Notes for Number theory (Fall semester)

Sophie Marques

August 2014

Contents

Introduction

The older term for number theory is arithmetic. By the early twentieth century, it had been superseded by "number theory". The word "arithmetic" (from the Greek, arithmos which means "number") is used by the general public to mean "elementary calculations"; it has also acquired other meanings in mathematical logic, as in Peano arithmetic, and computer science, as in floating point arithmetic. Arithmetic is the oldest and most elementary branch of mathematics, used very popularly, for tasks ranging from simple day-to-day counting to advanced science and business calculations. It involves the study of quantity, especially as the result of operations that combine numbers. The use of the term arithmetic for number theory regained some ground in the second half of the 20th century, arguably in part due to French influence. In particular, arithmetical is preferred as an adjective to number-theoretic.

Elementary arithmetic starts with the natural numbers and the written symbols (digits) which represent them. The process for combining a pair of these numbers with the four basic operations traditionally relies on memorized results for small values of numbers, including the contents of a multiplication table to assist with multiplication and division. Elementary arithmetic also includes fractions and negative numbers, which can be represented on a number line.

Number theory is devoted primarily to the study of the integers. Number theorists study prime numbers as well as the properties of objects made out of integers (e.g., rational numbers) or defined as generalizations of the integers (e.g., algebraic integers). Integers can be considered either in themselves or as solutions to equations (Diophantine geometry). Questions in number theory are often best understood through the study of analytical objects (e.g., the Riemann zeta function) that encode properties of the integers, primes or other number-theoretic objects in some fashion (analytic number theory). One may also study real numbers in relation to rational numbers, e.g., as approximated by the latter (Diophantine approximation).

Fixing notations

Symbol	Meaning
$\forall$	for all, for every;
$\exists$	there exists (at least one);
$\exists!$	there exists exactly one;
s.t.	such that;
$\Rightarrow$	implies;
$\Leftrightarrow$	if and only if;
$x \in A$	the point x belongs to a set A
$x \notin A$	the point x does not belongs to the set A
$\mathbb{N}$	the set of natural number (counting numbers) $1, 2, 3, \ldots$
$\mathbb{Z}$	the set of all the integers (positive, negative or zero)
$\mathbb{Q}$	the set of rational numbers
$\mathbb{R}$	the set of real numbers
$\mathbb{C}$	the set of complex numbers
$\{x \in A : P(x)\}$	the subset of the elements x in a set A such that the statement $P(x)$ is true
$\varnothing$	the empty set, the set with nothing in it
$x \in A$	means that the point x belongs to a set A or that x is a element of A
$A \subseteq B$	A is a subset of B i.e. any element of A also belongs to B (in symbolic notation: $x \in A \Rightarrow x \in B$ that we use when doing proofs).
$A = B$	the sets A and B contain exactly the same points This statement is equivalent to saying: $A \subseteq B$ AND $B \subseteq A$
$\{p\}$	singleton set (Logically speaking, the "point p" is not the same thing as "the sets $\{p\}$ whose only element is p.")
$A \cap B$	indicates the intersection of two sets; An element x is in $A \cap B \Leftrightarrow x \in A$ AND $x \in B$. Notice $A \cap B = B \cap A$.
$A \cup B$	the union of two sets. An element x lies in $A \cup B \Leftrightarrow$ Either $x \in A$ OR $x \in B$ (or BOTH). Notice $A \cup B = B \cup A$.

Symbol	Meaning
$\bigcap_{i=1}^{n} A_i = A_1 \cap \cdots \cap A_n$	the set $\{x : x \in A_i \textit{ for every } i\}$ where A_i are sets
$\bigcup_{i=1}^{n} A_i = A_1 \cup \cdots \cup A_n$	the set $\{x : \exists \textit{ some } i \textit{ such that } x \in A_i\}$ where A_i are sets
$\bigcap_{\alpha} A_\alpha$	the set $\{x : x \in A_\alpha \textit{ for every } \alpha \in I\}$ where A_α are sets and I a set of indexes
$\bigcup_{\alpha} A_\alpha$	the set $\{x : \exists \textit{ some } i \textit{ such that } x \in A_i\}$ where A_α are sets and I a set of indexes
$A \backslash B$	the difference set $\{x : x \in A \textit{ and } x \notin B\}$ (Note that $A \backslash B = A \cap B^c$.
A^c	the complement of a set A. Here A is a subset of some larger space X and its complement is the set $A^c = \{x \in X : x \notin A\} = X \backslash A$.
$A \times B$	the cartesian product $\{(a,b) \mid a \in A \textit{ and } b \in B\}$
$A_1 \times \cdots \times A_n = \prod_{i=1}^{n} A_i$	the product of the sets A_i $\{(a_1, \ldots, a_n) \mid a_i \in A_i\}$
$\prod_{i=1}^{\infty} A_i$	the product of the sets A_i $\{(a_1, \ldots, a_n, \ldots) \mid a_i \in A_i\}$
$\prod_{\alpha \in I} A_\alpha$	the set consisting of all indexed words $(a_\alpha)_{\alpha \in I}$, where $a_\alpha \in A_\alpha$. These are the maps $\phi : I \to \cup_{\alpha \in I} A_\alpha$ such that $\phi(\alpha) \in A_\alpha$ for every index $\alpha \in I$.

Mappings

$\phi : \begin{array}{ccc} X & \to & Y \\ x & \mapsto & \phi(x) \end{array}$	A map ϕ from a set X to another set Y is an operation that associates each element in X to a single element in Y. Unless stated otherwise, mapping $\phi(x)$ are assumed to be defined for every $x \in X$. If not,
$Def(\phi)$	domain of definition of ϕ, i.e. the points such that ϕ is defined.
$Range(\phi) = \phi(X)$	the range of the map ϕ i.e. $\{b \in Y : \exists a \in X \textit{ such that } b = \phi(a)\}$
$\phi(S)$	the forward image for any subset of $S \subseteq X$ i.e. $\{b \in Y : \exists a \in S \textit{ such that } b = \phi(a)\} = \{\phi(a) : a \in A\}$
$\phi : X \hookrightarrow Y$	ϕ is injective or "one-to-one" i.e. if $a_1 \neq a_2 \Rightarrow \phi(a_1) \neq \phi(a_2)$
$\phi : X \twoheadrightarrow Y$	ϕ is surjective i.e. if $\phi(X) = Y$
$\phi : X \simeq Y$	ϕ is bijective i.e. ϕ is both one-to-one and onto i.e. $\forall b \in Y, \exists! a \in X$ such that $\phi(a) = b$
$\psi = \phi$	$\phi, \psi : X \to Y$ are equal, i.e. they have same action: $\phi(a) = \psi(a)$ for all $a \in X$. (Ex: $(x^2 + x^4)/(1 + x^2) = x^2$.)
$\Gamma(\phi)$	the graph of $\Gamma(\phi)$ which is a subset of the Cartesian product set $X \times Y$: $\{(x,y) \in X \times Y : y = \phi(x)\} = \{(x, \phi(x)) : x \in X\}$
$(x) \times Y$	"vertical fiber" for each $x \in X$, $\{(x,y) : y \in Y\}$ $= \{\textit{all points } (a,b) \in X \times Y \textit{ such that } a = x\}$ $\Gamma(\phi) \cap ((x) \times Y) = \{(x,b)\}$ with $b = \phi(x)$, knowing ϕ is equivalent with knowing $\Gamma(\phi)$.
$id_X : X \to X$	the identity map on X sending each point $x \in X$ to x itself.
$\phi^{-1} : Y \to X$	the inverse map of $\phi : X \to Y$ such that $\phi^{-1}(\phi(a)) = a$, for all $a \in X$ and $\phi(\phi^{-1}(b)) = b$, for all $b \in Y$ $\phi^{-1}(b) =$ the unique element $a \in X$ such that $\phi(a) = b$.

Part I

Arithmetic of $\mathbb{Z}$, divisibility theory

Chapter 1

Interlude on natural numbers, induction and well ordering

Natural numbers are the set $\mathbb{N} = \{1, 2....\}$ will interest us along this course. There is an important principle, or method of proof, which applies to this number system, but not any other standard number systems , such as the set $\mathbb{Z}$ of all the integers, or the sets $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ of rational, real or complex numbers. There are three versions of this principle, known as the principle of induction, the most familiar, the principle of strong induction and the well-ordering principle; there are logically equivalent, in the sense that each implies the other, but in different contexts one of them may be more convenient to use than the other.

Theorem 1.0.1. *The following principles are equivalent:*

1. ***The principle of induction (version 1):*** *Let $P(n)$ be statements indexed by natural integers. If $P(1)$ is true, and $P(n)$ implies $P(n+1)$, for all $n \in \mathbb{N}$, then $P(n)$ is true for any $n \in \mathbb{N}$.*
2. ***The principle of induction (version 2):*** *Suppose that $A \subseteq \mathbb{N}$, that $1 \in A$, and that $n \in A$ implies $n+1 \in A$ for any $n \in \mathbb{N}$; then $A = \mathbb{N}$.*
3. ***The principle of strong induction (version 1):*** *If $P(1)$ is true, and $P(1)$, $P(2)$, ... , $P(n)$ together imply $P(n+1)$, then $P(n)$ is true for all $n \in \mathbb{N}$.*
4. ***The principle of strong induction (version 2):*** *Suppose that $B \subseteq \mathbb{N}$, that $1 \in B$, and that if $1, 2, .., n \in B$, then $n+1 \in B$; then $B = \mathbb{N}$*
5. ***The well-ordering principle:*** *If $C \subseteq \mathbb{N}$ and C is non-empty, then C has a least element for the order $\geqslant$ on $\mathbb{N}$ (that is there is a $c \in C$ such that $c \geqslant d$ for all $d \in C$).*

Proof. To see that 1. implies 2.. Assume 1., and suppose that A satisfies the hypothesis of 2.. Let $P(n)$ be the statement $n \in A$, so $P(1)$ is true, since $1 \in A$; if $P(n)$ is true then $n \in A$, so $n+1 \in A$, and hence $P(n+1)$ is true; thus $P(n)$ implies $P(n+1)$, so $P(n)$ is true for all $n \in \mathbb{N}$ by 1.; thus $n \in A$, for any $n \in \mathbb{N}$, so $A = \mathbb{N}$. For the converse (that 2. implies 1.), given $P(n)$ take $A = \{n \in \mathbb{N} | P(n) \textit{ is true}\}$, then $1 \in A$ (since $P(1)$ is true),

and if $n \in A$ then $P(n)$ is true, so $P(n+1)$ is true, giving $n+1 \in A$; hence $A = \mathbb{N}$ by **2.** so $P(n)$ is true for all $n \in \mathbb{N}$.
Similarly, we obtain that **3.** is equivalent to **4.**.
To see that **2.** implies **4.** Suppose that B satisfies the hypotheses of **4.**. Let

$$A = \{n \in \mathbb{N} | 1, ..., n \in B\}$$

Then $A \subseteq \mathbb{N}$, and $1 \in A$ (since $1 \in B$). If $n \in A$ then $1, 2, ..., n \in B$ and hence $n+1 \in A$ (by definition of A); thus $n \in A$ implies $n+1 \in A$, so $A = \mathbb{N}$, by **2.** This means that for each $n \in \mathbb{N}$, we have $1, 2, .., n \in B$, so, in particular $n \in B$; thus $B = \mathbb{N}$, as required.
To see that **4.** implies **5.**, we show that if $C \subseteq \mathbb{N}$, and C has no least element then C is empty. Let $B = \mathbb{N} \backslash C$, the complement of C in $\mathbb{N}$. Then $1 \in B$, for otherwise $1 \in C$ and so 1 is a least element of C (since it is a least element of $\mathbb{N}$). If $1, 2, ..., n \in B$ then $1, 2, ..., n \notin C$; it follows that $n+1 \notin C$ (for otherwise $n+1$ would be a least element of C), so $n+1 \in B$. Thus B satisfies the hypotheses of **4.**, so $B = \mathbb{N}$ and C is empty.
To see that **5.** implies **2.**, suppose that A satisfies the hypotheses of **2.**, and let $C = \mathbb{N} \backslash A$. If C is non empty, then it has a least element c. Since $1 \in A$ (since $0 \in A$) then $c \neq 1$, so $c - 1 \in \mathbb{N}$. Now, $c - 1 \notin C$ (for otherwise c could not be a least element of C), and hence $c - 1 \in A$. But $n \in A$ implies $n + 1 \in A$, then $c \in A$, which is a contradiction. So C is empty and $A = \mathbb{N}$. □

Remark 1.0.2.
1. *We can also start the induction process from $n_0 \neq 0$. For instance, the principle of induction becomes: If $P(n_0)$ is true, and $P(n)$ implies $P(n+1)$, for some $n > n_0$, then $P(n)$ is true for any $n \geqslant n_0$.*
2. *The principle of strong induction is used instead of the principle of induction the hypothesis $P(n)$ alone is not strong enough to prove $P(n+1)$.*
3. *The well-ordering principle is easily seen to be false if we replace $\mathbb{N}$ with any of the other standard number system: for instance, the set of the strictly positive rational numbers has no least element.*
4. ***The previous principle implies 0 element, the 1 element and the addition $+$ (as initial data) are enough to get all the natural integer.** We will see that it is not so simple with the multiplication.*

Chapter 2

Divisibility

2.1 Definition of divisibility

In mathematics, the notion of a divisor originally arose within the context of arithmetic of whole numbers. With the development of abstract rings, of which the integers are the archetype, the original notion of divisor found a natural extension. We recall here the notion of divisibility for integers.

Definition 2.1.1. *Let a and b be integers, $a \neq 0$. We say that* ***a divides b****, denoted by $a|b$, if there exist an integer c such that $b = ca$. We also say* ***b is divisible by a****, **b is a multiple of a** or **a is a divisor of b**.*

Example 2.1.2. $2|6$, $-3|9$, $-5|-10$, $4|0$, $3 \nmid 7$.

Remark 2.1.3. *Let's insist on the following trivial facts.*

1. $1|n$, *for any* $n \in \mathbb{Z}$,
2. $0 \nmid n$, *for any* $n \in \mathbb{Z}$.
3. $n|0$, *for any* $n \in \mathbb{Z}$ *which is non-zero.*

We enumerate some of the basic, trivial but essential properties about divisibility with the following theorem.

Theorem 2.1.4. *Let a, b, c, x, y be integers.*

1. *If $a|b$, the $a|xb$.*
2. *If $a|b$ and $a|c$, then $a|bx + cy$.*
3. *If $a|b$ then $xa|xb$.*
4. *If $a|b$, then $|a| \leqslant |b|$. In particular, if $a|b$ and $b|a$, then $a = \pm b$.*

2.2 Some divisibility tests

For practical as well as theoretical purposes we often want to establish test to see wether an integer is divisible by a certain number.

2.2.1 Divisibility by 10^n, 5, 25

We recall the following divisibility test. The proof is left to the reader, he can use a similar proof as the one of the following section.

Test 2.2.1. *1. A number is divisible by 10^n if and the last n digits are zeros.*

2. A number is divisible by 5 if and only if the last digit is 0 or 5.

3. A number is divisible by 25 if and only if the last two digits are divisible by 25.

2.2.2 Divisibility by a power of 2

Test 2.2.2. *Let n be a positive integer. A number is divisible by 2^n if and only if the last n digits are divisible by 2^n.*

Proof. Let $d_m d_{m-1}...d_1 d_0$ a m-digits number. We have

$$d_m d_{m-1}...d_2 d_1 = d_m d_{m-1}...d_{n+1} \times 10^n + d_n...d_1.$$

Note that $2^n | 10^n$, then also $2^n | d_m d_{m-1}...d_1 \times 10^n$. As a consequence, $2^n | d_m d_{m-1}...d_2 d_1$ if and only if $2^n | d_n...d_2 d_1$. □

Example 2.2.3. *Take 123456 as an example. Since 56 is divisible by 4, we know that 123456 is also divisible by 4.*

2.2.3 Divisibility by 3 and 9

Test 2.2.4. *A number is divisible by 3 (reps. 9) if and only if its sum of digits is divisible by 3 (resp. 9).*

Proof. Let $d_m d_{m-1}...d_1 d_0$ a $m+1$-digits number. Write $9_{(p)}$ for the p-digits number $9...9$. We have

$$\begin{aligned} d_m d_{m-1}...d_1 d_0 &= d_m \times 10^m + d_{m-1} \times 10^{m-1} + ... + d_0 \times 10^0 \\ &= d_m \times (1 + 9_{(m)}) + d_{m-1} \times (1 + 9_{(m-1)}) + ... + d_1 \times (1 + 9) + d_0 \\ &= 9 \times (d_m \times 1_{(m)} + d_{m-1} \times 1_{(m-1)} + ...d_1) + (d_m + ... + d_0). \end{aligned}$$

Note that 3 and 9 divides $9 \times (d_m \times 1_{(m)} + d_{m-1} \times 1_{(m-1)} + ...d_1)$. As a consequence, we have that 3 (resp. 9) divides $d_m d_{m-1}...d_1 d_0$ if and only if 3 (resp. 9) divides $(d_m + ... + d_0)$. □

Example 2.2.5. *Take 123456 as an example. Since $1+2+3+4+5+6 = 21$ is divisible by 3 but not 9, we know that 123456 is also divisible by 3 but not 9.*

2.2.4 Divisibility by 11

Test 2.2.6. *The $n+1$-digit number $a_n...a_0$ is divisible by 11 if and only if the alternating sum of the digits $(-1)^n a_n + (-1)^{n-1} a_{n-1} + ... - a_1 + a_0$ is divisible by 11.*

Proof. Let $d_m d_{m-1}...d_1 d_0$ a $m+1$-digits number. We have

$$\begin{aligned} & d_m d_{m-1}...d_1 d_0 \\ = \; & d_m \times 10^m + d_{m-1} \times 10^{m-1} + ... + d_0 \times 10^0 \\ = \; & d_m \times ((11-1)^m + d_{m-1} \times (11-1)^{m-1} + ... + d_1 \times (11-1)) + d_0 \\ = \; & 11 \times m + (d_m + (-1)^{m-1} d_{m-1} + ... + d_0). \end{aligned}$$

As a consequence, we have that 11 divides $d_m d_{m-1}...d_1 d_0$ if and only if 11 divides $(d_m + (-1)^{m-1} d_{m-1} + ... + d_0)$. □

2.2.5 More divisibility test

We have that

Test 2.2.7. *1. A number is divisible by* 6 *if and only if it is divisible by both* 2 *and* 3*,*

2. A number is divisible by 12 *if and only if it is divisible by* 3 *and* 4*.*

In general, if $p|n$, $q|n$, can we say that $pq|n$? If not what we can say ? You should be able to answer to this question after studying this and the next section.
More divisibility test will be discussed in the exercises.

2.3 G.C.D. and L.C.M.

In this section we shall go other the familiar concept of *G.C.D.* (or *H.C.F.*) and *L.C.M.*, as well as some of their important properties.

Definition 2.3.1. *Let a and b be integers, not both zeros. The* ***greatest common divisor*** *(also called* ***highest common factor****, abbreviated as G. C. D. or H. C. F.) of a and b, denoted as $gcd(a,b)$, is defined to be the largest integer which divides both a and b.*
That is $d = gcd(a,b)$.

1. $d|a$ and $d|b$;

2. $d > 0$;

3. For any $d' \in \mathbb{Z}$ such that $d'|a$ and $d'|b$ then $d'|d$.

Example 2.3.2. *1. $gcd(24,36) = 12$,*

2. $gcd(-8,6) = 2$,

3. $gcd(2,-9) = 1$.

Definition 2.3.3. *Let a and b be integers, not both zeros. The* ***lowest common divisor*** *(abbreviated as L. C. M.) of a and b, denoted as $lcm(a,b)$, is defined to be the largest integer which divides both a and b.*
That is $d = lcm(a,b)$.

1. $a|d$ and $b|d$;

2. $d > 0$*;*

3. For any $d' \in \mathbb{Z}$ *such that* $a|d'$ *and* $b|d'$ *then* $d|d'$*.*

Example 2.3.4. *1.* $lcm(24, 36) = 72$*,*

2. $lcm(-8, 6) = 24$*,*

3. $lcm(2, -9) = 18$*.*

The G. C. D and L. C. M. of more than two integers can be similarly defined.

2.4 Prime and coprime numbers

Definition 2.4.1. *We say that an integer* $p > 1$ *is a* ***prime integers*** *if its only divisors are* 1 *and itself. An integer* $n > 1$ *which is not prime (such as* 4, 6, 8, 9*...) is said to be* ***composite****; such an integer integer has the form* $n = ab$ *where* $1 < a < n$ *and* $1 < b < n$*.*

Example 2.4.2. 2, 3 ,5, 7 *are prime integers.*

Remark 2.4.3. *1. Note that* 1 *is not prime.*

2. The smallest prime is 2 *and the other prime are odd.*

Definition 2.4.4. *We say that two non-zero integers* a *and* b *are* ***coprime*** *if* $gcd(a, b) = 1$*.*

Example 2.4.5. *1.* 12 *and* 35 *are coprime since* $gcd(12, 35) = 1$*.*

2. 12 *and* 21 *are not coprime since* 3 *divides* 12 *and* 21*.*

3. Two distinct primes are always coprime.

In order to find specific examples of prime it seems reasonable to look at integers of the form $2^m \pm 1$, since many small primes, such as 3, 5, 7, 17, 31,...

Exercise 2.4.6 (Fermat numbers). If $2^m + 1$ is prime then $m = 2^n$ for some integer $n \geqslant 0$.

Indeed: *We prove the contrapositive, that if* m *is not a power of* 2 *then* $2^m + 1$ *is not prime. If* m *is not a power of* 2*, then* m *has the form* $2^n q$ *for some odd* $q > 1$*. Now the polynomial* $f(t) = t^q + 1$ *has a root* $t = -1$ *because* q *is odd, so it is divisible by* $t + 1$*; this is a proper factor since* $q > 1$*, so putting* $t = x^{2^n}$ *we see that the polynomial* $g(x) = f(x^{2^n}) = x^m + 1$ *has a proper factor* $x^{2^n} + 1$*. Taking* $x = 2$ *we see that* $2^{2^n} + 1$ *is a proper factor of the integer* $g(2) = 2^m + 1$*, which cannot therefore be prime.*

Numbers of the form $F_n = 2^{2^n} + 1$ *are called* ***Fermat numbers****, and those which are prime are called* ***Fermat primes****.*

Fermat conjecture that F_n *is prime for every* $n \geqslant 0$*. For* $n = 0, .., 4$ *the number* F_n *are indeed prime, but in 1732 Euler showed that the next Fermat number* $F_5 = 2^{2^5} + 1 = 641 \times 67000417$ *is a composite. The fermat numbers have been studied intensively, often*

with the aid of computers, but no further Fermat primes have been found. It is conceivable that there are further Fermat primes (perhaps infinitely many) which we have not yet found, but the evidence is not very convincing.

These primes are important in geometry: in 1801 Gauss showed that a regular polygon with k sides can be constructed by ruler-and-compass methods if and only if $k = 2^e p_1 ... p_r$ where $p_1, \ldots, p_r$ are Fermat primes.

Even if not many of the Fermat number F_n turn out to be composite, the following result shows that their factors include an infinite set of primes, since distincts Fermat numbers F_n are mutually coprime.
Indeed: *Let $d = (F_n, F_{n+k})$ be the G.C.D. of the two Fermat numbers F_n and F_{n+k}, where $k > 0$. The polynomial $x^{2^k} - 1$ has a root $x = -1$, so it is divisible by $x + 1$. Putting $x = 2^{2^n}$, we see that F_n divides $F_{n+k} - 2$, so d divides 2 and hence d is 1 or 2. Since all Fermat numbers are odd, $d = 1$.*

Exercise 2.4.7 (Mersenne numbers). If $m > 1$ and $a^m - 1$ is prime, then $a = 2$ and m is prime.
Indeed: *$a - 1 | a^m - 1$ so if $a \neq 2$, $a - 1 > 1$ and $a^m - 1$ is not prime. Suppose now that m is not prime write m as $m = pq$ where $0 < p < m$ and $0 < q < m$, $a^p - 1 | (a^p)^q - 1$ and $a^m - 1$ is not prime.*

Integers of the form $M_p = 2^p - 1$, where p is a prime, are called ***Mersenne numbers*** *after Mersenne who studied them in 1644; those which are called* ***Mersenne prime****. For $p = 2, 3, 5, 7$, the Mersenne numbers $M_p = 3, 7; 31; 127$ are indeed prime, but $M_{11} = 2047 = 23 \times 89$ is not prime, so M_p is not prime for every prime p. At the time of writing, 35 Mersenne primes have been found, the latest being $M_{1257787}$ and $M_{1398269}$ (discovered in 1996 by David Slowinski and Joel Armeugaud respectively, with the aid of computers). As in the case of the Fermat primes, it is not known whether there are finitely or infinitely many Mersennes primes. But we can also prove as for Fermat primes that two distinct Mersenne number are coprime.*

Chapter 3

Euclidean division, Bezout theorem, linear diophantine equations

3.1 Euclidean division

We recall the following lemma establishing the Euclidean division, which is intrinsic in our mind.

Lemma 3.1.1. *Let a and b be integers, $a \neq 0$. There exists unique integers q and r such that*

$$a = bq + r$$

with $0 \leqslant r < |a|$.

Proof. The proof consists of two parts: first, the proof of the existence of q and r, and second, the proof of the uniqueness of q and r.

— **Existence**

Consider first the case $b < 0$. Setting $b' = -b$ and $q' = -q$, the equation $a = bq + r$ may be rewritten $a = b'q' + r$ and the inequality $0 \leqslant r < |b|$ may be rewritten $0 \leqslant r < |b'|$. This reduces As a consequence, without loss of generality one can suppose that $b > 0$.

Now, if $a < 0$ and $b > 0$, setting $a' = -a$, $q' = -q - 1$ and $r' = b - r$, the equation $a = bq + r$ may be rewritten $a' = bq' + r'$ and the inequality $0 \leqslant r < b$ may be rewritten $0 \leqslant r' < b$. Thus the proof of the existence is reduced to the case $a \geqslant 0$ and $b > 0$ and we consider only this case in the remainder of the proof.

Let q_1 and r_1, both nonnegative, such that $a = bq_1 + r_1$, for example $q_1 = 0$ and $r_1 = a$. If $r_1 < b$, we are done. Otherwise $q_2 = q_1 + 1$ and $r_2 = r_1 - b$ satisfy $a = bq_2 + r_2$ and $0 < r_2 < r_1$. Repeating this process one gets $q = q_k$ and $r = r_k$ such that $a = bq + r$ and $0 \leqslant r < b$. Indeed $(r_n)_{n \in \mathbb{N}}$ is a decreasing sequence of positive integer so the process must terminates.

This proves the existence and also gives a simple division algorithm to compute the quotient and the remainder. However this algorithm needs q steps and is thus not efficient.

— **Uniqueness**
Suppose there exists q, q', r, r' with $0 \leqslant r,\ r' < |b|$ such that $a = bq + r$ and $a = bq' + r'$. Adding the two inequalities $0 \leqslant r < |b|$ and $-|b| < -r' \leqslant 0$ yields $-|b| < r - r' < |b|$, that is $|r - r'| < |b|$.
Subtracting the two equations yields: $b(q' - q) = (r - r')$. Thus $|b|$ divides $|r - r'|$. If $|r - r'| \neq 0$ this implies $|b| < |r - r'|$, contradicting previous inequality. Thus, $r = r'$ and $b(q' - q) = 0$. As $b \neq 0$, this implies $q = q'$, proving uniqueness.

□

Example 3.1.2. *Let* $a = 13$, $b = 100$. *Then* $100 = 13 \times 7 + 9$ *(i.e.* $q = 7$, $r = 9$*).*

3.2 Euclidean algorithm

In school we have learnt various methods of computing the G.C. D. and the L. C. M. of a given of integers. Property (4) suggests a useful, simple and yet less commonly used way of computing the G. C. D. by the **Euclidean algorithm**. An algorithm is a definite procedure for solving problems or performing tasks. Let first state a simple but essential lemma for establishing the Euclidean Algorithm.

Lemma 3.2.1. *If* a, b, q, r *are integers and* $a = bq + r$, *then* $gcd(a, b) = gcd(b, r)$.

Proof. Any common divisor of b and r also divides $qb + r = a$; similarly, since $r = a - qb$, it follows that any common divisor of a and b divides r. Thus two pair a, b and b , r have the same common divisors, so they have the same greatest common divisor. □

We can now describe the Euclidean algorithm. For simplicity we assume that we are going to find the G. C. D. to two positive integers.

Theorem 3.2.2. *Let* a *and* b *be positive integers,* $a > b$. *Then we apply a series of divisions as follows.*

$$\begin{array}{rcll} a & = & bq_0 + r_1 & 0 \leqslant r_1 < b, \\ b & = & r_1 q_1 + r_2 & 0 \leqslant r_2 < r_1, \\ r_1 & = & r_2 q_2 + r_3 & 0 \leqslant r_3 < r_2, \\ & & . & \\ & & . & \\ & & . & \\ r_{n-2} & = & r_{n-1} q_{n-1} + r_n & 0 < r_n < r_{n-1}, \\ r_{n-1} & = & r_n q_n. & \end{array}$$

The process of division comes to an end when $r_{n+1} = 0$. *The integer* r_n *is the G. C. D. of* a *and* b.

Proof. The idea is to keep repeating the division algorithm. We have:

$$\begin{array}{rcll} a & = & bq_1 + r_1, & 0 \leqslant r_1 < b, \quad gcd(a,b) = gcd(b,r_1), \\ b & = & r_1q_2 + r_2, & 0 \leqslant r_2 < r_1, \quad gcd(b,r_1) = gcd(r_1,r_2), \\ r_1 & = & r_2q_3 + r_3, & 0 \leqslant r_3 < r_2, \quad gcd(r_1,r_2) = gcd(r_2,r_3), \\ & & . & \\ & & . & \\ & & . & \\ r_{n-2} & = & r_{n-1}q_n + r_n, & 0 \leqslant r_n < r_{n-1}, \quad gcd(r_{n-2},r_{n-1}) = gcd(r_{n-1},r-n) \\ r_{n-1} & = & r_nq_{n+1}, & \quad gcd(r_{n-1},r_n) = r_n \end{array}$$

In fact, $(r_k)_k$ constitute a sequence strictly decreasing of positive integer, this insure that there is an n such that $r_n = 0$. Therefore

$$gcd(a,b) = gcd(b,r_1) = gcd(r_1,r_2) = ...gcd(r_{n-2},r_{n-1}) = gcd(r_{n-1},r_n) = r_n.$$

□

Example 3.2.3. *We want to find the G. C. D. of* 2445 *and* 652*. We have*

$$\begin{array}{rcl} 2445 & = & 652 \times 3 + 489 \\ 652 & = & 489 \times 1 + 163 \\ 489 & = & 163 \times 3 \end{array}$$

Then by this Euclidean algorithm, we get that $gcd(2445, 652) = 163$.

3.3 Bezout's identity

The following result uses Euclid's algorithm to give a simple expression for $d = gcd(a,b)$ in terms of a and b:

Theorem 3.3.1. *Let* a *and* b *be integers with* $gcd(a,b) = d$*. There exist integers* u *and* v *such that*

$$au + bv = d.$$

Such u*,* v *can be obtained by backward tracing of the Euclidean divisions in finding the G. C. D.*

Proof. Let apply the Euclidean algorithm to a and b, we have the following series of division

$$\begin{array}{rcll} a & = & bq_0 + r_1 & 0 < r_1 < b, \\ b & = & r_1q_1 + r_2 & 0 < r_2 < r_1, \\ r_1 & = & r_2q_2 + r_3 & 0 < r_3 < r_2, \\ & & . & \\ & & . & \\ & & . & \\ r_{n-2} & = & r_{n_1}q_{n-1} + r_n & 0 < r_n < r_{n-1}, \\ r_{n-1} & = & r_nq_n. & \end{array}$$

such that $r_n = d$ and $r_{n+1} = 0$.
Then we notice first that

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

Then, we have

$$d = r_{n-2}v_n + r_{n-1}u_n$$

with $v_n = 1$ and $u_n = -q_{n-1}$.
Injecting the following in the previous equality,

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

we find two integer u_{n-1} and v_{n-1}

$$d = r_{n-3}v_{n-1} - r_{n-2}u_{n-1}$$

So that reiterating the process until the top of the Euclidean algorithm, we finally find integers u and v such that

$$au + bv = d.$$

This is the process is known as the **extended Euclidean algorithm**. □

Theorem 3.3.2. *Let a and b be integers (not both 0) with greatest common divisor d. Then, an integer c has the form $ax + by$ for some $x, y \in \mathbb{Z}$ if and only if c is a multiple of d. In particular, d is the least positive integer of the form $ax + by$ $(x, y \in \mathbb{Z})$.*

Proof. If $c = ax + by$ where $x, y \in \mathbb{Z}$, then since d divides a and b, from Theorem 2.1.4, implies that d divides c. Conversely, if $c = de$ for some integer e, then by the previous theorem, by writing $d = au + bv$, we get $c = due + bve = ax + by$, where $x = ue$ and $y = ve$ are both integers. Thus the integers of the form $ax+by$ $(x, y \in \mathbb{Z})$ are multiple of d, and the least positive integers of this form is the least positive multiple of d, namely d itself. □

The next corollary follows easily.

Corollary 3.3.3. *Two integers a and b are coprime if and only if there exist integers x and y such the*

$$ax + by = 1.$$

Example 3.3.4. *Take the example of finding the G. C. D. of 2445 and 652 again. Again by the Euclidean algorithm, we have:*

$$\begin{aligned} 2445 &= 652 \times 3 + 489 \\ 652 &= 489 \times 1 + 163 \\ 489 &= 163 \times 3 \end{aligned}$$

Applying the extended Euclidean algorithm, we obtain:

$$\begin{aligned} 163 &= 652 - 489 \\ &= 652 - (2445 - 652 \times 3) \\ &= 652 \times 4 - 2445 \end{aligned}$$

We see that

$$163 = 2445 \times (-1) + 652 \times 4$$

as desired.

Thanks to the previous theorem, we obtain the next theorem which gives some basic properties of G. C. D. and L. C. M..

Corollary 3.3.5. *Let a, b, c and m be non-zero integers. Then*

1. $gcd(ma, mb) = |m|gcd(a, b)$.
2. $gcd(a, m) = gcd(b, m) = 1$ *if and only if* $gcd(ab, m) = 1$,
3. $c|ab$ *and* $gcd(b, c) = 1$ *imply* $c|a$,
4. $a|c$, $b|c$ *and* $gcd(a, b) = 1$ *imply* $ab|c$
5. $gcd(a, b) = gcd(b, a) = gcd(a, b + ma)$,
6. $gcd(a, b)lcm(a, b) = |ab|$.

Proof.

1. First, we have $m \cdot gcd(a, b)|ma$ and $m \cdot gcd(a, b)|mb$. Thus, $m \cdot gcd(a, b)|gcd(ma, mb)$. By Bezout theorem, there are integers x and y such that $ax + by = gcd(a, b)$. Multiplying by m, we get $max + mby = m \cdot gcd(a, b)$. So that $gcd(ma, mb)|m \cdot gcd(a, b)$.
2. If $gcd(ab, m) = 1$ then there are integers x and y such that $abx + my = a(bx) + my = b(ax) + my = 1$. Thus $gcd(a, m) = gcd(b, m) = 1$. Suppose now that $gcd(a, m) = gcd(b, m) = 1$ then there are integers x, y, x', y' such that $ax + my = bx' + my' = 1$, then multiplying the equation one gets $gcd(ax + my)gcd(bx' + my') = 1$, then $ab(xy') + m(ybx' + ymy' + axy') = 1$. Thus, $gcd(ab, m) = 1$.
3. Suppose that $c|ab$ and $gcd(b, c) = 1$ then there are integers x and y such that $1 = bx + cy$. Multiplying by a, we obtain $a = abx + acy$, since $c|abx$ and $c|acy$, then $c|a$.
4. We know that since $gcd(a, b) = 1$, there are integers x and y such that $ax + by = 1$. Moreover, since $a|c$ and $b|c$, there are integers e and f such that $c = ae$ and $c = bf$. Then $c = cax + cby = bfax + aeby = ab(fx + ey)$. Thus $ab|c$ as required.
5. $gcd(a, b)|a$ and $gcd(a, b)|b$ then also $gcd(a, b)|gcd(a, b + ma)$. We have $gcd(a, b)|a$ and $gcd(a, b)|b + ma$. By definition, $gcd(a, b + ma)|gcd(a, b)$. Then $gcd(a, b) = gcd(a, b + ma)$.
6. Suppose that a and b are positive for simplicity. Let $e = a/gcd(a, b)$ and $f = b/gcd(a, b)$, then $ab/gcd(a, b) = gcd(a, b)e \cdot gcd(a, b)f/gcd(a, b) = gcd(a, b)ef = af = eb$. Thus, $a|(ab/gcd(a, b))$ and $b|(ab/gcd(a, b))$. Let now consider an integer m such that $a|m$ and $b|m$. We know that there are integers x and y such that $gcd(a, b) = ax + by$ then $m \cdot gcd(a, b) = cax + cby$, but $ab|cax$ and $ab|cby$, so $ab|m \cdot gcd(a, b)$, in particular $ab/gcd(a, b)|m$. So that $lcm(a, b) = ab/gcd(a, b)$.

□

Example 3.3.6. *Prove that the fraction* $(21n + 4)/(14n + 3)$ *is irreducible for every natural number* n.

Solution
We have

$$gcd(21n+4, 14n+3) = gcd(7n+1, 14n+3) = gcd(7n+1, 1) = 1$$

for every natural number n*. This means that* $21n+4$ *and* $14n+3$ *have no common divisor and hence the fraction irreducible.*

3.4 Application: linear diophantine equations.

Theorem 3.4.1. *Let* a*,* b *and* c *be integers, with* a *and* b *not both* 0*, and let* $d = gcd(a, b)$*. Then the equation*

$$ax + by = c$$

has an integer solution x*,* y *if and only if* c *is a multiple of* d*, in which case there are infinitely many solutions. There are the pairs*

$$x = x_0 + \frac{bn}{d},\ y = y_0 - \frac{an}{d}\ (n \in \mathbb{Z}),$$

where x_0*,* y_0 *is any particular solution.*

Proof. The fact that there is a solution if and only if $d|c$ is merely a restatement of Theorem 3.3.2. Then, let x_0, y_0 be a particular solution found by the extended euclidian algorithm. So,

$$ax_0 + by_0 = c.$$

If we put

$$x = x_0 + \frac{bn}{d},\ y = y_0 - \frac{an}{d}$$

where n is any integer, then

$$ax + by = a\big(x_0 + \frac{bn}{d}\big) + b\big(y_0 - \frac{an}{d}\big) = ax_0 + by_0 = c,$$

so x*,* y is also a solution. (Note that x and y are integers since d divides b and a respectively.) This gives us infinitely many solutions, for different integers n. To show that these are the only solutions, let x, y be any integer solution, so $ax + by = c$. Since $ax + by = c = ax_0 + by_0$ we have

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

so dividing by d we get

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

Now a and b are not both 0, and we can suppose that $b \neq 0$ (if not, interchange the roles of a and b in what follows). Since b/d divides each side of the previous equality

and it is coprime to a/d by Theorem 3.3.5, a., it divides $x - x_0$ by Theorem 3.3.5, c. Thus $x - x_0 = bn/d$ for some integer n, so

$$x = x_0 + \frac{bn}{d}.$$

Substituting back for $x - x_0$, we get

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

So dividing by b/d (which is non-zero) we have

$$y = y_0 - \frac{an}{d}$$

. □

Example 3.4.2. *Find all the integer solutions of*

$$56x + 76y = 40 \quad (E)$$

Solution: *Run the EEA to find GCD and particular solution for the equation. From the EA, we have:*

$$\begin{aligned} 72 &= 56 \times 1 + 16 \\ 56 &= 16 \times 3 + 8 \\ 16 &= 8 \times 2 + 0 \end{aligned}$$

Then $gcd(56, 72) = 8$.
From the EEA we get :

$$\begin{aligned} 78 &= 56 - 16 \times 3 \\ &= 56 - (72 - 56) \times 3 \\ &= 4 \times 56 - 3 \times 72 \end{aligned}$$

Then

$$40 = 8 \times 5 = 56 \times 20 - 15 \times 72.$$

This give $x_0 = 20$ *and* $y_0 = -15$ *as a particular solution.*
Let (x, y) *be a general solution, we have then:*

$$56 \times x + 72 \times y = 40 = 56 \times x_0 + 72 \times y_0.$$

Then

$$7(x - x_0) = 9(y - y_0)$$

Since $(7, 9) = 1$ *then by Euclid's lemma, since* 7 *divides* $9(y - y_0)$, 7 *divides* $(y - y_0)$. *So, there is an integer* k *such that* $y - y_0 = 7k$. *Injecting this equation to the later one, we obtain* $x - x_0 = 9k$. *So, a general solution is of the form*

$$\begin{cases} x = 9k + 20 \\ y = 7k - 15 \end{cases}$$

where k *is a integer.*

Chapter 4

The fundamental theorem of arithmetic

4.1 The theorem

Lemma 4.1.1. *Let p be a prime, and let a and b any integers. Then*

1. *either p divides a, or a and p are coprime;*
2. *p divides ab if and only if p divides a or p divides b.*

Proof. 1. By definition, $gcd(a,p)$ divides p so it is either 1 or p, since p is prime. If $gcd(a,b) = p$, in particular $p|a$. Otherwise, $gcd(a,b) = 1$, and a and b are coprime.

2. If $p \mid a$ or $p \mid b$, then $p \mid ab$. Conversely, if $p|ab$. Suppose that $p \nmid a$, then $gcd(a,p) = 1$, by 1. So there are integers x and y such that $ax + py = 1$. Multiplying by b, we obtain $bax + bpy = b$. But then, $p|bax$ by assumption and clearly, $p|bpy$. Thus $p|b$.

□

Remark 4.1.2. *Both parts of the lemma can fail if p is not prime: take $p = 4$, $a = 6$ and $b = 10$, for instance.*

We can extend by induction 2. of the previous lemma to product of any numbers of factors.

Corollary 4.1.3. *If p is prime and p divides $a_1...a_k$, then p divides a_i for some i.*

Proof. We use induction on k. If $k = 1$ then the assumption is that $p|a_1$, so the conclusion is automatically true (with $i = 1$). Now assume that $k > 1$ and that the result is proved for all products of $k - 1$ factors a_i. If we put $a = a_1...a_{k-1}$ and $b = a_k$, then $a_1...a_k = ab$ and so $p|ab$. By the previous lemma part 2., it follows that $p|a$ or $p|b$. In the first case, we have $p|a_1....a_{k-1}$, so the induction hypothesis implies that $p|a_i$ for some $i = 1,...k-1$; in the second case we have $p|a_k$. Thus in either case $p|a_i$ for some i, as required. □

The next result, known as the fundamental theorem of arithmetic, explains why prime numbers are so important: they are the basic building blocks out of which all

integers can be constructed. We have seen that 0 and 1 are enough to build all the integers via addition. We have that prime numbers are enough to build all the integer via the multiplication.

Theorem 4.1.4. *Each integer $n > 1$ has a prime-power factorization*

$$n = p_1^{e_1} ... p_k^{e_k}$$

where p_1, ... , p_k are distinct primes and e_1, ... , e_k are positive integers; this factorization is unique, apart from permutations of the factors.

Proof. First we use the principle of strong induction to prove the existence of prime-power factorizations. Since we are assuming that $n > 1$, we start the induction with $n = 2$. As usual, this case is easy: the required factorization is simply $n = 2^1$. Now assume that $n > 2$ and that every integer strictly between 1 and n has a prime-power factorization. If n is prime then $n = n^1$ is the required factorization of n, so we can assume that n is composite, say $n = ab$ where $1 < a, b < n$. By the induction hypothesis, both a and b have prime factorizations, so by substituting these into the equation $n = ab$ and then collecting together powers of each prime p_i, we get a prime-power factorization of n.
Now we prove uniqueness. Suppose that n has prime-power factorization

$$n = p_1^{e_1} ... p_k^{e_k} = q_1^{f_1} ... q_l^{f_l}$$

where p_1, ... , p_k and q_1, ..., q_l are two sets of distinct primes, and the exponents e_i and f_j are all positive. The first factorization shows that $p_1 | n$, then applying the previous corollary to the second factorization we obtain $p_1 | q_j$ for some $j = 1, ..., l$. By permuting (or renumbering) the prime-powers in the second factorization we may assume that $j = 1$, so that $p_1 | q_1$. Since q_1 is prime, it follows that $p_1 = q_1$, so canceling this prime from the two factorizations we get:

$$p_1^{e_1 - 1} p_2^{e_2} ... p_k^{e_k} = q_1^{f_1 - 1} q_2^{f_2} .. q_l^{f_l}$$

We keep repeating this argument, matching primes in the two factorizations and then canceling them, until we run out of primes in one of factorizations. If one of factorization runs out before the other, then at that stage our reduced factorizations express 1 as a product of primes p_i or q_j, which is impossible since p_i, $q_j > 1$. It follows that both factorizations run out of primes simultaneously, so we must have cancelled the e_i copies of each p_i with the same number (f_i) of copies of q_i; thus $k = l$, each $p_i = q_i$ (after permuting factors), and each $e_i = f_i$ so we have proved uniqueness. □

Remark 4.1.5. *The previous theorem implies that the set of all the primes generates all the integers number, the prime are 'smallest' integers in relation of the division operation. That is a reason why there are so important in arithmetics.*

Definition 4.1.6. *The following notation is often useful: if p is prime, we write $p^e || n$ to indicate that p^e is the highest power of p dividing n, that is, p^e divides n but p^{e+1} does not.*

Example 4.1.7. *For instance,* $2^3||200$, $5^2||200$, *and* $p^0||200$ *for all prime* $p \neq 2, 5$.

Remark 4.1.8. *The prime-power factorizations allows us to calculate products, quotients, powers, greatest common divisors and least common multiples. Suppose that integers* a *and* b *have factorizations*

$$a = p_1^{e_1}...p_k^{e_k} \quad and \quad b = p_1^{f_1}...p_k^{f_k}$$

(where we have e_i, $f_i \geqslant 0$ *to allow for the possibility that some prime* p_i *may divide one but not both of* a *and* b*). Then we have*

$$\begin{aligned} ab &= p_1^{e_1+f_1}...p_k^{e_k+f_k}, \\ a/b &= p_1^{e_1-f_1}...p_k^{e_k-f_k} \ (if\ b|a), \\ a^m &= p_1^{me_1}...p_k^{me_k}, \\ gcd(a,b) &= p_1^{min(e_1,f_1)}...p_k^{min(e_k,f_k)} \\ lcm(a,b) &= p_1^{max(e_1,f_1)}...p_k^{max(e_k,f_k)} \end{aligned}$$

where $min(e, f)$ *and* $max(e, f)$ *are the minimum and maximum of* e *and* f*. Unfortunately, finding the factorization of a large integer can take a very long time!*
Then we note that if $p^e||a$ *and* $p^f||b$ *then* $p^{ef}||ab$, $p^{e-f}||a/b$ *(if* $b|a$*),* $p^{me}||a^m$, ...

Example 4.1.9. *Find the prime-power factorization of* 132, *of* 400 *and of* 1995. *Hence find* $gcd(132, 400)$, $gcd(132, 1995)$, $gcd(400, 1995)$, $gcd(132, 400, 1995)$.
Solution:

$$\begin{aligned} 132 &= 2^2 \times 3 \times 11 \\ 400 &= 2^4 \times 5^2 \\ 1995 &= 3 \times 5 \times 7 \times 19 \\ gcd(132, 400) &= 2^2 \\ gcd(132, 1995) &= 3 \\ gcd(400, 1995) &= 5 \\ gcd(132, 400, 1995) &= 1 \end{aligned}$$

4.2 Applications

As first application, the following result looks rather obvious and innocuous but it is extremely useful, especially in the case $m = 2$:

Lemma 4.2.1. *If* a_1, ... ,a_r *are mutually coprime positive integers (every two distinct of such integers are coprime), and* a_1, ..., a_r *is an* m*-th power for some integer* $m \geqslant 2$*, then each* a_i *is an* m*-th power.*

Proof. It follows from the above formula for a^m that a positive integer is an m-th power if and only if the exponent of each prime in its prime-power factorization is divisible by m. If $a = a_1...a_r$, where the factors a_i are mutually coprime then each p^e appearing in the factorization of any a_i also appear the full power of p in the factorization of a; since a is an m-th power, e is divisible by m, so a_i is an m-th power. □

Remark 4.2.2. *Of course, it is essential to assume that a_1, ..., a_r are mutually coprime here: for instance, neither* 24 *nor* 54 *are perfect square, but their product* $24 \times 54 = 1296 = 36^2$ *is a perfect square.*

We can use also the prime-power factorizations to generalize the classic result (known to Pythagoreans in the 5-th century BC) that $\sqrt{2}$ is irrational.

Definition 4.2.3. *A* ***rational number*** *is a real number of the form a/b, where a and b are integers and $b \neq 0$; all the other real numbers are* ***irrational****. A* ***perfect square*** *is an integer of the form $m = n^2$, where n is an integer.*

Corollary 4.2.4. *If a positive integer m is not a perfect square, then $\sqrt{m}$ is irrational.*

Proof. It is sufficient to prove the contrapositive, that if $\sqrt{m}$ is rational then m is a perfect square. Suppose that $\sqrt{m} = a/b$ where a and b are positive integers. Then

$$m = a^2/b^2$$

If a and b have prime-power factorizations

$$a = p_1^{e_1}...p_k^{e_k} \text{ and } b = p_1^{f_1}...p_k^{f_k}$$

as above, then

$$m = p_1^{2e_1-2f_1}...p_k^{2e_k-2f_k}$$

must be the factorization, and $e_i - f_i \geqslant 0$ for each i, so

$$m = (p_1^{e_1-f_1}...p_k^{e_k-f_k})^2$$

is a perfect square. □

Another application is the Euclid's theorem which says that there are infinitely many primes. It is one of the oldest and most attractive in mathematics. We have seen some proofs already of the result via the Fermat's numbers and the Mersenne numbers. We might see other proofs during this course, to illustrate important techniques in number theory. (⚠It is useful, rather than wasteful, to have several proofs of the same result, since one may be able to adapt these proofs to give different generalizations.)

Theorem 4.2.5. *There are infinitely many primes.*

Proof. The proof is by contradiction: we assume that there are only finitely many primes, and then we obtain a contradiction from this, so it follows that there must be infinitely many primes.
Suppose then that the only primes are p_1, p_2, ..., p_k. Let

$$m = p_1p_2...p_k + 1$$

Since m is an integer greater than 1, the Fundamental Theorem of Arithmetic implies that it is divisible by some prime p (this includes the possibility that $m = p$). By our assumption, this prime p must be one of the primes p_1, p_2, ..., p_k, so p divides their product $p_1p_2...p_k$. Since p divides both m and $p_1p_2...p_k$, it divides $m - p_1p_2...p - k = 1$, which is impossible. We deduce that our initial assumption was false, so there must be infinitely many primes. □

Another open question concerning prime numbers is *Goldbach's conjecture*, that every even integer $n \geqslant 4$ is the sum of two primes: thus $4 = 2+2$, $6 = 3+3$, $8 = 3+5$, and so on. The evidence for this is quite strong, but the best general result we have in this direction is a theorem of Chen Jing-Run (1973) that every sufficiently large even integer has the form $n = p + q$ where p is prime and q is the product of at most two primes. Similarly, Vinogradov proved in 1937 that every sufficiently large odd integer is the sum of three primes, so it immediately follows that every sufficiently large even integer is the sum of at most four primes.

4.3 Primality-testing and factorization

There are two practical problems which arise from the theory we have considered:

1. How do we determine whether a given integer n is prime?
2. How do we find the prime-power factorization of a given integer n?

Lemma 4.3.1. *An integer $n > 1$ is composite if and only if it is divisible by some $p \leqslant \sqrt{n}$.*

Proof. If n is divisible by such a prime p, then since $1 < p \leqslant \sqrt{n} < n$, it follows that n is composite. Conversely, if n is composite then $n = ab$ where $1 < a < n$ and $1 < b < n$; at least one of a and b is less than or equal to $\sqrt{n}$ (if not, $ab > n$), and this factor will be divisible by a prime $p \leqslant \sqrt{n}$, which then divides n. □

Example 4.3.2. *We can see that 97 is prime by checking that it is divisible by none of the primes $p \leqslant \sqrt{97}$, namely 2, 3, 5 and 7. This method requires us to test whether an integer n is divisible by various prime p. For certain small primes p there are simple ways of doing this, based on properties of the decimal number system.*

Remark 4.3.3. *In order to test the divisibility, we can use here all the techniques that we have seen before for divisibility by 2, 3, 5 and 11. Otherwise, one simply has to divide p into n and see whether or not the remainder is 0.*

This method of primality-testing is effective for fairly small integers n, since there are not too many primes p to consider, but when n becomes large it is very time consuming: by the Prime Number Theorem which says that the number of prime integers less than some integer x is equivalent to $x/ln(x)$, the number of prime $p \leqslant \sqrt{n}$ is given by equivalent to $\sqrt{n}/ln(\sqrt{n}) = 2\sqrt{n}/ln(n)$.
In cryptography (the study of secret code), one regularly uses integers with several hundred decimal digits, if $n \simeq 10^{100}$, for example, then this method would involve testing about 8×10^{47} primes p, and even the fastest available supercomputers would take far longer than the current estimate for the age of the universe (about 15 billion year) to complete this task! Fortunately there are alternative algorithms (using some very sophisticated number theory) which will determine primality for very large integers much more efficiently. Some fastest of these are probabilistic algorithms, such as the Solovay-Strassen test, which will always detect a prime integer n, but which may incorrectly declare a composite number n as veing prime; this may appear to be disastrous fault,

but in fact the probability of such an incorrect outcome is so low (far lower than the probability if computational error due to a machine fault) that for most practical purposes these tests are very reliable.

The sieve of Eratosthenes is a systematic way of compiling a list of the primes up to a given integer N. First, we list the integer 2, 3, ... N in increasing order. Then we underline 2 (which is prime) and cross out all the proper multiples 4, 6, 8, ... of 2 in the list (since these are composite). The first integer which is neither underlined nor crossed out 3: this is prime, so we underline it and then cross out all its proper multiples 6, 9, 12, ... At the next stage we underline 5 and cross out 10, 15, 20... We continue like this until every integer in the list is either underline or crossed out. At each stage, the first integer which is neither underline nor crossed must be a prime, for otherwise it would have been crossed out, as a proper multiple of an earlier prime; thus only primes are underlined at some stage, so when the process terminated the underlined numbers are precisely the prime $p \leqslant N$. (We can actually stop earlier, when the proper multiples of all the primes $p \leqslant \sqrt{N}$ have been crossed out, since the previous lemma implies that every remaining integer in the list must be prime.)

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Our second practical problem, factorization, is apparently much harder than primality-testing. (It cannot be any easier, since the prime-power factorization of an integer immediately tells us whether or not it is prime). In theory, we could factorize any integer n by testing it for divisibility by the primes 2, 3, 5, ... until a prime factor p is found; we then replace n with n/p and continue this process of n/p is found; eventually, we obtain all the prime factors of n with their multiplicities. This algorithm is quite effective for small integers, but when n is large we meet the same problem as in primality-testing, that there are just too many possible prime factors to consider. There are, of course, more subtle approaches to factorization, but at present the fastest known algorithms and computers cannot, in practice, factorize integers several hundred digits long (though nobody has yet proved that an efficient factorization algorithm will never be found). A very effective cryptographic system (known as the RSA public key system, after its inventors Rivest, Shamir and Adleman, 1978) is based on the fact that

it is relatively easy to calculate the product $n = pq$ of two very large primes p and q, while it is extremely difficult to reverse this process and obtain the factors p and q, while it is extremely difficult to reverse this process and obtain the factors p and q from n.

Part II

Arithmetic Functions

Chapter 5

Arithmetic Functions

5.1 Definitions, examples

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

1. The **unit function** e define by $e(1) = 1$ and $e(n) = 0$ for all $n > 1$.
2. The **identity function** E defined by $E(n) = 1$ for all $n \in \mathbb{N}$.
3. The **power functions** I_k defined by $I_k(n) = n^k$ for all $n \in \mathbb{N}$. In particular, $E = I_0$.
4. The number of prime divisors of n, denoted by $\Omega(n)$.
5. The number of distinct prime divisors of n, denoted by $\omega(n)$.
6. The divisor sums σ_l defined by

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

   In particular, we write $\sigma = \sigma_1$, the sum of divisor and σ_0, the number of divisors.
7. The **Euler ϕ-function or totient function**

$$\phi(n) = \sharp\{d \in \mathbb{N} | gcd(d, n) = 1 \text{ and } d \leqslant n\}$$

8. **Ramanujan's function** $\tau(n)$ defined by

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

9. The "sum of squares" function $r_d(n)$ given by the number of solutions x_1,...,x_d to $n = x_1^2 + ... + x_d^2$.

In general,

Definition 5.1.1. *An **arithmetic function** is a function $f : \mathbb{N} \to \mathbb{C}$.*

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

Definition 5.1.2. *Let f be an arithmetic function with $f(1) = 1$. Then f is called* ***multiplicative*** *if $f(mn) = f(m)f(n)$ for all m, n with $gcd(m,n) = 1$ and* ***strongly multiplicative*** *if $f(mn) = f(m)f(n)$, for all m, n.*

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

Theorem 5.1.3. *1. σ_l is a multiplicative function.*

2. Let $n = p_1^{k_1}...p_r^{k_r}$. Then

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

Proof. 1. The proof is based on the fact that if $d|mn$ and $gcd(m,n) = 1$ then d can be written uniquely in the form $d = d_1d_2$ where $d_1|m$ and $d_2|n$. In particular, $d_1 = gcd(m,d)$ and $d_2 = gcd(n,d)$. We have

$$\sigma_l(mn) = \sum_{d|mn} d^l = \sum_{d_1|m,d_2|n} (d_1d_2)^l = (\sum_{d_1|m} d_1^l)(\sum_{d_2|n} d_2^l) = \sigma_l(m)\sigma_l(n)$$

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

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

□

A very ancient problem is that of perfect numbers.

Definition 5.1.4. *A* ***perfect number*** *is a number $n \in \mathbb{N}$ which is equal to the sum of its divisors less than n. Stated alternatively, n is perfect if $\sigma(n) = 2n$.*

Examples of perfect numbers are 6, 28, 496, 8128, 33550336,.... It is not known whether there are infinitely many. It is not also known if there exist odd perfect numbers. If they do, they must be at least 10^{300}. For even perfect numbers there exists a characterization given by Euclid and Euler.

Theorem 5.1.5. *Let n be even. Then n is perfect if and only if it has the form $n = 2^{k-1}(2^k - 1)$ with $2^k - 1$ prime.*

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

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

not the other hand, n is perfect, so $\sigma(n) = 2n$, which implies that $2^k m = (2^k - 1)\sigma(m)$. Hence

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

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

Remark 5.1.6. *1. We recognize the Mersenne primes (that is the number of the form $2^k - 1$ which are also prime) in the theorem.*

*2. An equally classical subject is that of **amicable numbers** that is, pairs of numbers m, n such that n is the sum of all the divisors of m less than m and vice versa. In other words, $m + n = \sigma(n)$ and $n + m = \sigma(m)$. The pair 220, 284 was known to the ancient Greeks. Euler discovered some 60 pairs (for example 11498355, 12024045) and later computer searches yielded several thousands of new pairs, some of which are extremely large.*

5.2 Euler's function

Definition 5.2.1. *We define $\phi(n) = \{a \in \{1, ..., n\} | gcd(a, n) = 1\}$. This function ϕ is called the **Euler's function**. For small n, its values are as follows.*

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Theorem 5.2.2. *If $n \geqslant 1$, then*

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

Proof. Let $S = \{1, 2, ..., n\}$ and for each d dividing n let $S_d = \{a \in S | gcd(a, n) = n/d\}$. These sets S_d partition S into disjoint subsets, since if $a \in S$ then $gcd(a, n) = n/d$ for some unique divisor d of n. Thus $\sum_{d|n} |S_d| = |S| = n$, so it is sufficient to prove that $|S_d| = \phi(d)$ for each d. Now

$$a \in S_d \Leftrightarrow a \in \mathbb{Z} \text{ with } 1 \leqslant a \leqslant n \text{ and } gcd(a, n) = n/d.$$

If we define $a' = ad/n$ for each integer a, then a' is an integer since $n/d = gcd(a, n)$ divides a. Dividing on the right-hand side by n/d, we can therefore rewrite the above condition as

$$a \in S_d \Leftrightarrow a = n/da' \text{ where } a' \in \mathbb{Z} \text{ with } 1 \leqslant a' \leqslant d \text{ and } gcd(a'd) = 1.$$

Thus $|S(d)|$ is the number of integer a', between 1 and d inclusive which are coprime to d; this is the definition of $\phi(d)$, so $|S(d)| = \phi(d)$ as required. □

Example 5.2.3. *If $n = 10$, then the divisors are $d = 1, 2, 5$ and 10. We find that $S_1 = \{10\}$, $S_2 = \{5\}$, $S_5 = \{2, 4, 6, 8\}$ and $S_{10} = \{1, 3, 7, 9\}$ containing $\phi(d) = 1, 1, 4$ and 4 elements respectively. These four sets form a partition of $S = \{1, 2, ..., 10\}$, so $\phi(1) + \phi(2) + \phi(5) + \phi(10) = 10$.*

5.3 Convolution, Möbius inversion

Definition 5.3.1. *Let f and g be two arithmetic functions. Their **convolution product** denoted by $f \star g$ is defined by*

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

It is an easy exercise to verify that the convolution product is commutative and associative. Moreover, $f = e \star f$ for any f. (Hence arithmetic function form a semigroup under convolution).

Theorem 5.3.2. *The convolution product of two multiplicative functions is again multiplicative.*

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

$$\begin{aligned} (f \star g)(mn) &= \textstyle\sum_{d|mn} f(d)g(mn/d) \\ &= \textstyle\sum_{d_1|m} \sum_{d_2|n} f(d_1 d_2)g(m/d_1 n/d_2) \\ &= (\textstyle\sum_{d_1|m} f(d_1)g(m/d_1))(\sum_{d_2|n} f(d_2)g(n/d_2)) \\ &= (f \star g)(m)(f \star g)(n) \end{aligned}$$

□

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

Definition 5.3.3. *The **Möbius function** $\mu(n)$ is defined by $\mu(1) = 1$, $\mu(n) = 0$ if n is divisible by a square > 1 and $\mu(p_1 ... p_t) = (-1)^t$ for any product of distinct primes p_1, ... , p_t.*

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

Theorem 5.3.4. *(Möbius inversion) Let f be an arithmetic function and let F be defined by*

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

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

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

Proof. More cryptically we have $F = E \star f$ and we must prove that $f = \mu \star F$. It suffices to show that $e = E \star \mu (= \mu \star E)$ since this implies $\mu \star F = \mu \star E \star f = e \star f = f$.
The function $E \star \mu$ is again multiplicative, hence it suffices to compute $E \star \mu$ at prime powers p^k where $k > 0$ and show that it is zero there. Observe,

$$(E \star \mu)(p^k) = \sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + ... + \mu(p^k) = 1 - 1 + 0 + ... + 0 = 0$$

□

Theorem 5.3.5. *Let ϕ b the Euler ϕ-function. Then,*

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

2. *ϕ is multiplicative.*

3. $$\phi(n) = n \prod_{p|n} (1 - 1/p)$$

Proof. 1. (Already proven)

2. We have seen in part 1. that $I_1 = E \star \phi$. Hence, by Möbius inversion, $\phi = \mu \star I_1$. Multiplicativity of ϕ automatically follows from the multiplicativity of μ and I_1.
3. Because of the mutiplicativity of ϕ it suffices to show that $\phi(p^k) = p^k(1 - 1/p)$. This follows from $\phi(p^k) = (I_1 \star \mu)(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$.

□

Part III

Modular arithmetic on $\mathbb{Z}$

Chapter 6

Congruences

6.1 Motivation

When we think for example in what will the day of the week in 100 days. We can get a diary and count 100 days ahead. But, the quicker way is to think that a week is 7 days and every multiple of 7 days from now will be the same day as now, this tell us to just do the Euclidean division of 100 by 7 and to look at the remainder, that is:

$$100 = 7 \times 14 + 2$$

so the day will be the same as it is two days ahead, and this is easy to determine. So to solve this problem with n day it enough to just look the remainder of the division of n by 7.
Consider an integer n, to know if it is odd or even, we can look at remainder of n by the division by 2. So, there is just two category of integer when we look at them using the division by 2, there is the even integers of the form $2k$ for some integer k and the odd integers of the form $2k+1$, for some integer k.
We can do the same for the division by 4, an if you consider $4k$, $4k+1$, $4k+2$, $4k+3$ for any k integer, you cover all the integer. Now lets consider n^2, if n is even there is an integer k such that $n = 2k$, then $n^2 = 4k$ and if n is odd, there is an integer k such that $n = 2k+1$ then $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2+k) + 1$ but then a square is or of the form $4k$ or of the form $4k+1$ for some k. In other words, the remainder by the division 4 is either 0 or 1. ⚠We are not saying that all the integer of this form are square, for example 5 is not a square, nevertheless $5 = 4 \times 1 + 1$. Now, can you say if 22051946 is a perfect square without calculator? we know that $4|100$ so $4|22051900$ so to see the remainder of the division of 22051900 by 4 it is enough to look at the one of the division of 46 by 1 but $46 = 11 \times 4 + 2$, so it is not a perfect square.
The previous problems is not rare in arithmetic, there are many problems involving large integers that can be simplified by a technique called **modular arithmetic** where we use congruences in place of equation. The basic idea is to choose a particular integer n depending on the problem (in the previous example $n = 7$ resp. 4), called the **modulus**, and replace every integer with its remainder when divided by n. In general, this remainder is smaller and hence easier to deal with.

6.2 Definition and first properties

Definition 6.2.1. *Let n be a positive integer, and let a and b be any integers. We say that a **is congruent to** b **mod** (n), or a is a residue of b mod (n), written*

$$a \equiv b \ mod \ (n)$$

if a and b leave the same remainder when divided n.

(Other notations for this include $a \equiv b \ (mod \ n)$, $a \equiv b \ mod \ n$ and $a \equiv_n b$).

To be more precise, we use the division algorithm to put $a = qn + r$ with $a \leqslant r < n$, and $b = q'n + r'$ with $0 \leqslant r' < n$, and then

we say that $a \equiv b \ mod \ (n)$ if and only if $r = r'$.

We will use the notation $a \not\equiv b \ mod \ (n)$ to denote that a **and** *b* **are not congruent mod** *(n), that is, that they leave different remainders when divided by n.*

Example 6.2.2. *The two example of the first section can be translated as:*

1. $100 \equiv 2 \ mod \ (7)$;
2. $22051946 \equiv 46 \equiv 2 \ mod \ (4)$.

Our first result gives a useful alternative definition of congruence mod (n).

Lemma 6.2.3. *For any field $n \geqslant 1$ we have $a \equiv b \ mod \ (n)$ if and only if $n|(a-b)$*

Proof. We can write the Euclidean division of a and b by n, we get $a = qn + r$ and $b = q'n + r'$ with q and q' integers, $0 \leqslant r < n$ and $0 \leqslant r' < n$. Then we have $a - b = (q - q')n + (r - r')$ with $-n < r - r' < n$.

($\Rightarrow$) Now, if we suppose that $a \equiv b \ mod \ (n)$ then $r = r'$ so, $r - r'' = 0$ and $a - b = (q - q')n$, or in other word, $n|a - b$.

($\Leftarrow$) Suppose that $n|(a-b)$, then $n|(a-b) - (q-q')n = r - r'$, that implies that $r - r' = 0$ since $-n < r - r' < n$ □

We have the congruence relation is an "equivalence relation" on $\mathbb{Z}$, it is reflexive, symmetric and transitive or in other word we have the following lemma:

Lemma 6.2.4. *For any fixed $n \geqslant 1$ we have for any a, b and c integers:*

1. *$a \equiv a \ mod \ (n)$ (reflexivity);*
2. *if $a \equiv b \ mod \ (n)$ then $b \equiv a \ mod \ (n)$ (symmetry);*
3. *if $a \equiv b \ mod \ (n)$ and $b \equiv c \ mod \ (n)$ then $a \equiv c \ mod \ (n)$ (transitivity).*

Proof. 1. We have $n|(a-a)$, for all a.

2. If $n|(a-b)$ then $n|(b-a)$.
3. If $n|(a-b)$ and $n|(b-c)$ then $n|(a-b) + (b-c) = a - c$.

□

It follows that $\mathbb{Z}$ can be partitioned into disjoint equivalent classes:

Definition 6.2.5. *Let n be an integer. The equivalence class for the relation $\equiv$ mod (n) are called* ***congruence classes of a mod (n)****. For some a integer,*

$$\text{we denote by } [a] \text{ (or sometimes } [a]_n)$$

its congruence classes of a mod (n), that is

$$\begin{aligned} [a] &= \{b \in \mathbb{Z} | a \equiv b \bmod (n)\} \\ &= \{...., a-2n, a-n, a, a+n, a+2n, ...\} \end{aligned}$$

Each integer b such that $[b] = [a]$ is called a ***representative of the class*** $[a]$.

We denote by $\mathbb{Z}/n\mathbb{Z}$ the set of all the classes of congruences mod (n).

Clearly, we obtain the following lemma:

Lemma 6.2.6. *Let a and b be integers, if $b \in [a]$ then $[a] = [b]$.*

Remark 6.2.7. *Let n be an integer.*

1. ⚠ *An element of $\mathbb{Z}/n\mathbb{Z}$ is a class of elements of $\mathbb{Z}$.*
2. ⚠ *There is a unique representative of a class of an integer mod n on the set $\{0, ..., n-1\}$.*

   Indeed, for any a integer there exists $r \in \{0, ..., n-1\}$, such that $[a] = [r]$, that is the remainder of the division of a by n (Indeed, $r \in [a]$ and we can apply the previous lemma). Moreover, if r and r' are distinct integers in $\{0, ..., n-1\}$ then $[r] \neq [r']$. Otherwise, $r = r' + tn$ for some integer t, but then $r - r' = tn$ and this holds if and only if $r = r'$ which contradict the first assumption.
3. *By definition, for any a and b integers, $[a] = [b]$ if and only if $a \equiv b \bmod (n)$.*

Definition 6.2.8. *Let n be an integer. A set of n integers, containing one representative from each to the n congruence classes in $\mathbb{Z}/n\mathbb{Z}$ is called a* ***complete set of residues*** *mod (n).*

The integers $0, ..., n-1$ are called ***the least non-negative residues*** *mod (n).*

The integers r such that $-n/2 < r \leqslant n/2$ are ***the least absolute residue*** *mod (n).*

Remark 6.2.9.

1. *The set of all the least non-negative residues $\{0, ..., n-1\}$ is a complete set of residues mod (n). The set of all the least absolute residue mod (n) (that is $\{0, \pm 1, \pm 2, ..., \pm(n-1)/2\}$ if n is odd and $\{0, \pm 1, \pm 2, ..., \pm n/2 - 1, n/2\}$ if n is even) is a complete set of residues mod (n).*
2. *A sensitive choice of a complete set of residues can easy the calculations considerably. Many times the least non-negative residues are the most convenience, but the least absolute residues can be more convenient sometimes.*

We obtain a canonical description of $\mathbb{Z}/n\mathbb{Z}$:

Lemma 6.2.10. *For n an integer,*

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], ..., [n-1]\}$$

Example 6.2.11. $\mathbb{Z}/2\mathbb{Z} = \{[0], [1]\}$ *and the class* $[0]$ *is the set of all the even integers and the class* $[1]$ *is the set of all the odd integers.*

We want to define an addition $+$ and a multiplication $\cdot$ operation over the set $\mathbb{Z}/n\mathbb{Z}$. For this, we look at the behavior of the congruence under the addition on $\mathbb{Z}$.

Lemma 6.2.12. *For a given $n \geqslant 1$, if $a' \equiv a \ mod\ (n)$ and $b' \equiv b \ mod\ (n)$ then,*

$$\begin{array}{rcl} a' + b' & \equiv & a + b \ \ mod\ (n) \\ a' - b' & \equiv & a - b \ \ mod\ (n) \\ a' \cdot b' & \equiv & a \cdot b \ \ mod\ (n) \end{array}$$

In other words, if a, a', b and b' are integers such that $[a] = [a']$ and $[b] = [b']$ then

$$\begin{array}{rcl} [a + b] & = & [a' + b'], \\ [a - b] & = & [a' - b'], \\ [ab] & = & [a'b']. \end{array}$$

Proof. Since $a' \equiv a \ mod\ (n)$, there is an integer k such that $a' = a + kn$ and similarly since $b' \equiv b \ mod\ (n)$ there is an integer l such that $b' = b + ln$; then $a' \pm b' = (a \pm b) + (k \pm l)n \equiv a \pm b \ mod\ (n)$, and $a'b' = ab + (al + bk + kln)n \equiv ab \ mod\ (n)$. □

The following example illustrate the use of the complete sets of residues and of the previous lemma.

Example 6.2.13. *1. Let us calculate the least non-negative residue of* 28×33 *mod* 35.

Using the least absolute residues mod 35, *we have* $28 \equiv -7 \ mod\ (35)$ *and* $33 \equiv -2 \ mod\ (35)$, *so*

$$28 \times 33 \equiv (-7) \times (-2) \ mod\ (35) \equiv 14 \ mod\ (35)$$

Since $0 \leqslant 14 < 35$, *it follows that* 14 *is the required least non-negative residue.*

2. Let us calculate the least absolute residue of 15×59 *mod* 75.

We have

$$\begin{array}{rcl} 15 \times 59 & \equiv & 15 \times (-16) \ mod\ (75) \\ & \equiv & -60 \times 4 \ mod\ (75) \\ & \equiv & 15 \times 4 \mod (75) \\ & \equiv & 60 \ mod\ (75) \\ & \equiv & -15 \ mod\ (75) \end{array}$$

and since $-75/2 < -15 \leqslant 75/2$, *the required residue is* -15.

3. *Let us calculate the least non-negative residue of* 3^8 *mod* 13.

$$\begin{aligned} 3^8 = (3^2)^4 = 9^4 &\equiv (-4)^4 \ mod\ (13) \\ &\equiv 16^2 \ mod\ (13) \\ &\equiv 3^2 \ mod\ (13) \\ &\equiv 9 \ mod\ (13) \end{aligned}$$

The required residue is therefore 9.

Since n divides m if and only if $m \equiv 0 \ mod\ (n)$, it follows that problems about divisibility are equivalent to problems about congruences, and these can sometimes be easier to solve. Here is a typical example:

Example 6.2.14. *Let us prove that* $a(a+1)(2a+1)$ *is divisible by* 6 *for every integer* a.

By taking least absolute residues mod (6). *So, there are* 6 *case to consider:*

1. *If* $a \equiv 0 \ mod\ (6)$ *then* $a(a+1)(2a+1) \equiv 0 \ mod\ (6)$.
2. *If* $a \equiv 1 \ mod\ (6)$ *then* $a(a+1)(2a+1) \equiv 1 \times 2 \times 3 \ mod\ (6) \equiv 6 \ mod\ (6) \equiv 0 \ mod\ 6$.
3. *If* $a \equiv 2 \ mod\ (6)$ *then* $a(a+1)(2a+1) \equiv 2 \times 3 \times 5 \ mod\ (6) \equiv 6 \times 5 \ mod\ (6) \equiv 0 \ mod\ 6$.
4. *If* $a \equiv 3 \ mod\ (6)$ *then* $a(a+1)(2a+1) \equiv 3 \times 4 \times 7 \ mod\ (6) \equiv 6 \times 3 \times 7 \ mod\ (6) \equiv 0 \ mod\ 6$.
5. *If* $a \equiv 4 \ mod\ (6)$ *then* $a(a+1)(2a+1) \equiv 4 \times 5 \times 9 \ mod\ (6) \equiv 6 \times 2 \times 5 \times 3 \ mod\ (6) \equiv 0 \ mod\ 6$.
6. *If* $a \equiv 5 \ mod\ (6)$ *then* $a(a+1)(2a+1) \equiv 5 \times 6 \times 11 \ mod\ (6) \equiv 0 \ mod\ 6$.

This allows us to define addition, subtraction and multiplication.

Definition 6.2.15. *Let* n *be an integer.*

1. *We define an* ***addition*** $+$ *over* $\mathbb{Z}/n\mathbb{Z}$, *for any* a *and* b, *we put*

$$[a] + [b] := [a+b]$$

Similarly

$$[a] - [b] := [a-b]$$

2. *We define a* ***multiplication*** $\cdot$ *over* $\mathbb{Z}/n\mathbb{Z}$, *for any* a *and* b, *we put*

$$[a] \cdot [b] := [a \cdot b]$$

Remark 6.2.16. ⚠ *We cannot define a division congruence class since for some* a *and* b, a/b *is not necessary an integer.*

By induction, we have:

Lemma 6.2.17. *For any integers* $a_1, \ldots, a_n$ *and* a,

1. $[a_1] + [a_2] + \ldots + [a_n] = [a_1 + \ldots + a_n]$;

2. $[a_1] \cdot [a_2] \cdot ... \cdot [a_n] = [a_1 \cdot ... \cdot a_n]$;
3. $[a]^k = [a^k]$.

Remark 6.2.18. *When we work in $\mathbb{Z}/n\mathbb{Z}$, we have to be careful before defining an operation. We always have to check that taking different representatives does not change the class.*

⚠ *For example, if we work on $\mathbb{Z}/3\mathbb{Z}$, one cannot define $[a]^{[b]} = [a^b]$. In fact, $[1] = [4]$ and $[2]^{[1]} = [2^1] = [2]$ and $[2]^{[4]} = [16] = [1]$, so $[2]^{[1]} \neq [2]^{[4]}$. So, the relation $[a]^{[b]} = [a^b]$ is not well defined. In particular, exponentiation of congruence classes is not well defined.*

Chapter 7

Congruence equations

7.1 Congruences and polynomials

Lemma 7.1.1. *Let $f(x)$ be a polynomial with integer coefficients, and let $n \geqslant 1$. If $a \equiv b \ mod\ (n)$, then $f(a) \equiv f(b) \ mod\ (n)$.*

Proof. White $f(x) = c_0 + c_1x + ... + c_kx^k$, where each $c_i \in \mathbb{Z}$. If $a \equiv b \ mod\ (n)$, $a^i \equiv b^i \ mod\ (n)$ for any $i \geqslant 0$, so $c_ia^i \equiv c_ib^i$ for all i, and hence $f(a) \equiv f(b) \ mod\ (n)$ by adding congruences. □

Example 7.1.2. *Take $f(x) = x(x+1)(2x+1) = 2x^3 + 3x^2 + x$ and $n = 6$; we then used $0 \equiv 6 \ mod\ (6)$ so $f(0) \equiv f(6) \equiv 0 \ mod\ (6)$.*

Remark 7.1.3. *If a polynomial $f(x)$ with integer coefficients has an integer root a (that is $f(a) = 0$), then $f(a) \equiv 0 \ mod\ (n)$, for all integers $n \geqslant 1$. It is sometimes successful to use the contrapositive to prove that a polynomial has no integer root: that is if there is an integer n such that the congruence $f(x) \equiv 0 \ mod\ (n)$ has no solutions x, then the equation $f(x) = 0$ has no integer solution. By the previous lemma, it is enough to check the congruence at a complete set of residue. If n is small, it is fast to check if for any element x of a complete set of residues if $f(x) \equiv 0 \ mod\ (n)$ or not. ⚠ If for one integer n, $f(x) \equiv 0 \ mod\ (n)$ this does not mean nothing about the existence or not of a solution. We will see that there are polynomials such that $f(x) \equiv 0 \ mod\ (n)$ for EVERY integer n and still there are no integers roots.*

Let take a example to illustrate this remark.

Example 7.1.4. *Take the polynomial $f(x) = x^5 - x^2 + x - 3$.*
Take $n = 2$, a complete set of residue mod (2) is $\{0,1\}$. $f(0) = -3 \not\equiv 0 \ mod\ (2)$ but $f(1) = -2 \equiv 0 \ mod\ (2)$. So, we CANNOT conclude about the existence or not of integral roots.
Take $n = 3$, a complete set of residue mod (3) is $\{0,1,2\}$, $f(0) = -3 \equiv 0 \ mod\ (2)$. So, we CANNOT conclude nothing also with 3.
Take $n = 4$, a complete set of residue mod (4) is $\{0,1,2,3\}$,
— *$f(0) = -3 \not\equiv 0 \ mod\ (4)$,*
— *$f(1) = 2 \not\equiv 0 \ mod\ (4)$,*

— $f(2) = 4^5 - 4 + 2 - 3 \equiv -1 \not\equiv 0 \ mod\ (4)$,
— $f(3) \equiv (-1)^5 - (-1)^2 - 1 - 3 \equiv -2 \not\equiv 0 \ mod\ (4)$.
Then, we know that $f(x)$ has no integer roots.

One question which can come in mind is : Is there polynomials f such that $f(x)$ is prime for any integer x? The answer is no, apart of course the constant polynomials $f(x) = p$ for some prime p.

Theorem 7.1.5. *There is no non-constant polynomial $f(x)$, with integer coefficients, such that $f(x)$ is prime for all integers x.*

Proof. Suppose that $f(x)$ is prime for all integers x, and it is not constant. If we choose any integer a, then $f(a)$ is a prime p. For each $b \equiv a \ mod\ (p)$, we have $f(a) \equiv f(b) \ mod\ (p)$, so $f(b) \equiv 0 \ mod\ (p)$ and hence p divides $f(b)$. By our hypothesis, $f(b)$ is prime, so $f(b) = p$. There are infinitely many integers $b \equiv a \ mod\ (p)$, so the polynomial $g(x) = f(x) - p$ has infinitely many roots. However, this is impossible: having degree $d \geqslant 1$, $g(x)$ can have at most d roots, so such a polynomial $f(x)$ cannot exist. □

Remark 7.1.6. *A polynomial mod some n can be congruent to zero for a number of elements greater than its degree without being the zero polynomial. Indeed if we take $f(x) = 2x^3 + 3x^2 + x$, we can check that $f(0)$, $f(\pm 1)$, $f(\pm 2)$ or $f(3)$ are congruent to 0 mod (6).*

7.2 Linear congruences

7.2.1 Simple linear congruences

We have said that we cannot always speak about division since the quotient of two integers is not necessary an integer. However, for some integers n, a and b fixed, a good alternative to this problem is to find the solution of the congruence $ax \equiv b \ mod\ (n)$. But this problem can be seen as a equivalent form of the linear diophantine equation studied earlier. Indeed, there is an integer x such that $ax \equiv b \ mod\ (n)$ if and only if there is an integer x such that $ax - b$ is a multiple of n if and only if there are integers x and y such that $ax + ny = b$ (which is a linear diophantine equation. Into a congruence language, the theorem about diophantine equations becomes.

Theorem 7.2.1. *If $d = gcd(a, n)$, then the linear congruence*

$$ax \equiv b \ mod\ (n)$$

has a solution if and only if $d|b$. If d does divides b, and if x_0 is a particular solution, then the general solution is given by

$$x = x_0 + \frac{nt}{d}$$

where $t \in \mathbb{Z}$; in particular, the solutions form exactly d congruence classes mod (n), with representatives

$$x = x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, ..., x_0 + \frac{(d-1)n}{d}$$

Proof. The only part which is not part of the theorem about linear diophantine equations is the statement about congruence classes. First remark that if x is a solution then any element of $[x]$ is also a solution since for any integer x' such that $x \equiv x' \ mod\ (n)$, then $ax \equiv ax' \ mod\ (n)$. Now, note that

$$x_0 + \frac{nt}{d} \equiv x_0 + \frac{nt'}{d} \ mod\ (n)$$

if and only if n divides $n(t-t')/d$ that is if and only if d divides $t-t'$, so the congruence classes of solutions mod (n) are obtained by letting t range over a complete set of residues mod (d), such as $0, 1, ..., d-1$. □

Remark 7.2.2. *In order to find the particular solution after checking that such a solution exists, it is fast just trying with a complete set of residue. If n is too big, we can apply the algorithm of Chapter 1 to find this particular solution.*

Corollary 7.2.3. *If $gcd(a,n) = 1$ then the solution x of the linear congruence $ax \equiv b \ mod\ (n)$ form a single congruence class mod (n).*

Example 7.2.4. *1. Consider the congruence*

$$10x \equiv 3 \ mod\ (12)$$

We have that $gcd(10,12) = 2$ does not divide 3, so there are no solutions. (but it is expectable since $10x + 12y$ is even and 3 is odd.)

2. Consider the congruence

$$10x \equiv 6 \ mod\ (12)$$

Since $gcd(10,12) = 2$ divides 6, there are two classes of solutions. We can take $x_0 = 3$ as a particular solution, so the general solution has the form

$$x = x_0 + \frac{nt}{d} = 3 + \frac{12t}{2} = 3 + 6t,$$

where $t \in \mathbb{Z}$. These solutions form two congruence classes $[3]$ and $[9]$ mod (12), with representatives $x_0 = 3$ and $x_0 + d/n = 9$; (equivalently they form a single congruence class $[3]$ mod (6).

3. Consider the congruence

$$7x \equiv 3 \ mod\ (12)$$

Since $gcd(7,12) = 1$ there is a single congruence class of solutions; this is the class $[x] = [9]$, since $7 \times 9 = 63 \equiv 3 \ mod\ (12)$.

Lemma 7.2.5. *1. Let m divide a, b and n, and let $a' = a/m$, $b' = b/m$ and $n' = n/m$, then*

$$ax \equiv b \ mod\ (n) \text{ if and only if } a'x \equiv b' \ mod\ (n')$$

2. Let a and n be coprime, let m divide a and b, let $a' = a/m$ and $b' = b/m$; then

$$ax \equiv b \ mod\ (n) \text{ if and only if } a'x \equiv b' \ mod\ (n)$$

Proof. 1. We have $ax \equiv b \ mod\ (n)$ if and only if $ax - b = qn$ for some integer q; dividing by m, we see that this is equivalent to $a'x - b' = qn'$, that is, to $a'x \equiv b' \ mod\ (n')$.

2. If $ax \equiv b \ mod\ (n)$, then there is an integer n such that $ax - b = qn$ and hence $a'x - b' = qn/m$; in particular, m divides qn. Now m divides a, which is coprime to n, so m is also coprime to n and hence m must divide q. Thus $a'x - b' = (q/m)n$ is a multiple of n, so $a'x \equiv b' \ mod\ (n)$. For the converse, if $a'x \equiv b' \ mod\ (n)$ then $a'x - b' = q'n$ for some integer q', so multiplying through by m we have $ax - b = mq'n$ and hence $ax \equiv b \ mod\ (n)$.

□

Let see throughout example how we can use this lemma.

Example 7.2.6. *Consider the congruence*

$$10x \equiv 6 \ mod\ (14)$$

Since $gcd(10, 14) = 2$ *divides* 6*, so solutions do exist. If* x_0 *is a particular solution, then the general solution is* $x = x_0 + (14/2)t = x_0 + 7t$*, where* $t \in \mathbb{Z}$ *these form the congruence classes* $[x_0]$ *and* $[x_0 + 7]$ *in* $\mathbb{Z}/14\mathbb{Z}$*. By the previous lemma 1., dividing by* $gcd(10, 14)$ *which divide* 10*,* 14 *and* 6 *the previous congruence equation is equivalent to*

$$5x \equiv 3 \ mod\ (7)$$

Now, noting that $3 \equiv 10 \ mod\ (7)$*, we get*

$$5x \equiv 10 \ mod\ (7)$$

Thus $x_0 = 2$ *is a solution, so in the general solution has the form*

$$x = 2 + 7t \ (t \in \mathbb{Z})$$

1. *Consider the congruence*

$$4x \equiv 13 \ mod\ (47)$$

Since $gcd(4, 47) = 1$ *divides* 13*, the congruence has solutions. If* x_0 *is a particular solution then the general solution is* $x = x_0 + 47t$ *where* $t \in \mathbb{Z}$ *forming a single congruence class* $[x_0]$ *in* $\mathbb{Z}/47\mathbb{Z}$*. Noting that* $4 \times 12 = 48 \equiv 1 \ mod\ (47)$*, we multiply by* 12 *to give*

$$48x \equiv 12 \times 13 \ mod\ (47)$$

That is

$$x \equiv 3 \times 4 \times 13 \equiv 3 \times 52 \equiv 3 \times 5 \equiv 15 \ mod\ (47)$$

Thus, we can take $x_0 = 15$*, so the general solution is* $x = 15 + 47t$*.*

7.2.2 Simultaneous linear congruences, chinese remainder theorem

We can be lead to consider simultaneous linear congruence. To answer this problem we have the Chinese Remainder theorem.

Theorem 7.2.7. *Let n_1, n_2, ..., n_k be positive integers, with $gcd(n_i, n_j)$ whenever $i \neq j$, and let a_1, ..., a_k be any integers. Then the solutions of the simultaneous congruences*

$$x \equiv a_1 \ mod\ (n_1),\ x \equiv a_2 \ mod\ (n_2), ..., x \equiv a_k \ mod\ (n_k)$$

form a single congruence class $[x_0]$ mod (n), where $n = n_1 n_2 ... n_k$ (and

$$x_0 = a_1 c_1 d_1 + a_2 c_2 d_2 + ... + a_k c_k d_k$$

where $c_i = n/n_i$ and d_i is a solution of the congruence $c_i x \equiv 1 \ mod\ (n_i)$. In other words, the general solution is of the form $x = x_0 + nt$ where $t \in \mathbb{Z}$.

Proof. Let $c_i = n/n_i = n_1 ... n_{i-1} n_{i+1} ... n_k$ for each $i = 1, ..., k$. Since each of its factors n_j $(j \neq i)$ is coprime to n_i, so is c_i. Therefore for each i, the congruence $c_i x \equiv 1 \ mod\ (n_i)$ has a single congruence class $[d_i]$ of the solution mod (n_i). We now claim that the integer

$$x_0 = a_1 c_1 d_1 + a_2 c_2 d_2 + ... + a_k c_k d_k$$

simultaneously satisfies the given congruences, that is, $x_0 \equiv a_i \ mod\ (n_i)$ for each i. To see this, note that each c_j (other than c_i) is divisible by n_i, so $a_j c_j d_j \equiv 0 mod\ (n_i)$ and hence $x_0 \equiv a_i c_i d_i \ mod\ (n_i)$; now $c_i d_i \equiv 1 \ mod\ (n_i)$, by choice of d_i, so $x_0 \equiv a_i \ mod\ (n_i)$ as required. Thus x_0 is a solution of the simultaneous congruences, and it immediately follows that the entire congruence class $[x_0]$ of x_0 mod (n) consists of solutions.
To see that this class is unique, suppose that x is any solution; then $x \equiv a_i \equiv x_0 \ mod\ (n_i)$ for any n_i divides $x - x_0$. Since $n_1, ..., n_k$ are mutually coprime, then their product n also divides $x - x_0$, so $x \equiv x_0 \ mod\ (n)$. □

As a consequence, we obtain easily the interesting following corollary:

Corollary 7.2.8. *Let n have prime-power factorization*

$$n = p_1^{e_1} ... p_k^{e_k}$$

where p_1, ..., p_k are distinct primes. Then for any integers a and b we have $a \equiv b \ mod\ (n)$ if and only if $a \equiv b \ mod\ (p_i^{e_i})$ for each $i = 1, ..., k$.

Remark 7.2.9. *1. This result has applications in many areas, for instance in astronomy. If k events occur regularly with periods n_1, ..., n_k and with the i-th event happening at times $x = a_i$, $a_i + n_i$, $a_i + 2n_i$, ... then the k events occur simultaneously at time x where $x \equiv a_i \ mod\ (ni)$ for all i; the theorem shows that if the periods n_i are mutually coprime then such a coincidence occurs with period n. Planetary conjunctions and eclipses are obvious examples of such regular events, and predicting these may have been the original motivation for the theorem.*

2. *Let n_1, n_2, ..., n_k be positive integers, with $gcd(n_i, n_j)$ whenever $i \neq j$, and let a_1, ..., a_k, b_1, ..., b_k be any integers such that $gcd(a_i, n_i)|b_i$ for any i. Then the solutions of the simultaneous congruences*

$$b_1x \equiv a_1 \ mod\ (n_1),\ b_2x \equiv \ mod\ (n_2), ..., b_kx \equiv a_k \ mod\ (n_k)$$

can be find, solving first the congruences $b_1x \equiv a_1 \ mod\ (n_1)$ getting congruence classes mod n_i and then applying the previous theorem.

Example 7.2.10. 1. *Solve the following simultaneous congruences:*

$$x \equiv 2 \ mod\ (3),\ x \equiv 3 \ mod\ (5),\ x \equiv 2 \ mod\ (7)$$

we have $n_1 = 3$, $n_2 = 5$ and $n_3 = 7$, so $n = 105$, $c_1 = 35$, $c_2 = 21$ and $c_3 = 15$. We first need to find a solution $x = d_1$ of $c_1x \equiv 1 \ mod\ (n_1)$, that is, $35x \equiv 1 \ mod\ (3)$; this is equivalent to $-x \equiv 1 mod\ (3)$, so we can take $x = d_1 = -1$ for example. Similarly, $c_2x \equiv 1 \ mod\ (n_2)$, gives $21x \equiv 1 \ mod\ (5)$, that is, $x \equiv 1 \ mod\ (5)$, so we can take $x = d_2 = 1$, while $c_3x \equiv 1 \ mod\ (n_3)$ gives $15x \equiv 1 \ mod\ (7)$, that is, $x \equiv 1 \ mod\ (7)$, so we can also take $x = d_3 = 1$. Of course, different choices of d_i are possible here, leading to different values of x_0, but they will all give the same congruence class of solutions mod (105). We now have:

$$x_0 = a_1c_1d_1 + a_2c_2d_2 + a_3c_3d_3 = 2 \times 35 \times (-1) + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 23,$$

so the solutions form the congruence class $[23]$ mod (105), that is, the general solution is $x = 23 + 105t$, $(t \in \mathbb{Z})$.
We can also use the Chinese Remainder Theorem as the basis for second method for solving simultaneous linear congruences, which is less direct but often more efficient. We start by finding a solution $x = x_1$ of one of the congruences. It is usually best to start with the congruence involving the largest modulus. So, we could start with $x \equiv 2 \ mod\ (7)$, which has $x_1 = 2$ as an obvious solution. The remaining solutions of this congruence are found by adding or subtracting multiples of 7, and among these we can find an integer $x_2 = x_1 + 7t$ which also satisfies the second congruence $x \equiv 3 \ mod\ (5)$: trying x_1, $x_1 \pm 7$, $x_1 \pm 14$,... in turn, we soon find $x_2 = 2 - 14 = -12$. This satisfies $x \equiv 2 \ mod(7)$ and $x \equiv 3 \ mod\ (5)$, and by Chinese Remainder Theorem the general solution of this pair of congruences has the form $x_2 + 35t = -12 + 35t$ $(t \in \mathbb{Z})$. Trying x_2, $x_2 \pm 35$, $x_2 \pm 70$, ... in turn, we soon find a solution $x_3 = -12 + 35t$ which also satisfies all three congruence $x \equiv 2 \ mod\ (3)$, namely $x_3 = -12 + 35 = 23$. This satisfies all three congruences so by Chinese Remainder Theorem their general solution consists of the congruence class $[23]$ mod (105).

2. *Consider the simultaneous congruences*

$$7x \equiv 3 \ mod\ (12),\ 10x \equiv 6 \ mod\ (14)$$

We have solved these two linear congruences previously and they have respectively as general solution $x = 9 + 7t$ and $x = 2 + 7t$. It follows that we can replace the original pair of congruences with the pair

$$x \equiv 9 \ mod\ (12),\ x \equiv 2 \ mod\ (7)$$

Clearly, $x_0 = 9$ is a particular solution; since the moduli 12 and 7 are coprime, with product 84, the Chinese Remainder Theorem implies that the general solution has the form $9 + 84t$.

3. *Consider the linear congruence*

$$13x \equiv 71 \ mod \ (380)$$

Instead of using the algorithm described earlier for solving a single linear congruence, we can use the factorization $380 = 2^2 \times 5 \times 19$, together with the corollary of Chinese Remainder Theorem, we can replace this congruence with the three simultaneous congruences

$$13x \equiv 71 \ mod \ (4), \ 13x \equiv 71 \ mod \ (5), \ 13x \equiv 71 \ mod \ (19).$$

These immediately reduce to

$$x \equiv 3 \ mod \ (4), \ 3x \equiv 1 \ mod \ (5), \ 13x \ \equiv 14 \ mod \ (19)$$

Now these have mutually coprime moduli, so the Chinese Remainder Theorem applies, and we can use either of our two methods to find the general solution. Using the second method, we start with a solution $x_1 = 4$ of the third congruence; adding and subtracting multiples of 19, we find that $x_2 = 42$ also satisfies the second congruence and then adding and subtracting multiples of $19 \times 5 = 95$ we find that 327 (or equivalently -53) also satisfies the first congruence. Thus the general solution has the form $x = 327 + 380t$ ($t \in \mathbb{Z}$).

More generally, we can see the Chinese Remainder theorem as a particular case of the following theorem:

Theorem 7.2.11. *Let n_1, ..., n_k be positive integers and let a_1, ..., a_k be any integers. Then the simultaneous congruences*

$$x \equiv a_1 \ mod \ (n_1), ..., x \equiv a_k \ mod \ (n_k)$$

have a solution x if and only if $gcd(n_i, n_j)$ divides $a_i - a_j$ whenever $i \neq j$. When this condition is satisfied, the general solution forms a single congruence class mod (n), where n is the least common multiple of n_1, ..., n_k.

The reader can refer to the proof of the book of Jones (Theorem 3.12).

Remark 7.2.12. *If the moduli n_i are mutually coprime then $gcd(n_i, n_j) = 1$ for all $i \neq j$, so the condition $gcd(n_i, n_j)|(a_i - a_j)$ is always satisfied; moreover, the least common multiple n of n_1,..., n_k is then their product n_1, ..., n_k, so we obtain the Chinese Remainder theorem.*

Example 7.2.13. *Consider the congruences*

$$x \equiv 11 \ mod \ (36), \ x \equiv 7 \ mod \ (40), \ x \equiv 32 \ mod \ (75)$$

Here, $n_1 = 36$, $n_2 = 40$ and $n_3 = 75$, so we have

$$n_{12} = gcd(36, 40) = 4, n_{13} = gcd(36, 75) = 3 \ and \ n_{23} = gcd(40, 75) = 5$$

Since

$$a_1 - a_2 = 11 - 7 = 4,\ a_1 - a_3 = 11 - 32 = -21 \text{ and } a_2 - a_3 = 7 - 32 = -25$$

the conditions $n_{ij}|(a_i - a_j)$ *are all satisfied, so there are solutions forming a single congruence class mod* (n) *where* $n = lcm(36, 40, 75) = 1800$. *To find the general solution, the idea is to factorize each* n_i, *and replace the first congruence with*

$$x \equiv 11 \ mod\ (2^2) \text{ and } x \equiv 11 \ mod\ (3^2)$$

the second with

$$x \equiv 7 \ mod\ (2^3) \text{ and } x \equiv 7 \ mod\ (5)$$

and the third with

$$x \equiv 32 \ mod\ (3) \text{ and } x \equiv 32 \ mod\ (5^2)$$

This gives us a set of six congruences, in which the moduli are powers of the primes $p = 2, 3$ *and* 5. *From these, we select one congruence involving the highest power of each prime: for* $p = 2$ *we must choose* $x \equiv 7 \ mod\ (2^3)$ *(which implies* $x \equiv 11 mod\ (2^2)$*), for* $p = 3$, *we must choose* $x \equiv 11 \ mod\ (3^2)$ *(which implies* $x \equiv 32 \ mod\ (3)$*), and for* $p = 5$ *we must choose* $x \equiv 32 \ mod\ (5^2)$ *(which implies* $x \equiv 7 \ mod\ (5)$*). These three congruences, which can be simplified to*

$$x \equiv 7 \ mod\ (8),\ x \equiv 2 \ mod\ (9),\ x \equiv 7 \ mod\ (25),$$

have mutually comprise moduli, then we find using a method as before sugared by the proof of the Chinese Remainder Theorem, that the general solution is $x \equiv 407 \ mod\ (1800)$.

It is sometimes possible to solve simultaneous congruences by the Chinese Remainder Theorem, even when the congruences are not all linear.

Example 7.2.14. *Consider the simultaneous congruences*

$$x^2 \equiv 1 \ mod\ (3) \text{ and } x \equiv 2 \ mod\ (4)$$

Noticing that $x^2 \equiv 1 \ mod\ (3)$ *is equivalent to* $x \equiv 1 \ mod\ (3)$ *or* $x \equiv 2 \ mod\ (3)$, *so the pair of congruences are equivalent to*

$$x \equiv 1 \ mod\ (3) \text{ and } x \equiv 2 \ mod\ (4)$$

or

$$x \equiv 2 \ mod\ (3) \text{ and } x \equiv 2 \ mod\ (4)$$

Then we solve both cases thanks to Chinese Remainder Theorem. We find that the first case has general solution $x \equiv -2 \ mod\ (12)$ *while the second pair has general solution* $x \equiv 2 \ mod\ (12)$, *so the general solution for the initial simultaneous congruence is* $x \equiv \pm 2 \ mod\ (12)$.

Theorem 7.2.15. *Let* $n = n_1...n_k$ *where the integers* n_i *are mutually coprime, and let* $f(x)$ *be a polynomial with integer coefficients. Suppose that for each* $i = 1, ..., k$ *there are* N_i *congruence classes* $x \in \mathbb{Z}/n_i\mathbb{Z}$ *such that* $f(x) = 0 \ mod\ (n_i)$. *Then there are* $N = N_1...N_k$ *classes* $x \in \mathbb{Z}/n\mathbb{Z}$ *such that* $f(x) \equiv 0 \ mod\ (n)$.

Proof. Since the moduli n_i are mutually coprime, we have $f(x) \equiv 0 \ mod \ (n)$ if and only if $f(x) \equiv 0 \ mod \ (n_i)$ for all i. Thus each class of solution $x \in \mathbb{Z}/n\mathbb{Z}$ of $f(x) \equiv 0 \ mod \ (n)$ determines a class of solutions $x = x_i \in \mathbb{Z}/n_i\mathbb{Z}$ of $f(x_i) \equiv 0 \ mod \ (n_i)$ for each i. Conversely, if for each i we have a class of solutions $x_i \in \mathbb{Z}/n_i\mathbb{Z}$ of $f(x_i) \equiv 0 \ mod \ (n_i)$, then by the Chinese Remainder Theorem there is a unique class $x \in \mathbb{Z}/n\mathbb{Z}$ satisfying $x = x_i \ mod \ (n_i)$ for all i, and this class satisfies $f(x) \equiv 0 \ mod \ (n)$. Thus there is a one-to-one correspondence between classes $x \in \mathbb{Z}/n\mathbb{Z}$ satisfying $f(x) \equiv 0 \ mod \ (n)$, and k-tuples of classes $x_i \in \mathbb{Z}/n_i\mathbb{Z}$ satisfying $f(x_i) \equiv 0 \ mod \ (n_i)$ for all i. For each i there are N_i choices for the class $x_i \in \mathbb{Z}/n_i\mathbb{Z}$ so there are N_1, ..., N_k such k-tuples and hence this is the number of classes $a \in \mathbb{Z}/n\mathbb{Z}$ satisfying $f(x) \equiv 0 \ mod \ (n)$. □

7.2.3 Congruences with prime modulus

If we observe a linear equation of the form $ax \equiv b \ mod \ p$ with p a prime integer. We know that it has a unique solution if and only if $gcd(a, p)$ which is equal either to 1 or p divides b. We can see this in term of polynomial and we have just seen that if $a \not\equiv 0 \ mod \ p$, the polynomial $ax - b$ in $\mathbb{Z}/p\mathbb{Z}$ has at least a root in $\mathbb{Z}/p\mathbb{Z}$. More, generally, we have the following result.

Theorem 7.2.16. *Let p be prime, and let $f(x) = a_d x^d + ... + a_1 x + a_0$ be a polynomial with integer coefficients, where $a_i \not\equiv 0 \ mod \ p$ for some i. Then, the congruence $f(x) \equiv 0 \ mod \ p$ is satisfied by at most d congruence classes $[x] \in \mathbb{Z}/p\mathbb{Z}$.*

Proof. We use induction on d then if $f(x) = a_0$ with p not dividing a_0, so there are no solutions of $f(x) \equiv 0 \ mod \ p$, as required. for the inductive step, we now assume that $d \geqslant 1$, and that all polynomials $g(x) = b_{d-1}x^{d-1} + ... + b_0$ with some $b_i \not\equiv 0 \ mod \ p$ have at most $d - 1$ roots $[x] \in \mathbb{Z}/p\mathbb{Z}$.
Let $f(x) = a_d x^d + ... + a_0$ be a polynomial of degree d. If the congruence $f(x) \equiv 0 \ mod \ p$ has no solutions, there is nothing left to prove, so suppose that $[a]$ is a solution; thus $f(a) \equiv 0 \ mod \ p$, so p divides $f(a)$. Now

$$f(x) - f(a) = \sum_{i=0}^{d} a_i x^i - \sum_{i=0}^{d} a_i a^i = \sum_{i=0}^{d} a_i (x^i - a^i) = \sum_{i=1}^{d} a_i (x^i - a^i)$$

For each $i = 1, ..., d$, we can put:

$$x^i - a^i = (x - a)(x^{i-1} + ax^{i-2} + ... + a^{i-2}x + a^{i-1}),$$

so, that by taking out the common factor $(x - a)$ we have

$$f(x) - f(a) = (x - a)g(x)$$

for some polynomial $g(x)$ with integer coefficients, of degree at most $d-1$. Now p cannot divide all the coefficient of $g(x)$: if it did then since it also divides $f(a)$ it would have to divide all the coefficients of $g(x)$: if it did, then since it also divides $f(a)$, it would have to divide all the coefficients of $f(x) = f(a) + (x - a)g(x)$, against our assumption. We may therefore apply the induction hypothesis to $g(x)$, so that at most $d - 1$ classes

$[x]$ satisfy $g(x) \equiv 0 \ mod \ p$. We now count classes $[x]$ satisfying $f(x) \equiv 0 \ mod \ p$; if any class $[x] = [b]$ satisfies $f(b) \equiv 0 \ mod \ p$, then p divides both $f(a)$ and $f(b)$, so it divides $f(b) - f(a) = (b-a)g(b)$; since p divides both $f(a)$ and $f(b)$, so it divides $b-a$ to $g(b)$, so either $[b] = [a]$ or $g(b) \equiv 0 \ mod \ p$. There are at most $d-1$ classes $[b]$ satisfying $g(b) \equiv 0 \ mod \ p$, and hence at most $1 + (d-1) = d$ satisfying $f(b) \equiv 0 \ mod \ p$, as required. □

Remark 7.2.17. *1. If $a_d \equiv 0 \mod p$ in the previous theorem, $f(x)$ has strictly fewer that d classes $[x]$ satisfying $f(x) \equiv 0 \ mod \ p$. Even if $a_d \not\equiv 0 \ mod \ p$, we can have fewer that d class. For instance $f(x) = x^2 + 1$ has only one root in $\mathbb{Z}/2\mathbb{Z}$, which is the class $[1]$ and it has no roots in $\mathbb{Z}/3\mathbb{Z}$.*

2. The condition $a_i \not\equiv 0 \ mod \ p$ for some i ensures that $f(x)$ yields a non-trivial polynomial when we reduce it mod p. If $a_i \equiv 0 \ mod \ p$ for any i, then all p classes $[x] \in \mathbb{Z}/p\mathbb{Z}$ satisfy $f(x) \equiv 0 \ mod \ p$, so the result will fail if $d < p$

3. It is essential to suppose that the moduli is prime: for example, the polynomial $f(x) = x^2 - 1$, of degree 2, has four roots in $\mathbb{Z}/8\mathbb{Z}$, namely $[1]$, $[3]$, $[5]$ and $[7]$.

A useful equivalent vernon of the previous Lagrange's theorem is the contrapositive:

Corollary 7.2.18. *Let $f(x) = a_d x^d + ... + a_1 x + a_0$ be a polynomial with integer coefficients, and let p be prime. If $f(x)$ has more than d roots in $\mathbb{Z}/p\mathbb{Z}$, then p divides each of its coefficients a_i*

The following result useful in studying polynomials of high degree, is known as Fermat's Little Theorem:

Theorem 7.2.19. *If p is prime and $a \not\equiv 0 \ mod \ p$, then $a^{p-1} \equiv 1 mod \ p$.*

Proof. The integers 1, .., $p-1$ form a complete set of non-zero residues mod p. If $a \not\equiv 0 \ mod \ p$, then $xa \equiv xb \ mod \ p$ implies $x \equiv y \ mod \ p$, so that the integers a, $2a$, ..., $(p-1)a$ lie in distinct classes mod p. None of these integers is divisible by p, so they also form a complete set of non-zero residues. It follows the a, $2a$, ..., $(p-1)a$ are congruent to 1, 2, ..., $p-1$ in some order. Thus, the products of these two sets of integers must therefore lie in the same class, that is,

$$1 \times 2 \times .... \times (p-1) \equiv a \times 2a \times .... \times (p-1)a \ mod \ p,$$

or equivalently

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

Since $(p-1)!$ is coprime to p, we can divide through by $(p-1)!$ and deduce that $a^{p-1} \equiv 1 \ mod \ p$. □

Remark 7.2.20. *Another interpretation of the previous result is that all the classes in $\mathbb{Z}/p\mathbb{Z}$ except $[0]$ are roots of the polynomial $x^{p-1} - 1$. For a polynomial satisfied by all the classed in $\mathbb{Z}/p\mathbb{Z}$, we simply multiply by x, to get $x^p - x$.*

Example 7.2.21. *Fermat's little theorem fails if p is not prime, if $n = 4$ and $a = 3$, $a^{n-1} = 27 \not\equiv 1 \ mod \ 4$, for instance.*

Corollary 7.2.22. *If p is prime then $a^p \equiv a \ mod\ (p)$ for every integer a.*

Example 7.2.23. *1. Find $2^{68}\ mod\ 19$. 19 is prime we can apply the previous theorem, we have*

$$2^{68} \equiv 2^{18\times 3+14} \equiv (2^{18})^3 2^{14} \equiv 2^{14} \equiv (2^4)^3 \times 2^2 \equiv (-3)^3 \times 4 \equiv -8\times 4 \equiv -32 \equiv 6\ mod\ 19$$

2. Prove that $a^{25} - a$ is divisible by 30 for every integer a. Since $30 = 2 \times 3 \times 5$, it is enough to prove that $a^{25} - a$ is divisible by 2, 3 and 5. But,

$$a^{25} = (a^5)^5 \equiv a^5 \equiv a\ mod\ 5$$

$$a^{25} = (a^3)^8 a \equiv a^9 \equiv (a^3)^3 \equiv a^3 \equiv a\ mod\ 3$$

and

$$a^{25} = (a^2)^{12} a \equiv (a^2)^6 a \equiv (a^2)^3 a \equiv (a^2)^2 \equiv a^2 \equiv a\ mod\ 2$$

Remark 7.2.24. *The corollary of Fermat theorem proves that if $f(x)$ is any polynomial of degree $d \geqslant p$, then we can find a polynomial $g(x)$ of degree less than p with the property that $f(x) \equiv g(x)\ mod\ p$ for all integers x. In other words, when considering polynomials mod p, it is sufficient to restrict attention to those of degree $d < p$. Similarly, the coefficients can also be simplified by reducing them mod p.*

Example 7.2.25. *Find all the roots of the congruence*

$$x^{17} + 6x^{14} + 2x^5 + 1 \equiv 0\ smod\ 5$$

$$x^{17}+6x^{14}+2x^5+1 \equiv (x^5)^3x^2+(x^5)^2+2x+1 \equiv x^5+x^2+2x+1 \equiv x^2+3x+1 \equiv x^2-2x+1 \equiv (x-1)^2\ mod\ 5$$

So it is equivalent to solve

$$(x-1)^2 \equiv 0\ mod\ 5$$

and we find an unique solution which is $[x] = [1]$, so this class is the only solution of the first congruence equation.

One famous corollary of Fermat's little theorem, is the Wilson's theorem:

Corollary 7.2.26. *An integer n is prime if and only if $(n-1)! \equiv -1\ mod\ n$.*

Proof. Suppose that n is a prime p. If $p = 2$ then $(p-1)! = 1 \equiv -1\ mod\ p$, as required, so we may assume that p is odd. Define

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

a polynomial with integer coefficients. This has degree $d < p-1$, since when the product is expanded, the two terms in $f(x)$ involving x^{p-1} cancel. If $a = 1, 2, ..., p-1$, then $f(a) \equiv 0\ mod\ p$: the product $(1-a)(2-a)...(p-1-a)$ vanishes since it has a factor equal to 0, and $1 - a^{p-1} \equiv 0\ mod\ p$ by Ferma's little theorem. Thus, $f(x)$ has more that d roots mod p, then its coefficients are all divisible by p. In particular, p divide the constant term $(p-1)! + 1$, so $(p-1)! \equiv -1\ mod\ p$.
For the converse, suppose that $(n-1)! \equiv -1\ mod\ n$. We then have $(n-1)! \equiv -1\ mod\ n$. We then have $(n-1)! \equiv -1\ mod\ m$, for any factor m of n. If $m < n$ then m appears as a factor of $(n-1)!$, so $(n-1)! \equiv 0\ mod\ m$ and hence $-1 \equiv 0\ mod\ m$. This implies that $m = 1$, so we conclude that n has no proper factors and is therefore prime. □

Theorem 7.2.27. *Let p be an odd prime. Then the quadratic congruence $x^2 + 1 \equiv 0 \ mod \ p$ has a solution if and only if $p \equiv 1 \ mod \ 4$.*

Proof. Suppose that p is an odd prime, and let $k = (p-1)/2$. In the product

$$(p-1)! = 1 \times 2 \times ... \times k \times (k+1) \times ... \times (p-2) \times (p-1),$$

we have $p - 1 \equiv -1 \ mod \ p$, $p - 2 \equiv -2 \ mod \ p$, ... , $k + 1 = p - k \equiv -k \ mod \ p$, so by replacing each of the k factors $p - i$ with $-i$ for $i = 1, ..., k$, we see that

$$(p-1)! \equiv (-1)^k.(k!)^2 \ mod \ p$$

Now Wilson's theorem gives $(p-1)! \equiv -1 \ mod \ p$, so $(-1)^k(k!)^2 \equiv -1 \ mod \ p$ and hence $(k!)^2 \equiv (-1)^{k+1} \ mod \ p$. If $p \equiv 1 \ mod \ 4$ then k is even, so $(k!)^2 \equiv -1 \ mod \ p$ and hence $x = k!$ is a solution of $x^2 + 1 \equiv 0 \ mod \ p$.
On the other hand, suppose that $p \equiv 3 \ mod \ 4$, so that $k = (p-1)/2$ is odd. If x is any solution of $x^2 + 1 \equiv 0 \ mod \ p$, then x is coprime to p, so Fermat's Little theorem gives $x^{p-1} \equiv 1 \ mod \ p$. Thus $1 \equiv (x^2)^k \equiv (-1)^k \equiv -1 \ mod \ p$, which impossible since p is odd, so there can be no solution. □

Remark 7.2.28. *The previous theorem implies that if p is any prime then there are at most two classes $[x] \in \mathbb{Z}/p\mathbb{Z}$ of solutions of $x^2 + 1 \equiv 0 \ mod \ p$. When $p \equiv 1 \ mod \ 4$, there are two classes $\pm[k!]$, when $p \equiv 3 \ mod \ 4$, there are no solutions, and when $p = 2$ there is a unique class $[1]$ solutions.*

Example 7.2.29. *Let $p = 13$, so $p \equiv 1 \ mod \ 4$. Then $k = 6$, and $6! = 720 \equiv 5 \ mod \ 13$, so $x = 5$ is a solution of $x^2 + 1 \equiv 0 \ mod \ 13$, as is easily verified. The other solution is then $-5 \equiv 8 \ mod \ 13$.*

7.2.4 Congruences with prime power modulus

We consider the following situation. Let $f(x) = \sum_j a_j x^j$ be a polynomial with integer coefficients, and let the congruence $f(x) \equiv 0 \ mod \ p^i$ have a solution $x \equiv x_i \ mod \ p^i$. If $x_{i+1} = x_i + p^i k_i$, then the Binomial theorem gives

$$\begin{aligned} f(x_{i+1}) &= \sum_j a_j (x_i + p^i k_i)^j \\ &= \sum_j a_j x_i^j + \sum_j j a_j x_i^{j-1} p^i k_i \\ &= f(x_i) + f_0(x_i) p^i k_i \ mod \ p^{i+1} \end{aligned}$$

Where we ignore multiples of p^{i+1}. Putting $f(x_i) = p^i q_i$ and dividing through by p^i, we see that $f(x_{i+1}) \equiv 0 \ mod \ p^{i+1}$ if and only if

$$q_i + f'(x_i) k_i \equiv 0 \ mod \ p \ (\square)$$

There are now three possibilities:

1. if $f'(x_i) \not\equiv 0 \ mod \ p$ then $(\square)$ has a unique solution k_i mod p, so x_i gives rise to a unique solution $x_{i+1} \in \mathbb{Z}/p^{i+1}\mathbb{Z}$ of $f(x) \equiv 0 \ mod \ p^{i+1}$;

2. if $f'(x_i) \equiv 0 \not\equiv q_i \bmod p$, then ($\square$) has no solution k_i, and x_i gives no solution $x_{i+1} \in \mathbb{Z}/p^{i+1}\mathbb{Z}$;
3. if $f'(x_i) \equiv 0 \equiv q_i \bmod p$ then every $k_i \in \mathbb{Z}/p\mathbb{Z}$ satisfies ($\square$), so x_i gives rise to p solutions $x_{i+1} \in \mathbb{Z}/p^{i+1}\mathbb{Z}$.

This principle is part of a much more general result known as Hensel's Lemma.

Remark 7.2.30. *There is a close analogy with Newton's method where a solution $x \in \mathbb{R}$ of an equation $f(x) = 0$ is found as the limit of a convergent sequence of approximations x_i given by the recurrence relation*

$$x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$$

In our case, we have $x_{i+1} = x_i + p^i k_i$, where $q_i + f'(x_i)k_i \equiv 0 \bmod p$ and $f(x_i) = p^i q_i$, so writing $k_i = -q_i/f'(x_i)$ and substituting for k_i we get the same recurrence relation (though the arithmetic used is modular, rather than real). In Newton's method, convergence means that terms x_i and x_j become close together, in the sense that $|x_i - x_j| \to 0$ as $i, j \to \infty$, in our case, however we regard x_i and x_j as close (in modular arithmetic) if $x_i \equiv x_j \bmod p^e$ when e is large. Just as real numbers can be constructed as the limits of convergent sequences of rational numbers, this new concept of convergence gives rise to a new number system, namely the field $\mathbb{Q}_p$ of p-adic numbers (one field for each prime p). The importance of this number system is that it allows algebraic, analytic and topological methods to be applied to the study of congruences mod p^e.

Let's us study some examples:

Example 7.2.31. *1. To solve the congruence*

$$2x \equiv 3 \bmod 5^e$$

we take $p = 5$ and $f(x) = 2x-3$. By inspection, the only solution of $2x \equiv 3 \bmod 5$ is $x \equiv 4 \bmod 5$. Any solution of $2x \equiv 3 \bmod 5^2$ must satisfy $2x \equiv 3 \bmod 5$; and must therefore have the form $x \equiv 4 + 5k_1 \bmod 5^2$ for some integer k_1. Then $3 \equiv 2x \equiv 8 + 10k_1 \bmod 5^2$, so $10k_1 \equiv -5 \bmod 5^2$ and hence $2k_1 \equiv -1 \bmod 5$. This has solution $k_1 \equiv 2 \bmod 5$, so we obtain $x = 4 + 5k_1 \equiv 14 \bmod 5^2$ as the general solution of $2x \equiv 3 \bmod 5^2$. We can now repeat this process to solve $2x \equiv 3 \bmod 5^3$. Putting $x \equiv 14 + 5^2k_2 \bmod 5^3$ we see that $28 + 50k_2 \equiv 3 \bmod 5^3$. So $50k_2 \equiv -25 \bmod 5^3$ and hence $2k_2 \equiv -1 \bmod 5$, with solution $k_2 \equiv 2 \bmod 5$; thus $x \equiv 14 + 5^2k_2 \equiv 64 \bmod 5^3$ is the general solution of $2x \equiv 3 \bmod 5^3$.
We can iterate this as often as we like, a typical step being as follows. Suppose that, for some i, the general solution of $2x \equiv 3 \bmod 5^i$ is $x \equiv x_i \bmod 5^i$ for some x_i, so $2x_i - 3 = 5^i q_i$ for some integer q_i. (We took $x_1 = 4$ and $q_1 = 1$ in the above calculation, for instance.) We put $x \equiv x_i + 5^i k_i \bmod 5^{i+1}$, for some unknown integer k_i, so $3 \equiv 2x \equiv 2x_i + 2 \times 5^i k_i \bmod 5^{i+1}$, or equivalently $2k_i \equiv -q_i \bmod 5$, with solution $k_i \equiv 2q_i \bmod 5$. Thus $x \equiv x_{i+1} \equiv x_i + 2 \times 5^i q_i \bmod 5^{i+1}$ is the general solution of $2x \equiv 3 \bmod 5^{i+1}$.

2. Let us solve

$$f(x) = x^3 - x^2 + 4x + 1 \equiv 0 \ mod\ 5^e$$

for $e = 1, 2$ *and* 3. *By inspection, for* $e = 1$, *the only solutions of* $x \equiv \pm 1 \ mod\ 5$. *Let us take* $x_1 = -1$ *as our starting point, so* $f(x_1) = 5q_1$ *with* $q_1 = -1$. *To find a corresponding solution of* $f(x) \equiv 0 \ mod\ 5^2$, *we put* $x_2 \equiv x_1 + 5k_1 \equiv -1 + 5k_1 \ mod\ 5^2$. *Then*

$$\begin{aligned} f(x_2) &\equiv (x_1 + 5k_1)^3 - (x_1 + 5k_1)^2 + 4(x_1 + 5k_1) + 1 \\ &\equiv (x_1^3 - x_1^2 + 4x_1 + 1) + (3x_1^2 - 2x_1 + 4)5k_1 \\ &\equiv 5q_1 + 9 \times 5k_1 \ mod\ 5^2 \end{aligned}$$

where we have used the Binomial theorem to expand each power of $x_1 + 5k_1$; *we have included only the first two terms in each binomial expansion, since any subsequent terms are multiples of* 5^2 *and hence congruent to* 0. *Thus* $f(x_2) \equiv 0 \ mod\ 5^2$ *if and only if* $q_1 + 9k_1 \equiv 0 \ mod\ 5$; *since* $q_1 = -1$, *this is equivalent to* $k_1 \equiv -1 \ mod\ 5$, *so* $x \equiv x_2 \equiv x_1 + 5k_1 \equiv -6 \ mod\ 5^2$ *is the unique solution of* $f(x) \equiv 0 \ mod\ 5^2$ *satisfying* $x \equiv -1 \ mod\ 5$.

Repeating this process, we have $f(x_2) = -275 = 5^2 q_2$ *where* $q_2 = -11$. *If we put* $x_3 \equiv x_2 + 5^2 k_2 \equiv -6 + 5^2 k_2 \ mod\ 5^3$ *then*

$$\begin{aligned} f(x_3) &\equiv (x_2 + 5^2k_2)^3 - (x_2 + 5^2k_2)^2 + 4(x_2 + 5^2k_2) + 1 \\ &\equiv (x_2^3 - x_2^2 + 4x_2 + 1) + (3x_2^2 - 2x_2 + 4)5^2k_2 \\ &\equiv 5^2q_2 + 124 \times 5^2k_2 \ mod\ 5^3 \end{aligned}$$

so we require $q_2 + 124k_2 \equiv 0 \ mod\ 5$, *that is,* $k_2 \equiv -1 \ mod\ 5$. *This gives* $x \equiv x_3 \equiv x_2 + 5^2k_2 \equiv -31 \ mod\ 5^3$ *as the unique solution of* $f(x) \equiv 0 \ mod\ 5^3$ *satisfying* $x \equiv -1 \ mod\ 5$.

Chapter 8

The ring $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$, its group of unit U_n, applications

8.1 Algebraic interlude

A little of group theory

We will define briefly here what is a group and what is a ring.

Definition 8.1.1. *We say that G is a **group** if it is a set G with a binary operation $\star$ satisfying the following axioms:*

1. *if $g, h \in G$ then $g \star h \in G$ (stable under the multiplication).*
2. *if $f, g, h \in G$ then $f \star (g \star h) = (f \star g) \star h$ (associativity)*
3. *there is an element $e \in G$ such that $g \star e = e \star g$ for any $g \in G$. (Identity).*
4. *for each $g \in G$ there is an element $h \in G$ such that $g \star h = e = h \star g$. (inverse)*

We often omit the symbol $\star$, and write fg instead of $f \star g$. A product $g \star .... \star g$ with i factor will be written g^i.

- *e is called the **identity element**.*
- *The element h of the last axiom is called **the inverse of** g often written as g^{-1}.*
- *We call the **order of** G denoted by $|G|$ the number of elements of the set G; if this is finite, we say that G is a **finite group**.*
- *A group is said to be **abelian** or **commutative**, if moreover $gh = hg$ for any $g, h \in G$ (commutativity). For an abelian group $\star$ is often denoted by $+$, the identity by 0 (usually called the **zero element**) and the inverse of g by $-g$, so for instance, 3. becomes $g + 0 = g = 0 + g$.*

Example 8.1.2. *$(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathcal{M}_{n,m}(\mathbb{R}), +)$ are abelian groups. $(\mathbb{R}\setminus -\{0\}, .)$, $(\mathbb{C}\setminus -\{0\}, .)$ are also abelian group.*

Definition 8.1.3. *A **subgroup of a group** G is a subset H of G which is also a group with respect to the same binary operation as G; this is equivalent to the conditions:*

1. *the identity element e belongs to H,*
2. *$gh \in H$, for any $g, h \in H$,*

3. *if* $h \in H$ *then* $h^{-1} \in H$.

this is also equivalent to the conditions:

1. *the identity element* e *belongs to* H,
2. $gh^{-1} \in H$, *for any* $g,h \in H$,

We write $H \leqslant G$ *to denote that* H *is a subgroup of* G.

Example 8.1.4. $(\mathbb{Z},+)$ *is a subgroup of* $(\mathbb{R},+)$ *which is a subgroup of* $(\mathbb{C},+)$.

Definition 8.1.5. *A* ***homomorphism between groups*** G ***and*** G' *is a function* $\theta : G \to G'$ *such that* $\theta(gh) = \theta(g)\theta(h)$ *for any* $g,h \in G$; *if* θ *is a bijection, it is called* ***isomorphism****. If such an isomorphism exists, we say that* G *and* G' *are* ***isomorphic****, written* $G \simeq G'$. *This means that* G *and* G' *have the same algebraic structure, and differ only in the notation for their elements.*

Definition 8.1.6. *If* $H \leqslant G$ *and* $g \in G$ *the* ***right (resp. left) coset of*** H *containing* g *is the subset* $Hg = \{hg | h \in H\}$ *(resp.* $gH = \{gh | h \in H\}$*) of* G. *Each right coset of* H *contains* $|H|$ *elements. Right cosets* Hg_1 *and* Hg_2 *are either equal or disjoints, they partition* G *into disjoint subsets. The number of distinct right cosets of* H *in* G *is called the* ***index of*** H ***in*** G *denoted by* $[G : H]$.

Theorem 8.1.7. *If* G *is finite, then* $|G| = [G : H] \times |H|$. *In particular, we have Lagrange's theorem, that is* $|H|$ *divides* $|G|$.

Definition 8.1.8. ***The order of an element*** $g \in G$ *is the least integer* $n > 0$ *such that* $g^n = 1$, *provided such an integer exists; if it does not,* g *has infinite order.*

Remark 8.1.9. *If* G *is finite, then every element* g *has finite order* n *for some* n; *we group generated by* g *that is the set of the power of* g *is then* $< g >= \{e, g, g^2, ..., g^{n-1}\}$, *it forms a subgroup of* G, *then by Lagrange theorem we have that* $n||G|$. *Moreover, for any* $g \in G$, $g^{|G|} = e$.

Definition 8.1.10. *A group* G *is* ***cyclic*** *if there exists an element* $c \in G$, *called* ***generator for*** G, *such that every* $g \in G$ *has the form* $g = c^i$ *for some integer* i, *that is* G *is equal to the set generated by* c $G =< c >= \{c^k | k \in \mathbb{Z}\}$. *If* c *has finite order* n, *then* $|G| = n$, *and* G *is isomorphic to* $\mathbb{Z}/n\mathbb{Z}$.

Remark 8.1.11. *This group* G *has one subgroup* H *of order* m, *for each* m *dividing* n, *and no other subgroups;* H *is cyclic group of order* m, *with generator* $[n/m]$.

Definition 8.1.12. *The direct product* $G_1 \times G_2$ *of groups* G_1 *and* G_2 *consists of all ordered pairs* (g_1, g_2) *with* $g_i \in G_i$ *for* $i = 1, 2$. *This is a group, with binary operation* $(g_1, g_2)(h_1, h_2) = (g_1h_1, g_2h_2)$; *indeed, the identity element is* (e_1, e_2) *where* e_i *is the identity element in* G_i *for* $i = 1, 2$ *and the inverse of some* (g_1, g_2) *is* (g_1^{-1}, g_2^{-1}). *There are subgroups* $G_1' = \{(g_1, e_2) | g_1 \in G_1\} \simeq G_1$ *and* $G_2' = \{(e_1, g_2) | g_2 \in G_2\} \simeq G_2$. *Direct products* $G_1 \times ... \times G_k$ *are defined similarly for* $k > 2$.

A little of ring theory

Definition 8.1.13. *We say that a set R is a **unitary commutative ring** if it is provided with two binary operations (addition $r+s$ and multiplication $r.s$, usually written rs), and with distinct elements 0 and 1 (unit element) such that*

1. *Additive structure $(R,+)$ is an abelian group, with zero element 0;*
2. *$rs = sr$ for any $r,s \in R$ (commutativity);*
3. *$r(st) = (rs)t$ for any r, s, $t \in R$ (associativity);*
4. *$r(s+t) = rs + rt$, for any $r,s,t \in R$ (distributivity);*
5. *$r1 = r$, for any $r \in R$.*

Example 8.1.14. 1. *$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are all examples of rings.*

2. *The direct product $R_1 \times .... \times R_k$ of rings R_1, ..., R_k is defined in much the same way as the direct product of groups: its elements are the k-tuples $(r_1,...,r_k)$ such that $r_i \in R_i$ for any i, with component wise operations.*

Definition 8.1.15. *A **homomorphism between rings** R **and** R' is a function $\theta : R \to R'$ such that $\theta(r+s) = \theta(r) + \theta(s)$ and $\theta(rs) = \theta(r)\theta(s)$ for any $r,s \in R$, and $\theta(1) = 1$; if θ is a **bijection**, it is called an **isomorphism**. If such an isomorphism exists, we say that R and R' are **isomorphic**, written $R \simeq R'$.*

Definition 8.1.16. *An element $r \in R$ is a unit if $rs = 1$ for some $s \in R$; the units form a group under the multiplication, with 1 as the identity element. A **field** is a ring R in which every element $r \neq 0$ is a unit.*

Example 8.1.17. *$\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.*

8.2 The ring $(\mathbb{Z}/n\mathbb{Z},+,.)$ and its group of Units

Lemma 8.2.1. *The set of the congruence classes mod n $\mathbb{Z}/n\mathbb{Z}$ is a ring where the*

1. *addition operation is*

$$[a] + [b] = (n\mathbb{Z} + a) + (n\mathbb{Z} + b) = n\mathbb{Z} + (a+b) = [a+b]$$

2. *multiplication operation is*

$$[a].[b] = (n\mathbb{Z} + a)(n\mathbb{Z} + b) = n\mathbb{Z} + (ab) = [a].[b]$$

For n small we can write a addition and multiplication table on $\mathbb{Z}/n\mathbb{Z}$, Let observe few examples:

Example 8.2.2. 1. *For $n = 5$, we get this table in $\mathbb{Z}/n\mathbb{Z}$*

ADDITION

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

MULTIPLICATION

+	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

So $\mathbb{Z}/5\mathbb{Z}$ is a field since every non-zero element has an inverse.

2. For $n = 6$, we get this table in $\mathbb{Z}/n\mathbb{Z}$

ADDITION

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

MULTIPLICATION

+	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$\mathbb{Z}/6\mathbb{Z}$ is not a field since 2 has no inverse.

If we observe with attention these two multiplicative table. In the first one every line as a 1 except the one of 0 for n=5 which is not true for n=6, we get product of two non zeros elements giving zero.

We are looking for extending the arithmetic of $\mathbb{Z}$ to $\mathbb{Z}/n\mathbb{Z}$. But for instance in $\mathbb{Z}$ the product of two non zero element is non zero which is not always the case as we have seen by the previous examples; We will see what we can say and generalize or not. Let's recall once again the definition of an inverse:

Definition 8.2.3. *A **multiplicative inverse for a class** $[a] \in \mathbb{Z}/n\mathbb{Z}$ is a class $[b] \in \mathbb{Z}/n\mathbb{Z}$ such that $[a][b] = 1$. A class $[a] \in \mathbb{Z}/n\mathbb{Z}$ is a **unit** if it has a multiplicative inverse in $\mathbb{Z}/n\mathbb{Z}$. (In this case, we sometimes say that the integer a is a unit mod (n), meaning that $ab \equiv 1 \ mod \ (n)$, for some integer b.) We denote U_n the set of all the units mod (n).*

There is a way very explicit to describe the unit:

Lemma 8.2.4. *$[a]$ is a unit in $\mathbb{Z}/n\mathbb{Z}$ if and only if $gcd(a, n) = 1$.*

Proof. If $[a]$ is a unit then $ab = 1 + qn$ for some integer b and q; any common factor of a and n would therefore divide 1, so $gcd(a, n) = 1$. Conversely, if $gcd(a, n) = 1$ then $1 = au + nv$ for some u and v; so $[u]$ is a multiplicative inverse of $[a]$ □

Corollary 8.2.5. *For p prime, $U_p = (\mathbb{Z}/p\mathbb{Z})^\times$.*

Corollary 8.2.6. *$\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime.*

Proof. Indeed, for any $a = 1, 2, 3, ..., p-1$, $gcd(a, p) = 1$. Thus any non zero element has an inverse. If n is not prime, then there is a prime p which divides n and $gcd(p, n) = p \neq 1$ and p is a non zero element of $\mathbb{Z}/n\mathbb{Z}$, then p is not invertible. □

Remark 8.2.7. *Moreover, if n is not prime we have what we call **zero divisors**, non-zero elements whose product is 0.*

Example 8.2.8. *1. $\mathbb{Z}/5\mathbb{Z}$ is a field but not $\mathbb{Z}/6\mathbb{Z}$ as we have observed before.*

2. $U_8 = \{[1], [3], [5], [7]\}$ and $U_9 = \{[1], [2], [4], [5], [7], [8]\}$.

The next result allows us to study units algebraically.

Theorem 8.2.9. *For each integer $n \geqslant 1$, the set U_n forms an abelian group under multiplication mod n, with identity element $[1]$.*

Proof. We have to show that U_n that:

1. The product of two units is also a unit.
2. We have the associativity property.
3. The is a neutral element on U_n.
4. There is an inverse element for any unit.

The associativity on U_n is a direct consequence of the associativity on $\mathbb{Z}$.
Let $[a]$ and $[b]$ be two units denote by $[u]$ and $[v]$ respectively the two inverses so that $[a].[u] = [au] = [1]$ and $[b].[v] = [bv] = [1]$. We have by definition that $[a].[b] = [ab]$ then $[ab].[uv] = [abuv] = [au].[bv] = [1]^2 = [1]$. So, $[ab]$ has $[uv]$ as inverse and it is therefore a unit. This prove 1.
The identity element is clearly $[1]$, indeed for any unit $[a] \in U_n$, $[a].[1] = [a]$ and each element has an inverse by definition. The commutativity is a direct consequence of the commutativity on $\mathbb{Z}$. □

We can then speak about the order of an element.

Example 8.2.10.
1. *In U_5 the element 2 has order 4; its powers are $2^1 \equiv 2 \ mod\ 5$, $2^2 \equiv 4 \ mod\ 5$, $2^3 \equiv 3 \ mod\ 5$ and $2^4 \equiv 1 \ mod\ 5$, so $k = 4$ is the least positive exponent such that $2^k \equiv 1 \ mod\ 5$. Similarly, the element 1 has order 1, while the elements 3 and 4 have orders 4 and 2 respectively.*
2. *In U_8, the elements $1, 3, 5, 7$ have order $1, 2, 2, 2$ respectively.*

New proof of Little Fermat theorem Theorem.

Theorem 8.2.11. *If p is prime and $a \not\equiv 0 \ mod\ p$, then $a^{p-1} \equiv 1 mod\ p$.*

Proof. U_p is a group of order $p - 1$. Now, Lagrange theorem implies that for any class $[a] \in U_p$, $[a]^{p-1} = [1]$, so that any a such that $[a] \neq [0]$, is such that $a^{p-1} \equiv 1 \ mod\ p$. □

We have seen earlier that Mersenne numbers are coprime. We see now a justification of this result:

Lemma 8.2.12. *If l and m are coprime positive integers, then $2^l - 1$ and $2^m - 1$ are corprime. In particular, distinct Mersenne number are coprime.*

Proof. Let n be the highest common factor of $2^l - 1$ and $2^m - 1$. Clearly, n is odd, so 2 is a unit mod (n). Let k be the order of the element 2 in the group U_n. Since n divides $2^l - 1$, we have $[2^l] = [1]$ in U_n, so k divides l. Similarly k divides m. So k divides $gcd(l, m) = 1$.Thus $k = 1$, so the element 2 has order 1 in U_n. This means that $2^l \equiv 1 \ mod\ n$, so $n = 1$, as required. □

We recall that the Euler's function is defined to be $\phi(n) = |U_n|$, the number of units in $\mathbb{Z}/n\mathbb{Z}$. We have seen that we have also $\phi(n) = \{a \in \{1, ..., n\} | gcd(a, n) = 1\}$.
We have then some generalization of Fermat's little theorem, often called Euler's theorem.

Theorem 8.2.13. *If $gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1$ mod n.*

Proof. Since U_n is a group under the multiplication of order $\phi(n)$, Lagrange's theorem implies that $[a]^{\phi(n)} = [1]$ for all $[a] \in U_n$. □

Example 8.2.14. *If we take $n = 12$ then $U_{12} = \{\pm[1], \pm[5]\}$ and $\phi(12) = 4$; we have $(\pm 1)^4 = 1$ and $(\pm 5)^4 = 625 \equiv 1$ mod 12, so $a^4 \equiv 1$ mod 12 for each a coprime to 12.*

8.3 Another proof of the multiplicativity of the Euler function

Lemma 8.3.1. *If $n = p^e$ where p is prime then*

$$\phi(n) = p^e - p^{e-1} = p^{e-1}(p-1) = n(1 - 1/p)$$

Proof. $\phi(p^e)$ is the number of integers in $\{1, ..., p^e\}$ which are coprime to p^e, that is, not divisible by p; this set has p^e members, of which $p^e/p = p^{e-1}$ are multiple of p, so $\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$. □

In order to get a formula for ϕ evaluated at some arbitrary n we will need the following lemma about complete set of residues mod n.

Lemma 8.3.2. *If A is a complete set of residues mod n, and if m and c are integers with m coprime to n, then the set $Am + c = \{am + c | a \in A\}$ is also a complete set of residues mod n.*

Proof. If $am + c \equiv a'm + c$ mod n, where a, $a' \in A$, then by subtracting c and then canceling the unit m, we see that $a \equiv a'$ mod n, and hence $a \equiv a'$ mod n. Thus the n elements $am + c$ ($a \in A$) all lie in different congruence classes, so they form a complete set of residues mod n. □

Theorem 8.3.3. *If m and n are coprime, then $\phi(mn) = \phi(m)\phi(n)$*

Proof. We may assume m and $n > 1$, for otherwise the result is trivial since $\phi(1) = 1$. Let us arrange the mn integers 1, 2, ..., mn into an array with n roots and m columns, as follows:

1	2	3	...	m
$m+1$	$m+2$	$m+3$	...	$2m$
.	.	.	...	.
.	.	.	...	.
.	.	.	...	.
$(n-1)m+1$	$(n-1)m+2$	$(n-1)m+3$	...	nm

These integers i form a complete set of residues mod mn, so $\phi(mn)$ is the number of them coprime to mn, or equivalently satisfying $gcd(i, m) = gcd(i, n) = 1$. The integers

in a given column are all congruent mod m; thus exactly $\phi(m)$ of the columns consist of integers i coprime to m, and the other columns consist of integers with $gcd(i,m) > 1$. Now each column of integers coprime to m has the form c, $m+c$, $2m+c$, ..., $(n-1)m+c$, for some c; for the previous lemma this is a complete set of residues mod n, since $A = \{0,1,2,...,n-1\}$ is and since $gcd(m,n) = 1$. Such a column therefore contains $\phi(n)$ integers coprime to n, so these $\phi(m)$ columns yield $\phi(m)\phi(n)$ integers i coprime to both m and n. Thus $\phi(mn) = \phi(m)\phi(n)$, as required. □

Remark 8.3.4. *The result fails if* $gcd(m,n) > 1$*: for instance* $2^2 = 4$*, but* $\phi(2)^2 \neq \phi(4)$*.*

Example 8.3.5. *The integers* $m = 3$ *and* $n = 4$ *are coprime, with* $\phi(3) = \phi(4) = 2$*, here* $mn = 12$ *and* $\phi(12) = 2 \times 2 = 4$*.*

Corollary 8.3.6. *If* n *has prime-power factorization* $n = p_1^{e_1}...p_k^{e_k}$ *then*

$$\phi(n) = \prod_{i=1}^{k}(p_i^{e_i} - p_i^{e_i-1}) = \prod_{i=1}^{k} p_i^{e_i-1}(p_i - 1) = n\prod_{i=1}^{k}(1 - 1/p_i) = n\prod_{p|n}(1 - 1/p)$$

Proof. We can prove it by induction on the number k of the prime appearing on the decomposition. We have proven the case $k = 1$ before; Assume that $k > 1$ and the that the result is true for all integers divisible by fewer than k primes. We have $n = p_1^{e_1}...p_{k-1}^{e_{k-1}}p_k^{e_k}$, where $p_1^{e_1}$, ... , $p_{k-1}^{e_{k-1}}$ and $p_k^{e_k}$ are coprime, so then

$$\phi(n) = \phi(p_1^{e_1}...p_{k-1}^{e_{k-1}})\phi(p_k^{e_k})$$

The induction hypothesis gives

$$\phi(p_1^{e_1}...p_{k-1}^{e_{k-1}}) = \prod_{i=1}^{k-1}(p_i^{e_i} - p_i^{e_i-1})$$

and we have seen that

$$\phi(p_k^{e_k}) = (p_k^{e_k} - p_k^{e_{k-1}}),$$

so by combining these two results we get

$$\phi(n) = \prod_{i=1}^{k}(p_i^{e_i} - p_i^{e_i-1})$$

□

Example 8.3.7. *The primes dividing* 60 *are* 2, 3 *and* 5*, so*

$$\phi(60) = 60(1 - 1/2)(1 - 1/3)(1 - 1/5) = 60 \times 1/2 \times 2/3 \times 4/5 = 16$$

8.4 Application to cryptography

Important results to keep in mind

Recall Fermat's Little Theorem:

Theorem 8.4.1 (Fermat's Little Theorem)**.** *If p is prime and a is an integer not divisible by p (that is, $\gcd(a,p) = 1$), then*

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

Furthermore, for every integer a we have

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

Recall Euler's ϕ-function:

$$\begin{aligned} \phi(n) &= \text{the number of positive integers less than or equal to } n \\ &\quad \text{that are relatively prime to } n \\ &= n - \text{the number of integers less than or equal to } n \\ &\quad \text{that are not relatively prime to } n. \end{aligned}$$

Example 8.4.2. *1. $\phi(5) = 4$, because $1,2,3,4$ are all relatively prime to 5 and 5 is not.*

2. To compute $\phi(10)$, consider $\{\mathbf{1},2,\mathbf{3},4,5,6,\mathbf{7},8,\mathbf{9},10\}$. It is easy to see that $\phi(10) = 4$.

Remark 8.4.3. *Let p, q be primes. Then*

1. $\phi(p) = p - 1$.
2. $\phi(p^k) = p^k - p^{k-1}$ *for any positive integer k.*
3. $\phi(pq) = (p-1)(q-1)$.

Example 8.4.4. *1. $\{\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{4},\mathbf{5},\mathbf{6},7\}$, so $\phi(7) = 7 - 1$.*

2. $\{\mathbf{1},2,\mathbf{3},4,\mathbf{5},6,\mathbf{7},8\}$, so $\phi(2^3) = 2^3 - 2^2$.

3. $\{\mathbf{1},\mathbf{2},3,\mathbf{4},5,6,\mathbf{7},\mathbf{8},9,10,\mathbf{11},12,\mathbf{13},\mathbf{14},15\}$, so $\phi(3 \cdot 5) = (3-1)(5-1)$.

Recall Euler's ϕ-function

Theorem 8.4.5 (Euler's Theorem)**.** *Let a and n be positive integers with $\gcd(a,n) = 1$. Then*

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

Corollary 8.4.6. *As a special case, when $n = p$ is a prime, then we get Fermat's Little Theorem:*

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

RSA

Cryptography has a lot of applications such as *rock-paper-scissors over the phone* and *authentication (e-signature)*. We will focus on sending a message securely. For example, suppose Alice wishes to send the message "STOP" to Bob.

1. They use the following rule to get the numerical equivalent of each letter in alphabet: $A = 01,\ B = 02, \cdots,\ Z = 26$. For example, the numerical equivalent of "CAT" is 030120. Conversely, the alphabetical equivalent of 13012008 is "MATH".
2. Alice translates "STOP" into 19201516 and sends this number to Bob, and Bob decodes 19201516 using the rule to get "STOP" back.
3. Problem is, in practice, it is very likely that a potential code breaker, say Charlie, also knows this rule. So if the code breaker Charlie intercepts the number 19201516, then he also knows what the original plain text was.

How to fix this problem? Alice and Bob may want to change the rule, say:

$$A = 03,\ B = 04, \cdots,\ X = 26,\ Y = 01,\ Z = 02.$$

But this is not long-lived. There are several ways to figure out this new rule (e.g. frequency analysis).
Another problem is: if Alice wants to send a message to Charlie, then now Alice and Charlie must set up a different rule, because now Bob could be a possible code breaker!

As an idea of resolving this problem, in 1976, three researchers at M.I.T. – Ronald Rivest, Adi Shamir, and Leonard Adleman came up with an idea now called the **RSA System**.

1. Find $\phi(143)$. Since $143 = 11 \times 13$, $\phi(143) = 10 \times 12 = 120$.
2. Find $\phi(3127)$. Since $3127 = 53 \times 59$, $\phi(3127) = 52 \times 58 = 3016$.

KEY OBSERVATION

1. Computing $53 \times 59 = 3127$ is easy, but finding the prime factorization of 3127 (reverse process) is difficult!
2. If p, q are large primes (each with more than 200 digits, for example), then calculating the product pq is not difficult with a computer, but when the product pq is given, finding the individual prime numbers p, q is not easy, **even with a computer**.

Central Idea of RSA

1. Alice chooses two (large) prime numbers p_A and q_A. She computes $n_A = p_A q_A$ and $\phi(n_A) = (p_A - 1)(q_A - 1)$. She then chooses a number e_A so that $\gcd(e_A, (p_A - 1)(q_A - 1)) = 1$ (this can be done without difficulty). Since $\gcd(e_A, (p_A - 1)(q_A - 1)) = 1$, there exist positive integers s_A, t_A such that $s_A e_A - t_A(p_A - 1)(q_A - 1) = 1$

(Backward Euclidean Algorithm). Now she **makes public the pair** (n_A, e_A) **but does NOT disclose** s_A.

2. Bob does the same thing: he chooses two large prime numbers p_B and q_B, computes $n_B = p_B q_B$, chooses e_B, s_B, and t_B so that $\gcd(e_B, (p_B - 1)(q_B - 1)) = 1$ and $s_B e_B - t_B(p_B - 1)(q_B - 1) = 1$, and makes public the pair (n_B, e_B) while concealing s_B.
3. Charlie does the same thing (makes (n_C, e_C) public, keeps s_C), David does the same thing (makes (n_D, e_D) public, keeps s_D), etc.

How does Alice send a message to Bob?

1. Alice first translates her plain text to its numerical equivalent, say M.
2. She then looks up her phone book to find (n_B, e_B).
3. Then she computes the remainder C of M^{e_B} when divided by n_B (that is $M^{e_B} \equiv C \pmod{n_B}$).
4. Finally, Alice sends C to Bob.

Example 8.4.7. *Let's say* $p_B = 53$ *and* $q_B = 59$. *Then* $n_B = 53 \times 59 = 3127$ *and* $(p_B - 1)(q_B - 1) = 52 \times 58 = 3016$. *Pick* $e_B = 271$, *then* $\gcd(e_B, (p_B - 1)(q_B - 1)) = \gcd(271, 3016) = 1$. *Using Backward Euclidean Algorithm, one can see that* $2671 \cdot 271 - 240 \cdot 3016 = 1$, *which means* $s_B = 2671$. *Bob makes* $(n_B, e_B) = (3127, 271)$ *open to public while concealing* $s_B = 2671$.

1. *To send "GO" (which is equivalent to* $M = 715$*) to Bob, Alice looks up her phone book to find* $(n_B, e_B) = (3127, 271)$.
2. *She then computes the remainder* C *of* $M^{e_B} = 715^{271}$ *when divided by* 3127. C *turns out to be* 1657.
3. *Alice sends* $C = 1657$ *to Bob.*

How does Bob decode C to get the plain text back?

1. *Bob receives* C.
2. *He then computes the remainder of* C^{s_B} *when divided by* n_B. *Note that*

$$C^{s_B} \equiv (M^{e_B})^{s_B} = M^{e_B s_B} = M^{1 + t_B(p_B - 1)(q_B - 1)}.$$

By Euler's Theorem, $M^{(p_B - 1)(q_B - 1)} \equiv 1 \pmod{n_B}$ *and this means that*

$$M^{t_B(p_B - 1)(q_B - 1)} = (M^{(p_B - 1)(q_B - 1)})^{t_B} \equiv 1 \pmod{n_B}.$$

Consequently,

$$C^{s_B} \equiv M,$$

which means that the remainder of C^{s_B} *when divided by* n_B *equals* M.

3. *With this* M, *Bob can easily recover the original plain text.*

1. *Bob received* 1657.

2. *He then computes the remainder of* $1657^{s_B} = 1657^{2671}$ *when divided* $n_B = 3127$, *which turns out to be* 715.
3. *Bob then recovers "GO".*

Why is RSA robust?

Suppose that Charlie was able to intercept C. To get the plain text M, he must know s_B. Recall that s_B was determined so that $s_B e_B - t_B(p_B - 1)(q_B - 1) = 1$, that is

$$s_B e_B \equiv 1 \pmod{(p_B - 1)(q_B - 1)}.$$

Since e_B is known to Charlie, if Charlie knows $\phi(n_B) = (p_B - 1)(q_B - 1)$, then he can actually find s_B. But to get $(p_B - 1)(q_B - 1)$, Charlie should know p_B and q_B, and this is almost impossible even though he knows what $p_B q_B$ is.

Example 8.4.8. *Suppose Charlie managed to get* $C = 715$. *To obtain the plain text* M, *he needs to know* s_B, *which is hidden. If Charlie can find* $\phi(n_B) = \phi(p_B q_B) = (p_B - 1)(q_B - 1)$, *then there is a way to find* s_B *easily. Charlie knows* $(n_B, e_B) = (3127, 271)$, *but computing* $\phi(n_B) = \phi(3127)$ *is difficult without knowing the prime factorization of* 3127.

8.5 Modular arithmetic revisited by algebra

The chinese remainder theorem can be seen as follow

Theorem 8.5.1. *Let* $m, n \in \mathbb{Z}$ *and* $gcd(m, n) = 1$. *then the natural map*

$$\psi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

sending $a \bmod mn$ *to* $(a \bmod m, b \bmod n)$ *yields an isomorphism of the rings* $\mathbb{Z}/mn\mathbb{Z}$ *and* $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

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

As a consequence, arguing by induction we obtain.

Theorem 8.5.2. *Let* $m_1, \ldots, m_n \in \mathbb{Z}$ *and* $gcd(m_i, m_j) = 1$, *for any* $i \neq j$. *Let* $m = m_1 \ldots m_r$. *Then the map*

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

given by

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

yields a ring isomorphism.

From this we can deduce automatically that:

Theorem 8.5.3. *Let $m_1, \ldots, m_n \in \mathbb{Z}$ and $(m_i, m_j) = 1$, for any $i \neq j$. Let $m = m_1 \ldots m_r$. Then the map*

$$\psi : U_m \to U_{m_1} \times \ldots \times U_{m_r}$$

given by

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

yields a ring isomorphism.

Remark 8.5.4.

1. *From cardinality consideration, since if m and n are integer such that $(m, n) = 1$ we have that $\phi(mn) = \phi(m)\phi(n)$. (The multiplicity of the Euler function).*
2. *We have already proven Fermat little theorem and Euler theorem with an algebraic method.*
3. *Let p be a prime number. First we notice that the only number between 1 and $p-1$ such that $x = x^{-1}$ are 1 and -1 since then $x^2 = 1$ which implies that $x = \pm 1$ (since $\mathbb{Z}/p\mathbb{Z}$ is a field). Now the $(p-1)-2$ remaining element can be taken by pair inverse of each other. And we obtain easily that the product of $(p-1)!$ which is the product of all $p-1$ elements is equal to -1 mod p.*

Definition 8.5.5. *Let $m \in \mathbb{N}$. An integer g such that g mod m generates the group U_m is called a* ***primitive root modulo*** *m.*

Finding a primitive roots in U_n (if they exist is a non-trivial problem, and there is no simple solution. One obvious but tedious method is to ttry each of the $\phi(n)$ units $a \in U_n$ in turn, each time computing powers a^i mod n to find the order of a in U_n; if we find an element a of order $\phi(n)$ then we know that this must be a primitive root. The following result is a rather more efficient test for primitive roots:

Lemma 8.5.6. *An element $a \in U_n$ is a primitive root if and only if $a^{\phi(n)/q} \neq 1$ in U_n for each prime q dividing $\phi(n)$.*

Proof. ($\Rightarrow$) If a is a primitive root, then it has order $|U_n| = \phi(n)$, so $a^i \neq 1$ for all i such that $1 \leqslant i < \phi(n)$; in particular, this applies to $i = \phi(n)/q$ for each prime q dividing $\phi(n)$.
($\Leftarrow$) If a is not a primitive root, then its has order $|U_n| = \phi(n)$, so $a^i \neq 1$ for all i such that $1 \leqslant i < \phi(n)$, so $\phi(n)/k > 1$. If q is any prime factor of $\phi(n)/k$, then k divides $\phi(n)/q$, so that $a^{\phi(n)/q} = 1$ in U_n, against our hypothesis. Thus a must be a primitive root. □

Theorem 8.5.7. *If p is prime, then the group U_p has $\phi(d)$ elements of order d for each d dividing $p-1$.*

Proof. For each d dividing $p-1$ let us define:

$$\Omega_d = \{a \in U_p | a \text{ has order } d\} \text{ and } \omega(d) = |\Omega_d|$$

the number of elements of order d in U_p. Our aim is to prove that $\omega(d) = \phi(d)$ for all such d. We know by Lagrange's theorem that the order of each element of U_p divides $p-1$, so the sets Ω_d form a partition of U_p and hence

$$\sum_{d|p-1} \omega(d) = p-1$$

But we know that

$$\sum_{d|p-1} \phi(d) = p-1$$

so

$$\sum_{d|p-1} (\phi(d) - \omega(d)) = 0$$

If we can show that $\omega(d) \leqslant \phi(d)$ for all d dividing $p-1$, then each summand in this expression is non-negative; since their sum is 0, the summands must all be 0, so $\omega(d) = \phi(d)$, as required.
The inequality $\omega(d) \leqslant \phi(d)$ is obvious if ω_d is empty, so assume that ω_d contains an element a. By the definition of ω_d, the powers $a^i = a, a^2, ..., a^d$ $(= 1)$ are all distinct, and they satisfy $(a^i)^d = 1$, so they are d distinct roots of the polynomial $f(x) = x^d - 1$ in $\mathbb{Z}/p\mathbb{Z}$; but we have seen that $f(x)$ has at most $deg(f) = d$ roots in $\mathbb{Z}/p\mathbb{Z}$, so these are a complete set of roots of $f(x)$. We shall show that Ω_d consists of those roots a^i for some $i = 1, 2, ..., d$. If we let j denote $gcd(i, d)$, then

$$b^{d/j} = a^{id/j} = (a^d)^{i/j} = 1^{i/j} = 1$$

in U_p; but d is the order of b, so no lower positive power of b than b^d can be equal to 1, and hence $j = 1$. Thus every element b if order d has the form a^i where $1 \leqslant i < d$ and i is coprime to d. The number of such integers i is $\phi(d)$, so the number $\omega(d)$ of such elements b is at most $\phi(d)$, and the proof is complete. □

Corollary 8.5.8. *(Gauss theorem) If p is prime, then the group U_p has $\phi(d)$ elements of order d for each d dividing $p-1$.*

Proof. Putting $d = p-1$, in the previous theorem, we see that there are $\phi(p-1)$ elements of order $p-1$ in U_p. Since $\phi(p-1) \geqslant 1$, the group contains at least one element of this order. Now U_p has order $\phi(p) = p-1$, so such an element is a generator for U_p and hence this group is cyclic. □

Example 8.5.9. *As an illustration consider U_{17} and the powers of 3 modulo 17,*
- $3^1 \equiv 3 \ mod 17$
- $3^2 \equiv 9 \ mod 17$
- $3^3 \equiv 10 \ mod 17$
- $3^4 \equiv 13 \ mod 17$
- $3^5 \equiv 5 \ mod 17$
- $3^6 \equiv 15 \ mod 17$
- $3^7 \equiv 11 \ mod 17$
- $3^8 \equiv 16 \ mod 17$

— $3^9 \equiv 14 \ mod 17$
— $3^{10} \equiv 8 \ mod 17$
— $3^{11} \equiv 7 \ mod 17$
— $3^{12} \equiv 4 \ mod 17$
— $3^{13} \equiv 12 \ mod 17$
— $3^{14} \equiv 2 \ mod 17$
— $3^{15} \equiv 6 \ mod 17$
— $3^{16} \equiv 1 \ mod 17$

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

Lemma 8.5.10. *Let* G *be a finite abelian group. If* $ord(g)$ *and* $ord(h)$ *are relatively prime then* $ord(gh) = ord(h)ord(g)$.

Proof. Let $M = odd(gh)$. From $e = (gh)^M$ it follows that $e = (gh)^{Mord(g)} = h^{Mord(h)}$. Hence, $ord(h)|Mord(g)$. Since $(ord(g), ord(h)) = 1$, we conclude that $ord(h)|M$. Similarly, $ord(g)|M$. hence $ord(g)ord(h)|M$. On the other hand, $(gh)^{ord(h)ord(g)} = e$ an so $M|ord(g)ord(h)$ and thus we find that $M = ord(g)ord(h)$. □

Lemma 8.5.11. *Let* p *be an odd prime and* $r \in \mathbb{N}$

1. $(1 + p)^{p^{r-1}} \equiv 1 + p^r \ mod \ p^{r+1}$.
2. $5^{2^{r-2}} \equiv 1 + 2^r \ mod \ 2^{r+1}$, *for all* $r \geqslant 2$.

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

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

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

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

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

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

as asserted.

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

$$5^{2^{r-3}} \equiv 1 + 2^{r-1} \ mod \ 2^r$$

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

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

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

□

Theorem 8.5.12. *Let p be an odd prime and $k \in \mathbb{N}$. Then U_{p^k} is a cyclic group.*

Proof. For $k = 1$, it is just Gauss theorem. So, let us assume $k > 1$. Let g be a primitive root modulo p and let $ord(g)$ be its order in U_{p^k}. Since $g^{ord(g)} = 1 \ mod \ p^k$, we have $g^{ord(g)} \equiv 1 \ mod \ p$. Moreover, g is a primitive root module p and thus $p-1|ord(g)$. So $h = g^{ord(g)/(p-1)}$ has order $p-1$ in U_{p^k}. from the previous lemma with $r = k$,, it follows that $(1+p)^{p^{k-1}} \equiv 1 \ mod \ p^k$ and the same lemma with $r = k-1$ implies $(1+p)^{p^{k-2}} \equiv 1 - p^{k-1} \not\equiv 1 \ mod \ p^k$. Hence, $ord(1+p) = p^{k-1}$. Now, by the first previous lemma we know that $(p+1)h$ has order $(p-1)p^{k-1}$ and so U_{p^k} is cyclic. □

Theorem 8.5.13. *Let k be a integer greater that 3. Any element of U_{2^k} can be written uniquely in the form $(-1)^m 5^t \ mod \ 2^k$ with $m \in \{0,1\}$, $0 \leqslant t < 2^{k-2}$.*

Proof. By the second part of the pervious lemma, with $r = k$ we find $5^{2^{k-2}} \equiv 1 \ mod \ 2^k$ and with $r = k-1$ we find $5^{2^{k-3}} \equiv 1 + 2^{k-1} \not\equiv 1 \ mod \ 2^k$. So, $ord(5) = 2^{k-2}$. Notice that all elements 5^t, $0 \leqslant t < 2^{k-2}$ are distinct and $\equiv 1 \ mod \ 4$. Hence the remaining element of U_{2^k} are given by -5^t, $0 \leqslant t < 2^{k-2}$. □

Remark 8.5.14. *Not that this theorem implies that U_{2^k} is isomorphic to the product of a cyclic group of order 2 and a cyclic group of order 2^{k-2} when $k \geqslant 3$. Of course, U_4 and U_2 are cyclic.*

Chapter 9

Quadratic reciprocity

9.1 The legendre symbol

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

Definition 9.1.1. *Let p be an odd prime and $a \in \mathbb{Z}$ not divisible by p. Then a is called a **quadratic residue mod** p if $x^2 \equiv a \ mod \ p$ has a solution and a **quadratic non residue modulo** p if $x^2 \equiv a \ mod \ p$ has no solution.*

Example 9.1.2. *The quadratic residues modulo* 13 *read:* 1, 4, 9, 3, 12, 10 *and the quadratic non residues are* 2, 5, 6, 7, 8, 11.

Definition 9.1.3. *Let p be an odd prime. The **Legendre symbol** is defined by*

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

9.2 Euler's Criterion

Proposition 9.2.1 (Euler's Criterion)**.** *Let p be an odd prime and a an integer not divisible by p.*

1. *There are exactly $(p-1)/2$ quadratic residues mod p and $(p-1)/2$ quadratic non-residue mod p*
2. *$x^2 \equiv a \ mod \ p$ has a solution if and only if*

$$a^{(p-1)/2} \equiv 1 \ mod \ p.$$

More precisely,

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

Proof. 1. Consider the residue classes 1^2, 2^2, ..., $((p-1)/2)^2$ mod p. Since $a^2 \equiv (-a)^2 \ mod\ p$, these are all quadratic residues modulo p. They are also distinct, from $a^2 \equiv b^2 \ mod\ p$ would follow $a \equiv \pm b \ mod\ p$ and when $1 \leqslant a, b \leqslant (p-1)/2$ this implies $a = b$. So there are exactly $(p-1)/2$quadratic residues modulo p. The remaining $p - 1 - (p-1)/2 = (p-1)/2$ residue classes are of course quadratic non residues.

2. Clear, if $a \equiv 0 \ mod\ p$. So assume, $a \not\equiv 0 \ mod\ p$. Since $(a^{(p-1)/2})^2 \equiv a^{p-1} \equiv 1 \ mod\ p$ by Fermat's little theorem we see that $a^{(p-1)/2} \equiv \pm 1 \ mod\ p$. Suppose that a is a quadratic residue, i.e there is an integer x such that $x^2 \equiv a \ mod\ p$. Then $1 = x^{p-1} \equiv (x^2)^{(p-1)/2} \equiv a^{(p-1)/2} \ mod\ p$, which proves half of our assertion. Since we work in the field $\mathbb{Z}/p\mathbb{Z}$, the equation $x^{(p-1)/2} \equiv 1 \ mod\ p$ has at most $(p-1)/2$ solutions. We know these solutions to be the $(p-1)/2$ quadratic residues. Hence, $a^{(p-1)/2} \equiv -1 \ mod\ p$, for any quadratic non residue a mod p.

□

Corollary 9.2.2. *Let p be an odd prime and $a, b \in \mathbb{Z}$. Then,*

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

Proof.

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

Because Legendre symbols can only be 0, ± 1 and $p \geqslant 3$, the strict equality $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ follows. □

Corollary 9.2.3. *Let p be an odd prime. Then, $\left(\frac{1}{p}\right) = 1$ and*

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

Proof. Of course, $\left(\frac{1}{p}\right) = 1$ is trivial. Also, we know that $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \ mod\ p$. Since $p \geqslant 3$ strict equality follows. □

Example 9.2.4. *Suppose $p = 11$. By squaring each element of $(\mathbb{Z}/11\mathbb{Z})^*$, we see exactly which numbers are squares modulo 11:*

$$1^2 = 1,\ 2^2 = 4,\ 3^2 = 9,\ 4^2 = 5,\ 5^2 = 3,\ 6^2 = 3,\ 7^2 = 5,\ 8^2 = 9,\ 9^2 = 4,\ 10^2 = 1.$$

Thus the squares are $\{1, 3, 4, 5, 9\}$. Next, we compute $a^{(p-1)/2} = a^5$ for each $a \in (\mathbb{Z}/11\mathbb{Z})^*$.

$$1^5 = 1,\ 2^5 = -1,\ 3^5 = 1,\ 4^5 = 1,\ 5^5 = 1,\ 6^5 = -1,\ 7^5 = -1,\ 8^5 = -1,\ 9^5 = 1,\ 10^5 = -1.$$

The a with $a^5 = 1$ are $\{1, 3, 4, 5, 9\}$, which is exactly the same as the set of squares, just as Proposition 9.2.1 predicts.

Remark 9.2.5. *Proposition 9.2.1 can be reformulated in more group-theoretic language as follows. The map*

$$(\mathbb{Z}/p\mathbb{Z})^* \to \{\pm 1\}$$

that sends a to $a^{(p-1)/2}$ mod p is a homomorphism of groups, whose kernel is the subgroup of squares of elements of $(\mathbb{Z}/p\mathbb{Z})^*$.

9.3 The Quadratic Reciprocity Law

The symbol $\left(\frac{a}{p}\right)$ only depends on the residue class of a modulo p. Thus tabulating the value of $\left(\frac{a}{5}\right)$ for hundreds of a would be silly. *Would it be equally silly to make a table of $\left(\frac{5}{p}\right)$ for hundreds of primes p?* Let's begin making such a table and see whether or not there is an obvious pattern.

p	$\left(\frac{5}{p}\right)$	$p \bmod 5$
7	-1	2
11	1	1
13	-1	3
17	-1	2
19	1	4
23	-1	3
29	1	4
31	1	1
37	-1	2
41	1	1
43	-1	3
47	-1	2

The evidence suggests that $\left(\frac{5}{p}\right)$ depends only on the congruence class of p; more precisely, $\left(\frac{5}{p}\right) = 1$ if and only if $p \equiv 1, 4 \pmod 5$, i.e., p is a square modulo 5. Similarly it turns out that $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \bmod 12$.
Starting from such observations Euler conjectured the quadratic reciprocity law. Legendre gave an incomplete proof of it and late Gauss managed to give several complete proofs. Here, we give a proof which is basically a version given by Eisenstein.

Theorem 9.3.1 (The Law of Quadratic Reciprocity)**.** *Suppose that p and q are odd primes. Then*

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

In the case considered above, this theorem implies that

$$\left(\frac{5}{p}\right) = (-1)^{2\cdot\frac{p-1}{2}} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1 & \text{if } p \equiv 1, 4 \pmod 5 \\ -1 & \text{if } p \equiv 2, 3 \pmod 5. \end{cases}$$

Thus the quadratic reciprocity law "explains" why knowing p modulo 5 helps in computing $5^{\frac{p-1}{2}} \ mod\ p$.

9.4 A Lemma of Gauss

Definition 9.4.1. *The residue classes* $1, 2, \ldots, (p-1)/2$ *mod* p *are called* ***positive****, the residue classes* $-1, -2, \ldots, -(p-1)/2$ *mod* p *are called* ***negative****.*

Lemma 9.4.2. *Let* p *be an odd prime and let* a *be an integer* $\not\equiv 0 \ mod\ p$*. Form the numbers*

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

and reduce them modulo p *to lie in the interval* $(-\frac{p}{2}, \frac{p}{2})$*. Let* μ *be the number of negative residue classes mod* p*. Then*

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

Proof. In defining ν, we expressed each number in

$$S = \left\{a, 2a, \ldots, \frac{p-1}{2}a\right\}$$

as congruent to a number in the set

$$\left\{1, -1, 2, -2, \ldots, \frac{p-1}{2}, -\frac{p-1}{2}\right\}.$$

No number $1, 2, \ldots \frac{p-1}{2}$ appears more than once, with either choice of sign, because if it did then either two elements of S are congruent modulo p or 0 is the sum of two elements of S, and both events are impossible. Thus the resulting set must be of the form

$$T = \left\{\epsilon_1 \cdot 1, \epsilon_2 \cdot 2, \ldots, \epsilon_{(p-1)/2} \cdot \frac{p-1}{2}\right\},$$

where each ϵ_i is either $+1$ or -1. Multiplying together the elements of S and of T, we see that

$$(1a) \cdot (2a) \cdot (3a) \cdot \cdots \cdot \left(\frac{p-1}{2}a\right) \equiv (\epsilon_1 \cdot 1) \cdot (\epsilon_2 \cdot 2) \cdots \left(\epsilon_{(p-1)/2} \cdot \frac{p-1}{2}\right) \ mod\ p,$$

so

$$a^{(p-1)/2} \equiv \epsilon_1 \cdot \epsilon_2 \cdot \cdots \cdot \epsilon_{(p-1)/2} \ mod\ p.$$

The lemma then follows from Proposition 9.2.1. □

Theorem 9.4.3. *Let* p *be an odd prime. Then,* $\left(\frac{2}{p}\right) = \begin{cases} 1 & if\ p \equiv \pm 1 \ mod\ 8 \\ -1 & if\ p \equiv \pm 3 \ mod\ 8 \end{cases}$

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

$$\mu = \sharp\{n \text{ even} | (p+1)/2 \leqslant n \leqslant p-1\} = \sharp\{n | (p+1)/4 \leqslant n \leqslant (p-1)/2\}$$

Replace n by $(p+1)/2 - n$ to obtain

$$\mu = \sharp\{n | 1 \leqslant n \leqslant (p+1)/4\} = [(p+1)/4]$$

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

Remark 9.4.4. *Notice that*

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

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

Lemma 9.4.5. *Let p be an odd prime and $a \in \mathbb{Z}$ odd and not divisible by p. Define*

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

Then,

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

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

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

Take both sides modulo 2,

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

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

Theorem 9.4.6. *(Quadratic reciprocity law) Let p, q be two odd prime numbers. Then,*

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

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

Proof. Let $S(a,p)$ be as in the previous lemma. Then we assert

$$S(q,p) + S(p,q) = (p-1)/2(q-1)/2$$

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

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

□

Example 9.4.7. *Is 6 a square modulo 389? We have*

$$\left(\frac{6}{389}\right) = \left(\frac{2\cdot 3}{389}\right) = \left(\frac{2}{389}\right)\cdot\left(\frac{3}{389}\right) = (-1)\cdot(-1) = 1.$$

Here, we found that $\left(\frac{2}{389}\right) = -1$ and that $389 \equiv 3 \ mod\ 8$. We found $\left(\frac{3}{389}\right)$ as follows:

$$\left(\frac{3}{389}\right) = \left(\frac{389}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Thus 6 is a square modulo 389.

9.4.1 A group theoretic proof

It is know that Gauss gave six (more or less) different proofs of the quadratic reciprocity law. Since then the number of proof has increased dramatically to an estimated 200. The proof we have given above is essentially due to Eisenstein. In the article "On the quadratic reciprocity law" in J. Australian Math. Soc. 51(1991), 423-425 by G. Rousseau, we find a proof of the reciprocity law which is surprisingly simple if one acquainted with the elementary group theory. It turns out to be an application of the Chinese remainder theorem and we like to present it here.

Proof. (The quadratic reciprocity law): Let notations be as in the theorem. We work in the group $G = (U_p \times U_q)/U$ where $U = \{(1,1),(-1,-1)\}$. Clearly,

$$\{(i,j)|i = 1,...,p-1; j = 1,2,...,(q-1)/2\}$$

is a full set of representative of G. Their product π equals

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

Since,

$$((q-1)/2)!^2 \equiv (-1)^{(q-1)/2}(q-1)! \ mod\ q$$

we get

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

Another full set of representatives of G is given by

$$\{(k \ mod\ p, k \ mod\ q) | k = 1, 2, ..., (pq-1)/2; (k, pq) = 1\}$$

This is a consequence of $U_{pq} \simeq U_p \times U_q$, (chinese remainder theorem). The product of these elements modulo p equals

$$\frac{(\prod_{i=1}^{p-1} i(p+i)(2p+i)...(\frac{q-3}{2}p+i))\prod_{i=1}^{(p-1)/2}(\frac{q-1}{2}p+i)}{1\times q\times 2q\times ...\times \frac{p-1}{2}q}$$

which equals

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

Similarly we compute the product modulo q and we obtain:

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

Comparison of the two expression for π yields

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

and hence the reciprocity law. □

9.4.2 Applications

Example 9.4.8. *1. Is $x^2 \equiv 84$ mod 97 solvable ? Notice that*

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

Hence our congruence equation is not solvable.

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

$$\begin{aligned} 3x^2+4x+5 &\equiv 0 \ mod\ 4 \\ 3x^2+4x+5 &\equiv 0 \ mod\ 19 \end{aligned}$$

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

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

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

This follows from

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

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

4. *Let E_n be the integer whose digits in base 10 consist of n ones e.g. $E_{13} = 1111111111111$. These numbers are known as **reunits**. Alternatively $E_n = (10^n - 1)/9$. As an example, we like to show here that E_{33} is divisible by 67. We easily verify that*

$$\left(\frac{10}{67}\right) = \left(\frac{2}{67}\right)\left(\frac{5}{67}\right) = -\left(\frac{67}{5}\right) = -\left(\frac{2}{5}\right) = 1$$

Hence, by Euler's criterion, $10^{33} \equiv 1\ mod 67$ and hence $67|E_{33}$.
Extensive calculations show that among the numbers E_n with $n < 50000$ only

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

are prime and E_{49081} is probably prime.

Theorem 9.4.9. *Let p be a prime such that $p \equiv -1\ mod\ 4$ and $2p+1$ prime. Then $2p+1$ divides $2^p - 1$.*

Proof. Note that $2p+1$ is a prime which is $7\ mod\ 8$. Hence $\left(\frac{2}{2p+1}\right) = 1$. Then, by Euler's criterion,

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

□

As a corollary we see that the Mersenne numbers

$$2^{13} - 1,\ 2^{83} - 1,\ 2^{131} - 1$$

are not prime. For $p < 10000$ there are 100 values for which the previous Theorem applies. We also note that if p is a prime, then any prime divisor q of $2^p - 1$ has the form $q = 2pk + 1$. So, when looking for prime divisors of $2^p - 1$ it makes sense to start by trying $2p + 1$.

Theorem 9.4.10. *(Pépin, 1877) For any $n \in \mathbb{N}$ let $F_n = 2^{2^n} + 1$. Then, F_n is prime if and only if $3^{1/2(F_n - 1)} \equiv -1\ mod\ F_n$*

Proof. $\Rightarrow$ Because F_n is an odd prime we have

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

The second to last congruence follows from

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

$\Leftarrow$ Notice that $F_n - 1 = 2^{2^n}$ and $3^{F_n-1} \equiv 1 \ mod\ F_n$. Hence $ord(3)$ divides 2^{2^n} and equals 2^r for some $0 \leqslant r \leqslant 2^n$. Suppose $r < 2^n$ then we would have $3^{(F_n-1)/2} \equiv 1 \ mod\ F_n$, contradicting our assumption. Hence, $r = 2^n$ and $o(3) = F_n - 1$. In general, if we have $a \in \mathbb{Z}$ such that $ord(a)$ in U_m is $m - 1$ then m must be prime. In particular, F_n is prime. □

9.4.3 Jacobi symbols

To determine the Legendre symbol $\left(\frac{111}{137}\right)$ say, we must first factor 111 before being able to apply quadratic reciprocity. This is all right for small numbers likes 111, but what to do if we want to compute $\left(\frac{11111111111}{197002597249}\right)$? (197002597249 is prime) or Legendre symbols with even larger numbers? We know that factorization of large numbers is a major computational problem. Luckily this does not mean that the computation of Legendre symbols becomes difficult. The solution is to use the slightly more general *Jacobi symbol*.

Definition 9.4.11. *Let $n \in \mathbb{N}$ be odd and $m \in \mathbb{Z}$ such that $(m, n) = 1$. Let $n = p_1 ... p_r$ be the prime factorization of n. The **Jacobi symbol** $\left(\frac{m}{n}\right)$ is defined by*

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

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

Remark 9.4.12. *Note that if $\left(\frac{m}{n}\right) = -1$ then $x^2 \equiv m \ mod\ n$ is not solvable simply because $x^2 \equiv m \ mod\ p_i$ is not solvable for some i. on the other hand, if $\left(\frac{m}{n}\right) = 1$, we cannot say anything about the solubility of $x^2 \equiv m \ mod\ n$. For example, $\left(\frac{-1}{21}\right) = 1$ but $x^2 \equiv -1 \ mod\ 21$ is certainly not solvable.*

Theorem 9.4.13. *Let m, n be odd positive integers. Then,*

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

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

3.

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

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

$$\frac{u_1-1}{2} + ... + \frac{u_r-1}{2} \equiv \frac{u_1...u_r-1}{2} \ mod\ 2$$

To be more precise the sum on the left is modulo 2 equal to the number k of u_i which are -1 mod 4. If k is even, the product $u_1....u_r$ is 1 mod 4 and the term on the right is also even. If k is odd, we have $u_1...u_r \equiv -1\ mod\ 4$, hence the term on the right is also odd.
Let $n = p_1...p_r$ be the prime factorization of n. Then 1. follows from

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

and

$$\frac{p_1-1}{2} + ... + \frac{p_r-1}{2} \equiv \frac{p_1...p_r-1}{2} \equiv \frac{n-1}{2} \ mod\ 2$$

Similarly, 2. follows from

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

and

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

Let $m = q_1...q_s$ be the prime factorization of m. Then, 3. follows from

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

and

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

□

Example 9.4.14. *The computation of* $\left(\frac{11111111111}{197002597249}\right)$ *can now be done using a euclidean-like algorithm and the previous theorem. Notice that*

197002597249	=	1711111111111 + 8113708362
8113708362	=	2 × 4056854181
11111111111 = 2 × 4056854181 + 2997402749		
...		...

Hence,

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

We keep repeating these steps of the inversion and extraction of 2 *until we find the value of the Jacobi symbol to be* 1*. From this algorithm we see that computation of Jacobi symbols, and hence Legendre symbols, is polynomial in the length of the input.*

Chapter 10

Continued fractions

10.1 Introduction

Definition 10.1.1. *Every real number x is represented by a point on the real line, and falls between two successive integers, say n and $n+1$:*

$$n \leqslant x < n+1$$

*The integer n is often called the **floor of** x, and is written as:*

$$n = [x]$$

The number $\{x\} = x - n$ satisfies $0 \leqslant \{x\} < 1$. Thus, for a given real x there is a unique decomposition,

$$x = [x] + \{x\}$$

where n is an integer and $\{x\}$ satisfies $0 \leqslant \{x\} < 1$ On the case where x is an integer, then $n = x$ and $\{x\} = 0$.
*This decomposition is called the **mod one decomposition of a real number**.*

Definition 10.1.2. *Let $\alpha \in \mathbb{R}$. The **continued fraction algorithm** for α runs as follows as long as $x_n \neq 0$.*

$$\begin{array}{rcl} x_0 & = & \alpha \\ a_0 & = & [x_0], \quad x_1 = 1/\{x_0\} \\ a_1 & = & [x_1], \quad x_2 = 1/\{x_1\} \\ \ldots & & \\ a_n & = & [x_n], \quad x_{n+1} = 1/\{x_n\} \\ \ldots & & \end{array}$$

*Notice that $x_i \geqslant 1$, for all $i \geqslant 1$. The algorithm is said to **terminate** if $\{x_n\} = 0$ for some n. Notice that*

$$\alpha = a_0 + \frac{1}{\{x_1\}} = a_0 + \frac{1}{a_1 + \frac{1}{\{x_2\}}} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots}}$$

which is denoted as

$$\alpha = [a_0, x_1] = [a_0, a_1, x_2] = [a_0, a_1, a_2, \ldots.]$$

Theorem 10.1.3. *The continued fraction algorithm terminates if and only if $\alpha \in \mathbb{Q}$.*

Proof. Then $\alpha = [a_0, ..., a_{n-1}]$ and we see trivially that $\alpha \in \mathbb{Q}$. If $\alpha \in \mathbb{Q}$, then the x_i are all rational numbers, say $x_i = p_i/q_i$, with p_i, $q_i \in \mathbb{N}$ and $p_i > q_i$ for all i. Notice that $q_{i+1} = p_i - [p_i/q_i]q_i$, for all i, hence $q_1 > q_2 > q_3 > ... > 0$. So we see that the algorithm terminates.
In fact, when α is rational, $\alpha = p/q$ then the continued fraction algorithm is nothing but the Euclidean algorithm applied to p and q □

Theorem 10.1.4. *Let a_0, a_1, ..., $a_n \in \mathbb{R}$. Suppose*

$$\begin{array}{llll} p_{-2} = 0, & p_{-1} = 1, & p_0 = a_0, & p_n = a_n p_{n-1} + p_{n-2} \quad (n \geqslant 0) \\ q_{-2} = 1 & q_{-1} = 0 & q_0 = 1 & q_n = a_n q_{n-1} + q_{n-2} \quad (n \geqslant 0) \end{array}$$

Then,

$$[a_0, a_1, ..., a_n] = \frac{p_n}{q_n}$$

Proof. By induction on n we shall show that

$$[a_0, ..., a_n] = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}$$

For $n = 0$ this is trivial. Now suppose $n \geqslant 0$. Notice that

$$\begin{array}{rcl} [a_0, a_1, ...a_n, a_{n+1}] & = & [a_0, a_1, ..., a_{n-1}, a_n + \frac{1}{a_{n+1}}] \\ & = & \frac{(a_n + \frac{1}{a_{n+1}})p_{n-1} + p_{n-2}}{(a_n + \frac{1}{a_{n+1}})q_{n-1} + q_{n-2}} \\ & = & \frac{a_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_n q_{n-1} + q_{n-2}) + q_{n-1}} \\ & = & \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}} \end{array}$$

which completes our induction step. □

Definition 10.1.5. *From now on we shall adhere to the notation $\alpha = [a_0, a_1, ...]$, $[a_0, ..., a_n] = p_n/q_n$ for the continued fraction expansion of α. We call a_0, a_1, a_2, ... the* ***partial fractions of the continued fraction expansion of*** *α and the p_n/q_n the* ***convergents***

Why the p_n/q_n are called convergence will become clear from the following theorem.

Theorem 10.1.6. *Let notation be as above. Then, for all $n \geqslant 0$,*

1. $p_{n-1}q_n - p_n q_{n-1} = (-1)^n$.
2. $$\alpha - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(x_{n+1}q_n + q_{n-1})}$$

Proof. 1. By induction on n, the case $n = 0$ being trivial, suppose now that the property is true for some integer n, we shall prove it for $n + 1$,

$$p_n q_{n+1} - p_{n+1}q_n = p_n(a_{n+1}q_n + q_{n-1}) - (a_{n+1}p_n + p_{n-1})q_n = -(p_{n-1}q_n - p_n q_{n-1}) = (-1)^{n+1}$$

by the induction property.

2. It follows from $\alpha = [a_0, a_1, ..., a_n, x_{n+1}] = \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}}$ and a straightforward computation of the difference $\alpha - \frac{p_n}{q_n}$.

□

Corollary 10.1.7. *For all convergents p_n/q_n, we have*

$$|\alpha - \frac{p_n}{q_n}| < \frac{1}{q_{n+1}q_n} < \frac{1}{a_{n+1}q_n^2}$$

Remark 10.1.8. *1. By definition, $q_n = a_n q_{n-1} + q_{n-2}$. Since $1 \leqslant a_n$ and $q_{n-2} > 0$, we conclude that q_n is strictly increasing as n increases. Then we may conclude that the continued fraction of a number converges to that number by the inequality just given in the corollary. In other words,*

$$\alpha = lim_{n\to\infty}\frac{p_n}{q_n} = [a_0, a_1, a_2, ...]$$

2. We see from the previous corollary that convergence p/q of the continued fraction of an irrational number α have the property that

$$|\frac{p}{q} - \alpha| < \frac{1}{q^2}$$

In particular this means the convergent give very good rational approximations with respect to their denominator. As an example, consider

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1...]$$

From the theory we expect that $|\pi - p/q| < 1/(292q^2)$ where $p/q = [3, 7, 15, 1]$ which equals $355/113$. In fact,

$$\pi = -\frac{355}{113} = -0,000000266764$$

and $355/113$ approximates π up to 6 decimal places.

Theorem 10.1.9. *(Legendre) Suppose $\alpha \in \mathbb{R}$ and p, $q \in \mathbb{Z}$, $q > 0$ such that*

$$|\frac{p}{q} - \alpha| < \frac{1}{2q^2}$$

Then p/q is a convergent of the continued fraction of α.

Proof. Since $(q_n)_n$ form a strictly increasing sequence of positive integers. Therefore, for some n, $q_n \leqslant q \leqslant q_{n+1}$. Let us assume $p/q \neq p_n/q_n$, otherwise we are done. Then we have the following inequalities,

$$\frac{1}{qq_n} \leqslant |\frac{p}{q} - \frac{p_n}{q_n}| \leqslant |\alpha - \frac{p_n}{q_n}| + |\alpha - \frac{p}{q}| \leqslant \frac{1}{q_n q_{n+1}} + \frac{1}{2q^2}$$

Multiply these inequalities with qq_n to obtain $1 < \frac{q_n}{2q} + \frac{q}{q_{n+1}}$. When $q_{n+1} \geqslant 2q$, we find, using $q_n \leqslant q$ that $1 < 1/2 + 1/2$ which is a contradiction. So let us assume $q_{n+1} < 2q$. We now repeat our estimates with a little more care. Suppose first that $\alpha - p/q$ and $\alpha - p_n/q_n$ have the same sign. Then the absolute value of their difference, which is equal to $|p/q - p_n/q_n|$, is bounded above by $max(1/(2q^2), 1/(q_n q_{n+1})$. It is bounded below by $1/(qq_n)$. Multiplication by qq_n yields $1 < max(q_n/(2q), q/q_{n+1}) < max(1/2, 1) = 1$, again a contradiction.
Now suppose that $\alpha - p/q$ and $\alpha - p_n/q_n$ have opposite sign. Then, by Theorem 10.1.6, $\alpha - p/q$ and $\alpha - p_{n+1}/q_{n+1}$ have the same sign. Just as above we derive $1 < max(q_{n+1}/(2q), q/q_{n+2})$. Using $q_{n+1} < 2q$ we find $1 < max(1, 1) = 1$, again a contradiction. □

Here is a very useful lemma in all that follows.

Lemma 10.1.10. *Let* $\alpha = [a_0, a_1, ..., a_m, \beta]$. *Then* $-1/\beta = [a_m, ..., a_2, a_1, a_0, -1/\alpha]$.

Proof. This goes by induction on m. For $m = 0$, the lemma is clear,

$$\alpha = [a_0, \beta] \Rightarrow \alpha = a_0 + \frac{1}{\alpha} \Rightarrow -\frac{1}{\beta} = a_0 + \frac{1}{-\frac{1}{\alpha}} \Rightarrow -\frac{1}{\beta} = [a_0, -\frac{1}{\alpha}]$$

Suppose $m > 0$. Then, $\alpha = [a_0, ..., a_{m-1}, a_m + 1/\beta]$. By the induction hypothesis we obtain

$$-\frac{1}{a_m + \frac{1}{\beta}} = [a_{m-1}, ..., a_1, a_0, -\frac{1}{\alpha}]$$

Invert on both sides and add a_m to obtain

$$-\frac{1}{\beta} = [a_m, ..., a_2, a_1, a_0, -\frac{1}{\alpha}]$$

□

10.2 Continued fractions for quadratic irrationals.

Note that there does not seem to be any regularity in the continued fraction of π. Here are some other examples of continued fraction expansions:

$$\begin{aligned}
e &= [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, ...] \\
e^2 &= [7, 2, 1, 1, 3, 18, 5, 1, 1, 6, 30, 8, 1, 1, 9, 42, 11, 1, 1, ...] \\
e^3 &= [20, 11, 1, 2, 4, 3, 1, 5, 1, 2, 16, 1, 1, 16, 2, 13, 14, 4, 6, 2, 1, 1, 2, 2, ...] \\
\sqrt{2} &= [1, 2, 2, 2, 2, 2, 2, ...] \\
\sqrt{97} &= [9, 1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18, 1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18, 1, ...] \\
\sqrt{47} &= [6, 1, 5, 1, 12, 1, 5, 1, 12, 1, 5, 1, 12, 1, 5, 1, ...]
\end{aligned}$$

It is interesting to not the regularity in the expansion of $\sqrt{N}$, but not in e^3. We shall return to the periodicity of the expansion of $\sqrt{N}$ in the section.

Definition 10.2.1. *A real, non-rational number α which satisfies a polynomial equation of degree 2 over $\mathbb{Q}$ is called a* ***quadratic irrational****. Given a quadratic irrational there exist, up to common sign change, a unique triple of integers A, B, C such that $A\alpha^2 + B\alpha + C = 0$ and $gcd(A,B,C) = 1$, $AC \neq 0$. The polynomial $AX^2 + BX + C$ is called the* ***minimal polynomial of*** *α. The number $D = B^2 - 4AC$ is called the* ***discriminant of*** *α/ If $\alpha = a + b\sqrt{D}$ for some $a, b \in \mathbb{Q}$, we call $a - b\sqrt{D}$ its* ***conjugate*** *and denote it by $\bar{\alpha}$. A quadratic irrational α is called* ***reduced*** *if $\alpha > 1$ and $-1 < \bar{\alpha} < 0$.*

Theorem 10.2.2. *Let α be a quadratic irrational of discriminant D. Put $x_0 = \alpha$ and define recursively $x_{n+1} = 1/(x_n - [x_n])$. Then each x_n has discriminant D and there exists n_0 such that x_n is reduced for all $n > n_0$ such that x_n is reduced for all $n > n_0$.*

Proof. That the discriminant does not change is clear if we realize that α and $\alpha - m$ have the same discriminant for any $m \in \mathbb{Z}$ and that α and $1/\alpha$ have the same discriminant. Denote by $\overline{x_n}$ the conjugate of x_n. Notice that $x_n > 1$ for all $n \geqslant 1$. Verify also that if x_n is reduced the same holds for x_{n+1}, x_{n+2},...
Let m be the smallest index such that $[x_m] \neq [\overline{x_m}]$. If such an m would not exist, both α and $\overline{\alpha}$ have the same continued fraction expansion.
Suppose that $[\overline{x_m}] < [x_m]$. Then notice that $\overline{x_{m+1}} = 1/(\overline{x_m} - [x_m]) < 0$. From $\overline{x_{m+2}} = 1/(\overline{x_{m+1}} - [x_{m+1}])$ and $\overline{x_{m+1}} < 0$ we then conclude that $-1 < \overline{x_{m+2}} < 0$ hence x_{m+2} is reduced.
Now suppose that $[\overline{x_m}] > [x_m]$. Then $\overline{x_{m+1}} = 1/(\overline{x_m} - [x_m]) < 1$. Hence $[\overline{x_m}] = 0 < [x_m]$ and we continue as in the preceding case. □

Theorem 10.2.3. *There exist finitely many reduced quadratic irrationals of given discriminant D.*

Proof. Let α be such a quadratic irrational and write $\alpha = \frac{\sqrt{D}+P}{Q}$ with $P, Q \in \mathbb{Z}$, $Q \neq 0$ (we take $\sqrt{D} > 0$).
From $\alpha > 0 > \overline{\alpha}$, it follows that $Q > 0$. From $\alpha > 1 > \overline{\alpha}$, it follows that $2P/Q > 0$, hence $P > 0$. From $\overline{\alpha} < 0$, it follows that $P - \sqrt{D} < 0$, hence $P < \sqrt{D}$. From $\alpha > 1$, we conclude $P + \sqrt{D} > Q$, hence $Q < 2\sqrt{D}$.
Concluding, we find that $0 < P < \sqrt{D}$ and $0 < Q < 2\sqrt{D}$, hence we have at most finitely many possibilities.

□

Definition 10.2.4. *Let $[a_0, a_1, a_2, ...]$ be the continued fraction expansion of a real number. We say that the expansion is* ***periodic*** *if there exist $n_0 \in \mathbb{Z}$, $N \in \mathbb{Z}$, such that $a_{n+N} = a_n$ for all $n \geqslant n_0$. We call the expansion* ***purely periodic*** *if $n_0 = 0$.*

Theorem 10.2.5. *Let $\alpha \in \mathbb{R}$. Then the continued fraction expansion of α is periodic if and only if α is a quadratic irrational. It is purely periodic if and only if α is reduced.*

Proof. We first prove our theorem for purely periodic expansions. Suppose α has a purely periodic continued fraction. Then there exists an r such that $\alpha = [a_0, a_1, ..., a_r, \alpha]$. Hence,

$$\alpha = \frac{\alpha p_r + p_{r-1}}{\alpha q_r + q_{r-1}}$$

This implies $q_r\alpha^2 + (q_{r-1} - p_r)\alpha - p_{r-1} = 0$. First of all we see that α is a quadratic irrational. Since its continued fraction is purely periodic we must have $a_0 \geqslant 1$ hence $\alpha > 1$. From the quadratic equation we see that $\alpha\overline{\alpha} = -p_{r-1}/q_r$. Using either $p_{r-1}/q_r = (p_{r-1}/q_{r-1})(q_{r-1}/q_r)$ or $(p_{r-1}/p_r)(p_r/q_r)$, we conclude that $p_{r-1}/q_r < \alpha$, hence $-1 < \overline{\alpha} < 0$. So α is reduced.
Suppose conversely that α is reduced quadratic irrational. Let $x_0 = \alpha$ and recursively $x_{n+1} = 1/(x_n - [x_n])$. Since x_0 is reduced, all x_i are reduced. Moreover their discriminants are all the same, hence there exist only finitely many distinct x_i. So there exist $r < s$ such that $x_r = x_s$. Notice that the value of a_n follows uniquely from x_{n+1} by the condition that x_n is reduced, namely $a_n = [-1/\overline{x_{n+1}}]$. Hence $x_n = [-1/\overline{x_{n+1}}] + 1/x_{n+1}$. In particular, it follows from $x_r = x_s$ that $x_{r-1} = x_{s-1}$, etcetera, hence $x_0 = x_{s-r}$. So the continued fraction of $x_0 = \alpha$ is purely periodic.
Now, suppose that α has a periodic continued fraction. Then there exists β with a purely periodic expansion such that $\alpha = [a_0, a_1, ..., a_{n_0}, \beta]$ with β a quadratic irrational so is α. Conversely, if α is a quadratic irrational then there is β reduced quadratic irrational such that $\alpha = [a_0, a_1, ..., a_{n_0}, \beta]$ and then β is purely periodic, it follow easily that α is periodic. □

For quadratic irrational numbers of the form $\sqrt{N}$, $N \in \mathbb{N}$ not a square, we obtain the following theorem.

Theorem 10.2.6. *Let $N \in \mathbb{N}$ and suppose N is not a square. Then $\sqrt{N} = [a_0, \overline{a_1, ..., a_r, 2a_0}]$ where $a_0 = [\sqrt{N}]$. Moreover, $(a_1, a_2, ..., a_r) = (a_r, ..., a_2, a_1)$.*

Proof. First observe that $a_0 = [\sqrt{N}]$ is the result of the first step in the continued fraction algorithm. Now note that $\sqrt{N} + a_0$ is reduced quadratic irrational, since $\sqrt{N} + a_0 > 1$ and $-1 < -\sqrt{N} + a_0 < 0$. Hence it has purely periodic continued fraction of the form

$$\sqrt{N} + a_0 = [\overline{2a_0, a_1, a_2, ..., a_r}] = [2a_0, \overline{a_1, ..., a_r, 2a_0}]$$

as asserted. Notice also that $\sqrt{N} + a_0 = [2a_0, a_1, a_2, ..., a_r, \sqrt{N} + a_0]$. Substract $2a_0$, on both sides to find $\sqrt{N} - a_0 = [0, a_0, ...a_r, \sqrt{N} + a_0]$. Hence,

$$\frac{1}{\sqrt{N} - a_0} = [a_1, a_2, ..., a_r, \sqrt{N} + a_0]$$

Application of the last lemma of last section yield

$$-\frac{1}{\sqrt{N} + a_0} = [a_r, ..., a_2, a_1, a_0 - \sqrt{N}]$$

This algebraic identity remains true if we replace $\sqrt{N}$ by $-\sqrt{N}$ (conjugate),

$$-\frac{1}{-\sqrt{N} + a_0} = [a_0, ..., a_2, a_1, a_0 + \sqrt{N}]$$

. Invert both sider and add $2a_0$ to obtain

$$\sqrt{N} + a_0 = [2a_0, a_r, ..., a_2, a_1, \sqrt{N} + a_0]$$

So, we see that the continued fraction of $\sqrt{N} + a_0$ is also given by $[\overline{2a_0, a_r, ..., a_2, a_1}]$. □

10.3 Pell's equation

Suppose $N \in \mathbb{N}$ is not a square and consider the diophantine equation

$$x^2 - Ny^2 = 1$$

in the unknowns $x, y \in \mathbb{N}$. Although problems related to this equation have been around since antiquity, the first general method for solving it was given by W. Brouncker in 1657. He was able to use his method to obtain the smallest solution

$$(x, y) = (32188120829134849, 1819380158564160)$$

to $x^2 - 313y^2 = 1$!. Very soon Pell's name stuck to this equation. For several values of N we list the solution with minimal x,

$$\begin{aligned} 3^2 - 2 \times 2^2 &= 1 \\ 649^2 - 13 \times 180^2 &= 1 \\ 1766319049^2 - 61 \times 226153980^2 &= 1 \end{aligned}$$

Looking at these equations one observes that it is quite a miracle that any non-trivial solution for $x^2 - 61y^2 = 1$. Nevertheless, using continued fractions, it is possible to show that there always exists a non-trivial solution.

Proposition 10.3.1. *Let $N \in \mathbb{N}$ and suppose N is not a square. Then there exist $x \neq 1, y \neq 0 \in \mathbb{N}$ such that $x^2 - Ny^2 = 1$.*

Proof. For $N = 2, 3, 5, 6$ our theorem is true since we have $3^2 - 2 \times 2^2 = 1$, $2^2 - 3 \times 1^2 = 1$, $9^2 - 5 \times 4^2 = 1$, $5^2 - 6 \times 2^2 = 1$. So, we can assume that $N \geqslant 7$.
Consider the continued fraction expansion of $\sqrt{N}$ given by

$$\sqrt{N} = [a_0, \overline{a_1, ..., a_r, 2a_0}]$$

say. Let $p/q = [a_0, ..., a_r]$. Then, from our elementary estimates we find that

$$|\frac{p}{q} - \sqrt{N}| < \frac{1}{2a_0q^2}$$

Multiply on both side by $|p/q + \sqrt{N}| \leqslant (2\sqrt{N} + 1)$. We find,

$$|\frac{p^2}{q^2} - N| < \frac{2\sqrt{N} + 1}{2a_0q^2}$$

Multiply on both sides by q^2 to find $|p^2 - Nq^2| < (2\sqrt{N} + 1)/2[\sqrt{N}]$. When $N \geqslant 7$ we have

$$\frac{2\sqrt{N} + 1}{2[\sqrt{-N}]} < \frac{2\sqrt{N} + 1}{2(\sqrt{N} - 1)} < 2$$

Hence, $|p^2 - Nq^2| < 2$. So, we have either $p^2 - nq^2 = -1$ or $p^2 - Nq^2 = 1$. (why can't we have $p^2 - Nq^2 = 0$?). In case $p^2 - Nq^2 = 1$ we find $x = p$, $y = q$ as solution. In case $p^2 - Nq^2 = -1$ we notice that $(p^2 + Nq^2)^2 - N(2pq)^2 = (p^2 - Nq^2)^2 = 1$. Hence we have the solution $x = p^2 + Nq^2$, $y = 2pq$. □

Now that we established the existence of non-trivial solutions to Pell's equation we would like to have the full set. An important remark to this end is the following trick which we illustrate by an example. Notice that $3^2 - 2 \times 2^2 = 1$ is equivalent to $(3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 1$. Take the square on both sides and use the fact that

$$(3 \pm 2\sqrt{2})^2 = 17 \pm 12\sqrt{2}$$

Hence $(17 + 12\sqrt{2})(17 - 12\sqrt{2})$ which implies $17^2 - 2 \times 12^2 = 1$. We can also take the cube of $(3 + 2\sqrt{2})$ to obtain $99 + 70\sqrt{2}$). We then find $99^2 - 2 \times 70^2 = 1$. So, given one solution of Pell's equation we can construct infinitely many! If we start with the smallest positive solution we get all solutions in this way, as shown in the following theorem.

Theorem 10.3.2. *Choose the solution of Pell's equation with $x + y\sqrt{N} > 1$ and minimal. Call it (p, q). Then, to any solution $x, y \in \mathbb{N}$ of Pell's equation there exists $n \in \mathbb{N}$ such that $x + y\sqrt{N} = (p + q\sqrt{N})^n$.*

Proof. Notice that if $u, v \in \mathbb{Z}$ satisfy $u^2 - Nv^2 = 1$ and $u + v\sqrt{N} \geqslant 1$, then $u - v\sqrt{N}$, being equal to $(u+v\sqrt{N})^{-1}$ lies between 0 and 1. Addition of the inequalities $u+v\sqrt{N} \geqslant 1$ and $0 <\leqslant u-v\sqrt{N} \leqslant 1$ implies $u \geqslant 0$. Substraction of these inequalities yields $v > 0$. We call $u+v\sqrt{N}$ the size of the solution u, v. Now, let $x, y \in \mathbb{N}$ be any solution of Pell's equation. Notice that $(x + y\sqrt{N})(p - q\sqrt{N}) = (px - qyN) + (py - qx)\sqrt{N}$. Let $u = px-qyN$, $v = py-qx$ and we have $u^2-Nv^2 = 1$ and $u+v\sqrt{N} = (x+y\sqrt{N})/(p+q\sqrt{N})$. Observe that

$$1 \leqslant \frac{x + y\sqrt{N}}{p + q\sqrt{N}} < \frac{x + y\sqrt{N}}{2}$$

hence $1 \leqslant u+v\sqrt{N} < \frac{x+y\sqrt{N}}{2}$. So we have found a new solution with positive coordinates and size bounded by half the size of $x + y\sqrt{N}$. By repeatedly performing this operation we obtain a solution whose size is less than the size of $p + q\sqrt{N}$. By the minimality of p, q this implies that this last solution should be 1, 0. Supposing the number of steps is n we thus find that $x + y\sqrt{N} = (p + q\sqrt{N})^n$. □

In the existence proof for solution to Pell's equation we have used the continued fraction of $\sqrt{N}$. It turns out that we can use this algorithm to find the smallest solution and also all solutions of other equations of the form $x^2 - Ny^2 = k$ for small k.

Theorem 10.3.3. *Suppose we have $x, y \in \mathbb{N}$ such that $|x^2 - Ny^2| \leqslant \sqrt{N}$. Then x/y is a convergent to the continued fraction of $\sqrt{N}$.*

Proof. Let $M = [\sqrt{N}]$. Since $x^2 - Ny^2$ is integral the inequality $|x^2 - Ny^2| < \sqrt{N}$ implies $|x^2 - Ny^2| \leqslant M$. We first show that $x \geqslant My$. if $x < My$ we would have the following sequence of inequalities,

$$x^2 - Ny^2 < x^2 - M^2y^2 = (x - yM)(x + yM) < -M$$

contradicting $|x^2 - Ny^2| \leqslant M$ implies

$$|x - y\sqrt{N}| \leqslant \frac{M}{x + y\sqrt{N}} < \frac{M}{x + yM} \leqslant \frac{M}{2yM} = \frac{1}{2y}$$

Divide by y on both sides and use a Legendre theorem to conclude that x/y is a convergent. □

Chapter 11

Gaussian integers

11.1 Basic properties

Definition 11.1.1. *1. Let $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$, where $i^2 = -1$, $\mathbb{Z}[i]$ is a ring called the **ring of Gaussian integers**.*

*2. We can define a map called the **norm**:*

$$\begin{array}{rccc} N: & \mathbb{Z}[i] & \to & \mathbb{Z} \\ & a + bi & \mapsto & (a + bi)(a - bi) = a^2 + b^2 \end{array}$$

This permits to pass from $\mathbb{Z}[i]$ to $\mathbb{Z}$. The norm is multiplicative (Exercise!).

We can define the notion of divisibility as we were able to define in $\mathbb{Z}$

Definition 11.1.2. *Let $\alpha, \beta \in \mathbb{Z}[i]$. We say α **divides** β or $\beta|\alpha$, if $\alpha = \beta\gamma$ for some $\gamma \in \mathbb{Z}[i]$. We call **units of** $\mathbb{Z}[i]$ the invertible elements of $\mathbb{Z}[i]$ (that is the $\alpha \in \mathbb{Z}[i]$ such that there is $\gamma \in \mathbb{Z}[i]$, $\alpha\gamma = 1$). They are precisely the elements of norm 1, that is ± 1, $\pm i$. A **Gaussian prime element** is an element $\alpha \in \mathbb{Z}[i]$ which is not a unit such that if $\alpha = \beta \times \gamma$ where β and $\gamma \in \mathbb{Z}[i]$ then β or γ is a unit. In other word, its only divisor are up to units α and 1. Suppose that $\delta|\alpha$ and $\delta|\beta$. We say δ is a **common divisor of α and β**. We say that δ is a **greatest common divisor (gcd) of α and β** if it is a common divisor of α and β with maximum possible norm.*

Example 11.1.3. *2 is not a Gaussian prime, since $2 = (1 + i)(1 - i)$.*

We can relate divisibility in $\mathbb{Z}[i]$ with divisibility in $\mathbb{Z}$ via the norm map.

Lemma 11.1.4. *If $\beta|\alpha$ in $\mathbb{Z}[i]$ then $N(\beta)|N(\alpha)$ in $\mathbb{Z}$.*

Here, a easy characterization of Gaussian prime:

Lemma 11.1.5. *Let $\alpha \in \mathbb{Z}[i]$, α is a Gaussian prime if and only if $\beta|\alpha$ implies $N(\beta) = 1$ or $N(\beta) = N(\alpha)$.*

Corollary 11.1.6. *Let $\alpha \in \mathbb{Z}[i]$, α. If $N(\alpha)$ is prime then α is a Gaussian prime.*

As for integers we have the existence of the prime factorization and the proof is similar to the one for the integers.

Proposition 11.1.7. *Let $\alpha \in \mathbb{Z}[i]$ be a non-zero, non-unit. Then α factors into a finite product of Gaussian primes.*

Proposition 11.1.8. *Let $p \in \mathbb{N}$ be prime. Then p is also prime in $\mathbb{Z}[i]$ if and only if p is not the sum of two squares.*

Corollary 11.1.9. *Suppose $p \in \mathbb{N}$ is prime and $p = a^2 + b^2$. Then $\alpha = a + ib$ and $\bar{\alpha} = a - ib$ are prime in $\mathbb{Z}[i]$.*

Proof. We have just seen that $N(\alpha) = N(\bar{\alpha}) = p$ i.e. their norm is prime. Then α and $\bar{\alpha}$ are Gaussian primes. □

The proof of the following three following result is left as exercises.

Proposition 11.1.10. *If α, $\beta \in \mathbb{Z}[i]$ are non-zero, then there is a quotient $\mu \in \mathbb{Z}[i]$ and remainder $\rho \in \mathbb{Z}[i]$ such that $\alpha = \mu\beta + \rho$ where $N(\rho) < N(\beta)$.*

Proof. We have α, $\beta \in \mathbb{Z}[i]$ with $\beta \neq 0$ we want to construct γ, $\rho \in \mathbb{Z}[i]$ such that $\alpha = \beta\gamma + \rho$ where $N(\rho) \leqslant (1/2)N(\beta)$. Write

$$\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{\beta\bar{\beta}} = \frac{\alpha\bar{\beta}}{N(\beta)} = \frac{m + ni}{N(\beta)}$$

where we set $\alpha\bar{\beta} = m + ni$. Divide m and n by $N(\beta)$ using a modified division theorem in $\mathbb{Z}$,

$$m = N(\beta)q_1 + r_1, \; n = N(\beta)q_2 + r_2$$

where q_1 and q_2 are in $\mathbb{Z}$ and $0 \leqslant |r_1|, |r_2| \leqslant (1/2)N(\beta)$. Then,

$$\frac{\alpha}{\beta} = \frac{N(\beta)q_1 + r_1 + (N(\beta)q_2 + r_2)i}{N(\beta)} = q_1 + q_2 i + \frac{r_1 + r_2 i}{N(\beta)}$$

Set $\gamma = q_1 + q_2 i$ (this will be the desired quotient) , so after a little algebra the above equation becomes

$$\alpha - \beta\gamma = \frac{r_1 + r_2 i}{\bar{\beta}}$$

We will show $N(\alpha - \beta\gamma) \leqslant (1/2)N(\beta)$, so using $\rho = \alpha - \beta\gamma$ will settle the division theorem. Take norms of both sides of the previous equation and use that $N(\beta) = N(\bar{\beta})$, to get

$$N(\alpha - \beta\gamma) = \frac{r_1^2 + r_2^2}{N(\beta)}$$

Feeding the estimates $0 \leqslant |r_1|, |r_2| \leqslant (1/2)N(\beta)$ into the right side,

$$N(\alpha - \beta\gamma) \leqslant \frac{(1/4)N(\beta)^2 + (1/4)N(\beta)^2}{N(\beta)} = \frac{1}{2}N(\beta)$$

□

Lemma 11.1.11. *Suppose $\alpha = \mu\beta + \rho$ where $N(\rho) < N(\beta)$. Then $\rho = 0$ iff $\beta|\alpha$.*

Lemma 11.1.12. *Suppose $\alpha = \mu\beta + \rho$ wher $N(\rho) < N(\beta)$. If $\rho = 0$, β is a gcd for α and β. If not, a gcd for α and ρ is also a gcd for α and β (and vice versa).*

We get as for the integer the **Euclidean algorithm for $\mathbb{Z}[i]$**

1. Suppose $N(\alpha) \geqslant N(\beta)$. Let $gcd(\alpha_1, \beta_1) = gcd(\alpha, \beta)$. Set $i = 1$.
2. Write $\alpha_i = \mu_i\beta_i + \rho_i$ where $N(\rho_i) < N(\beta_i)$. If ρ_i is a gcd for α and β. If not, continue.
3. Let $\alpha_{i+1} = \beta_i$, $\beta_{i+1} = \rho_i$. Note that $N(\alpha_{i+1}) > N(\beta_{i+1})$ from step 2. Increase i by 1 and repeat Step 2 (i.e., repeat Step 2 for α_{i+1} and β_{i+1}).

We can run the Euclidean algorithm in reverse to get that some gcd of α and β must of the form $\mu\alpha + \nu\beta$ for some $\mu, \nu \in \mathbb{Z}[i]$.

Proposition 11.1.13. *Let π be a prime in $\mathbb{Z}[i]$. If $\pi|\alpha\beta$ then $\pi|\alpha$ or $\pi|\beta$.*

Theorem 11.1.14. *(Unique factorisation) Let $\alpha \neq 0$ be a non-unit in $\mathbb{Z}[i]$. Suppose $\alpha = \pi_1 ... \pi_m$ and $\alpha = \pi'_1 ... \pi'_n$ are two factorizations of α into Gaussian prime π_i and π'_j. Then $m = n$, and up to a reordering of π'_j 's, we have*

$$\pi_i = u_i \pi'_i$$

for each i, where u_i is a unit in $\mathbb{Z}[i]$.

Proposition 11.1.15. *The Gaussian primes, up to units, are precisely the following:*

1. *prime $p \in \mathbb{N}$ not of the form $x^2 + y^2$,*
2. *$\alpha = a + bi$ where $N(\alpha)$ is prime in $\mathbb{N}$.*

11.2 Fermat's two square theorem

Theorem 11.2.1. *Let p be a prime. Then p is a sum of two square if and only if $p \equiv 1 \ mod \ 4$ or $p = 2$.*

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

Corollary 11.2.2. *Let p be a prime which is not 3 mod 4. Then $p = x^2 + y^2$ has exactly 1 solution for $x, y \in \mathbb{N}$ with $x \geqslant y$.*

Proof. There is a solution $x^2 + y^2 = p$ by the theorem. We know that $p = (x + yi)(x - iy)$ is a factorization into primes in $\mathbb{Z}[i]$. (Exercise!) If we also have $p = x'^2 + y'^2$ then $p = (x' + iy')(x' - y'i)$ is also a prime factorization in $\mathbb{Z}[i]$. But since prime factorization

is unique, we have $x' + y'i = u(x + yi)$ or $u(x - yi)$ for some unit u.
Suppose the former. If $u = \pm 1$ then $x' = \pm x$ and $y' = \pm y$. If $u = \pm i$ then $u = \pm i$ then $x' = \pm y$ and $y' = \pm x$. Hence x' and y' are up to sign, x and y in some order. The case $x' + y'i = u(x - yi)$ is similar. So there is only solution to $p = x^2 + y^2$ with $x, y > 0$, up to interchanging x and y. □

Corollary 11.2.3. *The prime of $\mathbb{Z}[i]$ are precisely units times*

1. *p where $p = 4n + 3$ is a prime in $\mathbb{N}$,*
2. *$\alpha = a + bi$ where $N(\alpha)$ is either 2 or prime of $\mathbb{N}$ congruent to 1 mod 4.*

Theorem 11.2.4. *A natural number n is a sum of two squares if and only if any prime $p|n$ such that $p \equiv 3$ mod 4 occurs to an even power in the prime factorization of n.*

Proof. Clearly $n = x^2 + y^2$ if and only if $n = N(\alpha)$ where $\alpha = x + yi$, i.e. n is a sum of two squares if and only if it is the norm of some element of $\mathbb{Z}[i]$.
Let

$$n = \prod p_i^{e_i} \prod q_j^{f_j}$$

be the prime factorization of n in $\mathbb{N}$ where each $p_i \equiv 3$ mod 4 and $q_j \not\equiv 3$ mod 4. Each $q_j = \pi_j \bar{\pi}_j$ where π_j is some Gaussian prime. Thus

$$n = \prod p_i^{e_i} \prod \pi_j^{f_j} \bar{\pi}_j{}^{f_j}$$

is the prime factorization of n in $\mathbb{Z}[i]$, where each p_i is of type (1.) and each π_j, $\bar{\pi}_j$ is of type (2.), in the notation of the above corollary.
($\Rightarrow$) Suppose $n = x^2 + y^2$, i.e. $n = N(\alpha)$ for some $\alpha \in \mathbb{Z}[i]$. Let

$$\alpha = \prod r_i^{h_i} \prod \phi_j^{k_j}$$

be the prime factorization of α in $\mathbb{Z}[i]$, again where each r_i is of type (1.) and ϕ_j is of type (2.). Then,

$$\bar{\alpha} = \prod \bar{r}_i^{h_i} \prod \bar{\phi}_j^{k_j} = \prod r_i^{h_i} \prod \bar{\phi}_j^{k_j}$$

is the prime factorization of $\bar{\alpha}$ since each $r_i \in \mathbb{N}$. But then,

$$\alpha\bar{\alpha} = \prod r_i{}^{2h_i} \prod \phi_j{}^{k_j} \bar{\phi}_j^{k_j} = n = \prod p_i^{e_i} \prod \pi_j^{f_j} \bar{\pi}_j{}^{f_j}$$

Hence up to reordering the primes (assuming all were distinct), we have $e_i = 2h_i$ is eaten, which is what we wanted to prove.
$\Leftarrow$ Suppose now that $e_i = 2k_i$ where k_i is an integer. Each $p_i^{2k_i}$ and $q_j^{f_j}$ are norm of an element in $\mathbb{Z}[i]$. Then $n = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. □

We admit the following theorem:

Theorem 11.2.5. *Let $r_2(n)$ denote the number of solutions to $x^2 + y^2 = n$. Write $n = 2^f n_1 n_2$ where n_1 is a product of primes $\equiv 1$ mod 4 and n_2 is a product of primes $\equiv 3$ mod 4. Then $r_2(n) = 0$ if n_2 is not a perfect square, and $r_2(n)$ is 4 times the number of divisors of n_1 otherwise.*

11.3 Pythagorean triples

Definition 11.3.1. *Let $\alpha, \beta \in \mathbb{Z}[i]$. If the only common divisors of α and β are units, we say α and β are* ***relatively prime****.*

One of the ancient diophantine equations is the following.

Definition 11.3.2. *A triplet $a, b, c \in \mathbb{N}$ is called* ***Pythagorean triple*** *if*

$$a^2 + b^2 = c^2$$

Moreover, if a, b are coprime (thus a, b and c are coprime) then we say that it is a ***primitive Pythagorean triple****.*

Since if (x, y, z) is a Pythagorean triple, then $(\lambda x, \lambda y, \lambda z)$ is also a Pythagorean triple. It is also clear that all Pythagorean triples are multiples of the primitive ones. Hence to determine all Pythagorean triples it suffices to determine the primitive ones, which we now see how to do using $\mathbb{Z}[i]$.

Remark 11.3.3. *Notice that in a Pythagorean triplet a and b cannot be both odd. For then we would have $a^2+b^2 \equiv 1+1 \equiv 2 \ mod\ 4$ but c^2, being a square, cannot be $\equiv 2 \ mod\ 4$.*

Lemma 11.3.4. *Suppose (x, y, z) is a primitive Pythagorean triple. Then $x + yi$ and $x - yi$ are relatively prime in $\mathbb{Z}[i]$ i.e. they have no common prime divisors in $\mathbb{Z}[i]$.*

Proof. Suppose instead $x+iy$ and $x-iy$ have a common prime divisor $\pi \in \mathbb{Z}[i]$. Then π divides their sum $2x$ and their difference $2yi$. Since x and y have no common fractures in $\mathbb{Z}$, they have no common prime factors in $\mathbb{Z}[i]$. Thus must be a prime dividing 2, i.e., $\pi = \pm 1 + \pm i$. Then

$$N(\pi) = \pi\bar{\pi} = 2 | (x + yi)(x - yi) = x^2 + y^2 = z^2$$

This means z is even, so $x^2 + y^2 \equiv 0 \ mod\ 4$ which implies x and y are both even, a contradiction. □

Lemma 11.3.5. *Suppose $\alpha, \beta \in \mathbb{Z}[i]$ are relatively prime. If $\alpha\beta = \gamma^2$ is a square in $\mathbb{Z}[i]$, then $u\alpha$ and $u^{-1}\beta$ are squares for some unit u of $\mathbb{Z}[i]$.*

Proof. Note that this is trivial if γ is a unit (and vacuous if $\gamma = 0$). So assume $\alpha\beta$ is the square of some $\gamma \in \mathbb{Z}[i]$, where γ is a non-zero non-unit. Then γ has a prime factorization in $\mathbb{Z}[i]$:

$$\gamma = \prod \pi_i^{e_i}$$

Thus the prime factorization of

$$\alpha\beta = \prod \pi_i^{2e_i}$$

up to a reordering of primes, we have

$$\alpha = u^{-1}\pi_1^{2e_1} ... \pi_j^{2e_j}$$

$$\beta = u\pi_{i+2}^{2e_j+1} ... \pi_k^{2e_k}$$

for some unit u. □

Proposition 11.3.6. *(x, y, z) is a primitive Pythagorean triple if and only if x and y are (in some order) $u^2 - v^2$ and $2uv$ for u, v relatively prime in $\mathbb{N}$ with $u > v$ and u, v not both odd. In this case, $z = u^2 + v^2$.*

Proof. ($\Leftarrow$) Suppose we have u and v with the given properties. Clearly a, b and c satisfied $a^2 + b^2 = c^2$ and $gcd(a, c)$ divides $gcd(c - a, c + a) = gcr(2u^2, 2v^2) = 2$. But since $u \not\equiv v \ mod\ 2$, a and c are odd and so $gcd(a, c) = 1$. Hence, $gcd(a, b, c) = 1$.
($\Rightarrow$) Suppose (x, y, z) is a primitive Pythagorean triple, so $x^2+y^2 = (x+iy)(x-yi) = z^2$. By the first lemma, $x + iy$ and $x - iy$ are relatively prime, and by the second they are units times squares. In particular $x + iy = \pm\alpha^2$ or $x + yi = \pm i\alpha^2$ for $\alpha \in \mathbb{Z}[i]$. Since -1 is a square in $\mathbb{Z}[i]$, we may absorb the possible minus sign into α and write either $x + yi = \alpha^2$ or $x + iy = i\alpha^2$.
Write $\alpha = u + iv$, and we get in the first case

$$x + iy = (u + vi)^2 = u^2 + v^2 + 2uvi$$

and

$$x + yi = i(u + vi)^2 = -2uv + (u^2 + v^2)i$$

In the first case, we have $x = u^2 + v^2$, $y = 2uv$. In the second, we may replace u by $-u$ or v by $-v$ to write $x = 2uv$, $y = u^2 + v^2$ and to obtain u and v in $\mathbb{N}$. Then the conditions $gcd(u, v) = 1$, $u > v$ and u, v not both odd all follow from the facts that $gcd(x, y) = 1$ and $x, y > 0$.
The last statement is obvious. □

Remark 11.3.7. *When we rewrite the equation $a^2+b^2 = c^2$ as $(a/c)^2+(b/c)^2 = 1$ we see that finding Pythagorean triplets is equivalent to finding rational numbers p, q such that $p^2 + q^2 = 1$, in other words, finding rational points on the unit circle. Geometrically, the solution to this problem runs as follows. For any point $(p, q) \in \mathbb{Q}^2$ we draw the line between (p, q) and $(1, 0)$ which is given by $Y = t(1-X)$, where $t = q/(1-p)$. Conversely, any line through $(1, 0)$ is given by $Y = t(1 - X)$. THe second point of intersection with the unit circle is given by $\frac{t^2-1}{t^2+1}$, $\frac{2t}{t^2+1}$. Thus, we can conclude: there exists a bijection between the sets*

$$\{t \in \mathbb{Q}\} \text{ and } \{x, y \in \mathbb{Q} | x^2 + y^2 = 1, (x, y) \neq (1, 0)\}$$

given by

$$t = \frac{y}{1 - x}, \quad (x, y) = \left(\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{t^2 + 1}\right)$$

Corollary 11.3.8. *Let $p \in \mathbb{N}$ be prime. Then p occurs as the hypotenuse of a right-angle triangle with integer length sides if and only if $p > 2$ is a sum of two squares, i.e. if and only if $p \equiv 1 \ mod\ 4$.*

Proof. The second equivalence is Fermat's two square theorem, so it suffices to prove the first.
($\Rightarrow$) Suppose p is such a hypotenuse. Clearly $p \neq 2$. Now $x^2 + y^2 = p^2$. This implies $gcd(x, y) = 1$. Hence by the previous proposition $p = u^2 + v^2$ for some u, v.

($\Leftarrow$) Suppose $p = u^2 + v^2$ is odd. Then $u \neq v$, $gcd(u,v) = 1$ and u and v are not both odd. Futhermore, we may assume $u > v$. By the proposition $(u^2 - v^2, 2uv, p)$ is a primitive Pythagorean triple. □

It is very simple to find all α, β, $\gamma \in \mathbb{Q}$ such that $\alpha^2 + \beta^2 = \gamma^2$. They are all of the form

$$\left(\frac{u^2 - v^2}{M}\right)^2 + \left(\frac{2uv}{M}\right)^2 = \left(\frac{u^2 + v^2}{M}\right)^2,\ u, v \in \mathbb{Z}$$

Definition 11.3.9. *A number $n \in \mathbb{N}$ is called **congruent** if n is the surface area of a right-angled triangle with rational sides. In other words*

$$n \text{ is congruent } \Leftrightarrow \text{ there are } u,\ v,\ M \in \mathbb{Z} \text{ such that } n = \frac{1}{2}\frac{2uv}{M}\frac{u^2 - v^2}{M}$$

The latter equation is equivalent to $M^2 n = uv(u^2 - v^2)$. It is a classical problem to characterize congruent numbers. The smallest congruent number is 5. A notorious congruent number is $n = 157$. As an interesting curiosity we mention two results on congruent numbers.

Theorem 11.3.10. *(Birch, 1975) When n is prime and equal 5 or 7 modulo 8 then n is congruent. When n is twice a prime of the form -1 mod 4, then n is also congruent.*

Theorem 11.3.11. *(Tunnell, 1983) Suppose n is a congruent number then the number of integral solutions to $2x^2 + y^2 + 8z^2 = n$ equals twice the number of solutions to $2x^2 + y^2 + 32z^2 = n$.*

It is generally expected that the converse of Tunnell's theorem also holds.

11.4 Primes of the form $4n + 1$

I mentioned earlier that precisely half of the primes in $\mathbb{Z}$ remain prime in $\mathbb{Z}[i]$, and half factor in $\mathbb{Z}[i]$. We saw that the primes in the first groups are the primes which are 3 mod 4 and the primes in the second group are 2 and those 1 mod 4. My claim then is that, in a sense which can be made precise, half of the (odd) primes in $\mathbb{N}$ are 1 mod 4 and half are 3 mod 4. We will prove first that there are infinitely many primes of the form $4n + 3$.

Proposition 11.4.1. *There are infinitely many primes of the form $4n + 1$.*

Proof. We have seen that an odd prime p is of the form $4n + 1$ if and only if $p | x^2 + 1$ for some $x \in \mathbb{Z}$. Hence it suffices to show that there are infinitely many primes dividing the values of the polynomial $f(x) = x^2 + 1$. Suppose instead only finitely many primes p_1, ..., p_k (including 2) divide the values of $f(x)$. Let

$$g(y) = f(p_1 ... p_k y) = (p_1 ... p_k)^2 y^2 + 1$$

The values of $g(y)$ are a subset of the values of $f(x)$ so the only primes which divide values of $g(y)$ are p_1,...,p_k. However,

$$g(y) \equiv 1 \ mod\ p_i$$

for $i = 1, 2, ..., k$. Hence, $g(1) = (p_1...p_k)^2 + 1 > 1$ is not divisible by any prime, a contradiction. □

The above result is a special case of the following.

Theorem 11.4.2. *(Dirichlet's theorem on arithmetic progressions) Suppose* $gcd(a, n) = 1$. *There are infinitely many prime* $p \equiv a \ mod \ n$.

The proof was surprisingly novel, using an analytic tool that Dirichlet invented called **L-functions**, which form a central topic in modern number theory. Now that we know there are infinitely many primes which are 1 mod 4 and 3 mod 4, you might wonder whether there's something further about my assertion that half of the (odd) primes are 1 mod 4 and half 3 mod 4. The answer is yes, Dirichlet proved something even more precise than the above theorem.

Theorem 11.4.3. *(Dirichlet) The odd primes, with the natural ordering, are equally distributed in two congruence classes* $4\mathbb{Z} + 1$ *and* $4\mathbb{Z} + 3$, *i.e.,*

$$lim_{n\to\infty} \frac{\sharp\{p < n : p \equiv 1 \ mod \ 4 \ prime\}}{\sharp\{p < n : p \equiv 3 \ mod \ 4 \ prime\}} = 1$$

Dirichlet in fact proved that mod any n, the primes (not dividing n-, are equally distributed (in the above sense) among the $\phi(n)$ congruence classes $n\mathbb{Z} + a$ where $gcd(a, n) = 1$.
Nevertheless, Chebyshev noticed an interesting phenomenon, more amazing in light of equal distribution result of Dirichlet: there appear to be more primes of the latter form. Precisely, if we actually count the primes in each class less than n, "most of the time" we have:

$$\sharp\{p < n : p \equiv 1 \ mod \ 4 \ prime\} > \sharp\{p < n : p \equiv 3 \ mod \ 4 \ prime\}$$

For example, the first time the right hand side is greater is for $n = 26861$. One might wonder if Chebyshev's observation just happens to be true for small values of n. In fact for infinitely many n the left hand side is greater, and infinitely many n the right hand side is greater. Nevertheless, Chebyshev was right. In 1994, Rubinstein and Sarnak showed in an appropriate way of quantifying things, the above inequality holds about $99,50\%$ of the time. Very roughly, one reason why there are more primes in $4\mathbb{Z} + 3$ is because $4\mathbb{Z} + 1$ must contain all the odd squares, leaving less room for primes.

Chapter 12

Other diophantine equation

Let $F(x_1, ..., x_r) \in \mathbb{Z}[x_1, ..., x_r]$. An equation of the form

$$F(x_1, ..., x_r) = 0$$

in the unknowns x_1, ..., $x_r \in \mathbb{Z}$ or $\mathbb{Q}$ is called **diophantine equation**

12.1 Fermat's equation

After reading about pythagorean triples it seems natural to ask the following question. Let $n \in \mathbb{N}$ and $n > 2$. Does the equation

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

have any solutions in $x, y, z \in \mathbb{N}$? Fermat believed the answer to be 'no' and claims to have a 'remarkable proof'. unfortunately the margin of the book in which he made this claim was too narrow to write this proof down'. In June 1993 the English mathematician Andrew Wiles came quite close and for some time it was believed that he did have a proof. However, his 200 page manuscript of highly advanced mathematics turned out to have a gap and it took about a year of suspense before this gap was repaired with the help of R. Taylor, a former student of wiles. This happened in October 1994. Wiles's work not only resolves Fermat's last problem, it is also a major advance in the theory of elliptic curves, in particular the Shimura-Taniyama-Weil conjecture.
Before Wiles's discovery the equation had been solver for certain special values of n. For example, Fermat did prove the following theorem.

Theorem 12.1.1. *The equation $x^4 + y^4 = z^2$ has no non-trivial solution $x, y, z \in \mathbb{N}$.*

As a consequence we see that the equation $x^n + y^n = z^n$ has no solutions, with $n = 4$.

Proof. Suppose there exists a solution. Let x_0, y_0, z_0 be a solution with minimal z_0. We may assume that $gcd(x_0, y_0) = 1$ and that y_0 is even. We shall repeatedly use the characterization of the Pythagorean triple. From $x_0^4 + y_0^4 = z_0^2$ follows, there are r, $s \in \mathbb{Z}$:

$$gcd(r, s) = 1,\ x_0^2 = r^2 - s^2,\ y_0^2 = 2rs,\ z_0 = r^2 + s^2$$

From $x_0^2 + s^2 = r^2$, x_0 odd and $gcd(r,s) = 1$ follows, there are ρ, $\sigma \in \mathbb{Z}$:

$$gcd(\rho,\sigma) = 1,\ x_0 = \rho^2 - \sigma^2,\ s = 2\rho\sigma,\ r = \rho^2 + \sigma^2$$

Together with $y_0^2 = 2rs$ this yields $(y_0/2)^2 = \rho\sigma(\rho^2 + \sigma^2)$. Since the factor ρ, σ, $\rho^2 + \sigma^2$ are pairwise relatively prime and their product is a square, we get that there exist u, v, $w \in \mathbb{Z}$,

$$\rho = u^2,\ \sigma = v^2,\ \rho^2 + \sigma^2 = w^2$$

After elimination of ρ, σ we get $w^2 = u^4 + v^4$. A simple check shows $|w| = \sqrt{\rho^2 + \sigma^2} = \sqrt{r} < y_0 < z_0$, contradicting the minimality of z_0. Hence there can be no non-trivial solutions. □

The principle to construct a smaller solution out of a given (hypothetical) solution is known as Fermat's descending induction or descent. This principle, in disguised form with cohomology groups and all, is still often used for many diophantine equations. The case $n = 3$ was settled by Euler (1753), Dirichlet dealt with the case $n = 5$ in 1839. Notice that the case $n = 6$ follows from $n = 3$ because $x^6 + y^6 = z^6$ can be rewritten as $(x^2)^3 + (y^2)^3$. In general, since any number larger than 2 is divisible either by 4 or by an odd prime, it suffices to prove Fermat's conjecture for $n = 4$, which we have already done, and for n prime. The methods of solution all follow the same pattern. Let p be an odd prime and put $\zeta = e^{2\pi i/p}$. Then $x^p + y^p = z^p$ can be rewritten as

$$(x + y)(x + \zeta y)...(x + \zeta^{p-1} y) = z^p$$

The left hand side of the equation has been factored into linear factors at the price of introducing number from $\mathbb{Z}[\zeta]$. The right hand side of the equation is p-th power and the principle of the proof is now to show that the linear factor on the left are essentially p-th powers in $\mathbb{Z}[\zeta]$. To reach such a conclusion we would need the property that the factorization into irreducible elements is unique in $\mathbb{Z}[\zeta]$. Assuming this one would be able to conclude a proof of Fermat's conjecture, although it is still not easy. Unfortunately there is one more complicating factor, prime factorization in $\mathbb{Z}[\zeta]$ need not to be unique. Finding a way around this problem has been one of the major stimuli to the development of algebraic number theory. In 1847, E.Kummer proved the following remarkable theorem.

Theorem 12.1.2. *(Kummer) Denote by B_0, B_1, B_2, ... the sequence of Bernouilli numbers. If the odd prime number p does not divide the numerators of B_2, B_4, B_6, ... , B_{p-3} then $x^p + y^p = z^p$ has no solution in positive integers.*

Recall that the Bernouilli numbers B_0, B_1, B_2, ... are given by the Taylor series

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$$

It is not hard to see that $B_n = 0$ when n is odd and larger than 1. A small list of values,

$$\begin{aligned} B_2 &= 1/6 \\ B_4 &= -1/30 \\ B_6 &= 1/42 \\ B_8 &= -1/30 \\ B_{10} &= 5/66 \\ B_{12} &= -691/2730 \\ B_{14} &= 7/6 \\ B_{16} &= -3617/510 \\ B_{18} &= 43867/798 \\ B_{20} &= -174611/330 \end{aligned}$$

As an amusing aside we mention that the numerator of B_k with $k \leqslant p-3$, k even is divisible by p if and only if $1^k + 2^k + ... + (p-1)^k$ is divisible by p^2. Using the computer and further refinements of Kummer's theorem one had been able to verify Fermat's conjecture for $2 < n < 4 \times 10^6$, (Buhler, Crandall, Sompolski) around 1990. For some details about the history and proof of Kummer's theory we refer to the books of P.Ribenboim (13 lectures on Fermat's last theorem, Springler Verlag 1977). Of course, these books were pre-Wiles. For an introduction for a general audience to the technical to the techniques entering Wiles's proof I highly recommend Simon Singh's book Fermat's Enigma: The epic quest to solve the world's greatest mathematical problem (1998). It reads like a novel.
As a generalization of Fermat's conjecture Euler conjectured that for any $k \in \mathbb{N}$ there are no positive integers x_1, x_2, ... , x_k. such that $x_1^k + ... + x_{k-1}^k = x_k^k$. However, this was disproved by a counterexample of Lander and Parkin (1967) reading $144^5 = 27^5 + 84^5 + 110^5 + 133^5$. Only in 2004 a second example was discovered by J.Frye:

$$55^5 + 3183^5 + 28969^5 + 85282^5 = 85359^5$$

In 1998, N.Elkies found spectacular counter examples in the case $k = 4$, the smallest of which reads $95800^4 + 217519^4 = 422481^4$. He also showed that there exist infinitely many of such examples with $k = 4$.

12.2 Mordell's equation

Let $k \in \mathbb{Z}$ The equation

$$y^2 = x^3 - k$$

in $x, y \in \mathbb{Z}$ is known as Mordell's equation. This equation has been the subject of many investigation by many people. In fact, a whole book has been written about is (London, Finkelnstein: Mordell's equation $x^3 - y^2 = k$). The main theorem is.

Theorem 12.2.1. *(Mordell) The equation has finitely many solution.*

The proof uses algebraic number theory and is beyond the scope of these notes. Although Mordell's theorem is a finiteness theorem, one cannot deduce an algorithm

from it to actually determine the solutions of any given equation. Bounds, which in principle give an effective solution became available around 1968 by A. Baker who showed that $log|x| \leqslant c|k|^{10^4}$ and lightly improved by H. Stark $log|x| \leqslant C_\epsilon |k|^{1+\epsilon}$ for every $\epsilon > 0$. the constants c, c_ϵ can be computed explicitly. It turns out the solution set depends in a very erratic way on the value of k. For example a short computer search reveals the solutions:

$$\begin{aligned} 3^2 &= (-2)^2 + 17 \\ 4^2 &= (-1)^3 + 17 \\ 5^2 &= 2^3 + 17 \\ 9^2 &= 4^3 + 17 \\ 23^2 &= 8^3 + 17 \\ 282^2 &= 43^2 + 17 \\ 375^2 &= 52^3 + 17 \\ 378661^2 &= 5234^3 + 17 \end{aligned}$$

It is highly non-trivial task to show that this is the complete solution set of $y^2 = x^3 + 17$. Two examples which are easier to deal with are given in the following theorem.

Theorem 12.2.2. *The equation $y^2 = x^3 + 7$ has no solutions in x, $y \in \mathbb{Z}$. The only integral solutions to the equation $y^2 = x^3 - 2$ are $(x, y) = (3, \pm 5)$*

Proof. First we deal with $y^2 = x^3 + 7$. Note that x is odd because x even would implies that $y^2 \equiv 7 \ mod\ 8$, which is impossible. Now notice that

$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4)$$

Notice also that for any x, $x^2 - 2x + 4 = (x - 1)^2 + 3 \equiv 3 \ mod\ 4$. Hence $x^2 - 2x + 4$ always contains a prime divisor p which is 3 mod 4. So we get $y^2 + 1 \equiv 0 \ mod\ p$ which is impossible because of $p \equiv 3 \ mod\ 4$.
To deal with $y^2 = x^3 - 2$ we use arithmetic in the euclidean ring $R = \mathbb{Z}[\sqrt{-2}]$. Notice first of all that x is odd. If x were even, then $x^3 - 2$ cannot be a square. From $y^2 + 2 = x^3$ follows the factorization

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$$

The gcd of $y + \sqrt{-2}$ and $y - 2\sqrt{-2}$ divides their difference which is $2\sqrt{-2}$. So gcd is either 1 or divisible by $\sqrt{-2}$. Since y is odd the first possibility holds. Thus we find that there exist $a, b \in \mathbb{Z}$ such that $y + \sqrt{-2} = (a + b\sqrt{-2})^3$. Computing the cube, $y + \sqrt{-2} = a^3 - 6ab^2 + b(3a^2 - 2b^2)\sqrt{-2}$. Comparison of the coefficients of $\sqrt{-2}$ on both sides yields $1 = b(3a^2 - 2b^2)$. Hence $x = a^2 + 2b^2 = 3$. The values of y follow. □

An interesting difference between the equation $y^2 = x^3 + 7$ and $y^2 = x^3 - 2$ is that the second equation has infinitely many rational solutions. This can be seen by so-called chord and tangent method. In the point $(3, 5)$ of the algebraic curve $y^2 = x^3 - 2$ we draw the tangent to the curve. It is given by $y - 2 = (27/10)(x - 3)$. Now intersect this line with the curve $y^2 = x^3 - 2$. Elimination of y yields

$$x^3 - \frac{729}{100}x^2 + \frac{837}{50}x - \frac{1161}{100} = 0$$

Because of our tangent construction we already know that this equation has a double root in $x = 3$. So the third root must also be a rational number. And indeed we find

$$(x-3)^2(x-\frac{129}{100}) = 0$$

So the x coordinate of the third intersection point of the tangent with the curve equals $129/100$. The corresponding y coordinate is $383/1000$. Indeed we check that

$$(x, y) = (129/100, 383/1000)$$

is a rational solution of $y^2 = x^3 - 2$. Repetition of this procedure provides us with an infinite set of rational solutions. In fact, it turns out that the rational points on $y^2 = x^3 - 2$ together with the point 'at infinity' have a group structure known as the Modell-Weil group. This is the beginning of a fascinating subject of a rational points on elliptic curves. Excellent introduction can be found in Silverman and Tate. Rational points on elliptic curves.
By checking result for a large number of k M. Hall made the followingg conjecture.

Conjecture 12.2.3. *(Hall) There exists a constant $C > 0$ such that $|x^3 - y^2| > Cx^{1/2}$ for any x, $y \in \mathbb{N}$ with $x^3 - y^2 \neq 0$.*

It is also known that there exist infinitely many positive integers x, y such that

$$0 < |x^3 - y^2| < \sqrt{x}^{1/2}$$

(Danilov, 1982) so in this sense Hall's conjecture is sharpest possible.

12.3 The 'abc'-conjecture

In 1996, Masser and Oesterlè formulated a striking conjecture, the truth of which has far reachingg consequences for diophantine equations. For any $a \in \mathbb{Z}$ we let $N(a)$ (the **conductor or radical of** a) denote the product of all distinct primes of a.

Conjecture 12.3.1. *('abc' conjecture) Let $\epsilon > 0$. Then there exists $c(\epsilon) > 0$ such that for any triple of non-zero numbers a, b, $c \in \mathbb{Z}$ satisfying $a+b+c = 0$ and $gcd(a, b, c) = 1$, we have*

$$max(|a|, |b|, |c|) < c(\epsilon)N(abc)^{1+\epsilon}$$

To get a feeling for what this conjecture says it is best to consider a number of consequences.

ConsÈquences 12.3.2. *Let p, q, r be fixed number s larger than 1 and $(p, q, r) = 1$. Then,*

$$p^x + q^y = r^z$$

has only finitely many solutions $x, y, z \in \mathbb{N}$.

Proof. (ADMITTING THE CONJECTURE) Application of the conjecture shows that

$$r^z < c(\epsilon)N(p^x q^y r^z)^{1+\epsilon} \leqslant c(\epsilon)N(pqr)^{1+\epsilon}$$

Hence r^z is a bounded number and so p^x, q^y. In particular x, y, z are bounded. By other methods it is indeed possible to show that $p^x + q^y = r^z$ has infinitely many solutions. □

ConsÈquences 12.3.3. *Fermat's conjecture is true for sufficiently large n.*

Proof. Apply the 'abc' conjecture to $x^n + y^n = z^n$ with x, y, $z \in \mathbb{N}$ to obtain

$$z^n < c(\epsilon)N(x^n y^n z^n)^{1+\epsilon} \leqslant c(\epsilon)N(xyz)^{1+\epsilon} \leqslant c(\epsilon)^{3(1+\epsilon)}$$

Hence, assuming $z \geqslant 2$,

$$2^{n-3(1+\epsilon)} \leqslant z^{n-3(1+\epsilon)} \leqslant c(\epsilon)$$

and this implies $n \leqslant log(c(\epsilon))/log2 + 3(1+\epsilon)$. □

ConsÈquences 12.3.4. *Let p, q, $r \in \mathbb{N}$. Suppose*

$$x^p + y^q = z^r$$

has infinitely many solution $x, y, z \in \mathbb{N}$ with $gcd(x, y, z) = 1$. Then

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} \geqslant 1$$

Application of the 'abc' conjecture yields

$$z^r \leqslant c(\epsilon)N(x^p y^q z^r)^{1+\epsilon} \leqslant c(\epsilon)(xyz)^{1+\epsilon} \leqslant c(\epsilon)(z^{r/p} z^{r/q} z)^{1+\epsilon}$$

Taking $z \to \infty$ this implies $r \leqslant (1+r/p+r/q)(1+\epsilon)$ for any $\epsilon > 0$. Hence $r \leqslant 1+r/p+r/q$ and our assertion follows.

Considering the potential consequences of the 'abc' conjecture it is likely to be very difficult to prove. In fact, any weaker version with $1 + \epsilon$ replaced by another number would already be spectacular! The best that can be done by present day methods (1994) is

$$max(|a|, |b|, |c|) < \gamma exp(N(abc)^{15})$$

where γ is some (large) constant.

12.4 Mordell's conjecture

After seeing a good many particular examples one might wonder whether anything is known about diophantine equations in general. For a long time only one result in such a direction was known.

Theorem 12.4.1. *(C. L. Siegel 1929) Let $P(X, Y) \in \mathbb{Z}[X, Y]$ be a polynomial irreducible in $\mathbb{C}[X, Y]$. Suppose that the genus of the projective curve given by $P = 0$ is at least 1. Then $P(x, y) = 0$ has at most finitely many solutions in $x, y \in \mathbb{Z}$.*

The proof is quite difficult and involves ideas from diophantine approximation and arithmetic geometry. Standard examples of curves of genus $\geqslant 2$ are the hyper-elliptic curve $y^2 = q(x)$ where $q(x)$ is a polynomial of degree at least 5 and distinct zeros and the Fermat curve $x^n + y^n = 1$ with $n > 3$.
Already in 1922 L.J. Mordell conjectured that under the conditions of Siegek's theorem $P(x, y) = 0$ has at most finitely many solutions in $x, y \in \mathbb{Q}$. This conjecture withstood attempts to solve t for a long time until in 1983 G. Faltings managed to provide a proof of it. Unfortunately, this proof can only be understood by experts in arithmetic algebraic geometry. In 1990, P. Vojta's found a brilliant new proof which, unfortunately, had the same drawback as Faltings' proof in that it was accessible only to a very small group of experts. In 1990 E. Bombieri considerably simplified Vojta's proof, thus making it understandable for a large audience of number theorists and algebraic geometers. About polynomial diophantine equations in more than two variable almost nothing is known, although there exist a good many fascinating conjectures about them.