes. It is not known whether there is an infinite number of cousin primes or sexy primes.

Another important question about prime numbers is Goldbach’s conjecture, formulated by the German mathematician Goldbach in 1742, and which states that every even integer greater than 2 is the sum of two prime numbers. For example, we have

\[ 4 = 2 + 2, \ 6 = 3 + 3, \ 8 = 3 + 5, \ 10 = 5 + 5 = 3 + 7, \ 12 = 5 + 7, \ldots \]

This has been checked using computers for all even numbers up to a very high bound. However, a proof for all even numbers has not been found yet. There is a variant of this conjecture, called the weak (or ternary) Goldbach’s conjecture, which states that every odd number greater than 5 is a sum of three primes, for example:

\[ 7 = 2 + 2 + 3, \ 9 = 3 + 3 + 3, \ 11 = 3 + 3 + 5, \ 13 = 3 + 5 + 5, \ 15 = 5 + 5 + 5 = 3 + 5 + 7, \ldots \]

This conjecture has been proved in 2013. It is called the weak Goldbach conjecture, because it is implied by Goldbach’s conjecture.

**Exercise 1.2.1.** Check this by deducing it from Goldbach’s conjecture.
1.3 Topics covered in the course

One of the main number-theoretic notions is divisibility, which we will talk about in chapter 2. We will go on to introduce prime numbers in chapter 3 and prove some of their properties. Then we will spend time on congruences, which are a convenient mathematical way to talk about divisibility.

1.4 The integers and the well-ordering principle

We assume given the set of integers with some of their basic properties, among which we include the Well-Ordering principle, which will be used several times in this course:

**The Well-Ordering Principle** Every non-empty set $S$ of nonnegative integers contains a smallest element. In other words, there exists $a \in S$ such that for every $b \in S$, $a \leq b$.

2 Divisibility theory

2.1 Divisibility

**Definition 2.1.1.** If $a$ and $b$ are integers, we say that $a$ is divisible by $b$, or that $b$ divides $a$, if there exists an integer $k \in \mathbb{Z}$ such that $a = kb$.

We also say that $a$ is a multiple of $b$, or that $b$ is a factor, or a divisor, of $a$.

**Notation 2.1.2.** We denote this by $b | a$.

**Example 2.1.3.** The divisors of 6 are $-6, -3, -2, -1, 1, 2, 3, 6$.

**Remark 2.1.4.** For every positive divisor $b$ of $a$, we have the corresponding negative divisor $-a$. Therefore, in what follows, by divisor we mostly will mean positive divisor.

**Exercise 2.1.5.** Divisibility satisfies the following properties:

(a) For every integer $a$, the integers $1, -1, a$ and $-a$ divide $a$.

(b) Transitivity: If $a | b$ and $b | c$ then $a | c$.

(c) $0$ does not divide any non-zero integer.

(d) All integers divide $0$.

(e) If $a, b$ are non-zero then $a | b$ and $b | a$ implies $a = b$ or $a = -b$.

(f) If $a | b$ and $a | c$ then $a | (kb + lc)$ for all integers $k$ and $l$. 

5
2.2 Euclidean division

**Proposition 2.2.1.** Let \( a, b \) be integers, with \( b \neq 0 \). There is a unique way of writing \( a \) in the form

\[
a = bq + r
\]

where \( q, r \) are integers, with \( r \) satisfying \( 0 \leq r < |b| \). The integer \( q \) is called the quotient in the Euclidean division of \( a \) by \( b \), and \( r \) is called the remainder.

**Proof.** We start by proving existence. Assume first that \( b > 0 \). Consider the set \( S \) of all integers which are nonnegative and which are of the form \( a - bk \) for some \( k \in \mathbb{Z} \). It is clearly non-empty (it contains \( a \) if \( a \) is nonnegative, and \( a - ba = -a(b-1) \) if \( a \) is negative). Therefore it contains a least element \( r \). Let \( q \) be an integer such that \( r = a - bq \). We claim that \( r < b \). Indeed, if we had \( r \geq b \), then we would have

\[
a - b(q + 1) = r - b \geq 0
\]

and so \( r - b \) would be an element of \( S \) which is smaller than \( r \), and this contradicts the definition of \( r \). Therefore, we indeed have \( r < b \).

Assume now \( b < 0 \). Then we may apply the statement for positive \( b \), which we just proved, to \( a \) and \( -b \), finding \( q' \) and \( r \) such that \( 0 \leq r < -b = |b| \) and \( a = (-b)q' + r \). We now put \( q = -q' \), which yields \( a = bq + r \).

Now we prove that \( q \) and \( r \) satisfying such conditions are unique. For this, assume we have two pairs \((q, r)\) and \((q', r')\) such that

\[
a = bq + r = bq' + r'.
\]

Then we have \( b(q - q') = r - r' \). Since we have \( 0 \leq r, r' < |b| \), we have

\[
-|b| < r - r' < |b|
\]

so that \( -|b| < |b|(q - q') < |b| \). Dividing everything by \( b \), we see that the integer \( q - q' \) satisfies \(-1 < q - q' < 1\), so that we necessarily have \( q - q' = 0 \), which implies \( r - r' = 0 \), so \( q = q' \) and \( r = r' \).

**Example 2.2.2.** The Euclidean division of 37 by 4 is written

\[
37 = 4 \times 9 + 1
\]

The Euclidean division of 37 by \(-4\) is written

\[
37 = (-4) \times (-9) + 1.
\]
2.3 GCD and Euclid’s algorithm

**Definition 2.3.1.** Let \(a, b\) be two integers, not both zero. The *greatest common divisor* of \(a, b\), denoted \(\gcd(a, b)\) is the largest positive integer that divides both \(a\) and \(b\). We say that \(a\) and \(b\) are *relatively prime*, or *coprime*, if \(\gcd(a, b) = 1\).

**Example 2.3.2.**
1. \(\gcd(6, 15) = 3\).
2. If \(b > 0\) and \(b | a\), then \(\gcd(a, b) = b\).
3. \(\gcd(-6, -4) = 2\).
4. For any non-zero integer \(a\), \(\gcd(a, 0) = |a|\).

**Lemma 2.3.3.** Let \(a\) and \(b\) be two integers, with \(b \neq 0\), and write
\[
a = bq + r
\]
the Euclidean division of \(a\) by \(b\). Then \(\gcd(a, b) = \gcd(b, r)\).

**Proof.** Let \(d\) be a common divisor of \(a\) and \(b\). Then \(d\) divides \(a - bq = r\). Conversely, let \(e\) be a common divisor of \(b\) and \(r\). Then \(e\) divides \(bq + r = a\). Thus, the two sets
\[
\{ \text{positive common divisors of } a \text{ and } b \}\]
and
\[
\{ \text{positive common divisors of } b \text{ and } r \}\]
are the same. In particular, their largest elements are the same, so \(\gcd(a, b) = \gcd(b, r)\). \(\square\)

The greatest common divisor may be computed using *Euclid’s algorithm*, which works as follows:

Let \(a\) and \(b\) be positive integers, with \(a > b\). Then we may write a sequence of Euclidean divisions in the following manner:
\[
\begin{align*}
a &= bq_0 + r_1, & 0 &\leq r_1 < b \\
b &= r_1q_1 + r_2, & 0 &\leq r_2 < r_1 \\
r_1 &= r_2q_2 + r_3, & 0 &\leq r_3 < r_2 \\
\vdots \\
r_{n-2} &= r_{n-1}q_{n-1} + r_n, & 0 &\leq r_n < r_{n-1} \\
r_{n-1} &= r_nq_n.
\end{align*}
\]

The sequence \(r_1, r_2, \ldots\) of successive remainders is a strictly decreasing sequence of non-negative integers, therefore it must hit zero at some point. The last non-zero remainder \(r_n\) will be the greatest common divisor of \(a\) and \(b\).

Indeed, by the result of exercise 2.3.3 we have
\[
\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n.
\]
Example 2.3.4. Let us compute the greatest common divisor of 234 and 51.

\[ 234 = 51 \times 4 + 30 \]
\[ 51 = 30 \times 1 + 21 \]
\[ 30 = 21 \times 1 + 9 \]
\[ 21 = 9 \times 2 + 3 \]
\[ 9 = 3 \times 3. \]

The last non-zero remainder is 3, therefore \( \gcd(234, 51) = 3 \).

Proposition 2.3.5. Let \( a \) and \( b \) be two integers, not both zero. Then there exist integers \( u \) and \( v \) such that

\[ au + bv = \gcd(a, b). \]

Remark 2.3.6. In particular, any integer \( d \) which divides both \( a \) and \( b \) will divide \( \gcd(a, b) \). In other words, \( \gcd(a, b) \) is divisible by all the common divisors of \( a \) and \( b \).

Corollary 2.3.7. Let \( a, b \) be two integers, not both zero. The set

\[ \mathbb{Z}a + \mathbb{Z}b = \{ua + vb, \ u, b \in \mathbb{Z}\} \]

is equal to the set \( \mathbb{Z}\gcd(a, b) = \{w \gcd(a, b), \ w \in \mathbb{Z}\} \). In other words, the integers that can be written in the form \( ua + vb \) for some \( u, v \in \mathbb{Z} \) are exactly the multiples of \( \gcd(a, b) \).

Proof. Since \( \gcd(a, b) \) divides \( a \) and \( b \), it also divides any integer of the form \( ua + vb \), so all the elements of the set \( \mathbb{Z}a + \mathbb{Z}b \) are multiples of \( \gcd(a, b) \). Conversely, let \( c \in \mathbb{Z}\gcd(a, b) \). Then there exists \( w \in \mathbb{Z} \) such that \( c = w \gcd(a, b) \). Using proposition 2.3.5 we may find integers \( u \) and \( v \) such that \( ua + vb = \gcd(a, b) \). Multiplying everything by \( w \), we see that \( c = (wu)a + (wv)b \in \mathbb{Z}a + \mathbb{Z}b \). \( \square \)

Exercise 2.3.8. Find \( u, v \) such that

\[ 234u + 51v = \gcd(234, 51). \]

Proposition 2.3.9 (Bézout's theorem). Let \( a \) and \( b \) be two integers, not both zero. Then \( a \) and \( b \) are coprime if and only if there exist integers \( u \) and \( v \) such that

\[ au + bv = 1. \]

Proof. If \( a \) and \( b \) are coprime, then the existence of \( u \) and \( v \) follows from proposition 2.3.5 Conversely, assume that there exist integers \( u \) and \( v \) such that \( au + bv = 1 \). Let \( d = \gcd(a, b) \). Since \( d \) divides \( a \) and \( d \) divides \( b \), \( d \) divides \( au + bv = 1 \). Since \( d \) is a positive integer, this implies that \( d = 1 \), whence the result. \( \square \)

Let us give some additional properties of the gcd.
Proposition 2.3.10. 1. Let $a$ and $b$ be two integers, not both zero, and let $d = \gcd(a, b)$. Then \( \frac{a}{d} \) and \( \frac{b}{d} \) are integers, and \( \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \).

2. Let $a, b$ be two integers, not both zero, and let $k$ be a non-zero integer. Then \( \gcd(ka, kb) = |k| \gcd(a, b) \).

We now prove two lemmas about divisibility which will be very useful to us in the future.

Proposition 2.3.11 (Gauss’s lemma). Let $a, b, c$ be integers. If $a$ divides $bc$ and $a$ is relatively prime to $b$ then $a$ divides $c$.

Proof. Since $a$ is relatively prime to $b$, there exist integers $u$ and $v$ such that $au + bv = 1$. Multiplying everything by $c$, we get

\[ uac + vbc = c. \]

Since $a$ divides $bc$, there exists an integer $k$ such that $bc = ka$. Therefore, we have

\[ a(uc + vk) = c, \]

which means that $a$ divides $c$.

Lemma 2.3.12. Let $a, b, c$ be integers. If $a$ divides $c$, $b$ divides $c$ and $\gcd(a, b) = 1$ then $ab$ divides $c$.

Proof. Since $a | c$ and $b | c$, there exist integers $k$ and $l$ such that $c = ka$ and $c = lb$. Since $\gcd(a, b) = 1$, there exist integers $u, v$ such that $ua + vb = 1$. Multiplying both sides by $c$, we get

\[ uac + vbc = c. \]

Substituting $c = lb$ and $c = ka$, respectively, on the left-hand side, we get

\[ ab(ul + vk) = c, \]

so $ab$ divides $c$.

2.4 The least common multiple

Let $a$ and $b$ be two non-zero integers. By the Well-ordering principle, the set of positive multiples of both $a$ and $b$ (which is non-empty, since it contains either $ab$ or $-ab$) contains a smallest element, called the least common multiple of $a$ and $b$, and denoted by $\lcm(a, b)$.

Example 2.4.1. The positive multiples of 12 are 12, 24, 36, 48, 60, ... and the positive multiples of 15 are 15, 30, 45, 50, ..., so $\lcm(12, 15) = 60$. 
Proposition 2.4.2. For positive integers $a$ and $b$,

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab.$$ 

In particular, if $a$ and $b$ are relatively prime, then their least common multiple is $ab$.

Example 2.4.3. The integers 10 and 17 are relatively prime, so their least common multiple is $10 \times 17 = 170$.

2.5 The Diophantine equation $ax + by = c$

In this section, we are going to study linear Diophantine equations, that is, equations of the type

$$ax + by = c$$

where $a, b, c \in \mathbb{Z}$ and $a, b$ not both zero. We are going to describe all integral values of $x$ and $y$ satisfying such an equation. Let us start with a few examples.

Example 2.5.1. The equation $x + y = 5$ has many solutions: $(2, 3), (1, 4), (0, 5), \ldots$ In fact, it has an infinite number of solutions, because whenever $n$ is an integer, $(n, 5 - n)$ is a solution of this equation.

Example 2.5.2. The equation $2x + 4y = 3$, on the other hand, does not have any integral solutions. Indeed, if we had an integral solution $(x, y)$, the left-hand side would be divisible by two, but not the right-hand side.

To explain these examples, let us first of all state a necessary and sufficient condition for the equation $ax + by = c$ to have a solution.

Proposition 2.5.3. The Diophantine equation $ax + by = c$ has a solution if and only if $\gcd(a, b)$ divides $c$.

Proof. We denote $\gcd(a, b)$ by $d$ in this proof.

Assume first that the equation has a solution $(x_0, y_0)$. Since $d$ divides both $a$ and $b$, $d$ divides $ax_0 + by_0$, that is, $d$ divides $c$.

Conversely, assume $d$ divides $c$. Then $c$ is an element of $\mathbb{Z} \cdot \gcd(a, b)$, and, therefore, by corollary 2.3.7, $c$ is an element of $\mathbb{Z}a + \mathbb{Z}b$. This means that there exist $x_0, y_0 \in \mathbb{Z}$ such that $c = x_0a + y_0b$, so $(x_0, y_0)$ gives us a solution of the equation.

Thus, in example 2.5.2, we had $\gcd(2, 4) = 2$, which does not divide 3.

The following theorem shows how to deduce all the solutions of the equation from one particular solution.

Theorem 2.5.4. If $(x_0, y_0)$ is any particular solution of the Diophantine equation $ax + by = c$, then all the solutions of this equation are exactly the integers of the form

$$x = x_0 - \frac{b}{d} t, \quad y = y_0 + \frac{a}{d} t,$$

where $d = \gcd(a, b)$ and $t$ is an integer.
Proof. Let \((x, y)\) be a solution of the equation. Then we have
\[ax_0 + by_0 = c = ax + by,\]
and therefore
\[a(x_0 - x) = b(y - y_0).\]
Since \(d\) is the greatest common divisor of \(a\) and \(b\), there exist relatively prime integers \(a'\) and \(b'\) such that \(a = da'\) and \(b = db'\). Dividing both sides of the above equality by \(d\) yields
\[a'(x_0 - x) = b'(y - y_0).\]
Since \(a\) and \(b\) are not both zero, \(a'\) and \(b'\) are not both zero as well, so we may assume, for example, that \(a' \neq 0\). By Gauss’s lemma, since \(a'\) divides \(b'(y - y_0)\) and is relatively prime to \(b'\), we have that \(a'\) divides \(y - y_0\), so there exists an integer \(t\) such that \(y - y_0 = a't\). Substituting this, and dividing by \(a'\) (which is allowed since \(a' \neq 0\)), we get \(x_0 - x = b't\). Thus, our solution \((x, y)\) is indeed of the form \((x_0 - b't, y_0 + a't)\) for some integer \(t\). Conversely, we can easily check that any pair of the form \((x_0 - b't, y_0 + a't)\) gives a solution to the equation.

Remark 2.5.5. In particular, if \(\gcd(a, b) = 1\), the solutions of the equation are given by \(x = x_0 - bt\) and \(y = y_0 + at\), where \((x_0, y_0)\) is a particular solution.

3 Prime numbers

3.1 The fundamental theorem of Arithmetic

Definition 3.1.1. A positive integer \(p\) is a prime number (or simply a prime) if its only positive divisors are 1 and \(p\). A positive integer which is not prime is called composite.

Proposition 3.1.2 (Fundamental theorem of arithmetic). Let \(n \geq 2\) be an integer. Then the integer \(n\) may be written as a product
\[n = p_1 p_2 \ldots p_k,\]
where \(p_1, \ldots, p_k\) are primes (not necessarily distinct). Furthermore, this factorization is unique, that is, if \(n = q_1 q_2 \ldots q_l\) where \(q_1, \ldots, q_l\) are primes, then \(k = l\) and the \(q_i\)‘s are just the \(p_i\)’s rearranged.

Remark 3.1.3. One may use exponents if one wants the primes in the decomposition to be distinct. More precisely, \(n\) may be written in the form
\[n = p_1^{a_1} \ldots p_r^{a_r}\]
where \(p_1, \ldots, p_r\) are distinct primes, and \(a_1, \ldots, a_r\) are positive integers. This decomposition is unique up to rearranging the \(p_i\)’s.
Proof. We need to prove existence and uniqueness. For existence, assume there exists an integer \( n \geq 2 \) which has no such decomposition. Then the set \( S \) of nonnegative integers not having such a decomposition is nonempty, and by the Well-ordering principle, we may consider its smallest element \( m \). This integer \( m \) cannot be a prime, because a prime obviously has a decomposition into prime factors. Therefore, \( m \) is composite, that is, there exist integers \( k, l \) such that \( m = kl \) and such that \( 1 < k, l < m \). Since \( m \) is the smallest element in \( S \), \( k \) and \( l \) do not lie in \( S \), so they do have prime factorizations

\[
k = p_1 \ldots p_r, \quad l = p'_1 \ldots p'_s.
\]

This leads to a contradiction, as \( m = p_1 \ldots p_r p'_1 \ldots p'_s \) is a prime factorization of \( m \).

It remains to prove uniqueness. \qed

Remark 3.1.4. We have that a prime \( p \) divides \( n \) if and only if \( p \) appears in the factorization of \( n \) into prime factors.

Example 3.1.5. We have

\[
24 = 2^3 \times 3, \\
30 = 2 \times 3 \times 5.
\]

Remark 3.1.6. How do we check if a number is prime or not? One important remark is that if \( n \) is composite, then there exist integers \( 1 < a \leq b < n \) such that \( n = ab \). Therefore, \( n \geq a^2 \), and so \( a \leq \sqrt{n} \). This means that to check if a number is composite, it suffices to check if it is divisible by some prime number smaller than \( \sqrt{n} \).

### 3.2 Irrationality of \( \sqrt{2} \)

Recall that in the proof of uniqueness of prime factorization, we used the following lemma:

**Lemma 3.2.1.** Let \( a, b \in \mathbb{Z} \) and let \( p \) be a prime number. If \( p|ab \) then \( p|a \) or \( p|b \).

In particular, if \( p|a^2 \) for some integer \( a \), then \( p|a \).

A number \( r \) is rational if it can be written in the form \( r = \frac{a}{b} \) for some integers \( a, b \) with \( b \neq 0 \), and irrational otherwise.

**Proposition 3.2.2.** The number \( \sqrt{2} \) is irrational.

**Proof.** Assume that \( \sqrt{2} \) is rational. Then there exist \( a, b \in \mathbb{Z} \), with \( b \neq 0 \), such that \( \sqrt{2} = \frac{a}{b} \). We may moreover assume gcd\((a, b)\) = 1. Then \( 2b^2 = a^2 \). We therefore have that \( 2|a^2 \), so \( 2|a \). Then there exists \( a' \in \mathbb{Z} \) such that \( a = 2a' \). Substituting this into the equation, we have \( 2b^2 = 4a'^2 \), that is, \( b^2 = 2a'^2 \). In the same way as above, we may conclude that \( 2|b \). Thus, 2 is a common divisor of \( a \) and \( b \), which contradicts the fact that gcd\((a, b)\) = 1. \qed
3.3 $p$-adic valuation

The proof of the previous proposition can be formulated more elegantly by using the notion of $p$-adic valuation.

Definition 3.3.1. Let $n$ be a non-zero integer, and let $p$ be a prime number. The $p$-adic valuation of $n$, denoted by $v_p(n)$, is the exponent of $p$ in the unique factorization of $n$ into prime factors.

Remark 3.3.2. If $n = p_1^{a_1} \cdots p_r^{a_r}$ where $p_1, \ldots, p_r$ are distinct primes and $a_1, \ldots, a_r$ are non-negative integers, then for every $i \in \{1, \ldots, r\}$, $v_{p_i}(n) = a_i$, and for all $p \not\in \{p_1, \ldots, p_r\}$, $v_p(n) = 0$.

Remark 3.3.3. There exists an integer $m$, relatively prime to $p$, such that $n = p^{v_p(n)}m$. Indeed, by the fundamental theorem of arithmetic, there exist $p = p_1, p_2, \ldots, p_r$ distinct primes such that $n = p_1^{a_1} \cdots p_r^{a_r}$. Then $a_1 = v_p(n)$ and $m = p_2^{a_2} \cdots p_r^{a_r}$.

Remark 3.3.4. Conversely, if $n$ can be written in the form $n = p^a m$ where $m$ is not divisible by $p$, then $v_p(n) = a$.

Example 3.3.5. We have $v_2(6) = 1$, and $v_5(12) = 0$.

Proposition 3.3.6. The $p$-adic valuation satisfies the following properties: for all integers $m, n \not= 0$,

1. $v_p(mn) = v_p(m) + v_p(n)$.
2. $v_p(m + n) \geq \min\{v_p(m), v_p(n)\}$, with equality if $v_p(m) \not= v_p(n)$.

If $\sqrt{2} = \frac{a}{b}$, then we get $2a^2 = b^2$. In terms of $2$-adic valuations, we get $2v_2(a) + 1 = 2v_2(b)$. The left-hand side is odd, but the right-hand side is even, whence a contradiction.

Proposition 3.3.7. Let $a, b$ be positive integers. Then $a | b$ if and only if $v_p(a) \leq v_p(b)$ for all prime numbers $p$.

Remark 3.3.8. If $a$ is a positive integer, then $a = \prod_{p \in \mathbb{P}} p^{v_p(a)}$. If $a$ is negative, then $a = -\prod_{p \in \mathbb{P}} p^{v_p(a)}$. In particular, if two integers $a, b$ are such that $v_p(a) = v_p(b)$ for all prime numbers $p$, then $a = b$ or $a = -b$.

Proposition 3.3.9. Let $a$ and $b$ be integers. For all primes $p$, we have

$$v_p(\gcd(a, b)) = \min\{v_p(a), v_p(b)\} \quad \text{and} \quad v_p(\text{lcm}(a, b)) = \max\{v_p(a), v_p(b)\}.$$ 

3.4 Infiniteness of primes

Proposition 3.4.1. The set of prime numbers is infinite.

Proposition 3.4.2. The set of prime numbers of the form $4k + 3$ is infinite.
This result is a special case of the following general theorem, the proof of which is beyond the scope of this course.

**Theorem 3.4.3. (Dirichlet)** Let $a$ and $b$ be relatively prime integers. The arithmetic progression

$$a, \ a+b, \ a+2b, \ a+3b, \ldots$$

contains infinitely many prime numbers.

### 4 Pythagorean triples

#### 4.1 Primitive triples

**Remark 4.1.1.** We defined the gcd only for pairs of integers above. In fact, it makes sense to consider the gcd of any finite number of integers: $\gcd(a_1, \ldots, a_n)$ is the greatest integer dividing all of the integers $a_1, \ldots, a_n$ simultaneously. If $\gcd(a_1, \ldots, a_n) = 1$, we say that $a_1, \ldots, a_n$ are relatively prime. Pay attention to the fact that if $a_1, \ldots, a_n$ are relatively prime, this does not necessarily mean that the $a_i$ are pairwise relatively prime (that is, for all $i, j$, $a_i$ and $a_j$ are relatively prime). Indeed, for example $\gcd(2, 3, 4) = 1$, but $\gcd(2, 4) = 2$.

**Definition 4.1.2.** A Pythagorean triple is a triple $(x, y, z)$ of non-zero integers such that

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

If $\gcd(x, y, z) = 1$, it’s called a primitive Pythagorean triple.

**Example 4.1.3.** The triples $(3, 4, 5)$, $(5, 12, 13)$, $(12, 35, 37)$ are primitive Pythagorean triples. The Pythagorean triple $(6, 8, 10)$ is not primitive.

**Remark 4.1.4 (Getting primitive triples from non-primitive ones).** Let $(x, y, z)$ be a Pythagorean triple, and $d = \gcd(x, y, z)$. Then we may write $x = dx_1$, $y = dx_2$, $z = dx_3$ where $x_1, x_2, x_3$ are relatively prime, and $(x_1, y_1, z_1)$ is a primitive Pythagorean triple. Thus, it suffices to find all primitive Pythagorean triples, and all of the other ones will be obtained from those upon multiplication by a non-zero integer.

**Remark 4.1.5 (Reducing to positive triples).** We may also reduce to looking for triples $(x, y, z)$ such that $x, y, z > 0$, because all the other ones are obtained from those by changing the sign.

**Remark 4.1.6.** If $(x, y, z)$ is a primitive Pythagorean triple, then $\gcd(x, y) = \gcd(y, z) = \gcd(x, z) = 1$. Indeed, if some prime number $p$ divides $x$ and $y$, then $p$ divides $x^2 + y^2$, and therefore $p|z^2$, so $p|z$. This contradicts $\gcd(x, y, z) = 1$. Therefore $\gcd(x, y) = 1$. A similar argument works for $\gcd(y, z)$ and $\gcd(x, z)$.

**Proposition 4.1.7.** Let $(x, y, z)$ be a primitive Pythagorean triple. Then one of the integers $x, y$ is even, and the other one is odd. In particular, $z$ is odd.

**Remark 4.1.8.** Up to exchanging $x$ and $y$, we may therefore look only for the solutions with $x$ odd and $y$ even.
4.2 Complete characterization of Pythagorean triples

We are going to need the following lemma:

**Lemma 4.2.1.** Let \(a, b, c\) be integers and let \(n\) be a positive integer. If \(\gcd(a, b) = 1\) and \(ab = c^n\), then \(a\) and \(b\) are both \(n\)-th powers.

**Theorem 4.2.2.** All the primitive Pythagorean triples \((x, y, z)\) satisfying the conditions

\[
x, y, z > 0, \quad x \text{ odd}
\]

are given by the formulas

\[
x = st, \quad y = \frac{s^2 - t^2}{2}, \quad z = \frac{s^2 + t^2}{2}
\]

for integers \(s > t > 0\) such that \(\gcd(s, t) = 1\) and such \(s\) and \(t\) are both odd.

**Proof.** See theorem 2.1 here: [https://www.math.brown.edu/~jhs/frintch1ch6.pdf](https://www.math.brown.edu/~jhs/frintch1ch6.pdf)

4.3 A geometric application

**Proposition 4.3.1.** The radius of the inscribed circle of a right triangle with integral side lengths is an integer.

4.4 Pythagorean triples and the unit circle

(See chapter 3 here: [https://www.math.brown.edu/~jhs/frintch1ch6.pdf](https://www.math.brown.edu/~jhs/frintch1ch6.pdf))

5 Congruences

5.1 Definition and basic properties

Let \(n > 1\) be an integer. If \(a, b \in \mathbb{Z}\), we say \(a\) is congruent to \(b\) modulo \(n\), and write \(a \equiv b \pmod{n}\), if \(n\) divides \(a - b\). We have the following equivalent characterizations:

\[
a \equiv b \pmod{n} \iff a = b + nk \text{ for some } k \in \mathbb{Z}
\]

\[
\iff a \in b + n\mathbb{Z} = \{b + nk, \ k \in \mathbb{Z}\}.
\]

**Proposition 5.1.1.** Let \(n > 1\) be an integer, and let \(a, b, c, d \in \mathbb{Z}\). The following properties hold:

1. \(a \equiv a \pmod{n}\).
2. If \(a \equiv b \pmod{n}\), then \(b \equiv a \pmod{n}\).
3. If \(a \equiv b \pmod{n}\) and \(b \equiv c \pmod{n}\) then \(a \equiv c \pmod{n}\).
4. If \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \) then \( a + c \equiv b + d \pmod{n} \).

5. If \( a \equiv b \pmod{n} \) then \( a + c \equiv b + c \pmod{n} \) and \( ac \equiv bc \pmod{n} \).

6. If \( a \equiv b \pmod{n} \) then for every positive integer \( k \), we have \( a^k \equiv b^k \pmod{n} \).

**Proposition 5.1.2.** An integer \( a \) is congruent modulo \( n \) to exactly one integer in the set \( \{0, \ldots, n - 1\} \), namely the remainder in the Euclidean division of \( a \) by \( n \).

**Proof.** Write \( a = qn + r \), where \( 0 \leq r < n \) (that is, \( r \in \{0, \ldots, n - 1\} \) ), the Euclidean division of \( a \) by \( n \). Then \( n \) divides \( a - r \), so \( a \equiv r \pmod{n} \).

Conversely, assume \( a \) is congruent modulo \( n \) to some integer \( r \in \{0, \ldots, n - 1\} \). Then there exists \( q \in \mathbb{Z} \) such that \( a - r = nq \), that is, \( a = nq + r \) with \( 0 \leq r < n \). By uniqueness of Euclidean division, \( r \) is the remainder in the Euclidean division of \( a \) by \( n \). \( \square \)

**Proposition 5.1.3.** We have \( a \equiv b \pmod{n} \), if and only if \( a \) and \( b \) have the same remainder in the Euclidean division by \( n \).

**Proof.** Let \( r \in \{0, \ldots, n - 1\} \) be the remainder in the Euclidean division of \( b \) by \( n \). Then \( b \equiv r \pmod{n} \), so \( a \equiv r \pmod{n} \). By proposition 5.1.2, \( r \) must be the remainder in the Euclidean division of \( a \) by \( n \). Conversely, if \( a \) and \( b \) have the same remainder \( r \) in the Euclidean division by \( n \), then they are both congruent to \( r \) modulo \( n \), so we have \( a \equiv b \pmod{n} \). \( \square \)

**Example 5.1.4.** Let us find the remainder in the Euclidean division of \( 2^{50} \) by 7. Note that \( 2^3 \equiv 1 \pmod{7} \). Writing the Euclidean division of 50 by 3, we get 50 = 3 \times 16 + 2, so that

\[
2^{50} = 2^{3 \times 16 + 2} = (2^3)^{16} \times 2^2 \equiv 4 \pmod{7}.
\]

Thus, the remainder is 4.

**Example 5.1.5.** A perfect square is congruent to 0,1 or 4 modulo 8. Indeed, it suffices to determine the squares modulo 8 of the integers 0,1,...,7:

\[
\begin{array}{cccccccc}
  a & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
  a^2 & 0 & 1 & 4 & 1 & 0 & 1 & 4 & 1 \\
\end{array}
\]

Note that it suffices to compute the squares of 0,1,2,3,4, and then the others are completed by symmetry, because \( 7^2 \equiv (-1)^2 \equiv 1^2 \pmod{8} \), \( 6^2 \equiv (-2)^2 \equiv 2^2 \pmod{8} \), etc. We see in particular that an odd square is congruent to 1 modulo 8.

### 5.2 Complete systems of residues

**Definition 5.2.1.** A collection of \( n \) integers \( a_1, \ldots, a_n \) is said to form a complete system of residues modulo \( n \) if every integer is congruent modulo \( n \) to exactly one of the \( a_i \).

**Proposition 5.2.2.** Let \( a_1, \ldots, a_n \) be \( n \) integers. The following are equivalent:
(i) The integers \( a_1, \ldots, a_n \) form a complete system of residues modulo \( n \).

(ii) The integers \( a_1, \ldots, a_n \) are pairwise incongruent modulo \( n \) (that is, we have \( a_i \not\equiv a_j \pmod{n} \) for all integers \( i, j \in \{1, \ldots, n\} \)).

(iii) The integers \( a_1, \ldots, a_n \) are congruent modulo \( n \) to \( 0, 1, \ldots, n-1 \) taken in some order.

Proof. We are going to prove \((i) \Rightarrow (ii)\), \((ii) \Rightarrow (iii)\), and \((iii) \Rightarrow (i)\).

\((i) \Rightarrow (ii)\): Assume \( a_1, \ldots, a_n \) form a complete system of residues. For every \( i \), by definition \( a_i \) is congruent to exactly one of the integers \( a_1, \ldots, a_n \), and incongruent to the others. Since it is congruent to itself, we have \( a_i \not\equiv a_j \pmod{n} \) for all integers \( j \neq i \).

\((ii) \Rightarrow (iii)\): Assume \( a_1, \ldots, a_n \) to be pairwise incongruent modulo \( n \), and let \( r_1, \ldots, r_n \) be their respective remainders in the Euclidean division by \( n \). By proposition 5.1.3 we have that \( r_1, \ldots, r_n \) are \( n \) distinct integers in the set \( \{0, 1, \ldots, n-1\} \). Since this set contains exactly \( n \) integers, we see that \( r_1, \ldots, r_n \) must be equal to the integers \( 0, 1, \ldots, n-1 \) (in some order).

\((iii) \Rightarrow (i)\): Assume that \( a_1, \ldots, a_n \) are congruent to \( 0, 1, \ldots, n-1 \) taken in some order. Let \( x \) be an integer and let \( r \) be its remainder in the Euclidean division by \( n \). By assumption, there exists \( i \) such that \( a_i \equiv r \pmod{n} \). Then \( x \equiv a_i \pmod{n} \). This shows that \( a_1, \ldots, a_n \) is a complete system of residues modulo \( n \).

Example 5.2.3. 1. For every \( n \), the collection \( 0, 1, \ldots, n-1 \) is a complete system of residues. So are \( 1, 2, \ldots, n \), as well as \( n, n+1, \ldots, 2n-1 \).

2. The collection \(-9, -1, 13, 2, 20\) is a complete system of residues modulo \( 5 \). Indeed, we have

\[-9 \equiv 1 \pmod{5}, \quad -1 \equiv 4 \pmod{5}, \quad 13 \equiv 3 \pmod{5}, \quad 2 \equiv 2 \pmod{5}, \quad 20 \equiv 0 \pmod{5}.

5.3 Invertible integers modulo \( n \)

We know that if \( a \equiv b \pmod{n} \), then for all integers \( c \), \( ca \equiv cb \pmod{n} \). However, the converse is in general not true, that is, in general one cannot divide both sides of a congruence by some integer.

Example 5.3.1. We have \( 2 \times 3 \equiv 4 \times 3 \pmod{6} \), but \( 2 \not\equiv 4 \pmod{6} \).

We do however have the following:

Proposition 5.3.2. If \( ca \equiv cb \pmod{n} \), then \( a \equiv b \pmod{\frac{n}{d}} \), where \( d = \gcd(c, n) \).

In particular, we can cancel out by \( c \) in a congruence modulo \( n \) if \( \gcd(c, n) = 1 \):

Corollary 5.3.3. If \( ca \equiv cb \pmod{n} \) and \( \gcd(c, n) = 1 \), then \( a \equiv b \pmod{n} \).
Another way to understand this is through the notion of invertible element:

**Definition 5.3.4.** We say that an integer \( c \) is invertible modulo \( n \) if there exists an integer \( d \) such that \( cd \equiv 1 \pmod{n} \). We say that \( d \) is an inverse of \( c \) modulo \( n \).

**Example 5.3.5.** 3 is an inverse of 4 modulo 11.

**Proposition 5.3.6.** If \( ca \equiv cb \pmod{n} \) and \( c \) is invertible modulo \( n \), then \( a \equiv b \pmod{n} \).

*Proof.* Let \( d \) be an inverse of \( c \) modulo \( n \). Multiply both sides of the congruence \( ca \equiv cb \pmod{n} \) by \( d \) to get the result. \( \square \)

We have seen that for an integer \( c \), both the condition of being relatively prime with \( n \) and the condition of being invertible modulo \( n \) allow to divide by \( c \). In fact these two conditions are equivalent:

**Proposition 5.3.7.** An integer \( c \) is invertible modulo \( n \) if and only if \( \gcd(c,n) = 1 \).

*Proof.* Assume \( c \) is invertible and let \( d \) be an inverse of \( c \) modulo \( n \). Then there exists an integer \( k \) such that \( cd = 1 + nk \), that is, \( cd - nk = 1 \). By Bézout’s theorem, \( \gcd(c,n) = 1 \). Conversely, if \( \gcd(c,n) = 1 \), then by Bézout’s theorem there exist \( u \) and \( v \) such that \( cu + nv = 1 \). Then \( cu \equiv 1 \pmod{n} \), so \( c \) is invertible modulo \( n \). \( \square \)

**Remark 5.3.8.** In particular, if \( n \) is equal to a prime \( p \), then all integers which are non-zero modulo \( n \) are invertible modulo \( n \), so we have the following property:

**Proposition 5.3.9.** If \( ab \equiv 0 \pmod{p} \) then \( a \equiv 0 \pmod{p} \) or \( b \equiv 0 \pmod{p} \).

**Remark 5.3.10.** This is false modulo \( n \) which is not a prime. For example, \( 2 \times 2 \equiv 0 \pmod{4} \).

Invertible elements also preserve complete systems of residues:

**Proposition 5.3.11.** If \( a_1, \ldots, a_n \) is a complete system of residues modulo \( n \) and \( a \) is invertible modulo \( n \), then \( aa_1, \ldots, aa_n \) is again a complete system of residues modulo \( n \).

### 5.4 Linear congruences

The aim of this section is to solve congruences of the form

\[
a x \equiv b \pmod{n}
\]

for integers \( a, b, a \neq 0 \). When solving such a congruence, we will treat solutions that are congruent modulo \( n \) as equal: we are therefore looking for a maximal set *incongruent* integers satisfying this congruence.
Theorem 5.4.1. The linear congruence \( ax \equiv b \pmod{n} \) has solutions if and only if \( d = \gcd(a, n) \) divides \( b \). If \( d \) divides \( b \), then it has \( d \) pairwise incongruent solutions modulo \( n \), given by

\[
x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d - 1)n}{d},
\]

where \( x_0 \) is one particular solution.

Corollary 5.4.2. If \( \gcd(a, n) = 1 \), then the linear congruence \( ax \equiv b \pmod{n} \) has exactly one solution modulo \( n \). In particular, in this case the congruence \( ax \equiv 1 \pmod{n} \) has exactly one solution modulo \( n \). Thus, the inverse of \( a \) modulo \( n \) is unique modulo \( n \).

This means that whenever \( k \) and \( l \) are two inverses of \( a \) modulo \( n \), we have \( k \equiv l \pmod{n} \).

Example 5.4.3. Let us solve the congruence \( 9x \equiv 12 \pmod{60} \). We see that \( \gcd(3, 60) = 3 \), which divides 12, so by the theorem we have 3 pairwise incongruent solutions. Dividing by 3, we get \( 3x \equiv 4 \pmod{20} \). By inspection, we find that \( x = 8 \) is a solution (we could also use the extended Euclidean algorithm to come up with integers \( u \) and \( v \) such that \( 3u + 20v = 4 \), so that \( x = u \) would be a solution). According to the theorem, the two other solutions are given by \( 8 + 20 = 28 \) and \( 8 + 2 \times 20 = 48 \).

Remark 5.4.4. Start with the linear congruence \( ax \equiv b \pmod{n} \) such that \( d = \gcd(a, n) \) divides \( b \). Write \( a = da', b = db' \) and \( n = dn' \) with \( a', b', n' \) integers such that \( \gcd(a', n') = 1 \). Then, dividing by \( d \), we get \( a'x \equiv b' \pmod{n'} \). Let \( a'' \) be the inverse of \( a' \) modulo \( n \). Multiplying both sides by \( a'' \), we get \( x \equiv b'a'' \pmod{n'} \). Thus, a particular solution to the initial congruence is given by \( b'a'' \).

Thus, in the previous example, we can note that 7 is an inverse of 3 modulo 20, so multiplying both sides of \( 3x \equiv 4 \pmod{20} \) by 7, we get \( 21x \equiv 28 \pmod{20} \), so \( x \equiv 8 \pmod{20} \), so that we recover the particular solution 8 from before.

5.5 The Chinese remainder theorem

Theorem 5.5.1. Let \( n_1, \ldots, n_r \geq 2 \) be integers which are pairwise relatively prime. Then for all integers \( a_1, \ldots, a_r \), the system of congruences

\[
x \equiv a_1 \pmod{n_1} \\
x \equiv a_2 \pmod{n_2} \\
\vdots \\
x \equiv a_r \pmod{n_r}
\]

has a solution which is unique modulo \( n_1 \ldots n_r \) (that is, any two integers solving this system are congruent modulo \( n_1 \ldots n_r \)).
Remark 5.5.2. The proof of this theorem (see Burton, theorem 4.8 for a writeup) is constructive, in the sense that it proves that the solution exists by actually exhibiting a solution. Thus, you can use the idea in the proof to solve concrete systems of congruences.

Exercise 5.5.3. Solve the following system of simultaneous congruences:

\[
\begin{align*}
 x &\equiv 1 \pmod{3} \\
 x &\equiv 2 \pmod{5} \\
 x &\equiv 3 \pmod{7}
\end{align*}
\]

Example 5.5.4. Solve $19x \equiv 2 \pmod{60}$.

5.6 Fermat’s little theorem

Theorem 5.6.1. Let $p$ be a prime number and $a$ an integer not divisible by $p$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Corollary 5.6.2. Let $p$ be a prime number. For every integer $a$, $a^p \equiv a \pmod{p}$.

Example 5.6.3. Observe this for $p = 5$:

<table>
<thead>
<tr>
<th>$a$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a^2$</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>$a^4$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Note that in the table in the previous example, all squares of numbers not divisible by 5 are either 1 or -1. In general, we have:

Proposition 5.6.4. Let $p$ be an odd prime and $a$ be an integer not divisible by $p$. Then either $a^{p-1} \equiv 1 \pmod{p}$ or $a^{p-1} \equiv -1 \pmod{p}$.

Example 5.6.5. We are going to show that 17 divides $11^{104} + 1$. Indeed, we have $104 = 16 \times 6 + 8$, so that $11^{104} \equiv 11^8 \pmod{17}$. Now, $11^2 \equiv (-6)^2 \equiv 2 \pmod{17}$, so that $11^8 \equiv 2^4 \equiv -1 \pmod{17}$.

5.7 Wilson’s theorem

Theorem 5.7.1. If $p$ is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Remark 5.7.2. The converse is also true: if $(n-1)! \equiv -1 \pmod{n}$, then $n$ is prime. Indeed, if $n$ wasn’t prime, then $n$ would have a divisor $d$ such that $1 < d < n$. But then $d$ would divide $(n-1)!$. Since $d$ divides $(n-1)! + 1$, we then would have $d|1$, contradiction.

So far we have only solved linear congruences, but Wilson’s theorem allows us to solve our first quadratic congruence modulo an odd prime. The existence of a solution depends on the congruence class of $p$ modulo 4.

Proposition 5.7.3. Let $p$ be an odd prime. The congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.

Thus, $-1$ is a square modulo $p$ if and only if $p \equiv 1 \pmod{4}$.
6 Euler’s theorem

6.1 Euler’s phi function

(Burton Section 7.2)

**Definition 6.1.1.** For any positive integer \( n \), let \( \phi(n) \) denote the number of positive integers smaller than \( n \) and coprime to \( n \).

This defines a function \( \phi \) on the positive integers, taking integral values, called Euler’s totient function, or Euler’s phi function.

**Example 6.1.2.** We have \( \phi(1) = 1 \), \( \phi(2) = 1 \), \( \phi(3) = 2 \). We have \( \phi(6) = 2 \) since the only positive integers smaller than 6 and relatively prime to 6 are 1 and 5.

**Example 6.1.3.** Let \( p \) be a prime number. Then all the numbers \( 1, 2, \ldots, p - 1 \) are relatively prime to \( p \), so \( \phi(p) = p - 1 \).

The following proposition is a generalization of this example:

**Proposition 6.1.4.** For any prime number \( p \) and any integer \( k \geq 1 \), we have

\[
\phi(p^k) = p^k - p^{k-1}.
\]

We sometimes write this \( \phi(p^k) = p^k \left( 1 - \frac{1}{p} \right) \).

**Proposition 6.1.5.** The phi function is a multiplicative function, meaning that for any relatively prime integers \( m \) and \( n \), \( \phi(mn) = \phi(m)\phi(n) \).

**Remark 6.1.6.** It is not true that \( \phi(mn) = \phi(m)\phi(n) \) if \( m \) and \( n \) are not assumed relatively prime (that is, \( \phi \) is not totally multiplicative). For example, \( \phi(4) = 2 \neq \phi(2)^2 \).

**Theorem 6.1.7.** Let \( n > 1 \) be an integer with prime factorization \( n = p_1^{k_1} \ldots p_r^{k_r} \). Then

\[
\phi(n) = (p_1^{k_1} - p_1^{k_1-1}) \ldots (p_r^{k_r} - p_r^{k_r-1}) = n \left( 1 - \frac{1}{p_1} \right) \ldots \left( 1 - \frac{1}{p_r} \right).
\]

**Example 6.1.8.** Let us compute \( \phi(504) \). We have 504 = \( 2^3 \times 3^2 \times 7 \), so \( \phi(504) = (8 - 4) \times (9 - 3) \times (7 - 1) = 144 \).

**Proposition 6.1.9.** For \( n > 2 \), \( \phi(n) \) is an even integer.
6.2 Euler’s theorem

(Burton Section 7.3)

**Definition 6.2.1.** A reduced system of residues modulo \( n \) is a collection of \( \phi(n) \) integers that are relatively prime to \( n \) and that are pairwise incongruent modulo \( n \).

**Example 6.2.2.** \( 1,5,7,11 \) is a reduced system of residues modulo \( 12 \). Another one is given by \(-11,19,29,-1\).

**Example 6.2.3.** If \( n \) is prime, then a reduced system of residues modulo \( n \) is obtained by taking a complete system of residues modulo \( n \) and removing the one integer in this system that is congruent to 0 modulo \( n \).

**Proposition 6.2.4.** Let \( a_1, \ldots, a_{\phi(n)} \) be a reduced system of residues modulo \( n \) and let \( a \) be relatively prime to \( n \). Then \( aa_1, \ldots, aa_{\phi(n)} \) is again a reduced system of residues modulo \( n \).

**Proof.** If \( i,j \) are such that \( aa_i \equiv aa_j \pmod{n} \) then, since \( a \) is invertible, we get \( a_i \equiv a_j \pmod{n} \). Since \( a_1, \ldots, a_{\phi(n)} \) are mutually incongruent, this means that \( i = j \). Thus, \( aa_1, \ldots, aa_{\phi(n)} \) are pairwise incongruent. On the other hand, since for every \( i, \gcd(a_i, n) = 1 \), we have \( \gcd(aa_i, n) = 1 \). Thus, we indeed get a reduced system of residues. \( \square \)

**Proposition 6.2.5.** Let \( a_1, \ldots, a_{\phi(n)} \) be the integers in \( \{1, \ldots, n\} \) that are relatively prime to \( n \).

1. They form a reduced system of residues modulo \( n \).
2. Any reduced system of residues modulo \( n \) is congruent modulo \( n \) to \( a_1, \ldots, a_{\phi(n)} \) in some order.

**Proof.** The first point follows easily from the definition. Now, let \( b_1, \ldots, b_{\phi(n)} \) be another reduced system of residues. Denote by \( c_1, \ldots, c_{\phi(n)} \) their respective remainders in the Euclidean division by \( n \). Since the \( b_i \) are mutually incongruent, the \( c_i \) are all distinct. Since the \( b_i \) are relatively prime to \( n \), so are the \( c_i \). Thus, \( c_1, \ldots, c_{\phi(n)} \) are \( \phi(n) \) distinct elements of the set \( \{a_1, \ldots, a_{\phi(n)}\} \), so they are exactly the \( a_i \) in some order. \( \square \)

**Theorem 6.2.6.** Let \( n \) be an integer. For any integer \( a \) relatively prime to \( n \), we have

\[ a^{\phi(n)} \equiv 1 \pmod{n} \]

**Proof.** Let \( a_1, \ldots, a_{\phi(n)} \) be the reduced system of residues from proposition 6.2.5. By propositions 6.2.4 and 6.2.5, the integers \( aa_1, \ldots, aa_{\phi(n)} \) are congruent modulo \( n \) to \( a_1, \ldots, a_{\phi(n)} \) in some order. Thus, multiplying them together we get

\[ (aa_1) \cdot (aa_2) \cdot \ldots \cdot (aa_{\phi(n)}) \equiv a_1 \cdot a_2 \cdot \ldots \cdot a_{\phi(n)} \pmod{n}. \]

This simplifies to

\[ a^{\phi(n)}a_1 \ldots a_{\phi(n)} \equiv a_1 \ldots a_{\phi(n)} \pmod{n}. \]

Now, denoting by \( b_i \) an inverse of \( a_i \) modulo \( n \), multiplying by \( b_{\phi(n)} \ldots b_1 \) on both sides we get the result. \( \square \)
Example 6.2.7. For $n$ prime, we recover Fermat’s little theorem by example 6.1.3.

Example 6.2.8. Let $n$ be an odd integer not divisible by 5. We are going to show that it divides an integer all of the digits of which are 9. Indeed, we have $\gcd(n, 10) = 1$, so by Euler’s theorem, $10^{\phi(n)} \equiv 1 \pmod{n}$. This means that $n$ divides $10^{\phi(n)} - 1$ which is an integer written using $\phi(n)$ times the digit 9 only.

This example can be improved: we may in fact prove that $n$ divides an integer all of the digits of which are 1 (the previous result then follows by multiplying this integer by 9). For this, note that we in fact have $\gcd(9n, 10) = 1$, so we may apply Euler’s theorem to $9n$ instead of $n$, which yields $10^{\phi(9n)} \equiv 1 \pmod{9n}$. This implies that $9n$ divides $10^{\phi(9n)} - 1$, so $n$ divides $\frac{1}{9}(10^{\phi(9n)} - 1)$, which is the integer written with $\phi(9n)$ times the digit 1 only.

6.3 RSA cryptosystem

RSA (which stands for Rivest-Shamir-Adleman) is a public-key cryptosystem, first described in 1978 and widely used for secure data transmission.

Assume Alice wants to give her friends a way to send encrypted messages to her. Here is what she has to do:

Creating the public and private keys

1. Choose two (large) prime numbers $p$ and $q$.
2. Compute $n = pq$.
3. Compute $\phi(n) = (p - 1)(q - 1)$.
4. Choose (randomly) an integer $e$ such that $1 < e < \phi(n)$ and such that $\gcd(e, \phi(n)) = 1$.
5. Compute $d$ such that $de \equiv 1 \pmod{\phi(n)}$.

After having done this, Alice keeps $p, q, \phi(n)$ and $d$ secret, and sends $n$ and $e$ to her friends through a reliable, but not necessarily confidential canal. It is not important if some third party knows $n$ and $e$, as long as all the other parameters remain secret. The pair $(n, e)$ is called the public key, and $d$ is called the private key.

Assume now Bob wants to send a secure message to Alice. He is going to use the public key $(n, e)$ to encrypt his message. First of all, Alice and Bob need to agree on a way to transform messages into integers smaller than $n$.

If Bob has a message $M$, he first transforms it into an integer $m$ such that $1 \leq m < n$. Then he computes $m^e \pmod{n}$ (there are fast algorithms to achieve this). To decrypt Bob’s message without access to the private key, one then needs to be able to take $e$-th roots modulo $n$. What makes RSA secure is the fact that there is no known fast algorithm to do this. The message is not secure for eternity, but it is so during a sufficiently long period of time.

Bob sends the result of his computation, that is, an integer $k$ such that $k \equiv m^e \pmod{n}$ to Alice. Alice then simply needs to compute $k^d \pmod{n}$ to recover the message $m$. 

23
Proof By definition, since \(de \equiv 1 \pmod{\phi(n)}\), there exists an integer \(a\) such that \(de - a\phi(n) = 1\). Then

\[
k^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{1+a\phi(n)} \pmod{n}.
\]

It remains to show that \(m^{1+a\phi(n)} \equiv m \pmod{n}\). There are several cases to consider:

- If \(m\) is relatively prime to \(n\) (which will be true with overwhelming probability), this follows from Euler’s theorem.

- If \(m\) is not relatively prime to \(n\), then \(m\) is divisible by \(p\) or \(q\). It cannot be divisible by both, because it is in the set \(\{1, \ldots, n-1\}\). If \(m\) is divisible by \(p\) and not by \(q\), then by Fermat’s little theorem, \(m^{q-1} \equiv 1 \pmod{q}\), so, taking \(a(p-1)\)th powers, \(m^{a\phi(n)} \equiv 1 \pmod{q}\). Thus, we have that \(q\) divides \(m^{a\phi(n)} - 1\) and \(p\) divides \(m\), so \(n = pq\) divides the product \(m(m^{a\phi(n)} - 1)\), so we have the result. Same if \(m\) is divisible by \(q\) but not by \(p\).

## 7 Number-theoretic functions

(Burton Chapter 6)

### 7.1 The sum and the number of divisors

A number-theoretic function is a function defined on the positive integers (and usually also taking integral values).

**Definition 7.1.1.** For every positive integer \(n\), we define \(\tau(n)\) to be the number of positive divisors of \(n\), and \(\sigma(n)\) to be the sum of the positive divisors of \(n\).

**Example 7.1.2.**

1. One has \(\tau(n) = 1\) if and only if \(n = 1\), and \(\sigma(n) = 1\) if and only if \(n = 1\).

2. We have \(\tau(12) = 6\) and \(\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28\).

3. For a prime number \(p\), \(\tau(p) = 2\) and \(\sigma(p) = 1 + p\). More precisely, \(\tau(n) = 2\) if and only if \(n\) is prime, and \(\sigma(n) = n + 1\) if and only if \(n\) is prime.

4. For a product of two distinct primes \(p\) and \(q\), \(\tau(pq) = 4\) and \(\sigma(pq) = 1 + p + q + pq = (1 + p)(1 + q)\).

5. For a prime power \(p^k\), \(\tau(p^k) = k + 1\) and \(\sigma(p^k) = 1 + p + \ldots + p^k = \frac{p^{k+1} - 1}{p-1}\).

**Proposition 7.1.3.** If \(n\) is a positive integer with prime factorization \(n = p_1^{k_1} \ldots p_r^{k_r}\) (where \(p_1, \ldots, p_r\) are distinct primes), then

(a) \(\tau(n) = (k_1 + 1) \ldots (k_r + 1)\), and
(b) \( \sigma(n) = \frac{p^{k_1+1}-1}{p-1} \cdot \ldots \cdot \frac{p^{k_r+1}-1}{p-1} \).

**Proposition 7.1.4.** Let \( n > 1 \) be an integer. Then \( \tau(n) \) is odd if and only if \( n \) is a perfect square.

*Proof.* Write \( n = p_1^{k_1} \ldots p_r^{k_r} \). Then by proposition 7.1.3, \( \tau(n) = (k_1 + 1) \ldots (k_r + 1) \).

Thus, \( \tau(n) \) is odd if and only if all of the \( k_i \) are even, that is, if and only if \( k_i = 2k'_i \) for some integers \( k'_i \), that is, if and only if \( n = (p_1^{k'_1} \ldots p_r^{k'_r})^2 \).

**Proposition 7.1.5.** Let \( n > 1 \) be an integer. The product of the positive divisors of \( n \) is \( n^{\tau(n)/2} \).

**Remark 7.1.6.** Note that \( n^{\frac{\tau(n)}{2}} \) is indeed always an integer: if \( \tau(n) \) is even it is obvious, and if \( \tau(n) \) is odd, then by proposition 7.1.4, \( n \) is a perfect square, \( n = m^2 \) for some integer \( m \), and so \( n^{\frac{\tau(n)}{2}} = m^{\tau(n)} \).

**Example 7.1.7.** The product of all divisors of 12 is:

\[
(1 \times 12) \times (2 \times 6) \times (3 \times 4) = 12^3.
\]

The product of all divisors of 16 is:

\[
(1 \times 16) \times (2 \times 8) \times 4 = 16^\frac{3}{2}
\]

*Proof.* Note that there is an exact correspondence between

\[ \{ \text{divisors of } n \text{ smaller than } \sqrt{n} \} \]

and

\[ \{ \text{divisors of } n \text{ greater than } \sqrt{n} \} \]

given by associating to every divisor \( d < \sqrt{n} \) of \( n \), the divisor \( \frac{n}{d} \), which is larger than \( \sqrt{n} \). Thus, these two sets have the same number of elements.

If \( n \) is not a square, they contain all of the divisors of \( n \), and therefore each of these sets has \( \frac{\tau(n)}{2} \) elements. Thus, writing the product of all the divisors and gathering every divisor \( d \) smaller than \( \sqrt{n} \) with the corresponding divisor \( \frac{n}{d} \), we get

\[
\prod_{d|n \atop d<\sqrt{n}} d \times \prod_{d|n \atop d>\sqrt{n}} d = n^{\frac{\tau(n)}{2}}.
\]

Now, if \( n = m^2 \) is a square, then \( n \) has an extra divisor \( m = \sqrt{n} \), and each of the two above sets has \( \frac{\tau(n)-1}{2} \) elements. We have

\[
\prod_{d|n} d = m \times \prod_{d|n \atop d<\sqrt{n}} d \times \prod_{d|n \atop d>\sqrt{n}} d = n^{\frac{3}{2}} \times \prod_{d|n \atop d<\sqrt{n}} d \times \frac{n}{d} = n^{\frac{3}{2}} n^{\frac{\tau(n)-1}{2}} = n^{\frac{\tau(n)}{2}}.
\]
7.2 Multiplicative functions

Definition 7.2.1. A number-theoretic function \( f \) is said to be multiplicative if for all relatively prime integers \( m \) and \( n \),

\[
f(mn) = f(m)f(n).
\]

Remark 7.2.2. By induction, if \( f \) is multiplicative then for all collections of pairwise relatively prime \( m_1, \ldots, m_k \), we have

\[
f(m_1 \ldots m_k) = f(m_1) \ldots f(m_k).
\]

In particular, if \( n \) is an integer with prime factorization \( n = p_1^{k_1} \ldots p_r^{k_r} \), then we have

\[
f(n) = f(p_1^{k_1}) \ldots f(p_r^{k_r}).
\]

Proposition 7.2.3. The functions \( \tau \) and \( \sigma \) are multiplicative.

Proposition 7.2.4. If \( f \) is a multiplicative function and \( F \) is defined by

\[
F(n) = \sum_{d \mid n} f(d),
\]

then \( F \) is also multiplicative.

Remark 7.2.5. Since \( \tau(n) = \sum_{d \mid n} 1 \) and \( \sigma = \sum_{d \mid n} d \), this gives a new proof of the fact that \( \sigma \) and \( \tau \) are multiplicative.

7.3 Möbius inversion

Definition 7.3.1. For a positive integer \( n \), define

\[
\mu(n) = \begin{cases} 
1 & \text{if } n = 1 \\
0 & \text{if } p^2 \mid n \text{ for some prime } p \\
(-1)^r & \text{if } n = p_1 \ldots p_r \text{ for distinct primes } p_i
\end{cases}
\]

In other words, \( n \) is zero exactly when \( n \) is not square-free. If \( n \) is square-free, then \( n \) is a product of a certain number \( r \) of distinct primes, and \( \mu(n) = (-1)^r \).

Example 7.3.2. We have \( \mu(2) = -1, \mu(3) = -1, \) and more generally, \( \mu(p) = -1 \) for any prime \( p \). We have \( \mu(4) = 0, \mu(6) = 1, \mu(8) = 0, \mu(9) = 0, \mu(10) = 1 \ldots \)

Proposition 7.3.3. The function \( \mu \) is a multiplicative function.

Proof. Let \( m \) and \( n \) be relatively prime integers. If one of them is not square-free, then so is the product \( mn \), and the equality \( \mu(mn) = \mu(m)\mu(n) \) is satisfied because both sides are zero. Assume now that \( m \) and \( n \) are square-free, with \( m = p_1 \ldots p_r \) and \( n = q_1 \ldots q_s \) where \( p_1, \ldots, p_r, q_1, \ldots, q_s \) are primes, distinct because \( m \) and \( n \) are relatively prime. Then

\[
\mu(mn) = \mu(p_1 \ldots p_r q_1 \ldots q_s) = (-1)^{r+s} = (-1)^r (-1)^s = \mu(m)\mu(n).
\]
Proposition 7.3.4. For each positive integer $n$,
\[
\sum_{d|n} \mu(d) = \begin{cases} 
1 & \text{if } n = 1 \\
0 & \text{if } n > 1
\end{cases}
\]

Theorem 7.3.5 (Möbius inversion formula). Let $F$ and $f$ be two number-theoretic functions related by the formula
\[
F(n) = \sum_{d|n} f(d).
\]
Then
\[
f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d).
\]

Example 7.3.6. Since $\tau(n) = \sum_{d|n} 1$, we have that
\[
1 = \sum_{d|n} \mu\left(\frac{n}{d}\right) \tau(d).
\]
In the same way, since $\sigma(n) = \sum_{d|n} d$, we have that
\[
n = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma(d).
\]

Proposition 7.3.7. Let $F$ and $f$ be two number-theoretic functions related by the formula
\[
F(n) = \sum_{d|n} f(d).
\]
If $F$ is multiplicative, then so is $f$.

7.4 Some additional properties of Euler’s $\phi$ function

Remark 7.4.1. Recall that for an arithmetic function $f$, $\sum_{d|n} f(d)$ denotes the sum of the values of $f$ at all divisors $d$ of $n$. But as $d$ ranges over all divisors of $n$, so does $\frac{n}{d}$, so this sum is equal to $\sum_{d|n} f\left(\frac{n}{d}\right)$.

Proposition 7.4.2. Let $n$ be a positive integer. Then
\[
n = \sum_{d|n} \phi(d),
\]
where the sum runs over all positive divisors of $n$.

Proof. For every positive divisor $d$ of $n$, consider
\[
S_d = \{k \in \{1, \ldots, n\} \text{ such that } \gcd(k, n) = d\}.
\]
Note that every element $k$ of $\{1, \ldots, n\}$ is an element of exactly one $S_d$, namely the one with $d = \gcd(k, n)$. Thus, the set $\{1, \ldots, n\}$ is the disjoint union of the $S_d$ for $d|n$, so that,
comparing numbers of elements, we have \( n \equiv \sum_{d|n} |S_d| \). Let us now compute \(|S_d|\). We have \( \gcd(k, n) = d \) if and only if \( d \) divides \( k \) and \( n \), and \( \gcd(\frac{k}{d}, \frac{n}{d}) = 1 \). Thus, the elements of the set \( S_d \) are exactly the elements of the set

\[
\left\{ m \in \{1, \ldots, \frac{n}{d}\} \mid \gcd(m, \frac{n}{d}) = 1 \right\}
\]
multiplied by \( d \): there are therefore \( \phi\left(\frac{n}{d}\right) \) of them. We have shown that \( n \equiv \sum_{d|n} \phi\left(\frac{n}{d}\right) \).

We conclude by the remark.

**Example 7.4.3.** We have

\[
\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12.
\]

**Corollary 7.4.4.** For any positive integer \( n \),

\[
\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.
\]

**Remark 7.4.5.** Using this corollary, we can recover the formula for \( \phi(n) \): if \( n = p_1^{k_1} \cdots p_r^{k_r} \), when expanding the product

\[
\prod_{i=1}^r \left( \mu(1) + \frac{\mu(p_i)}{p_i} + \ldots + \frac{\mu(p_i^{k_i})}{p_i^{k_i}} \right),
\]

we get the sum of all the terms of the form

\[
\frac{\mu(p_1^{m_1}) \cdots \mu(p_r^{m_r})}{p_1^{m_1} \cdots p_r^{m_r}} = \frac{\mu(p_1^{m_1}) \cdots \mu(p_r^{m_r})}{p_1^{m_1} \cdots p_r^{m_r}}
\]

(the latter equality being obtained by multiplicativity), where \( 0 \leq m_i \leq k_i \). This is exactly the sum of terms \( \frac{\mu(d)}{d} \) over all divisors of \( n \)

\[
n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{i=1}^r \left( \mu(1) + \frac{\mu(p_i)}{p_i} + \ldots + \frac{\mu(p_i^{k_i})}{p_i^{k_i}} \right) = n \prod_{i=1}^r \left( 1 - \frac{1}{p_i} \right).
\]

8 Orders and roots

8.1 Orders of integers modulo \( n \)

**Definition 8.1.1.** Let \( n > 1 \) be an integer and let \( a \) be an integer relatively prime to \( n \). The order of \( a \) modulo \( n \) is the smallest positive integer \( k \) such that \( a^k \equiv 1 \pmod{n} \).

**Remark 8.1.2.** By Euler’s theorem, the order of \( a \) modulo \( n \) is at most \( \phi(n) \).
Example 8.1.3. The order of 3 modulo 8 is 2, since $3^2 \equiv 1 \pmod{8}$. On the other hand, $\phi(8) = 4$, which shows that the order of a modulo $n$ can be strictly smaller than $\phi(n)$.

Remark 8.1.4. The notion of order only makes sense for $a$ relatively prime to $n$. For any $a$ not relatively prime to $m$, a positive integer $k$ such that $a^k \equiv 1 \pmod{n}$ does not exist, since its existence would imply that $a$ has an inverse modulo $n$, namely $a^{k^{-1}}$.

We have seen that the order can be smaller than $\phi(n)$. However, there are restrictions on what it can be equal to: in fact, as we can see in the following proposition, it must be a divisor of $\phi(n)$.

Proposition 8.1.5. Let $a$ be an integer relatively prime to $n$ and denote by $k$ its order modulo $n$. For any integer $m$, we have $a^m \equiv 1 \pmod{n}$ if and only if $k|m$. In particular, $k|\phi(n)$.

Example 8.1.6. This gives a way of finding the order faster. For example, if we want to find the order of 5 modulo 18, since $\phi(18) = 6$, it suffices to check $5^2$ and $5^3$. Since $5^2 \equiv 7 \pmod{18}$ and $5^3 \equiv -1 \equiv 18$, we see that the order must be 6.

Example 8.1.7. One may ask oneself, for some fixed $n$, does there exist an element of order $d$ modulo $n$ for every divisor $d$ of $\phi(n)$? In fact, this is not necessarily true. For example, modulo 12, though $\phi(12) = 4$, no integer relatively prime to 12 has order 4. Indeed, 1 has order 1, and

$$5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$$

so 5, 7 and 11 have order 2.

Proposition 8.1.8. If the integer $a$ has order $k$ modulo $n$, then $a^i \equiv a^j \pmod{n}$ if and only if $i \equiv j \pmod{k}$.

Corollary 8.1.9. If $a$ has order $k$ modulo $n$, then the integers $a, a^2, \ldots, a^k$ are incongruent modulo $n$.

Example 8.1.10. The integer 2 is of order 3 modulo 7. We have that $2, 2^2$ and $2^3$ are congruent, respectively, to 2, 4 and 1 modulo 7, so they are indeed incongruent.

Proposition 8.1.11. If the integer $a$ has order $k$ modulo $n$, then for every positive integer $m$, the integer $a^m$ has order $\frac{k}{\gcd(m,k)}$ modulo $n$.

Proof. Write $d = \gcd(m,k)$, $k = dk'$ and $m = dm'$ where $k'$ and $m'$ are relatively prime. Denote the order of $a^m$ by $r$. First of all, we can easily check that $(a^m)^{k'} \equiv 1 \pmod{n}$, which means that $r$ divides $k'$.

On the other hand, we have $a^{mr} = (a^m)^r \equiv 1 \pmod{n}$. This means that $mr$ is divisible by $k$, that is, there exists an integer $s$ such that $ks = mr$. Dividing both sides by $d$, we get $k's = m'r$. Since $\gcd(k', m') = 1$, by Gauss’s lemma we get that $k'$ divides $r$.

Since $k'|r$ and $r|k'$, and both are positive integers, we have that $r = k'$. □
In particular, we have:

**Corollary 8.1.12.** Let \( a \) be an integer with order \( k \) modulo \( n \). Then \( a^m \) is also of order \( k \) if and only if \( \gcd(k, m) = 1 \).

**Example 8.1.13.** The integer 3 is of order 6 modulo 7. We have \( 3^2 \equiv 2 \pmod{7} \), and \( \gcd(2, 6) = 2 \), so 2 is of order 3 modulo 7, which is consistent with what we saw in example 8.1.10. In the same manner, \( 3^3 \) is of order 2, \( 3^4 \) is of order 3, and \( 3^5 \) is of order 6.

### 8.2 Primitive roots

Primitive roots modulo \( n \) are integers modulo \( n \) which have the highest order possible.

**Definition 8.2.1.** An integer \( a \) such that \( \gcd(a, n) = 1 \) and which is of order \( \varphi(n) \) modulo \( n \) is called a primitive root of \( n \).

**Remark 8.2.2.** As seen in example 8.1.7, primitive roots do not always exist.

In other words, \( a \) is a primitive root modulo \( n \) if \( a^{\varphi(n)} \equiv 1 \pmod{n} \), but \( a^k \not\equiv 1 \pmod{n} \) for all positive integers \( k < \varphi(n) \). In fact, these powers form a reduced system of residues modulo \( n \):

**Proposition 8.2.3.** Let \( a \) be an integer relatively prime to \( n \). If \( a \) is a primitive root modulo \( n \), then the integers \( a, a^2, \ldots, a^{\varphi(n)} \) form a reduced system of residues modulo \( n \).

**Remark 8.2.4.** Recall that if \( a_1, \ldots, a_{\varphi(n)} \) is a reduced system of residues modulo \( n \), then any integer \( b \) relatively prime to \( n \) is congruent to exactly one of the \( a_i \). Indeed, we know that, denoting by \( b_1, \ldots, b_{\varphi(n)} \) the integers in \( \{1, \ldots, n\} \) that are relatively prime to \( n \), the integers \( a_1, \ldots, a_{\varphi(n)} \) are congruent to \( b_1, \ldots, b_{\varphi(n)} \) in some order. On the other hand, let \( r \) be the remainder in the Euclidean division of \( b \) by \( n \): it is relatively prime to \( n \), and satisfies \( 0 \leq r < n \), so it is equal to \( b_i \) for some \( i \). This means that \( b \equiv b_i \pmod{n} \), but \( b_i \) is itself congruent to exactly one \( a_j \), so \( b \equiv a_j \pmod{n} \).

**Example 8.2.5.** Let us check that 2 is a primitive root modulo 9. We have \( 2^2 \equiv 4 \pmod{9} \), \( 2^3 \equiv 8 \pmod{9} \), and \( \varphi(9) = 9 - 3 = 6 \), so 2 must be of order 6. Using proposition 8.1.11, we may determine quickly the orders of all invertible elements modulo 9:

<table>
<thead>
<tr>
<th>power</th>
<th>2</th>
<th>2^2</th>
<th>2^3</th>
<th>2^4</th>
<th>2^5</th>
<th>2^6</th>
</tr>
</thead>
<tbody>
<tr>
<td>modulo 9</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>7</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>order</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

The only other primitive root modulo 9 is 5.

**Corollary 8.2.6.** Let \( a \) be a primitive root modulo \( n \). For any integer \( b \) relatively prime to \( n \), there exists a unique \( i \in \{1, \ldots, \varphi(n)\} \) such that \( b \equiv a^i \pmod{n} \).

**Proof.** This is a direct consequence of remark 8.2.4 and proposition 8.2.3.
Corollary 8.2.7. If $n$ has a primitive root, then it has exactly $\phi(\phi(n))$ of them.

Proof. By corollary 8.2.6, every primitive root is congruent modulo $n$ to $a^i$ for some $i \in \{1, \ldots, \phi(n)\}$. On the other hand, $a$ being of order $\phi(n)$, by corollary 8.1.12, $a^i$ is of order $\phi(n)$ if and only if $\gcd(i, \phi(n)) = 1$. Thus, there are as many primitive roots as there are integers $i$ relatively prime to $\phi(n)$ in the set $\{1, \ldots, \phi(n)\}$, that is, $\phi(\phi(n))$. \qed

8.3 Existence of primitive roots modulo $p$

In this section, we fix a prime $p$ and we are going to work modulo $p$.

We will start by stating a fact that we will use without proof so that we don’t need to get into too many considerations about polynomials. The proof is not hard, you can read it e.g. in Burton, Theorem 8.5.

Remark 8.3.1. [Number of solutions of a polynomial equation modulo $p$] Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

be a polynomial with $a_0, \ldots, a_n \in \mathbb{Z}$ and $a_n \not\equiv 0 \pmod{p}$. Then the congruence $f(x) \equiv 0 \pmod{p}$ has at most $n$ incongruent solutions modulo $p$. For example, if $a_1 \not\equiv 0 \pmod{p}$, the congruence

$$a_1 x + a_0 \equiv 0 \pmod{p}$$

has exactly one solution modulo $p$, given by $-a_0 a_1^{-1}$ where we denote by $a_1^{-1}$ an inverse of $a_1$ modulo $p$.

The idea of the proof of the general statement is the following: we do an induction on $n$. The basis step is dealt with in the above example. Assume that the statement is true for all polynomials of degree $n$ for some integer $n$, and consider a polynomial $f$ of degree $n + 1$. If the congruence $f(x) \equiv 0 \pmod{p}$ has no solutions, we are done. If it has some solution $a$, then we may write $f(x) = (x - a)g(x)$ where $g$ is a polynomial of degree $n$ with integral coefficients and with leading coefficient not divisible by $p$. If $b$ is any solution of the congruence $g(x) \equiv 0 \pmod{p}$ incongruent to $a$, then we have $(b - a)g(b) \equiv 0 \pmod{p}$, so since $p$ is prime, $b - a \equiv 0 \pmod{p}$ or $g(b) \equiv 0 \pmod{p}$. The former being impossible by the assumption on $b$, we have that $b$ is a solution of the congruence $g(x) \equiv 0 \pmod{p}$. In other words, any solution of the congruence $f(x) \equiv 0 \pmod{p}$ incongruent to $a$ is a solution of $g(x) \equiv 0 \pmod{p}$. By the induction hypothesis, the latter has at most $n$ incongruent solutions, so $f(x) \equiv 0 \pmod{p}$ has at most $n + 1$ incongruent solutions.

Proposition 8.3.2. For every divisor $d$ of $p - 1$, the congruence

$$x^d \equiv 1 \pmod{p}$$

has exactly $d$ incongruent solutions modulo $p$.

Proof. Write $p - 1 = dk$ for some positive integer $k$. Then we may check that

$$x^{p-1} - 1 = x^{dk} - 1 = (x^d - 1)f(x),$$
where
\[ f(x) = (x^{d(k-1)} + x^{d(k-2)} + \ldots + x^d + 1) \]
is a polynomial with integral coefficients and of degree \( p - 1 - d \). The congruence \( f(x) \equiv 0 \pmod{p} \) has at most \( p - 1 - d \) incongruent solutions, and the congruence \( x^{d-1} \equiv 0 \pmod{p} \) has at most \( d \) solutions. On the other hand, by Fermat’s little theorem, the integers \( 1, 2, \ldots, p - 1 \) are solutions of the congruence \( x^{p-1} - 1 \equiv 0 \pmod{p} \), so this congruence has exactly \( p - 1 \) incongruent solutions. Let \( a \) be any integer among \( 1, 2, \ldots, p - 1 \). We have
\[ (a^d - 1)f(a) = a^{p-1} - 1 \equiv 0 \pmod{p}, \]
so, since \( p \) is prime, \( a \) is either a solution of \( x^d - 1 \equiv 0 \pmod{p} \) or of \( f(x) \equiv 0 \pmod{p} \). Since this holds for any of the integers \( 1, \ldots, p - 1 \), this means that these two congruences must have \( p - 1 \) solutions in total, which can only be achieved if the first one has exactly \( d \) solutions, and the other one has exactly \( p - 1 - d \) solutions.

\[ \Box \]

**Proposition 8.3.3.** If \( d \) divides \( p - 1 \) then there are exactly \( \phi(d) \) incongruent integers having order \( d \) modulo \( p \).

**Proof.** For every \( d \mid p - 1 \), denote by \( \psi(d) \) the number of integers in the set \( \{1, \ldots, p - 1\} \) having order \( d \). Since every integer in \( \{1, \ldots, p - 1\} \) has some order \( d \) dividing \( p - 1 \), we have
\[ p - 1 = \sum_{d \mid p - 1} \psi(d). \]
On the other hand, we know that
\[ p - 1 = \sum_{d \mid p - 1} \phi(d). \]
The idea, now, is to show that for all \( d \), \( \psi(d) \leq \phi(d) \), for if this is the case, we would have
\[ p - 1 = \sum_{d \mid p - 1} \psi(d) \leq \sum_{d \mid p - 1} \phi(d) \leq p - 1. \]
Since the two sides are equal, this would mean that the inequality in the middle is actually an equality, so \( \psi(d) = \phi(d) \) for all \( d \).

So, now we prove that for every \( d \mid p - 1 \), \( \psi(d) \leq \phi(d) \). If \( \psi(d) = 0 \), that is, if there are no elements of order \( d \), then the inequality is indeed satisfied. If it is not zero, this means that we have an element \( a \) of order \( d \) modulo \( p \). Then, all of the incongruent powers \( a, a^2, \ldots, a^d \) provide \( d \) incongruent solutions to the congruence \( x^d - 1 \equiv 0 \pmod{d} \), so there are no other solutions. Since all elements of order \( d \) must be solutions of this congruence, this means that any element of order \( d \) must be congruent to one of them. But by corollary \[8.1.11\] only the \( a^i \) with \( i \) relatively prime to \( d \) have order exactly \( d \), and there are \( \phi(d) \) of them. This means that \( \psi(d) > 0 \), then in fact \( \psi(d) = \phi(d) \).

\[ \Box \]

**Corollary 8.3.4.** There are exactly \( \phi(p - 1) \) primitive roots modulo a prime \( p \). 

32


9 Quadratic reciprocity
(Burton Chapter 9)

9.1 Quadratic residues

Quadratic reciprocity deals with quadratic congruences.

Remark 9.1.1. Let $p$ be an odd prime. We may reduce solving the quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

where $a, b, c \in \mathbb{Z}$ are such that $p \nmid a$, to solving a congruence of the form $x^2 \equiv \alpha \pmod{p}$. Thus, we are going to deal only with quadratic congruences of this latter, simpler, form.

Lemma 9.1.2. Let $p$ be an odd prime. The quadratic congruence

$$x^2 \equiv a \pmod{p}$$

where $p \nmid a$ has either no solutions, or exactly two incongruent solutions.

Proof. If it has no solutions, we are done. If it has a solution $x_0$, it has another solution $p - x_0$. These two are incongruent, because if we had $x_0 \equiv p - x_0 \pmod{p}$, we would have $2x_0 \equiv 0 \pmod{p}$, so, since $p$ is odd, $x_0 \equiv 0 \pmod{p}$. This is impossible because this would imply $a \equiv 0 \pmod{p}$. By the result in remark 8.3.1, we cannot have more than two solutions.

Definition 9.1.3. Let $p$ be an odd prime, and $a$ an integer not divisible by $p$. The integer $a$ is said to be a quadratic residue modulo $p$ if the congruence $x^2 \equiv a \pmod{p}$ has a solution, and a quadratic nonresidue modulo $p$ otherwise.

Remark 9.1.4. If $a \equiv b \pmod{p}$, then $a$ is a quadratic residue modulo $p$ if and only if $b$ is. Thus, to know the list of all quadratic residues modulo $p$, it suffices to find the quadratic residues in the set $\{1, \ldots, p-1\}$.

Example 9.1.5. Let us determine all quadratic residues and nonresidues modulo 11. Because $x^2 \equiv (p-x)^2 \pmod{p}$, it suffices to compute the squares of the integers $1, 2, 3, 4, 5$.

<table>
<thead>
<tr>
<th>$x$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^2$</td>
<td>1</td>
<td>4</td>
<td>9</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>

Thus the quadratic residues modulo $p$ are 1, 3, 4, 5, 9 (and all the integers congruent to those), and the quadratic nonresidues modulo $p$ are 2, 6, 7, 8, 10. Note that there is the same number of residues and nonresidues: this is always the case.

Proposition 9.1.6 (Euler’s criterion). Let $p$ be an odd prime and $a$ an integer not divisible by $p$. Then $a$ is a quadratic residue modulo $p$ if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$
Remark 9.1.7. Let $p$ be an odd prime, and let $r$ be a primitive root modulo $p$. Recall that every integer $a$ is congruent to $r^k$ for a unique $k \in \{1, \ldots, p-1\}$. Then $a$ is a quadratic residue modulo $p$ if and only if $k$ is even. In particular, a primitive root is never a quadratic residue.

Recall from proposition 5.6.4 that in fact, we always have either $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ or $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Thus, these cases correspond exactly to quadratic residues and non-residues:

**Corollary 9.1.8.** Let $p$ be an odd prime and $a$ an integer not divisible by $p$. Then $a$ is a quadratic residue or nonresidue modulo $p$ according to whether

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{or} \quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

**Corollary 9.1.9.** There are exactly $\frac{p-1}{2}$ incongruent quadratic residues modulo $p$, and exactly $\frac{p-1}{2}$ incongruent quadratic nonresidues.

**Example 9.1.10.** Let us go back to the example $p = 11$. We have $2^5 = 32 \equiv -1 \pmod{11}$, so we recover the fact the 2 is a quadratic nonresidue modulo 11. On the other hand, $3^5 = 81 \times 3 \equiv 4 \times 3 \equiv 1 \pmod{11}$, so we recover the fact that 3 is a quadratic residue modulo 11.

If we are asked whether 5 is a quadratic residue modulo 17 or not, we currently have two options:

- Compute $x^2 \pmod{17}$ for $x = 1, 2, 3, \ldots, 8$ and see if you find 5 among them.
- Compute $5^8 \pmod{17}$ and see if it is congruent to 1 or $-1$.

**Example 9.1.11.** Note that $(-1)^{\frac{p-1}{2}}$ is equal to 1 if $p \equiv 1 \pmod{4}$ and $-1$ if $p \equiv 3 \pmod{4}$. Thus, $-1$ is a quadratic residue modulo $p$ if and only if $p \equiv 1 \pmod{4}$ and a quadratic nonresidue if $p \equiv 3 \pmod{4}$

Another consequence of Euler’s criterion is the following.

**Proposition 9.1.12.** Let $p$ be a prime and $a$ and $b$ two integers not divisible by $p$. Then

- $ab$ is a quadratic residue if either $a$ and $b$ are both quadratic residues, or $a$ and $b$ are both quadratic nonresidues.
- $ab$ is a quadratic nonresidue if one of the integers $a$ and $b$ is a quadratic residue, and the other one is a quadratic nonresidue.

### 9.2 The Legendre symbol

**Definition 9.2.1.** Let $p$ be an odd prime and $a$ an integer not divisible by $p$. The *Legendre symbol* $(\frac{a}{p})$ is defined by

$$
\left(\frac{a}{p}\right) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue modulo } p \\
-1 & \text{if } a \text{ is a quadratic nonresidue modulo } p
\end{cases}
$$
Here are some basic properties of the Legendre symbol:

**Proposition 9.2.2.** Let \( p \) be an odd prime and \( a, b \) two integers not divisible by \( p \). The following properties are satisfied:

(a) If \( a \equiv b \pmod{p} \) then \( \left( \frac{a}{p} \right) = \left( \frac{b}{p} \right) \).

(b) \( \left( \frac{a^2}{p} \right) = 1 \).

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

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

(e) \( \left( \frac{ab^2}{p} \right) = \left( \frac{a}{p} \right) \).

(f) \( \left( \frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases} \)

**Remark 9.2.3.** Property (d) is a more concise reformulation of proposition 9.1.12.

**Exercise 9.2.4.** Compute the following Legendre symbols: \( \left( \frac{500}{11} \right), \left( \frac{333}{5} \right), \left( \frac{-35}{17} \right) \).

### 9.3 Quadratic reciprocity law

We are first going to state the quadratic reciprocity law, and explain how it should be used.

**Theorem 9.3.1** (Quadratic reciprocity law). Let \( p \) and \( q \) be distinct odd primes. Then

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

In other words, since a Legendre symbol is always 1 or \(-1\), this may be reformulated as:

\[
\left( \frac{q}{p} \right) = \begin{cases} \left( \frac{p}{q} \right) & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ -\left( \frac{p}{q} \right) & \text{if } p \equiv q \equiv 3 \pmod{4} \end{cases}
\]

Of course, this is only useful when computing Legendre symbols with odd entries. There is a separate formula for the Legendre symbol with the upper entry equal to \( 2 \):

**Theorem 9.3.2.** Let \( p \) be an odd prime. Then

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

Equivalently,

\[
\left( \frac{2}{p} \right) = \begin{cases} 1 & \text{if } p \equiv \pm1 \pmod{8} \\ -1 & \text{if } p \equiv \pm3 \pmod{8} \end{cases}
\]
In other words:

\[
\left(\frac{2}{p}\right) = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{8} \text{ or } p \equiv 7 \pmod{8} \\
-1 & \text{if } p \equiv 3 \pmod{8} \text{ or } p \equiv 5 \pmod{8}
\end{cases}
\]

Remark 9.3.3. It is implicit in the statement of this theorem that \(p^2 - 1\) is divisible by 8. In fact, for any odd number \(n\), \(n^2 \equiv 1 \pmod{8}\). Indeed, an odd number is congruent to 1, 3, 5 or 7 modulo 8. It is easy to check that the squares of these numbers are all congruent to 1 modulo 8.

Remark 9.3.4. Let us check that the two statements in theorem 9.3.2 are indeed equivalent. Let \(p\) be of the form \(8k \pm 1\). Then

\[
\frac{p^2 - 1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k
\]

is even. In the same way, if \(p\) is of the form \(8k \pm 3\),

\[
\frac{p^2 - 1}{8} = \frac{64k^2 \pm 48k + 8}{8} = 8k^2 \pm 6k + 1,
\]

which is odd. Thus, we see that \((-1)^{\frac{p^2 - 1}{8}}\) is indeed equal to 1 if and only if \(p \equiv \pm 1 \pmod{8}\), and to \(-1\) if and only if \(p \equiv \pm 3 \pmod{8}\).

Exercise 9.3.5. Compute the following Legendre symbols:

\[
\left(\frac{5}{43}\right), \left(\frac{7}{43}\right), \left(\frac{7}{41}\right), \left(\frac{7}{103}\right), \left(\frac{85}{101}\right), \left(\frac{14}{101}\right)
\]