

A FIRST COURSE IN NUMBER THEORY

ALEXANDRU BUIUM

CONTENTS

1. Introduction	2
2. The integers	4
3. Induction	6
4. Finite sets, finite sums, finite products	7
5. The rationals	8
6. Divisibility and Euclid division	10
7. Polynomial time algorithms	12
8. Primes	13
9. Greatest common divisor	14
10. Unique factorization	15
11. Applications of unique factorization	17
12. Congruences: generalities	19
13. Complete residue systems	20
14. Residue classes	21
15. Inverses mod m	22
16. Groups	23
17. Linear congruences	25
18. Systems of linear congruences	25
19. Fermat's little theorem	26
20. Euler's theorem	27
21. Polynomial congruences	28
22. Langrange's theorem	30
23. Order	31
24. Primitive roots	32
25. Discrete logarithm	33
26. Legendre symbol	35
27. Gaussian integers	37
28. Fundamental Theorem of Arithmetic for Gaussian integers	38
29. Factoring prime integers in the Gaussian integers	39
30. Real and complex numbers	40
31. Algebraic integers	40
32. Non-unique factorization in Kummer integers	42
33. Proof of Quadratic Reciprocity	42
34. Appendix: Cryptography	44

1. INTRODUCTION

This is an introduction to number theory at the undergraduate level. For most of the course the only prerequisites are the basic facts of arithmetic learned in elementary school (although these will have to be critically revisited) plus some basic facts of logic and naive set theory. In this Introduction we discuss the plan of the course and some of our prerequisites.

Plan of the course. We start by introducing the integers and the rationals. We next present Euclid's theory of divisibility and prime decomposition (3rd century BC). The results of this theory are taught (without proof!) in elementary school and are being used, of course, throughout mathematics and even in everyday life; most of the students "believe" these results and few go back to question their validity (which sometimes depends on rather subtle arguments). The most blatant example of this is the uniqueness of prime factorization of integers which is usually perceived as "obvious" but is indeed a delicate result (which fails, as we shall show, in more general contexts.) With the exception of the work of Diophantus (3rd century AD) little has been achieved in number theory in the interval between Euclid's time and the 17th century when Fermat revisited the subject. The main body of the course will consist of presenting some of the classical number theoretic results obtained in the 17th century (by Fermat), 18th century (by Euler and Lagrange), and early 19th century (by Gauss). In spite of the wide variety of these results they are all concerned essentially with the following central problem in number theory: given a polynomial $f(x)$ with integer coefficients "understand" the prime divisors of the numbers of the form $f(c)$ where c are integers. This problem is still largely open today in spite of the impressive work done on important special cases during the 19th and 20th century (by Dirichlet, Eisenstein, Kummer, Kronecker, Dedekind, Hilbert, Artin, Hasse, Weil, Tate, Shimura, Deligne, Wiles, etc.) None of the work done after Gauss will be presented here. We will include, however, a brief appendix on the applications of classical number theory to modern cryptography; this can be read right after the section on primitive roots. There is a multitude of exercises, both numerical and theoretical; the theoretical exercises are an integral part of the exposition so they should not be skipped. Some exercises have hints provided for them; some of the hints are actually complete solutions. In what follows we review logic and set theory.

Prerequisites. We assume familiarity with basic facts of logic and proofs. We only note here that statements of theorems are usually in the form "if H then C "; H is then called the hypothesis and C is the conclusion. There are two strategies to prove such a theorem: direct proof and proof by contradiction. (Later we will use another strategy that works sometimes namely induction.) In a direct proof we assume H is true and derive that C is true using the laws of logic. In a proof by contradiction we assume H is true and C is false and we seek a contradiction (i.e. we seek to show that some statement A is both true and false).

Set theory operates with symbols a, b, A, B, \dots that are supposed to mean "sets". One also has a symbol \in meaning "belongs to" or "is an element of". So $a \in A$ means " a belongs to A " (equivalently " a is an element of A "); $b \notin A$ means " b is not an element of A ". Meaning here is not important: one could let a, A mean "crocodiles" and one could let $a \in A$ mean "crocodile a in dreamt by crocodile A ".

If $a, b, c, \dots \in A$ we write $A = \{a, b, c, \dots\}$. Elements of sets are always assumed to be distinct. We write $\{x \in A; P\}$ for the set of all $x \in A$ that have property P (i.e. for which the statement P is true). There is a set (called the empty set) \emptyset such that for all x , $x \notin \emptyset$. Sets can be elements of other sets. E.g. $\{\{a, b\}, a, \{\{a\}, b, c, \emptyset\}\}$ is a set. Also $\{\emptyset\} \neq \emptyset$. A is a subset of B if $x \in A$ implies $x \in B$; we write $A \subset B$. $A = B$ if and only if $A \subset B$ and $B \subset A$. For instance $\{a, b, c\} = \{b, c, a\}$. Given two sets A and B there is a set (called their union) $A \cup B$ such that $x \in A \cup B$ if and only if $x \in A$ or $x \in B$. The intersection of two sets A and B is the set $A \cap B := \{x \in A; x \in B\}$. The difference is the set $A \setminus B := \{x \in A; x \notin B\}$. E.g. if $A = \{a, b, c\}$ and $B = \{c, d\}$ then $A \cup B = \{a, b, c, d\}$, $A \cap B = \{c\}$, $A \setminus B = \{a, b\}$. A pair (a, b) is a set of the form $\{\{a\}, \{a, b\}\}$. The product $A \times B$ is the set of pairs (a, b) with $a \in A$ and $b \in B$. E.g., if A and B are in the example above then $A \times B = \{(a, c), (a, d), (b, c), (b, d), (c, c), (c, d)\}$.

A map of sets $F: A \rightarrow B$ (or a function) is a subset $F \subset A \times B$ such that for any $a \in A$ there is a unique $b \in B$ with $(a, b) \in F$; we write $b = F(a)$ and $a \mapsto F(a)$. For instance if A and B are as in the example above then $F = \{(a, c), (b, c), (c, d)\}$ is a map and $F(a) = c$, $F(b) = c$, $F(c) = d$. Also $a \mapsto c$, $b \mapsto c$, $c \mapsto d$. On the other hand $\{(a, b), (a, c), (b, d)\}$ is not a map. There is a unique map $1_A: A \rightarrow A$, called the identity map, such that $1_A(a) = a$ for all $a \in A$. A map F is injective (or is an injection) if $F(a) = F(c)$ implies $a = c$. A map F is surjective (or is a surjection) if for any $b \in B$ there exists $a \in A$ such that $F(a) = b$. A map is bijective (or is a bijection) if it is both injective and surjective. Two sets are in bijection if there exists a bijection from one to the other. The composition $F \circ G: A \rightarrow C$ of two maps $G: A \rightarrow B$ and $F: B \rightarrow C$ is defined by $(F \circ G)(a) := F(G(a))$. The composition of two injective maps is injective and the composition of two surjective maps is surjective. If $F: A \rightarrow B$ is bijective then there exists a unique map $F^{-1}: B \rightarrow A$ (which is also bijective) called its inverse such that $F \circ F^{-1} = 1_B$ and $F^{-1} \circ F = 1_A$.

If A is a set then a relation on A is a subset $R \subset A \times A$. If $(a, b) \in R$ we write aRb . A relation R is called an order if (writing $a \leq b$ instead of aRb) we have, for all $a, b, c \in A$, that 1) $a \leq a$ (reflexivity), 2) $a \leq b$ and $b \leq c$ imply $a \leq c$ (transitivity), 3) $a \leq b$ and $b \leq a$ imply $a = b$ (antisymmetry). An order relation is called total if for any $a, b \in A$ either $a \leq b$ or $b \leq a$. For instance if $A = \{a, b, c, d\}$ and $R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (b, c), (a, c)\}$ is an order but not a total order. A relation R is called an equivalence relation if (writing $a \sim b$ instead of aRb) we have, for all $a, b, c \in A$, that 1) $a \sim a$ (reflexivity), 2) $a \sim b$ and $b \sim c$ imply $a \sim c$ (transitivity), 3) $a \sim b$ implies $b \sim a$ (symmetry); we also say that \sim is an equivalence relation. Given an equivalence relation \sim as above for any $a \in A$ we may consider the set $\hat{a} := \{c \in A; c \sim a\}$ called the equivalence class of a . Note that we have $\hat{a} = \hat{b}$ if and only if $a \sim b$; moreover if $\hat{a} \cap \hat{b} \neq \emptyset$ then $\hat{a} = \hat{b}$. The set of equivalence classes $\{\hat{a}; a \in A\}$ is denoted by A/\sim and is called the quotient of A by the relation \sim . For instance if $A = \{a, b, c\}$ and $R = \{(a, a), (b, b), (c, c), (a, b), (b, a)\}$ then R is an equivalence relation, $\hat{a} = \hat{b} = \{a, b\}$, $\hat{c} = \{c\}$, and $A/\sim = \{\{a, b\}, \{c\}\}$.

A binary operation \star on a set A is a map $\star: A \times A \rightarrow A$, $(a, b) \mapsto \star(a, b)$. We usually write $a \star b$ instead of $\star(a, b)$. Hence, for instance, we write $(a \star b) \star c$ instead of $\star(\star(a, b), c)$. Instead of \star we sometimes use notation like $+$, \times , \circ , ... A

unary operation $'$ on a set A is a map $' : A \rightarrow A$, $a \mapsto '(a)$. We usually write a' or $'a$ instead of $'(a)$. Instead of $'$ we sometimes use notation like $-$, i , \dots

What are the integers? A naive answer is: the integers are the elements of the set

$$\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}.$$

Also the natural numbers are the elements of the set

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}.$$

Integers can be added and multiplied and these operations satisfy the “usual” rules familiar from elementary school. We could proceed with such vague definitions but, instead, we will revisit these matters below and make them more precise. There are two ways to define mathematical objects: axiomatically or constructively. An axiomatic definition assumes the objects are “given” together with a list of basic properties that they satisfy (axioms). A constructive definition shows how to construct the objects from more elementary objects. In this course we will define the integers axiomatically. Later we will define rational numbers, real numbers, and complex numbers constructively from the integers.

2. THE INTEGERS

Definition 2.1. Throughout this course we fix the following data:

- a) A set \mathbb{Z} (whose elements are called integers or integer numbers)
- b) Two distinct elements $0 \neq 1$ of \mathbb{Z} ,
- c) Two binary operations $+$ and \times on \mathbb{Z} (called addition and multiplication) and one unary operation $-$ on \mathbb{Z} (called negative); we usually write $a \times b = ab$, $a - b = a + (-b)$, $-a = -(a)$,
- d) A subset $\mathbb{N} \subset \mathbb{Z}$ not containing 0 (whose elements are called natural numbers).

We assume that for all $a, b, c \in \mathbb{Z}$ the following conditions (axioms) are satisfied:

- Z1) $a + (b + c) = (a + b) + c$, $a + 0 = a$, $a + (-a) = 0$, $a + b = b + a$,
- Z2) $a(bc) = (ab)c$, $1a = a$, $ab = ba$,
- Z3) $a(b + c) = ab + ac$,
- Z4) If $a, b \in \mathbb{N}$ then $a + b \in \mathbb{N}$ and $ab \in \mathbb{N}$,
- Z5) If $a \neq 0$ then either $a \in \mathbb{N}$ or $-a \in \mathbb{N}$,

Z6) For any non-empty subset $S \subset \mathbb{N}$ there exists $m \in S$ such that for any $s \in S$ with $s \neq m$ we have $s - m \in \mathbb{N}$; we write $m = \min S$ and we call m the minimum element of S .

Remark 2.2. For $a, b \in \mathbb{Z}$ we write $a < b$ (or $b > a$) if $b - a \in \mathbb{N}$; we also write $a \leq b$ (or $b \geq a$) if either $a < b$ or $a = b$. (If $a > 0$ we say a is positive. If $a < 0$ we say a is negative. Note that \mathbb{N} coincides with the set of positive integers.) Then Z4, Z5, Z6 can be restated as follows:

- Z4) if $a, b \in \mathbb{Z}$ and $a > 0, b > 0$ then $a + b > 0$ and $ab > 0$;
- Z5) if $a \in \mathbb{Z}$ and $a \neq 0$ then $a < 0$ or $a > 0$;

Z6) for any non-empty subset $S \subset \mathbb{N}$ there exists $m \in S$ such that for any $s \in S$ we have $s \geq m$.

The statement $a + (b + c) = (a + b) + c$ in Z1 is called the associativity of addition; we write $a + b + c$ instead of $(a + b) + c$. The statement $(ab)c = a(bc)$ in Z2 is called the associativity of multiplication and again we write abc for $(ab)c$. Z3 is called distributivity. The axioms Z1-Z3 are called the ring axioms. Axiom Z5 is called the

Total Ordering Axiom. Z6 is the Well Ordering Axiom. If S in axiom Z6 is the set of all natural numbers having a property P we also refer to $\min S$ as the minimum natural number with property P . The above axiom says that if there are natural numbers with property P then there is minimum natural number with property P . Axioms Z1-Z5 are satisfied by many other “number systems”; e.g. they are satisfied if one replaces \mathbb{Z} by the rational (or real) numbers and \mathbb{N} by the positive rational (or real) numbers (to be introduced later). Axiom Z6 is, however, “specific” to the integers (and is violated in the case of the rationals and the reals).

Exercise 2.3. Prove that $0 \times a = 0$. Hint (actually a complete proof): By Axiom Z1 we have $0 + 0 = 0$. Multiplying by a to get $a \times (0 + 0) = a \times 0$. By Z3 we get $a \times 0 + a \times 0 = a \times 0$. Adding $-(a \times 0)$ to both terms we get by Axiom Z1 that $a \times 0 = 0$.

Exercise 2.4. Prove that $-(-a) = a$, and $-a = (-1) \times a$ for all $a \in \mathbb{Z}$. Prove that $(-1) \times (-1) = 1$.

Exercise 2.5. Prove that if $a, b \in \mathbb{Z}$ and $ab = 0$ then either $a = 0$ or $b = 0$.

Exercise 2.6. Prove that $1 \in \mathbb{N}$. Hint (actually a complete proof): we assume $1 \notin \mathbb{N}$ and we seek a contradiction. Since $1 \notin \mathbb{N}$ and $1 \neq 0$ it follows by Axiom Z5 that $-1 \in \mathbb{N}$. So by Axiom Z4 $(-1) \times (-1) \in \mathbb{N}$. But, by Exercise 2.3, $(-1) \times (-1) = 1$. Hence $1 \in \mathbb{N}$, a contradiction.

Exercise 2.7. Prove that if $a \leq b$ and $c \leq d$ then $a + c \leq b + d$. If in addition $e \geq 0$ then $ae \leq be$. Also if $a < b$ and $e > 0$ then $ae < be$.

Exercise 2.8. Prove that if $a, b \in \mathbb{Z}$ either $a \leq b$ or $b \leq a$. Prove that $a \leq b$ and $b \leq c$ implies $a \leq c$. Prove that $a \leq b$ and $b \leq a$ implies $a = b$. Prove that $a \leq a$. In other words \leq is a total order on \mathbb{Z} .

Definition 2.9. Define the natural numbers 2, 3, ..., 9 by

$$\begin{aligned} 2 &= 1 + 1 \\ 3 &= 2 + 1 \\ &\dots \\ 9 &= 8 + 1 \end{aligned}$$

Define $10 = 2 \times 5$. Define $10^2 = 10 \times 10$, etc. Define symbols like 423 as being $4 \times 10^2 + 2 \times 10 + 3$, etc. This is called a decimal representation. (We will later prove that any natural number has a decimal representation.)

Exercise 2.10. Prove that $12 = 9 + 3$. Hint (actually a complete proof): we have:

$$\begin{aligned} 12 &= 10 + 2 \\ &= 2 \times 5 + 2 \\ &= (1 + 1) \times 5 + 2 \\ &= 1 \times 5 + 1 \times 5 + 2 = 5 + 5 + 2 \\ &= 5 + 5 + 1 + 1 = 5 + 6 + 1 = 5 + 7 = 4 + 1 + 7 \\ &= 4 + 8 = 3 + 1 + 8 = 3 + 9 = 9 + 3 \end{aligned}$$

Exercise 2.11. Prove that $48 + 76 = 124$. Prove that $13 \times 4 = 52$.

Remark 2.12. (for the philosophically minded) In Kant’s *Critique of pure reason* statements like the ones in the previous exercise were viewed as synthetic a priori (in Kant’s sense); in contemporary mathematics, hence in the approach we follow, all these statements are, on the contrary, analytic statements (in Kant’s sense).

Exercise 2.13. Prove that $9 \leq 12$.

Notation 2.14. For any integers $a, b \in \mathbb{Z}$ the set $\{x \in \mathbb{Z}; a \leq x \leq b\}$ will be denoted, for simplicity, by $\{a, \dots, b\}$. This set is clearly empty if $a > b$. If other numbers in addition to a, b are specified then the meaning of our notation will be clear from the context; for instance $\{0, 1, \dots, n\}$ means $\{0, \dots, n\}$ whereas $\{2, 4, 6, \dots, 2n\}$ will mean $\{2x; 1 \leq x \leq n\}$, etc. A similar convention applies if there are no numbers after the dots.

Example 2.15. $\{-2, \dots, 11\} = \{-2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$.

Example 2.16. $\{3, 7, 11, 15, 19, \dots\} = \{4k + 3; k \in \mathbb{Z}, k \geq 0\}$.

Exercise 2.17. Prove that if $a \in \mathbb{Z}$ then the set $\{x \in \mathbb{Z}; a - 1 < x < a\}$ is empty. Hint (actually a complete proof): It is enough to show that $S = \{x \in \mathbb{Z}; 0 < x < 1\}$ is empty. Assume S is non-empty and let $m = \min S$. Then $0 < m^2 < m$, hence $0 < m^2 < 1$ and $m^2 < m$, a contradiction.

Exercise 2.18. Prove that if $a \in \mathbb{N}$ then $a = 1$ or $a - 1 \in \mathbb{N}$. Conclude that $\min \mathbb{N} = 1$. Hint (actually a complete proof): Proceed by contradiction so assume $a \in \mathbb{N}$, $a \neq 1$, and $a - 1 \notin \mathbb{N}$. But then $1 - a \in \mathbb{N}$ so $0 < 1 - a < 1$. This contradicts the previous exercise.

Definition 2.19. A subset $A \subset \mathbb{N}$ is bounded if there exists $b \in \mathbb{N}$ such that $a \leq b$ for all $a \in A$; we say that A is bounded by b .

Exercise 2.20. Prove that \mathbb{N} is not bounded. Prove that $\{2, 4, 6, 8, \dots\}$ is not bounded.

Exercise 2.21. Prove that if a subset $A \subset \mathbb{N}$ is bounded then there exists $M \in A$ such that for all $x \in A$, $x \leq M$. Write $M = \max A$ and call M the maximum (or greatest) element of A . Hint (not a complete proof): If A is bounded by b consider the set $\{b - x; x \in A\}$.

From now on we will not specify if hints are complete proofs or not; the reader should decide that by himself/herself.

3. INDUCTION

Sometimes the Well Ordering Axiom is used through the following Proposition called the Induction Principle.

Proposition 3.1. (*Induction Principle*) Assume $P = P(n)$ is a certain property involving a letter n that stands for a natural number. Assume

- 1) $P(1)$ is true.
- 2) For any natural number $n > 1$ if $P(n - 1)$ is true then $P(n)$ is true.

Then $P(n)$ true for all n .

We refer to the above as *induction on n* .

Proof. Assume $P(n)$ is false for some n and let n be the minimum natural number for which $P(n)$ is false. By 1) $n \neq 1$. By Exercise 2.18 $n - 1 \in \mathbb{N}$. By minimality of n , $P(n - 1)$ is true. By 2) $P(n)$ is true, a contradiction. \square

Exercise 3.2. Define $n^2 = n \times n$ and $n^3 = n^2 \times n$ for any integer n . Prove that for any natural n there exists an integer m such that $n^3 - n = 3m$. (Later we will say that 3 divides $n^3 - n$.) Hint: proceed by induction on n as follows.

Let $P(n)$ be the sentence: for all natural n there exists an integer m such that $n^3 - n = 3m$. $P(1)$ is true because $1^3 - 1 = 3 \times 0$. Assume now that $P(n-1)$ is true i.e. $(n-1)^3 - (n-1) = 3q$ for some integer q and let us check that $P(n)$ is true i.e. that $n^3 - n = 3m$ for some integer m . The equality $(n-1)^3 - (n-1) = 3q$ reads $n^3 - 3n^2 + 3n - 1 - n + 1 = 3q$. Hence $n^3 - n = 3(n^2 - n)$ and we are done.

Exercise 3.3. Define $n^5 = n^3 \times n^2$. Prove that for any natural n there exists an integer m such that $n^5 - n = 5m$.

Proposition 3.4. *If there exists a bijection $\{1, \dots, n\} \rightarrow \{1, \dots, m\}$ then $n = m$.*

Proof. We proceed by induction on n . Let $P(n)$ be the statement of the Proposition. Clearly $P(1)$ is true; cf. the Exercise below. Assume now $P(n-1)$ is true and let's prove that $P(n)$ is true. So consider a bijection $F : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$; we want to prove that $n = m$. Let $i = F(n)$ and define the map $G : \{1, \dots, n-1\} \rightarrow \{1, \dots, m\} \setminus \{i\}$ by $G(j) = F(j)$ for all $1 \leq j \leq n-1$. Then clearly G is a bijection. Now consider the map $H : \{1, \dots, m\} \setminus \{i\} \rightarrow \{1, \dots, m-1\}$ defined by $H(j) = j$ for $1 \leq j \leq i-1$ and $H(j) = j-1$ for $i+1 \leq j \leq m$. (The definition is correct because for any $j \in \{1, \dots, m\} \setminus \{i\}$ either $j \leq i-1$ or $j \geq i+1$; cf. Exercise 2.17.) Clearly H is a bijection. We get a bijection

$$H \circ G : \{1, \dots, n-1\} \rightarrow \{1, \dots, m-1\}.$$

Since $P(n-1)$ is true we get $n-1 = m-1$. Hence $n = m$ and we are done. \square

Exercise 3.5. Check that $P(1)$ is true in the above Proposition.

4. FINITE SETS, FINITE SUMS, FINITE PRODUCTS

Definition 4.1. A set A is finite if there exists an integer $n \geq 0$ and a bijection $F : \{1, \dots, n\} \rightarrow A$. (n is then unique by Proposition 3.4.) We write $|A| = n$ and we call this number the *cardinality* of A or the *number of elements* of A . (Note that $|\emptyset| = 0$.) If $F(i) = a_i$ we write $A = \{a_1, \dots, a_n\}$. A set is infinite if it is not finite.

Exercise 4.2. Prove that $|\{2, 4, -6, 9, -100\}| = 5$.

Exercise 4.3. For any finite sets A and B we have that $A \cup B$ is finite and

$$|A \cup B| + |A \cap B| = |A| + |B|.$$

Hint: Reduce to the case $A \cap B = \emptyset$. Then if $F : \{1, \dots, a\} \rightarrow A$ and $G : \{1, \dots, b\} \rightarrow B$ are bijections prove that $H : \{1, \dots, a+b\} \rightarrow A \cup B$ defined by $H(i) = F(i)$ for $1 \leq i \leq a$ and $H(i) = G(i-a)$ for $a+1 \leq i \leq a+b$ is a bijection.

Exercise 4.4. Let $F : \{1, \dots, n\} \rightarrow \mathbb{Z}$ be an injective map and write $F(i) = a_i$. We refer to such a map as a (finite) family of numbers. Prove that there exists a unique map $G : \{1, \dots, n\} \rightarrow \mathbb{Z}$ such that $G(1) = a_1$ and $G(k) = G(k-1) + a_k$ for $2 \leq k \leq n$. Hint: induction on n .

Definition 4.5. In the notation of the above Exercise define the (finite) sum $\sum_{i=1}^n a_i$ as the number $G(n)$. We also write $a_1 + \dots + a_n$ for this sum. If $a_1 = \dots = a_n = a$ the sum $a_1 + \dots + a_n$ is written as $a + \dots + a$ (n times).

Exercise 4.6. Prove that for any $a, b \in \mathbb{N}$ we have

$$a \times b = a + \dots + a \text{ (} b \text{ times)} = b + \dots + b \text{ (} a \text{ times)}.$$

Exercise 4.7. Define in a similar way the (finite) product $\prod_{i=1}^n a_i$ (which is also denoted by $a_1 \dots a_n = a_1 \times \dots \times a_n$). Prove the analogues of associativity and distributivity for sums and products of families of numbers. Define a^b for $a, b \in \mathbb{N}$ and prove that $a^{b+c} = a^b \times a^c$ and $(a^b)^c = a^{bc}$.

Exercise 4.8. Prove that if a is an integer and n is a natural number then

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \dots + a + 1).$$

Hint: induction on n .

Exercise 4.9. Prove that if a is an integer and n is an integer then

$$a^{2n+1} + 1 = (a + 1)(a^{2n} - a^{2n-1} + a^{2n-2} - \dots - a + 1).$$

Hint. Set $a = -b$.

Exercise 4.10. Prove that a subset $A \subset \mathbb{N}$ is bounded if and only if it is finite.

Hint: To prove that bounded sets are finite assume this is false and let b be the minimum natural number with the property that there is a set A bounded by b and infinite. If $b \notin A$ then A is bounded by $b - 1$ (Exercise 2.17) and we are done. If $b \in A$ then, by minimality of b , that there is a bijection $A \setminus \{b\} \rightarrow \{1, \dots, m\}$ and one constructs a bijection $A \rightarrow \{1, \dots, m + 1\}$ which is a contradiction. To prove that finite sets are bounded assume this is false and let n be minimum natural number with the property that there is a finite subset $A \subset \mathbb{N}$ of cardinality n which is not bounded. Let $F : \{1, \dots, n\} \rightarrow A$ be a bijection, $a_i = F(i)$. Then $\{a_1, \dots, a_{n-1}\}$ is bounded by some b and conclude that A is bounded by either b or a_n .

Exercise 4.11. Prove that any subset of a finite set is finite. Hint: use the previous exercise.

Exercise 4.12. Prove that if $A \subset \mathbb{Z}$ is a finite subset of \mathbb{N} of cardinality n then there exists a bijection $F : \{1, \dots, n\} \rightarrow A$ such that $F(i) \leq F(j)$ whenever $i \leq j$.

Hint: induction on n . Note: if $a_i = F(i)$ we will write

$$a_1 \leq a_1 \leq \dots \leq a_n.$$

Since for $i < j$ we actually have $F(i) < F(j)$ we can also write

$$a_1 < a_2 < \dots < a_n.$$

5. THE RATIONALS

The first results in the theory of integers (and indeed most results in this course) can be proved using the integers only. But as we progress towards less and less elementary levels more general numbers (rational, real, complex) will be required to prove results about the integers. For now we shall introduce the rational numbers; these will become helpful along the way. Towards the end of the course we will need to introduce real and complex numbers.

Definition 5.1. For any $a, b \in \mathbb{Z}$ with $b \neq 0$ define the fraction $\frac{a}{b}$ to be the set of all pairs (c, d) with $c, d \in \mathbb{Z}$, $d \neq 0$ such that $ad = bc$. Call a and b the numerator and the denominator of the fraction $\frac{a}{b}$. Denote by \mathbb{Q} the set of all fractions. So

$$\frac{a}{b} = \{(c, d) \in \mathbb{Z} \times \mathbb{Z}; d \neq 0, ad = bc\},$$

$$\mathbb{Q} = \left\{ \frac{a}{b}; a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

Example 5.2.

$$\frac{6}{10} = \{(6, 10), (-3, -5), (9, 15), \dots\} \in \mathbb{Q}.$$

Remark 5.3. One is tempted to define $\frac{a}{b}$ are the “unique real number” x with the property that $bx = a$. Such a definition is fallacious because the concept of *real number* has not been defined yet; the multiplication bx is also undefined for x not an integer. (We will define real numbers later using the rationals as a stepping stone.) Our definition of a rational number has to use (and does use) the concept of integer only.

Exercise 5.4. Prove that $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$. Hint: assume $ad = bc$ and let us prove that $\frac{a}{b} = \frac{c}{d}$. We need to show that $\frac{a}{b} \subset \frac{c}{d}$ and that $\frac{c}{d} \subset \frac{a}{b}$. Now if $(x, y) \in \frac{a}{b}$ then $xb = ay$; hence $xbd = ayd$. Since $ad = bc$ we get $xbd = bcy$. Hence $b(xd - cy) = 0$. Since $b \neq 0$ we have $xd - cy = 0$ hence $xd = cy$ hence $(x, y) \in \frac{c}{d}$. We proved that $\frac{a}{b} \subset \frac{c}{d}$. The other inclusion is proved similarly. So the equality $\frac{a}{b} = \frac{c}{d}$ is proved. Conversely if one assumes $\frac{a}{b} = \frac{c}{d}$ one needs to prove $ad = bc$; I leave this to the reader.

Exercise 5.5. On the set $A = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ one can consider the relation: $(a, b) \sim (c, d)$ if and only if $ad = bc$. Prove that \sim is an equivalence relation. Then observe that $\frac{a}{b}$ is the equivalence class of (a, b) . Also observe that $\mathbb{Q} = A / \sim$ is the quotient of A by the relation \sim .

Notation 5.6. Write $\frac{a}{1} = a$; this identifies \mathbb{Z} with a subset of \mathbb{Q}

Definition 5.7. Define $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, $\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$.

Exercise 5.8. Show that the above definition is correct (i.e. if $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'}$ then $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$ and similarly for the product.)

It is convenient to make the following:

Definition 5.9. Assume we are given a set R , two elements $0, 1 \in R$, and assume that we are given two binary operations $+, \times$ (write $a \times b = ab$) and a unary operation $-$ on R such that for any $u, v, w \in R$ the following hold:

- 1) $u + (v + w) = (u + v) + w$, $u + 0 = u$, $u + (-u) = 0$, $u + v = v + u$;
- 2) $u(vw) = (uv)w$, $1u = u$, $uv = vu$,
- 3) $u(v + w) = uv + uw$.

Then we say that R (together with, or with respect to, the operations $+, \times$) is a commutative ring with identity (or for simplicity a ring; 1 is the identity.) A ring R is called a field if $0 \neq 1$ and for any $u \in R$ such that $0 \neq u$ there exists $u' \in R$ such that $uu' = 1$; this u' is then easily proved to be unique and is denoted by u^{-1} .

Remark 5.10. \mathbb{Z} is a ring but not a field. \mathbb{N} is not a ring.

Exercise 5.11. Prove that \mathbb{Q} is a field (with respect to the operations $+$ and \times defined above.)

Remark 5.12. Later we will define the fields \mathbb{R} and \mathbb{C} of real and complex numbers respectively; we will have the inclusions

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Definition 5.13. For $\frac{a}{b}, \frac{c}{d}$ with $b, d > 0$ write $\frac{a}{b} \leq \frac{c}{d}$ if $ad - bc \leq 0$. Also write $\frac{a}{b} < \frac{c}{d}$ if $\frac{a}{b} \leq \frac{c}{d}$ and $\frac{a}{b} \neq \frac{c}{d}$.

Exercise 5.14. Let $x = \frac{a}{b}$ be a rational number. Prove that there exists a unique integer $[x]$ such that

$$[x] \leq x < [x] + 1.$$

Definition 5.15. $[x]$ is called the integral part of x .

Example 5.16. $[\frac{13}{2}] = 6$; $[-\frac{13}{2}] = -7$.

Exercise 5.17. Compute $[-\frac{4578}{1999}]$.

6. DIVISIBILITY AND EUCLID DIVISION

Definition 6.1. For $a, b \in \mathbb{Z}$ we say b divides a (and write $b|a$) if there exists $c \in \mathbb{Z}$ such that $a = bc$. Then b is called a divisor of a . We write $b \nmid a$ if b does not divide a .

Example 6.2. $3|15$, $-3|15$, $7 \nmid 15$.

Exercise 6.3. Prove that if $a, b \in \mathbb{N}$ and $a|b$ then $a \leq b$.

Proposition 6.4. Let $a, b, c, m, n \in \mathbb{Z}$ and assume $a|b$ and $a|c$. Then $a|mb + nc$.

Proof. By hypothesis $b = ax$, $c = ay$, with $x, y \in \mathbb{Z}$. Then

$$mb + nc = max + nay = a(mx + ny).$$

□

Exercise 6.5. Prove that if $a|b$ and $b|c$ then $a|c$.

Exercise 6.6. Prove that if $n|m$ are natural numbers then $a^n - 1$ divides $a^m - 1$.

Exercise 6.7. Let $\frac{a}{b}$ be a rational number. Prove that $\frac{a}{b}$ is an integer if and only if $b|a$.

Proposition 6.8. (Euclid division) For any $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.

Notation 6.9. We write $r = r_b(a)$ and we call r the remainder when a is divided by b or the reduction of a modulo b (or simply mod b); we call q the quotient when a is divided by b . E.g. $r_7(23) = 2$, $r_7(-23) = 5$. The notation $r_b(a)$ is not classical but will be adopted in these notes.

Proof. We prove the existence of q, r . The uniqueness is left to the reader. We may assume $a \in \mathbb{N}$. Fix b and assume there exists $a \in \mathbb{N}$ such that for all $q, r \in \mathbb{Z}$ with $0 \leq r < b$ we have $a \neq qb + r$. We may assume a is minimum with this property. If $a < b$ we can write $a = 0 \times b + a$, a contradiction. If $a = b$ we can write $a = 1 \times a + 0$, a contradiction. If $a > b$ set $a' = a - b$. Since $a' < a$, there exist $q', r \in \mathbb{Z}$ such that $0 \leq r < b$ and $a' = q'b + r$. But then $a = qb + r$, where $q = q' + 1$, a contradiction. □

Exercise 6.10. Prove the uniqueness in the above Proposition.

Exercise 6.11. Give an alternative proof of Proposition 6.8 using rational numbers. Hint: set $q = [\frac{a}{b}]$ and $r = a - bq$.

Exercise 6.12. Prove that for any finite sets A and B the product set $A \times B$ is finite and

$$|A \times B| = |A| \times |B|.$$

Hint. We may assume $A = \{0, \dots, a-1\}$ and $B = \{0, \dots, b-1\}$. Then prove that $F : A \times B \rightarrow \{0, \dots, ab-1\}$ given by $F(q, r) = bq + r$ is a bijection.

Exercise 6.13. Fix $1 \neq b \in \mathbb{N}$. Prove that any $a \in \mathbb{N}$ can be uniquely written as

$$a = r_n b^n + r_{n-1} b^{n-1} + \dots + r_1 b + r_0$$

where $r_0, \dots, r_n \in \mathbb{Z}$, $0 \leq r_i \leq b-1$. Write

$$a = (r_n r_{n-1} \dots r_1 r_0)_b$$

and call this the (digital) representation of a to base b ; the r_i are called the digits in this representation. Hint: assume this is not true, let a be the minimum number for which this is not true, divide a by b with remainder, and derive a contradiction.

Example 6.14. $42 = (42)_{10} = 2^5 + 2^3 + 2^1 = (101010)_2 = 5^2 + 3 \times 5 + 2 = (132)_5$.

Exercise 6.15. Let $d_b(a)$ be the number of digits in the representation of a to base b . Prove that $b^{d_b(a)-1} \leq a < b^{d_b(a)}$. E.g., if $b = 10$, $10^2 \leq 321 < 10^3$.

Definition 6.16. Say that a number $a \in \mathbb{Z}$ is of the form $bk + r$ if there exist $k, r \in \mathbb{Z}$ such that $a = bk + r$.

Definition 6.17. Say that a number is odd if it is of the form $2k + 1$ and even if it is of the form $2k$.

Example 6.18. 11 is of the form $4k + 3$; -7 is of the form $4k + 1$; 6 is even; 9 is odd.

Exercise 6.19. Prove that any integer is either even or odd and it cannot be both even and odd.

Exercise 6.20. Prove that any integer is either of the form $3k$ or of the form $3k + 1$ or of the form $3k + 2$. And it cannot be simultaneously of two of these three forms.

Exercise 6.21. Prove that any integer is either of the form $4k$ or of the form $4k + 1$ or of the form $4k + 2$ or of the form $4k + 3$. And it cannot be simultaneously of two of these four forms.

Exercise 6.22. Prove that any integer is either of the form $4k$ or of the form $4k - 1$ or of the form $4k - 2$ or of the form $4k - 3$. And it cannot be simultaneously of two of these four forms.

Exercise 6.23. Prove that the product of two odd numbers is odd.

Exercise 6.24. Prove that if 3 divides the product of two integers then it divides one of the integers. Prove the same thing for 3 replaced by 5 and then by 7. Hint: for 3 write the two numbers in the form $3k + r$ and $3k + s$ and examine all the possibilities for r, s . (Remark: later we will prove a general statement with 3 replaced by any prime.)

Exercise 6.25. Prove that any product of numbers of the form $4k + 1$ is of the form $4k + 1$. Generalize this by replacing 4 with other numbers.

Exercise 6.26. Prove that there is no rational number $x \in \mathbb{Q}$ such that $x^2 = 2$. (This is the famous “irrationality of $\sqrt{2}$ ”; but we have not introduced yet the concept of $\sqrt{2}$.) Hint: assume there exists a rational number x such that $x^2 = 2$ and seek a contradiction. Let $a \in \mathbb{N}$ be minimal with the property that $x = \frac{a}{b}$ for some b . Now $\frac{a^2}{b^2} = 2$ hence $2b^2 = a^2$. Hence a^2 is even. Hence a is even (because if a were odd then a^2 would be odd.) Hence $a = 2c$ for some integer c . Hence $2b^2 = (2c)^2 = 4c^2$. Hence $b^2 = 2c^2$. Hence b^2 is even. Hence b is even. Hence $b = 2d$ for some integer d . Hence $x = \frac{2c}{2d} = \frac{c}{d}$ and $c < a$. This contradicts the minimality of a which ends the proof.

Remark 6.27. The above proof is probably one of the “first” proofs by contradiction in the history of mathematics; this proof appears, for instance, in Aristotle (4th century BC), and it is believed to have been discovered by the Pythagoreans. The irrationality of $\sqrt{2}$ was interpreted by the Greeks as evidence that arithmetic is insufficient to control geometry ($\sqrt{2}$ is the length of the diagonal of a square with side 1) and arguably created the first crisis in the history of mathematics, leading to a separation of algebra and geometry that lasted until Descartes (17th century).

Exercise 6.28. Prove that there is no rational number $x \in \mathbb{Q}$ such that $x^2 = 3$ or $x^2 = 5$ or $x^2 = 7$. (Once we know what square roots are this will be equivalent to $\sqrt{3}, \sqrt{5}, \sqrt{7}$ being irrational.) Hint: imitate the above proof using the fact (proved in a previous exercise) that if one of the numbers 3, 5, 7 divides a^2 for $a \in \mathbb{Z}$ then that number divides a . (Later on in the course this will be revisited and proved in a more general situation.)

7. POLYNOMIAL TIME ALGORITHMS

The following discussion does not meet the standards of mathematical rigor but is nevertheless useful for the computational applications of number theory.

Definition 7.1. Assume we are given a function $F : A \rightarrow B$ where A and B are subsets of \mathbb{N} (or $\mathbb{N} \times \mathbb{N}$, etc.) By an algorithm that computes F we mean a “set of instructions” (a “program”) that, once followed, leads to the computation of $F(a)$ if $a \in A$ is given in digital representation to base 2. The computation, for each a , involves a number of “elementary” operations (like add two digits and multiply two digits). This number is denoted by $T(a)$ and is called running time of the algorithm for in the input a . We say that the algorithm runs in polynomial time if there exist natural numbers C, n such that for any $a \in A$ we have

$$T(a) \leq C \times d_2(a)^n$$

where $d_2(a)$ is the number of digits in the digital representation to base 2 of the number a (or, in case $A \subset \mathbb{N} \times \mathbb{N}$, $d_2(a)$ is the maximum of the number of digits in the components of a , etc.) A computation in polynomial time is considered a fast computation.

Exercise 7.2. Give an argument (but not necessarily a formal proof) showing that the algorithm that computes addition and multiplication of numbers in decimal form runs in polynomial time.

Exercise 7.3. Give an argument (but not necessarily a formal proof) showing that 1) the long division algorithm learned in elementary school correctly gives the quotient and the remainder when an integer is divided by another integer and 2) that this algorithm runs in polynomial time.

8. PRIMES

Definition 8.1. A *prime* number is a number $p \in \mathbb{Z}$, $p \geq 2$, whose only positive divisors are 1 and p . Equivalently p is prime if $p \geq 2$ and whenever $p = ab$ with $a, b \in \mathbb{N}$ it follows that either $a = 1$ or $b = 1$.

Example 8.2. 2, 3, 5, 7, 11 are prime. 0, 1, -3, 15 are not prime.

Proposition 8.3. Any $a \in \mathbb{N}$ with $a \neq 1$ is a product of primes.

Here any prime is viewed as a product of primes (with only one prime involved in the product).

Proof. Let S be the set of all $a \in \mathbb{N}$, $a \neq 1$, which are not products of primes. We want to show $S = \emptyset$. Assume not and let $m = \min S$. Then m is not prime. So $m = ab$ with a, b positive and $\neq 1$. So $a, b \notin S$ and hence a and b are products of primes. Hence so is m , a contradiction. \square

Theorem 8.4. (Euclid) There are infinitely many primes.

Proof. Assume there are only finitely many primes, i.e. the set of primes is finite, $\{p_1, \dots, p_n\}$. By Proposition 8.3

$$N := p_1 \dots p_n + 1 = q_1 \dots q_m$$

with q_i primes. Since $q_1 = p_j$ for some j we have $q_1 | N$ and $q_1 | N - 1$ so

$$q_1 | N - (N - 1) = 1,$$

a contradiction. \square

Exercise 8.5. Prove that there are infinitely many primes of the form $4k + 3$. (Hint: assume there are only finitely many p_1, \dots, p_n and consider the number $N = 4p_1 \dots p_n - 1$.) Generalize this by proving that for any $m \geq 3$ there are infinitely many primes which are not of the form $mk + 1$.

Remark 8.6. We will be able to prove (later) that there are infinitely many primes of the form $4k + 1$.

Remark 8.7. An algorithm running in polynomial time was recently found to compute the function f defined as follows: $f(n) = 1$ if n is prime and $f(n) = 0$ if n is not prime. In other words one can decide in polynomial time if a given integer is prime.

Exercise 8.8. Prove that if m is a natural number and $2^m + 1$ is prime then $m = 2^n$ for some natural number n .

Exercise 8.9. Prove that if m is a natural number and $2^m - 1$ is prime then m is prime.

Definition 8.10. A Fermat prime is a prime of the form $F_n = 2^{2^n} + 1$. A Mersene prime is a prime of the form $M_p = 2^p - 1$, (where p is necessarily a prime).

Exercise 8.11. Prove that F_n is prime for $n = 1, 2, 3, 4$.

Remark 8.12. Fermat conjectured that F_n is prime for any $n \geq 1$. Euler gave a counterexample:

$$F_5 = 641 \times 6700417.$$

There is no known $n \geq 5$ with F_n prime.

Exercise 8.13. Prove that $F_n | F_m - 2$ for $m > n$.

Remark 8.14. M_p is prime for some p 's and non-prime for other p 's. It is conjectured that M_p is prime for infinitely many p 's.

9. GREATEST COMMON DIVISOR

Definition 9.1. If $a, b \in \mathbb{Z}$ then a common divisor of a, b is an integer that divides both a and b . Let $\gcd(a, b)$ denote the greatest common divisor of a and b . (The definition is correct because the set of common divisors of a and b is bounded so it has a greatest element.)

The $\gcd(a, b)$ is sometimes denoted simply by (a, b) but we will avoid the latter notation (to avoid confusion with the notation for pairs).

Example 9.2. The common divisors of 28 and 36 are 1, 2, 4 and their negatives. So $\gcd(28, 36) = 4$.

Definition 9.3. Two integers a and b are relatively prime (or coprime) if $\gcd(a, b) = 1$.

Example 9.4. 10 and 77 are relatively prime.

Remark 9.5. According to a theorem of Dirichlet if a, b are coprime integers then there exist infinitely many primes of the form $ak + b$. Dirichlet's proof uses analysis and will not be included in our course.

Definition 9.6. Let x, y be integers. An integer x is a \mathbb{Z} -linear combination of y, z if there exist integers m, n such that $x = my + nz$.

Exercise 9.7. Prove that if x is a \mathbb{Z} -linear combination of y, z and each of y, z is a \mathbb{Z} -linear combination of u, v then x is a \mathbb{Z} -linear combination of u, v .

Theorem 9.8. If $c = \gcd(a, b)$ then c is a \mathbb{Z} -linear combination of a, b ; in other words there exist $m, n \in \mathbb{Z}$ such that $c = ma + nb$. In particular if $d|a$ and $d|b$ then $d|c$.

Remark 9.9. Even if $a, b \geq 0$ one cannot choose $m, n \geq 0$ in general. Also m, n are not unique.

Proof of Theorem 9.8. We may assume $b \geq 1$. Let J be the set of \mathbb{Z} -linear combinations of a and b . Let t be the smallest element in $J \cap \mathbb{N}$. We claim that a and b are divisible by t . Indeed if $a = tq + r$ with $0 \leq r < t$ and $r \neq 0$ then $r \in J \cap \mathbb{N}$ which contradicts the minimality of t . So $r = 0$ and hence $t|a$. Similarly $t|b$. But then t is a common divisor of a, b and being in J is divided by any other common divisor. So $t = \gcd(a, b)$. \square

Exercise 9.10. Compute $c = \gcd(86, 24)$ and find m, n such that $c = m \times 86 + n \times 24$. Hint: We have

$$\begin{aligned} 86 &= 3 \times 24 + 14 \\ 24 &= 1 \times 14 + 10 \\ 14 &= 1 \times 10 + 4 \\ 10 &= 2 \times 4 + 2 \\ 4 &= 2 \times 2. \end{aligned}$$

Hence:

$$\gcd(86, 24) = \gcd(24, 14) = \gcd(14, 10) = \gcd(10, 4) = \gcd(4, 2) = 2.$$

To find m, n we express each of the numbers **86, 24, 14, 10, 4, 2** as a linear combination of the 2 preceding ones: $\mathbf{2} = \mathbf{10} - 2 \times \mathbf{4} = \mathbf{10} - 2 \times (\mathbf{14} - 1 \times \mathbf{10}) = (-2) \times \mathbf{14} + 3 \times \mathbf{10} = \dots = (-5) \times \mathbf{86} + 18 \times \mathbf{24}$.

Exercise 9.11. Prove that 691 and 1000 are relatively prime and find m, n such that $1 = m \times 691 + n \times 1000$.

Exercise 9.12. Prove that the algorithm behind Exercise 9.11 (computing $\gcd(a, b)$ for given a, b) runs in polynomial time. Hint: The algorithm requires to perform Euclidean divisions:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\dots \\ r_{n-2} &= r_{n-1}q_n + r_n \\ r_{n-1} &= r_nq_{n+1} + r_{n+1} \\ r_n &= r_{n+1}q_{n+2}. \end{aligned}$$

with $b =: r_0 > r_1 > r_2 > \dots > r_n > r_{n+1} > 0$; then $\gcd(a, b) = r_{n+1}$. For each k we have $r_{k-2} \geq r_{k-1} + r_k \geq 2r_k$. So $b =: r_0 \geq 2r_2 \geq 4r_4 \geq 8r_6 \geq \dots \geq 2^m r_{2m} \geq 2^m$ if $2m = n$ or $2m = n + 1$. So $2^m \leq b \leq 2^{d_2(b)}$. So $m \leq d_2(b)$. Now note that the running time is a constant times m times $d_2(a)$.

10. UNIQUE FACTORIZATION

Lemma 10.1. (*Euclid's Lemma*). Let p be a prime and a, b two integers. If $p|ab$ then either $p|a$ or $p|b$.

Proof Assume $p|ab$, $p \nmid a$, $p \nmid b$ and seek a contradiction. Since $p \nmid a$ it follows that $\gcd(a, p) = 1$ hence by Theorem 9.8

$$1 = ma + np$$

for some $m, n \in \mathbb{Z}$. Since $p \nmid b$ it follows that $\gcd(b, p) = 1$ hence by the same Theorem

$$1 = xb + yp$$

for some $x, y \in \mathbb{Z}$. Multiplying the two equations above we get

$$1 = (ma + np)(xb + yp) = mxab + mayp + npxb + nyp^2.$$

Since all terms in the right hand side of the latter equation are divisible by p we get $p|1$, a contradiction. \square

Corollary 10.2. Let p be a prime and a_1, \dots, a_n integers. If $p|a_1a_2\dots a_n$ then either $p|a_1$ or $p|a_2, \dots$, or $p|a_n$.

Proof. Assume this is false for some p and seek a contradiction. Let n be minimum such that there exist a_1, \dots, a_n with $p|a_1a_2\dots a_n$ and $p \nmid a_1, p \nmid a_2, \dots, p \nmid a_n$. By Euclid's Lemma either $p|a_1$ or $p|a_2\dots a_n$. Since $p \nmid a_1$ we must have $p|a_2\dots a_n$. This contradicts the minimality of n . \square

Theorem 10.3. (*Fundamental Theorem of Arithmetic*). Any integer $a \in \mathbb{N}$, $a \neq 1$, can be written uniquely as a product of (not necessarily distinct) primes

$$a = p_1 p_2 \dots p_n$$

with $p_1 \leq p_2 \leq \dots \leq p_n$.

Proof. The existence of this representation is Proposition 8.3. To prove the uniqueness of the representation assume there are a 's with non-unique representations and let a be the smallest one; we seek a contradiction. Let

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$$

with $p_1 \leq p_2 \leq \dots \leq p_n$ primes and $q_1 \leq q_2 \leq \dots \leq q_m$ primes. Note that

$$p_1 | q_1 q_2 \dots q_m.$$

By the Corollary above $p_1 | q_1$ or $p_1 | q_2, \dots$, or $p_1 | q_m$. Hence $p_1 = q_1$ or $p_1 = q_2, \dots$, or $p_1 = q_m$. Say $p_1 = q_i$. Then we get

$$p_2 \dots p_n = q_1 \dots q_{i-1} q_{i+1} \dots q_m$$

which contradicts the minimality of a . □

Exercise 10.4. Write $1^1 \times 2^2 \times 3^3 \times 4^4 \times \dots \times 20^{20}$ as a product of primes.

Exercise 10.5. Without using Euclid's Lemma (or the Fundamental Theorem of Arithmetic) prove that if $11|ab$ then either $11|a$ or $11|b$. Same for 13 instead of 11.

Exercise 10.6. Prove that if a and b are coprime and $a|bc$ then $a|c$. Hint: assume this is false and consider the minimum a for which this is false.

Remark 10.7. No algorithm running in polynomial time is known that computes the prime factorization of an integer. Any such algorithm would compromise the security of some important public key cryptography schemes that are in use today.

Remark 10.8. The following remark shows the non-triviality of the Fundamental Theorem of Arithmetic: the analogue of this theorem in similar contexts may fail as we shall see presently. Let S be the collection of all natural numbers of the form $4k + 1$:

$$S = \{1, 5, 9, 13, 17, 21, 25, 29, \dots\}.$$

Refer to the elements of S as *numbers*. The product of any two numbers is a number. Say that a number p is *brime* if whenever $p = ab$ with a, b numbers it follows that $a = 1$ or $b = 1$. For instance 9 is brime because it is not a product of any two numbers both unequal to 1. Also 21, 33, 77 are brimes. It is easy to prove that any number is a product of brimes. But note that some numbers, like 693, have several distinct decompositions into products of brimes:

$$693 = 9 \times 77 = 21 \times 33.$$

Exercise 10.9. Prove that any number is a product of brimes; cf. the Remark above.

Exercise 10.10. Note that S in Remark 10.8 is the set of natural numbers of the form $4k + 1$. Generalize Remark 10.8 by replacing 4 with an arbitrary number.

11. APPLICATIONS OF UNIQUE FACTORIZATION

The Fundamental Theorem of Arithmetic has the following obvious:

Corollary 11.1. Any integer $a \geq 2$ can be written uniquely as a product

$$a = \prod_p p^{v_p(a)} = 2^{v_2(a)} 3^{v_3(a)} \dots$$

where p runs through the set of primes and $v_p(a)$ are integers ≥ 0 , all except finitely many of them 0 (so the product above is finite).

Example 11.2. $56 = 2^3 \times 7$ so $v_2(56) = 3$, $v_5(56) = 0$, $v_7(56) = 1$, $v_{11}(56) = 0, \dots$

Definition 11.3. For any prime p and any integer $n \geq 2$ we define the p -adic valuation of $a \geq 2$ at p as being the number $v_p(a)$ in the above Corollary. We also set $v_p(1) = 0$, $v_p(-a) = v_p(a)$ for $a \geq 1$.

Exercise 11.4. Prove that

- 1) $v_p(ab) = v_p(a) + v_p(b)$.
- 2) $a|b$ if and only if $v_p(a) \leq v_p(b)$ for all p .
- 3) If $a^8|b^5$ then $a|b$.

Recall that $n! = 1 \times 2 \times 3 \times \dots \times n$ for $n \in \mathbb{N}$.

Proposition 11.5. For any natural n we have:

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

Proof. Let $A_i = \{a; 1 \leq a \leq n, v_p(a) \geq i\}$, $a_i = |A_i|$, and let

$$B_i = A_i \setminus A_{i+1} = \{a; 1 \leq a \leq n, v_p(a) = i\}, \quad b_i = |B_i|.$$

Note that $a_i = \left[\frac{n}{p^i} \right]$ (because the map $\{1, \dots, \left[\frac{n}{p^i} \right]\} \rightarrow A_i, j \mapsto p^i j$ is a bijection).

Let β_i be the product of all numbers in B_i ; so $v_p(\beta_i) = ib_i$. We have

$$n! = \beta_1 \times \beta_2 \times \beta_3 \times \dots$$

so we have

$$\begin{aligned} v_p(n!) &= v_p(\beta_1) + v_p(\beta_2) + v_p(\beta_3) + \dots \\ &= b_1 + 2b_2 + 3b_3 + \dots \\ &= (a_1 - a_2) + 2(a_2 - a_3) + 3(a_3 - a_4) + \dots \\ &= a_1 + a_2 + a_3 + \dots \end{aligned}$$

and we are done. □

Exercise 11.6. Give an alternative proof of Proposition 11.5 by induction on n . Hint: Call $P(n)$ the assertion of the Proposition. Clearly $P(1)$ is true. Now assume $P(n-1)$ is true, i.e.

$$v_p((n-1)!) = \left[\frac{n-1}{p} \right] + \left[\frac{n-1}{p^2} \right] + \left[\frac{n-1}{p^3} \right] + \dots$$

To prove $P(n)$ note that $v_p(n!) = v_p((n-1)!) + v_p(n)$. Write $n = ap^i$ with $p \nmid a$. Then $v_p(n) = i$. Now for $j \leq i$ we have $\left[\frac{n}{p^j} \right] = ap^{i-j}$, hence

$$\left[\frac{n-1}{p^j} \right] = \left[ap^{i-j} - \frac{1}{p^j} \right] = ap^{i-j} - 1 = \left[\frac{n}{p^j} \right] - 1.$$

For each $j > i$ divide a by p^{j-i} with remainder: $a = p^{j-i}q + r$ and compute:

$$\left[\frac{n}{p^j} \right] = \left[\frac{a}{p^{j-i}} \right] = \left[q + \frac{r}{p^{j-i}} \right] = q,$$

hence:

$$\left[\frac{n-1}{p^j} \right] = \left[\frac{a}{p^{j-i}} - \frac{1}{p^j} \right] = \left[q + \frac{r}{p^{j-i}} - \frac{1}{p^j} \right] = q = \left[\frac{n}{p^j} \right],$$

because

$$0 \leq \frac{r}{p^{j-i}} - \frac{1}{p^j} < 1.$$

Then $P(n)$ follows.

Exercise 11.7. Prove that $v_p(n!) \leq \frac{n}{p-1}$.

Exercise 11.8. Prove that if $n = (a_d \dots a_0)_p = a_d p^d + \dots + a_0$ is the expansion of n to base p then

$$\left[\frac{n}{p} \right] + \left[\frac{n}{p^2} \right] + \left[\frac{n}{p^3} \right] + \dots = \frac{1}{p-1} [n - (a_0 + \dots + a_d)].$$

This, of course, implies the statement in Exercise 11.7.

Exercise 11.9. Use Exercise 11.8 to give an alternative proof to Proposition 11.5. Hint: Induction on n ; examine two cases: the case when the last digit of $n-1$ is $p-1$ and the case when the last digit of $n-1$ is not $p-1$. In the first case consider the longest sequence of consecutive digits equal to $p-1$ at the end of $n-1$.

Exercise 11.10. For all integers $n \geq m \geq 0$ one defines the binomial coefficients

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}.$$

Here $0! = 1$. Prove that the binomial coefficients (which are a priori in \mathbb{Q}) belong to \mathbb{N} . Hint: show that v_p applied to the numerator is greater than or equal to the value of v_p applied to the denominator.

Exercise 11.11. Prove that if p is prime and $1 \leq m \leq p-1$ is an integer then

$$p \mid \binom{p}{m}.$$

Hint: p divides the binomial coefficient times its denominator; it does not divide the denominator by Euclid's Lemma. So by Euclid's Lemma again, it divides the binomial coefficient.

Exercise 11.12. Prove the binomial formula:

$$(a+b)^n = \sum_{m=0}^n \binom{n}{m} a^m b^{n-m}.$$

Hint: induction on n .

Definition 11.13. For any natural number n and any integer $k \geq 0$ define

$$\sigma_k(n) = \sum_{d|n} d^k$$

where d runs through the set of all (positive!) divisors of n (including 1 and n).

Example 11.14. $\sigma_3(10) = 1^3 + 2^3 + 5^3 + 10^3$; $\sigma_0(10) = 1^0 + 1^0 + 1^0 + 1^0 = 4$.

Exercise 11.15. Prove that $\sigma_k(p^n) = 1 + p^k + p^{2k} + \dots + p^{nk}$ if p is prime.

Exercise 11.16. Prove that if $n = p_1^{e_1} \dots p_s^{e_s}$ with p_1, \dots, p_s distinct then

$$\sigma_k(n) = (1 + p_1^k + \dots + p_1^{e_1 k}) \dots (1 + p_s^k + \dots + p_s^{e_s k}).$$

Conclude that $\sigma_k(nm) = \sigma_k(n)\sigma_k(m)$ if n and m are coprime.

Definition 11.17. A natural number n is perfect if $\sigma_1(n) = 2n$.

Example 11.18. 6 is perfect because $1 + 2 + 3 + 6 = 2 \times 6$. Also 28 is perfect.

Exercise 11.19. (Euclid) Let p be a prime. If $M_p = 2^p - 1$ is prime then $2^{p-1}M_p$ is perfect.

12. CONGRUENCES: GENERALITIES

Definition 12.1. (Gauss). For $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ write

$$a \equiv b \pmod{m}$$

if and only if $m|b - a$. We say that a and b are congruent mod m . Write

$$a \not\equiv b \pmod{m}$$

if and only if $m \nmid b - a$.

Example 12.2. $7 \equiv 13 \pmod{3}$ because $3|13 - 7$. But $7 \not\equiv 13 \pmod{5}$ because $5 \nmid 13 - 7$.

Exercise 12.3. Prove that the following are equivalent:

- 1) $a \equiv b \pmod{m}$;
- 2) $r_m(a) = r_m(b)$, i.e. a and b have the same remainder when divided by m ;
- 3) a is of the form $mk + b$, i.e. there exists $k \in \mathbb{Z}$ such that $a = mk + b$.

Proposition 12.4.

- 1) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$. In particular $a^n \equiv b^n \pmod{m}$ for any $n \geq 1$.
- 2) If $ca \equiv cb \pmod{m}$ and $\gcd(c, m) = 1$ then $a \equiv b \pmod{m}$.
- 3) If $c \neq 0$ we have that $ca \equiv cb \pmod{cm}$ is equivalent to $a \equiv b \pmod{m}$.

Proof. 1) Let's show that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ imply $ac \equiv bd \pmod{m}$. (The other statement is proved similarly.) By hypothesis $m|b - a$ and $m|d - c$. It follows that

$$m| -d(b - a) + b(d - c) = da - bc.$$

2) If $ca \equiv cb \pmod{m}$ then $mx = cb - ca = c(b - a)$ for some $x \in \mathbb{Z}$. So for any prime p we have that

$$v_p(m) \leq v_p(c) + v_p(b - a)$$

so

$$v_p(m) \leq v_p(b - a)$$

because $v_p(c) = 0$ whenever $v_p(m) \neq 0$. So $m|b - a$ and hence $a \equiv b \pmod{m}$.

3) is proved similarly. \square

Exercise 12.5. State and prove a generalization of 1) in the above proposition involving sums and products of more than two numbers.

Exercise 12.6. Compute the remainder when 3^{1034} is divided by 7. Hint: write 1034 as a sum of powers of 2:

$$1034 = 1024 + 8 + 2 = 2^{10} + 2^3 + 2,$$

compute

$$\begin{aligned} 3 &\equiv 3 && (mod\ 7) \\ 3^2 &\equiv 9 &\equiv 2 && (mod\ 7) \\ 3^{2^2} &\equiv (3^2)^2 &\equiv 2^2 &\equiv 4 && (mod\ 7) \\ 3^{2^3} &\equiv (3^{2^2})^2 &\equiv 4^2 &\equiv 16 &\equiv 2 && (mod\ 7) \\ 3^{2^4} &\equiv (3^{2^3})^2 &\equiv 2^2 &\equiv 4 && (mod\ 7) \\ 3^{2^5} &\equiv (3^{2^4})^2 &\equiv 4^2 &\equiv 16 &\equiv 2 && (mod\ 7) \end{aligned}$$

It is clear (already from the 4th line) that we have a pattern: the remainders when

$$3, 3^2, 3^{2^2}, 3^{2^3}, 3^{2^4}, 3^{2^5}, \dots$$

is divided by 7 are

$$3, 2, 4, 2, 4, 2, \dots$$

(This is called eventual periodicity, i.e. periodicity from some point on, and this is a general phenomenon.) In particular we will get $3^{2^{10}} \equiv 4 \pmod{7}$. We get

$$3^{1034} \equiv 3^{2^{10}+2^3+2} \equiv 3^{2^{10}} \times 3^{2^3} \times 3^2 \equiv 4 \times 2 \times 2 \equiv 8 \times 2 \equiv 1 \times 2 \equiv 2 \pmod{7}.$$

So $\text{rem}(3^{1034}, 7) = 2$.

Exercise 12.7. Give an argument showing that the algorithm behind the previous exercise (computing $r_m(a^n)$ when a, n, m are given) runs in polynomial time.

Exercise 12.8. Prove that if a number x is a sum of two squares (i.e. $x = a^2 + b^2$ with $a, b \in \mathbb{Z}$) then $x \not\equiv 3 \pmod{4}$. Hint: We have $a, b \equiv 0, 1, 2, 3 \pmod{4}$ so $a^2, b^2 \equiv 0, 1, 4, 9 \pmod{4}$ i.e. $a^2, b^2 \equiv 0, 1 \pmod{4}$ so $a^2 + b^2 \equiv 0+0, 0+1, 1+0, 1+1 \pmod{4}$.

Exercise 12.9. Prove the ‘‘Freshman’s Dream’’: for p prime and a, b integers:

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

More generally prove

$$(a_1 + \dots + a_n)^p \equiv a_1^p + \dots + a_n^p \pmod{p}$$

for integers a_1, \dots, a_n .

13. COMPLETE RESIDUE SYSTEMS

Definition 13.1. Let $m \in \mathbb{N}$. A complete residue system mod m is a subset $S \subset \mathbb{Z}$ such that:

- 1) $|S| = m$ and
- 2) for any two $a, b \in S$ with $a \neq b$ we have $a \not\equiv b \pmod{m}$.

Exercise 13.2. Prove that $\{0, \dots, m-1\}$ is a complete residue system mod m .

Exercise 13.3. Prove that a set $\{a_1, \dots, a_m\}$ of m integers is a complete residue system if and only if the remainders $r_m(a_1), \dots, r_m(a_m)$ are distinct. (Remark: If this is the case then this set of remainders is the whole of $\{0, 1, \dots, m-1\}$.)

Exercise 13.4. Let a be any integer. Prove that

$$\{a, a + 1, \dots, a + m - 1\}$$

is a complete residue system mod m .

Exercise 13.5. Let a be an integer coprime to m (recall this means $\gcd(a, m) = 1$). Then prove that

$$\{0, a, 2a, 3a, \dots, (m - 1)a\}$$

is a complete residue system mod m .

Proposition 13.6. If S is a complete residue system mod m then for any $z \in \mathbb{Z}$ there exists a unique $x \in S$ such that $z \equiv x \pmod{m}$.

Proof. Uniqueness is part of the definition. To prove the existence of x we proceed as follows. Consider the map $F : S \rightarrow \{0, \dots, m - 1\}$, $F(a) = r_m(a)$. Then F is injective. Since $|S| = m = |\{0, \dots, m - 1\}|$ it follows that F is surjective. So $r_m(z) = r_m(x)$ for some $x \in S$. But then $z \equiv x \pmod{m}$. \square

Exercise 13.7. Prove that if p is prime then 1 and $p - 1$ are the only numbers c in the complete residue system $\{0, 1, \dots, p - 1\}$ such that $c^2 \equiv 1 \pmod{p}$. Hint: if $p|c^2 - 1 = (c - 1)(c + 1)$ then, by Euclid's Lemma, either $p|c + 1$ or $p|c - 1$.

14. RESIDUE CLASSES

Definition 14.1. A residue class mod m is a subset $C \subset \mathbb{Z}$ such that

- 1) For any $a, b \in C$ we have $a \equiv b \pmod{m}$;
- 2) If $a \in C$, $c \in \mathbb{Z}$, and $a \equiv c \pmod{m}$ then $c \in C$.

Example 14.2. The odd integers are a residue class mod 2. The set

$$C = \{x \in \mathbb{Z}; x \equiv 2 \pmod{7}\} = \{\dots, -5, 2, 9, \dots\}$$

is a residue class mod 7.

Example 14.3. Fix m . For each $a \in \mathbb{Z}$ set

$$\bar{a} := \{km + a; k \in \mathbb{Z}\} = \{x \in \mathbb{Z}; x \equiv a \pmod{m}\}$$

is a residue class. The upper bar notation is standard but may introduce some confusion in that it forgets about m ; so, for instance, for $m = 3$,

$$\bar{2} = \{\dots, -1, 2, 5, \dots\}$$

whereas for $m = 7$,

$$\bar{2} = \{\dots, -5, 2, 9, \dots\}.$$

Other notations for \bar{a} are \hat{a} or $[a]$ or $[a]_m$; the latter can be especially useful because it remembers m . We will mostly use the notation \bar{a} .

Exercise 14.4. Let S be a complete residue system. Prove that any residue class mod m is of the form \bar{a} for some unique $a \in S$. Prove that $\bar{a} = \bar{b}$ if and only if $a \equiv b \pmod{m}$. Prove that if $\bar{a} \neq \bar{b}$ then $\bar{a} \cap \bar{b} = \emptyset$.

Notation 14.5. We denote by $\mathbb{Z}/m\mathbb{Z}$ the set of residue classes mod m ; hence

$$\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{m - 1}\}.$$

Example 14.6.

$$\begin{aligned} \mathbb{Z}/3\mathbb{Z} &= \{\bar{0}, \bar{1}, \bar{2}\} \\ &= \{\{\dots, -6, -3, 0, 3, 6, \dots\}, \{\dots, -5, -2, 1, 4, 7, \dots\}, \{\dots, -4, -1, 2, 5, 8, \dots\}\}. \end{aligned}$$

Definition 14.7. For any two subsets $A, B \subset \mathbb{Z}$ define the subset $A + B \subset \mathbb{Z}$ by $A + B = \{a + b; a \in A, b \in B\}$.

Example 14.8.

$$\{1, 10, 100, \dots\} + \{2, 4, 6, \dots\} = \{3, 5, 7, \dots, 12, 14, 16, \dots, 102, 104, 106, \dots\}.$$

Example 14.9.

$$\{\dots, -5, 2, 9, \dots\} + \{\dots, -4, 3, 10, \dots\} = \{\dots, -9, -2, 5, 12, 19, \dots\}.$$

Exercise 14.10. Prove that if A and B are residue classes mod m then:

- 1) $A + B$ is a residue class mod m ,
- 2) The set $\{ab; a \in A, b \in B\}$ is contained in a unique residue class mod m (which we call AB or $A \cdot B$). Give an example showing that the set $\{ab; a \in A, b \in B\}$ itself is not necessarily a residue class.
- 3) Prove that $\overline{a + b} = \overline{a} + \overline{b}$ and $\overline{ab} = \overline{a} \cdot \overline{b}$.

Exercise 14.11. Prove that $\mathbb{Z}/m\mathbb{Z}$ with the operations $+$ and \cdot is a ring. Prove that if m is not prime then $\mathbb{Z}/m\mathbb{Z}$ is not a field. (In the next section we will see that the converse is also true: if m is prime then $\mathbb{Z}/m\mathbb{Z}$ is a field.)

Exercise 14.12. Fix m and consider the relation on \mathbb{Z} defined by $a \sim b$ if and only if $a \equiv b \pmod{m}$. Prove that \sim is an equivalence relation. Observe that \overline{a} is the equivalence class of a with respect to this relation. Observe that $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/\sim$ is the quotient of \mathbb{Z} by this relation..

15. INVERSES MOD m

Definition 15.1. An inverse of an integer a mod m is an integer a' such that $aa' \equiv 1 \pmod{m}$.

Example 15.2. 3 is an inverse of 7 mod 10 because $7 \times 3 \equiv 1 \pmod{10}$. On the other hand 3 has no inverse mod 9.

Exercise 15.3. Prove that if an inverse of a mod m exists then there is only one such inverse in any given complete residue system mod m .

Proposition 15.4. a has an inverse mod m if and only if $\gcd(a, m) = 1$. (If this is the case we denote by $i_m(a)$ the unique inverse of a mod m in the complete residue system $\{0, \dots, m - 1\}$.)

Proof. If $aa' \equiv 1 \pmod{m}$ then $aa' - 1 = km$ for some $k \in \mathbb{Z}$ so any common divisor of a and m must divide 1. Conversely if $\gcd(a, m) = 1$ then, by Theorem 9.8, $1 = na + km$ for some integers n, k and we can take $a' = n$. \square

Exercise 15.5. Show that 12 has an inverse mod 43 and find such an inverse. Hint: as in Exercise 9.11 we get $1 = (-5) \times 43 + 18 \times 12$ hence 18 is an inverse of 12 mod 43; so $i_{43}(12) = 18$ and hence also $i_{43}(18) = 12$.

Theorem 15.6. (Wilson). If p is prime then $(p - 1)! \equiv -1 \pmod{p}$.

Proof. We may assume $p \neq 2$. By Exercise 13.7 the only elements of the set

$$\{1, 2, \dots, p - 1\}$$

which are equal to their own inverse mod p are 1 and $p - 1$. So one can write

$$\{1, 2, \dots, p - 1\} = \{1, p - 1, a_1, a'_1, a_2, a'_2, \dots\}$$

where $a'_1 = i_p(a_1)$ is the inverse of $a_1 \pmod p$, etc. Then

$$(p-1)! \equiv 1 \times (p-1) \times a_1 \times a'_1 \times a_2 \times a'_2 \times \dots \equiv p-1 \equiv -1 \pmod p.$$

□

Exercise 15.7. Prove the converse of the above Theorem: if $n \geq 2$ is an integer such that $(n-1)! \equiv -1 \pmod n$ then n is prime.

Exercise 15.8. Prove that if p is a prime then the ring $\mathbb{Z}/p\mathbb{Z}$ is a field. (This field is sometimes denoted by \mathbb{F}_p and is called the prime field with p elements. In the old literature this field was called a Galois field and was denoted by $GF(p)$. Galois (early 19th century) proved that for any $n \geq 1$ there exists a field $GF(p^n)$ with p^n elements. In some modern algebra books \mathbb{F}_p is denoted by \mathbb{Z}_p ; in many other books \mathbb{Z}_p stands for a different ring, the ring of p -adic integers.)

16. GROUPS

This section can be skipped: the concepts introduced next will not play an essential role later (although some exercises later will involve these concepts). In abstract algebra courses one introduces the concept of group (see below) which generalizes some of the features of objects defined above; in its most abstract form below this concept is due to Cayley, although it essentially originates, in the form of various examples, in work of Lagrange, Gauss, and Galois.

Definition 16.1. Assume we are given a set G together with an element $e \in G$ and we are given a binary operation \star on G and a unary operation $'$ on G (write $'(x) = x'$) such that for any $x, y, z \in G$ the following axioms are satisfied:

- 1) $x \star (y \star z) = (x \star y) \star z$;
- 2) $x \star e = e \star x = x$;
- 3) $x \star x' = x' \star x = e$.

If in addition $x \star y = y \star x$ for all $x, y \in G$ we say G is commutative (or Abelian in honor of Abel).

Notation 16.2. Sometimes one writes $e = 1$, $x \star y = xy$, $x' = x^{-1}$, $x \star \dots \star x = x^n$ ($n \geq 1$ times). In the Abelian case one sometimes writes $e = 0$, $x \star y = x + y$, $x' = -x$, $x \star \dots \star x = nx$ ($n \geq 1$ times). These notations depend on the context and are justified by the following examples.

Example 16.3. If R is a ring then R is an Abelian group with $e = 0$, $x \star y = x + y$, $x' = -x$. Hence $\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}, \mathbb{Q}$ are groups “with respect to addition”.

Example 16.4. If R is a field then $R^\times = R \setminus \{0\}$ is an Abelian group with $e = 1$, $x \star y = xy$, $x' = x^{-1}$. Hence $\mathbb{Q}^\times, \mathbb{F}_p^\times$ are groups “with respect to multiplication”.

Example 16.5. (Assumes linear algebra). If R is a field then the set $GL_n(R)$ of $n \times n$ matrices with entries in R and with non-zero determinant is a (non-Abelian) group with $e = I_n$ (the identity matrix), $A \star B = AB$ (usual multiplication of matrices), A^{-1} = inverse of A .

Example 16.6. The set $S(X)$ of bijections $\sigma : X \rightarrow X$ from a set X into itself is a (non-Abelian) group with $e = 1_X$ (the identity map), $\sigma \star \tau = \sigma \circ \tau$ (composition), σ^{-1} = inverse map. If $X = \{1, \dots, n\}$ then one writes $S_n = S(X)$ and call this group the symmetric group.

Example 16.7. Let R be a field and consider the set

$$C(R) = \{(x, y) \in R \times R; x^2 + y^2 = 1\};$$

one can refer to this set as the “circle over R ”. Then $C(R)$ is an Abelian group with $e = (1, 0)$, $(x, y)' = (x, -y)$,

$$(x_1, y_1) \star (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1).$$

Exercise 16.8. Consider the circle $C(\mathbb{F}_{17})$. Show that $(\bar{3}, \bar{3}), (\bar{1}, \bar{0}) \in C(\mathbb{F}_{17})$ and compute $(\bar{3}, \bar{3}) \star (\bar{1}, \bar{0})$ and $2(\bar{1}, \bar{0})$ (where the latter is of course $(\bar{1}, \bar{0}) \star (\bar{1}, \bar{0})$).

Example 16.9. Let R be a field in which $2 := 1 + 1 \neq 0$, $3 := 1 + 1 + 1 \neq 0$, let $a, b \in R$ be such that $4a^3 + 27b^2 \neq 0$, and consider what is called an “elliptic curve” over R :

$$E(R) = \{(x, y) \in R \times R; y^2 = x^3 + ax + b\} \cup \{\infty\},$$

where ∞ here is just a symbol. We call $E(R)$ the elliptic curve over R defined by the equation $y^2 = x^3 + ax + b$. If $(x, y) \in E(R)$ define $(x, y)' = (x, -y)$. Also define $\infty' = \infty$. Define $(x, y) \star (x, -y) = \infty$, $\infty \star (x, y) = (x, y) \star \infty = (x, y)$, and $\infty \star \infty = \infty$. Finally, for $(x_1, y_1), (x_2, y_2) \in E(R)$ with $(x_2, y_2) \neq (x_1, -y_1)$ we define

$$(x_1, y_1) \star (x_2, y_2) = (x_3, -y_3)$$

where (x_3, y_3) is the “third point of intersection of $E(R)$ with the line L_{12} passing through (x_1, y_1) and (x_2, y_2) ”. The latter needs an explanation/definitions. If $(x_1, y_1) \neq (x_2, y_2)$ then L_{12} is by definition the set

$$L_{12} = \{(x, y) \in R \times R; y - y_1 = m(x - x_1)\}$$

where

$$m = (y_2 - y_1)(x_2 - x_1)^{-1}$$

which looks like the usual expression for the line passing through the two points in analytic geometry (and m plays the role of slope). If $(x_1, y_1) = (x_2, y_2)$ and $y_1 \neq 0$ one needs to replace m in the above definition of L_{12} by

$$m = (3x_1^2 + a)(2y_1)^{-1}$$

which looks like the slope of the tangent to the curve in analytic geometry. Once we defined L_{12} we define (x_3, y_3) by solving the system consisting of the equations defining $E(R)$ and L_{12} : replacing y in $y^2 = x^3 + ax + b$ by $y_1 + m(x - x_1)$ we get a cubic equation in x :

$$(y_1 + m(x - x_1))^2 = x^3 + ax + b$$

which can be rewritten as

$$x^3 - m^2x^2 + \dots = 0.$$

x_1, x_2 are known to be roots of this equation. We define x_3 to be the third root which is then

$$x_3 = m^2 - x_1 - x_2;$$

so we define

$$y_3 = y_1 + m(x_3 - x_1).$$

Then $E(R)$ with above definitions is an Abelian group; it is one of the most interesting groups encountered in number theory. Note that if $R = \mathbb{F}_p$ then $E(R)$ is a finite group. Its cardinality $|E(\mathbb{F}_p)|$ is an extremely interesting number depending on p, a, b .

Exercise 16.10. Check that in all of the examples above the axioms for a group are satisfied. N.B. This is rather intricate in the last example.

Exercise 16.11. Consider the group $E(\mathbb{F}_{13})$ defined by the equation $y^2 = x^3 + \bar{8}$. Show that $(\bar{1}, \bar{3}), (\bar{2}, \bar{4}) \in E(\mathbb{F}_{13})$ and compute $(\bar{1}, \bar{3}) \star (\bar{2}, \bar{4})$ and $2(\bar{2}, \bar{4})$ (where the latter is of course $(\bar{2}, \bar{4}) \star (\bar{2}, \bar{4})$).

17. LINEAR CONGRUENCES

Definition 17.1. A linear congruence is an expression of the form $ax \equiv b \pmod{m}$. A solution $x = c$ to this congruence is an integer c such that $ac \equiv b \pmod{m}$. Two linear congruences are equivalent if they have the same solutions.

Proposition 17.2. Let $ax \equiv b \pmod{m}$ be a linear congruence. Let $d = \gcd(a, m)$ and let S be a complete residue system mod m .

- 1) If $d \nmid b$ the congruence has no solution in S .
- 2) If $d \mid b$ the congruence has d solutions in S .

Proof. 1) Assume there is a solution $x = c$. Then $m \mid ac - b$. Since $d \mid a$ and $d \mid m$ we get $d \mid b$, a contradiction.

2) Let $a = da_1$, $b = db_1$, $m = dm_1$. Then our congruence is equivalent to $a_1x \equiv b_1 \pmod{m_1}$. Since $\gcd(a_1, m_1) = 1$ a_1 has an inverse a_1' mod m_1 so the latter congruence is equivalent to $a_1'a_1x \equiv a_1'b_1 \pmod{m_1}$ hence to $x \equiv a_1'b_1 \pmod{m_1}$. The latter has a unique solution c in $\{0, \dots, m_1 - 1\}$ and hence the solutions

$$c, c + m_1, c + 2m_1, \dots, c + (d - 1)m_1$$

in $\{0, \dots, m - 1\}$. Hence there are d solutions in $\{0, \dots, m - 1\}$. Hence there are d solutions in S . \square

Exercise 17.3. Solve the congruence $33x \equiv 27 \pmod{51}$.

Exercise 17.4. Find the remainder when $26!$ is divided by 29. Hint: By Wilson $26! \times (29 - 2) \times (29 - 1) \equiv -1 \pmod{29}$. So $26! \equiv -2' \pmod{29}$ where $2'$ is an inverse of 2 mod 29.

18. SYSTEMS OF LINEAR CONGRUENCES

Theorem 18.1. (*Chinese Remainder Theorem*). Assume one is given a system of linear congruences

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\dots \\ x &\equiv b_n \pmod{m_n} \end{aligned}$$

such that $\gcd(m_i, m_j) = 1$ for all $i \neq j$ and let S be a complete residue system modulo $M = m_1m_2\dots m_n$. Then the system has a unique solution in S .

Proof. To prove existence of the solution let $M_i = M/m_i$ and let M_i' be an inverse of M_i mod m_i i.e. $M_iM_i' \equiv 1 \pmod{m_i}$. Then it is easy to check that $c = b_1M_1M_1' + \dots + b_nM_nM_n'$ is a solution of the system. Uniqueness of the solution is easy. \square

Exercise 18.2. Why does M_i' in the above proof exist? Why is c a solution? Prove uniqueness.

Exercise 18.3. Find a solution to the system:

$$\begin{aligned}x &\equiv 23 \pmod{56} \\x &\equiv 11 \pmod{27} \\x &\equiv 10 \pmod{65}\end{aligned}$$

Exercise 18.4. A famous battle is known to have taken place not more than 3000 years ago. It is known that it took place 2 years after a solar eclipse and 7 years after a Moon eclipse. Assume (this is definitely not the case in our world) that solar eclipses take place every 41 years and Moon eclipses take place every 53 years. Assume moreover that a solar eclipse took place in 2009 and a Moon eclipse took place in 1999. Find the year when the battle took place. Note: although this exercise is not realistic, the method suggested by this exercise (to date historical events based on eclipses) is one of the main methods originally used by astronomers (e.g. by Scaliger and Petavius in the 17th century) to establish the chronology of world history accepted today.

19. FERMAT'S LITTLE THEOREM

Theorem 19.1. (*Fermat's Little Theorem*). *If a is an integer and p is a prime then $a^p \equiv a \pmod{p}$ (i.e. $p \mid a^p - a$).*

We will give two proofs.

Euler's Proof. If $p \nmid a$ we are done so we may assume $p \mid a$. Consider the complete residue system mod p , $\{0, 1, 2, 3, \dots, p-1\}$. Then

$$\{0, a, 2a, 3a, \dots, (p-1)a\}$$

is also a complete residue system mod p because if $ia \equiv ja \pmod{p}$ for some $i \neq j$ then (since $\gcd(a, p) = 1$) we get $i \equiv j \pmod{p}$ hence $i = j$, a contradiction. So we have

$$\{r_p(0), r_p(a), r_p(2a), \dots, r_p((p-1)a)\} = \{0, 1, 2, \dots, p-1\}.$$

Since $r_p(0) = 0$ and $r_p(ia) \equiv ia \pmod{p}$ we have

$$\begin{aligned}(p-1)! &= 1 \times 2 \times 3 \times \dots \times (p-1) \\ &= r_p(a) \times r_p(2a) \times r_p(3a) \times \dots \times r_p((p-1)a) \\ &\equiv (a) \times (2a) \times (3a) \times \dots \times ((p-1)a) \pmod{p} \\ &\equiv (p-1)! \times a^{p-1} \pmod{p}.\end{aligned}$$

By Euclid's Lemma $\gcd((p-1)!, p) = 1$ so we may divide by $(p-1)!$ to get

$$1 \equiv a^{p-1} \pmod{p}.$$

Multiplying by a we get $a \equiv a^p \pmod{p}$. □

Leibniz's Proof. It is enough to prove the theorem for $a \in \mathbb{N}$. We proceed by induction on a . The statement is clear for $a = 1$. Now assume the statement is true for $b = a - 1$, i.e. $b^p \equiv b \pmod{p}$. By "Freshman's Dream" (Exercise 11.10, 4)) we get

$$a^p \equiv (b+1)^p \equiv b^p + 1 \equiv b + 1 \equiv a \pmod{p},$$

a contradiction. □

Remark 19.2. There are examples of primes p such that $p^2 | 2^p - 2$ and examples of primes p such that $p^2 \nmid 2^p - 2$. It is conjectured that there are infinitely many primes p such that $p^2 \nmid 2^p - 2$.

Exercise 19.3. Prove that for any integers a, b and any prime p we have $p | a^p b - b^p a$.

Exercise 19.4. Prove that if p is prime and $a \equiv b \pmod{p^n}$ then $a^p \equiv b^p \pmod{p^{n+1}}$.

20. EULER'S THEOREM

Recall that two integers are called coprime if their \gcd is 1.

Definition 20.1. For any integer $n \geq 2$ let $\phi(n)$ be the number of positive integers less than n and coprime to n . Equivalently, if

$$U_n = \{x \in \mathbb{N}; 1 \leq x \leq n-1, \gcd(x, n) = 1\}$$

then $\phi(n) = |U_n|$. We also set $\phi(1) = 1$.

Proposition 20.2. If p is prime and $n \geq 1$ then $\phi(p^n) = p^n - p^{n-1}$.

Proof. U_{p^n} is obtained from $S = \{0, 1, 2, \dots, p^n - 1\}$ by removing the set T of all the numbers divisible by p . The number of elements of S is p^n . Now the set T is in bijection with $S' = \{0, \dots, p^{n-1}\}$ (the bijection is given by $F : S' \rightarrow T, F(x) = px$, cf. the Exercise below). So T has p^{n-1} elements and we are done. \square

Exercise 20.3. Check that F in the proof above is bijective.

Proposition 20.4. $\phi(mn) = \phi(m)\phi(n)$ for m and n coprime.

Proof. The map $F : U_{mn} \rightarrow U_m \times U_n$ defined by

$$F(x) = (r_m(x), r_n(x))$$

is bijective by the Chinese Remainder Theorem (cf. the Exercise below). So $|U_{mn}| = |U_m \times U_n| = |U_m| \times |U_n|$ and we are done. \square

Exercise 20.5. Check that F in the proof above is bijective.

Corollary 20.6. If $n = p_1^{e_1} \dots p_s^{e_s}$ with p_1, \dots, p_s distinct primes and $e_1, \dots, e_s \geq 1$ then

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \dots (p_s^{e_s} - p_s^{e_s-1}).$$

Exercise 20.7. Compute $\phi(7200)$.

Exercise 20.8. Prove that for each integer c the set $\{n; \phi(n) = c\}$ is finite.

Theorem 20.9. (Euler). For any integer a coprime to an integer $m \geq 1$ we have $a^{\phi(m)} \equiv 1 \pmod{m}$

Proof. Entirely analogous to the proof given above (due to Euler) of Fermat's Little Theorem; cf. the Exercise below. \square

Exercise 20.10. Provide the proof for the above Theorem. More generally prove that if G is an Abelian group with n elements then $a^n = e$ for all $a \in G$; here $a^n = a \star a \star \dots \star a$ (n times). (This statement is also true if G is not Abelian but the proof is harder.)

Exercise 20.11. Find the last 2 digits in the decimal expansion of $13^{40,000,000,002}$. Hint: we need the remainder when this number is divided by 100; use the fact that $\phi(100) = 40$ and $3^{40} \equiv 1 \pmod{100}$.

Exercise 20.12. Prove that if m is square free (i.e. not divisible by any square of a prime) and if a is *any* integer (not necessarily coprime to m) then

$$a^{\phi(m)+1} \equiv a \pmod{m}.$$

Hint: it is enough to prove the above congruence mod p for any prime $p|m$. For each such p apply then Fermat's Little Theorem 19.1. (So Euler's theorem is not necessary for this Exercise.)

21. POLYNOMIAL CONGRUENCES

Definition 21.1. A polynomial with integer coefficients is an expression of the form

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

where $a_0, \dots, a_n \in \mathbb{Z}$. (A more rigorous way to define a polynomial would be to identify it with a map $a : \{0, 1, \dots, n\} \rightarrow \mathbb{Z}$ with $a(k) = a_k$.) The number a_k is called the coefficient of x^k in $f(x)$. If $a_n \neq 0$ we say that f has degree n and write $\deg(f) = n$; a_n is then called the top coefficient of $f(x)$. For an integer $c \in \mathbb{Z}$ we set

$$f(c) = a_n c^n + a_{n-1} c^{n-1} + \dots + a_1 c + a_0.$$

If the top coefficient is 1 we say that $f(x)$ is monic. We denote by $\mathbb{Z}[x]$ the set of all polynomials with integer coefficients.

Example 21.2. $f(x) = 5x^3 - 4x^2 - 17$ is a polynomial of degree 3 and $f(2) = 5 \times 2^3 - 4 \times 2^2 - 17$. This polynomial is not monic. The polynomial $g(x) = x^8 - 3x^5 + x - 7$ is monic. The polynomial $f(x) = 0$ is taken to be of degree zero.

Definition 21.3. The sum and the product of two polynomials

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

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$$

are the polynomials denoted by $f(x) + g(x)$ and $f(x) \times g(x) = f(x)g(x)$ defined by asking that the coefficient of x^k in $f(x) + g(x)$ be $a_k + b_k$ and the coefficient of x^k in $f(x)g(x)$ be

$$a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \dots + a_k b_0.$$

Example 21.4.

$$\begin{aligned} & (3x^2 + 5x + 1)(8x^3 + 7x^2 - 2x - 1) = \\ & = (3 \times 8)x^5 + (3 \times 7 + 5 \times 8)x^4 + (3 \times (-2) + 5 \times 7 + 1 \times 8)x^3 + \dots \end{aligned}$$

Exercise 21.5. Prove that $\mathbb{Z}[x]$ is a ring with respect to the operations $+$ and \times defined above.

Proposition 21.6. (*Long division*). Let $f(x), g(x) \in \mathbb{Z}[x]$ with $g(x)$ monic of degree ≥ 1 . Then there exist unique $q(x), r(x) \in \mathbb{Z}[x]$ such that

$$f(x) = g(x)q(x) + r(x)$$

and $\deg(r) < \deg(g)$.

Proof. Fix g (of degree m) and let us prove by induction on n that the statement above is true if $\deg(f) \leq n$. The case $\deg(f) = 0$ is clear because we can then take $q(x) = 0$ and $r(x) = f(x)$. For the induction step we may take f of degree n and let a_n be the top coefficient of f . We may assume $n \geq m$. Then $\deg(f - a_n x^{n-m} g) \leq n - 1$ so by the induction hypothesis $f(x) - a_n x^{n-m} g(x) = g(x)q(x) + r(x)$ with $\deg(r) < m$. So $f(x) = g(x)(a_n x^{n-m} + q(x)) + r(x)$, and we are done. \square

Definition 21.7. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial and p a prime. An integer $c \in \mathbb{Z}$ is called a root of $f(x) \pmod{p}$ (or a solution to the congruence $f(x) \equiv 0 \pmod{p}$) if $f(c) \equiv 0 \pmod{p}$, in other words if $p|f(c)$. We denote by $N_p(f)$ the number of roots of $f(x) \pmod{p}$ contained in a fixed complete residue system. If f, g are polynomials we write $N_p(f = g)$ for $N_p(f - g)$. If $Z_p(f)$ is the set of roots of $f \pmod{p}$ in the complete residue system $\{0, 1, \dots, p-1\}$ then of course $N_p(f) = |Z_p(f)|$.

Example 21.8.

- 1) 3 is a root of $x^3 + x - 13 \pmod{17}$.
- 2) Any integer a is a root of $x^p - x \pmod{p}$; this is Fermat's Little Theorem. In particular $N_p(x^p - x) = p$, $N_p(x^{p-1} - 1) = p - 1$.
- 3) Any solution to a linear congruence $ax \equiv b \pmod{p}$ is a root of $ax - b \pmod{p}$ hence a solution to $ax - b \equiv 0 \pmod{p}$. So $N_p(ax - b) = 1$ if $p \nmid a$.
- 4) $N_p(x^2 - 1) = 2$ if $p \neq 2$.

Proposition 21.9. For any two polynomials $f, g \in \mathbb{Z}[x]$ we have

$$N_p(fg) \leq N_p(f) + N_p(g).$$

Proof. Clearly $Z_p(fg) \subset Z_p(f) \cup Z_p(g)$. Hence

$$|Z_p(fg)| = |Z_p(f) \cup Z_p(g)| \leq |Z_p(f)| + |Z_p(g)|.$$

\square

Remark 21.10. Fix a polynomial $f(x) \in \mathbb{Z}[x]$. Some of the deepest problems and theorems in number theory can be formulated as special cases of the following two problems:

- 1) Understand the set of primes p such that the congruence $f(x) \equiv 0 \pmod{p}$ has a solution or, equivalently, such that $p|f(c)$ for some $c \in \mathbb{Z}$.
- 2) Understand the set of primes p such that $p = f(c)$ for some $c \in \mathbb{Z}$.

In regards to problem 1) one would like more generally to understand the function whose value at a prime p is the number $N_p(f)$. In particular one would like to understand the set of all primes p such that $N_p(f) = k$ for a given k (equivalently such that the congruence $f(x) \equiv 0 \pmod{p}$ has k solutions in a complete residue system mod p .) We note that if $\deg(f) = 1$ the problem is trivial. For $\deg(f) = 2$ the problem is already highly non-trivial although a complete answer was given by Gauss in his Quadratic Reciprocity Law. For the quadratic polynomial $f(x) = x^2 + 1$, for instance one can prove (without using quadratic reciprocity) that $p|f(c)$ for some c if and only if p is of the form $4k+1$. For $\deg(f)$ arbitrary the problem (and its generalizations for polynomials $f(x, y, z, \dots)$ of several variables) is essentially open and part of an array of tantalizing conjectures (called the Langlands program) that link the function $N_p(f)$ to Fourier analysis and the theory of complex analytic functions. This is beyond the scope of our course.

In regards to problem 2) note that the statement that there are infinitely many primes of the form $4k + 3$ can be restated as saying that there are infinitely many primes p such that $p = f(c)$ for some c where $f(x) = 4x + 3$. This was generalized by Dirichlet to any linear polynomial $f(x) = ax + b$ for which a and b are coprime. But it is not known, for instance, if there are infinitely many primes p such that $p = f(c)$ for some c when $f(x)$ is a quadratic polynomial such as $f(x) = x^2 + 1$. Problem 2) has an obvious analogue for polynomials in several variables. The result (which will be proved later) stating that the primes p with $p \equiv 1 \pmod{4}$ are exactly the primes such that $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$ fits then into the pattern of 2): one needs only to take $f(x, y) = x^2 + y^2$.

22. LANGRANGE'S THEOREM

Theorem 22.1. (*Lagrange*). *Assume $f \in \mathbb{Z}[x]$ is a polynomial of degree d and p is a prime not dividing all the coefficients of f . Then the congruence $f(x) \equiv 0 \pmod{p}$ has at most d solutions in any complete residue system mod p . In other words $N_p(f) \leq d$.*

Proof. Assume there exists a polynomial f of degree d such that p does not divide all the coefficients of f and such that $N_p(f) > d$. Choose f such that d is minimal and seek a contradiction. Let $a_1, \dots, a_{d+1} \in \mathbb{Z}$ be distinct roots of $f \pmod{p}$ in a complete residue system mod p . By Long Division we can write

$$f(x) = (x - a_{d+1})g(x) + r(x)$$

with $\deg(r) < \deg(x - a_{d+1}) = 1$. So $\deg(r) = 0$ i.e. $r(x) = c \in \mathbb{Z}$. Since $f(a_{d+1}) \equiv 0 \pmod{p}$ we get $p|f(a_{d+1}) = c$. Since $p|f(a_k) = (a_k - a_{d+1})g(a_k) + c$ for $k = 1, \dots, d$ it follows that $p|(a_k - a_{d+1})g(a_k)$. Since p is prime and $p \nmid a_k - a_{d+1}$ for $k = 1, \dots, d$ it follows that $p|g(a_k)$ for $k = 1, \dots, d$. By the minimality of d this implies that p divides all the coefficients of $g(x)$. Since $p|c$ this implies that p divides all the coefficients of $f(x)$, a contradiction. \square

Corollary 22.2. *Assume $p \equiv 1 \pmod{d}$. Then $N_p(x^d - 1) = d$.*

Proof. By Lagrange's Theorem $N_p(x^d - 1) \leq d$. Assume $N_p(x^d - 1) < d$ and seek a contradiction. If $p - 1 = kd$ then $x^{p-1} - 1 = (x^d - 1)g(x)$ where

$$g(x) = x^{d(k-1)} + x^{d(k-2)} + \dots + x^d + 1.$$

Since by Lagrange's Theorem $N_p(g) \leq d(k-1)$ we get

$p-1 = N_p(x^{p-1} - 1) = N_p((x^d - 1)g) \leq N_p(x^d - 1) + N_p(g) < d + d(k-1) = dk = p-1$, a contradiction. \square

Corollary 22.3.

1) *If $p \equiv 1 \pmod{4}$ then $N_p(x^2 = -1) = 2$. Equivalently any prime p of the form $4k + 1$ divides some number of the form $c^2 + 1$.*

2) *If $p \equiv 3 \pmod{4}$ then $N_p(x^2 = -1) = 0$. Equivalently no prime p of the form $4k + 3$ can divide a number of the form $c^2 + 1$.*

Proof. 1) By Corollary 22.2 if $p \equiv 1 \pmod{4}$ then $N_p(x^4 - 1) = 4$. But $4 = N_p(x^4 - 1) \leq N_p((x^2 - 1)(x^2 + 1)) \leq N_p(x^2 - 1) + N_p(x^2 + 1) \leq N_p(x^2 + 1) + 2$ hence $N_p(x^2 + 1) \geq 2$ and we are done.

2) Assume $p \equiv 3 \pmod{4}$ so $p = 4k + 3$ and assume $N_p(x^2 = -1) > 0$ so there exists $c \in \mathbb{Z}$ such that $c^2 \equiv -1 \pmod{p}$; we want to derive a contradiction. We have (by Fermat's Little Theorem) that $c^p \equiv c \pmod{p}$. Since $p \nmid c$ we get $c^{p-1} \equiv 1 \pmod{p}$. But

$$c^{p-1} \equiv c^{4k+2} \equiv (c^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \pmod{p},$$

a contradiction. \square

Exercise 22.4. Consider the polynomials

$$f(x) = x^{p-1} - 1 \text{ and } g(x) = (x-1)(x-2)\dots(x-p+1) \in \mathbb{Z}[x].$$

Prove that all the coefficients of the polynomial $f(x) - g(x)$ are divisible by p . Conclude that p divides the sums

$$\sum_{a=1}^{p-1} a = 1 + 2 + 3 + \dots + (p-1)$$

and

$$\sum_{1 \leq a < b \leq p-1} ab = 1 \times 2 + 1 \times 3 + \dots + 1 \times (p-1) + 2 \times 3 + \dots + 2 \times (p-1) + \dots + (p-2) \times (p-1).$$

Exercise 22.5. Assume $p \geq 5$ is a prime. Prove that the numerator of any fraction that is equal to

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1}$$

is divisible by p^2 .

Exercise 22.6. Prove that there are infinitely many primes of the form $4k + 1$. Hint: Assume this is false and let p_1, \dots, p_n be all the primes of the form $4k + 1$. By Corollary part 2) in 22.3 all the primes dividing the number

$$N = (2p_1 \dots p_n)^2 + 1$$

are of the form $4k + 1$ and derive a contradiction.

Exercise 22.7. Prove that:

1) If $p \equiv 1 \pmod{3}$ then $N_p(x^2 + x + 1) = 2$. Equivalently any prime p of the form $3k + 1$ divides some number of the form $c^2 + c + 1$.

2) If $p \equiv 2 \pmod{3}$ then $N_p(x^2 + x + 1) = 0$. Equivalently no prime p of the form $3k + 2$ can divide a number of the form $c^2 + c + 1$.

23. ORDER

Definition 23.1. Let a and m be coprime integers. The order of $a \pmod{m}$ is the smallest positive integer k such that $a^k \equiv 1 \pmod{m}$. We write $k = o_m(a)$.

In other words:

- 1) $a^k \equiv 1 \pmod{m}$,
- 2) $a^n \equiv 1 \pmod{m}$ for $n \geq 1$ implies $k \leq n$.

The definition makes sense because the set of positive integers n such that

$$a^n \equiv 1 \pmod{m}$$

is non-empty (it contains $\phi(m)$ by Euler's Theorem).

Exercise 23.2. Prove that $o_{31}(2) = 5$.

Proposition 23.3. $o_m(a) = k$ if and only if

- 1) $a^k \equiv 1 \pmod{m}$,
- 2) $a^N \equiv 1 \pmod{m}$ for $N \geq 1$ implies $k|N$.

Proof. The if part is clear because $k|N$ implies $k \leq N$. To prove the only if part assume $o_m(a) = k$. Then 1) is clear. To check 2) write $N = kq + r$ with $0 \leq r < k$. Then

$$1 \equiv a^N \equiv (a^k)^q \times a^r \equiv a^r \pmod{m}$$

so $r = 0$ by 2) in Definition 23.1. □

Corollary 23.4. $o_m(a) | \phi(m)$.

Proposition 23.5. Assume $o_m(a)$ and $o_m(b)$ are coprime. Then

$$o_m(ab) = o_m(a)o_m(b).$$

Proof. Set $k = o_m(a)$, $l = o_m(b)$. We use Proposition 23.3. Clearly

$$(ab)^{kl} \equiv (a^k)^l (b^l)^k \equiv 1 \pmod{m}.$$

Now assume $(ab)^N \equiv 1 \pmod{m}$. Raising to power l we get $a^{Nl}b^{Nl} \equiv 1 \pmod{m}$ hence $a^{Nl} \equiv 1 \pmod{m}$ hence $k|Nl$. Since k and l are coprime $k|N$. In a similar way raising $(ab)^N \equiv 1 \pmod{m}$ to power k we get $a^{Nk}b^{Nk} \equiv 1 \pmod{m}$ hence $b^{Nk} \equiv 1 \pmod{m}$ hence $l|Nk$ hence $l|N$. Again since k and l are coprime $l|N$ and $k|N$ imply $kl|N$ and we are done. □

Exercise 23.6. Prove that if $o_m(a) = kl$ then $o_m(a^k) = l$.

Exercise 23.7. Let G be a finite group and let $|G|$ denote the number of elements of G (the number $|G|$ is called the order of G). Prove that for any $x \in G$ there exists an integer $n \geq 1$ such that $x^n = e$. Define the order of an element $x \in G$ as the smallest integer $n \geq 1$ such that $x^n = e$. Denote by $|x|$ the order of x . Prove that for G Abelian $|x|$ divides $|G|$. (This statement is also true for G non-Abelian but the proof is harder.)

Remark 23.8. If $a \in \mathbb{Z}$ is not divisible by a prime p and $\bar{a} \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is the residue class of a then $o_p(a)$ is equal to the order $|\bar{a}|$ of \bar{a} in the group \mathbb{F}_p^\times .

24. PRIMITIVE ROOTS

Definition 24.1. An integer g is a primitive root mod m if it is coprime to m and $o_m(g) = \phi(m)$.

Exercise 24.2. Prove that g is a primitive root mod m if and only if it is coprime to m and

$$g^{\phi(m)/q} \not\equiv 1 \pmod{m}$$

for all prime $q | \phi(m)$.

Exercise 24.3. Prove that there is no primitive root mod 8

Exercise 24.4. Prove that 3 is a primitive root mod 7.

Exercise 24.5. Let g be a primitive root mod m and let a, b be integers. Prove that

$$g^a \equiv g^b \pmod{m}$$

if and only if

$$a \equiv b \pmod{\phi(m)}.$$

Exercise 24.6. Prove that if g is a primitive root mod a prime p then

$$\{0, 1, g, g^2, g^3, \dots, g^{p-2}\}$$

is a complete residue system mod p .

Exercise 24.7. Solve the congruence $3^{5x+2} \equiv 3^3 \pmod{7}$.

The following Theorem was proved by Gauss:

Theorem 24.8. (*Existence of primitive roots*). If p is a prime there exists a primitive root mod p .

Proof. Let $p - 1 = p_1^{e_1} \dots p_s^{e_s}$ with p_1, \dots, p_s distinct primes and $e_1, \dots, e_s \geq 1$. Let $i \in \{1, \dots, s\}$. By Corollary 22.2 $N_p(x^{p_i^{e_i}} - 1) = p_i^{e_i}$ and $N_p(x^{p_i^{e_i-1}} - 1) = p_i^{e_i-1}$. So $x^{p_i^{e_i}} - 1$ has a root c_i mod p which is not a root mod p of $x^{p_i^{e_i-1}} - 1$. So

$$c_i^{p_i^{e_i}} \equiv 1 \pmod{p},$$

$$c_i^{p_i^{e_i-1}} \not\equiv 1 \pmod{p}.$$

It follows that the order of c_i is a divisor of $p_i^{e_i}$ but not a divisor of $p_i^{e_i-1}$. Hence

$$o_p(c_i) = p_i^{e_i}.$$

By Proposition 23.5

$$o_p(c_1 \dots c_s) = p_1^{e_1} \dots p_s^{e_s} = p - 1$$

so $c_1 \dots c_s$ is a primitive root mod p . \square

Exercise 24.9. Prove that if p and n is a natural number not divisible by $p - 1$ then p divides the sum

$$\sum_{a=1}^{p-1} a^n = 1^n + 2^n + 3^n + \dots + (p-1)^n.$$

Hint: If g is a primitive root mod p then the above sum is congruent mod p to $S = \sum_{i=0}^{p-2} g^{in}$; also

$$(g^n - 1)S = g^{n(p-1)} - 1 \equiv 0 \pmod{p}.$$

25. DISCRETE LOGARITHM

Definition 25.1. Assume g is a primitive root mod a prime p and consider the map

$$\exp_g : \{0, 1, \dots, p-2\} \rightarrow \{1, \dots, p-1\}$$

defined by $\exp_g a = r_p(g^a)$. Since $o_p(g) = p - 1$ this map is injective and hence surjective. Its inverse is called the discrete logarithm and is denoted by

$$\log_g : \{1, \dots, p-1\} \rightarrow \{0, 1, \dots, p-2\}.$$

So if $b \equiv g^a \pmod{p}$ for $a \in \{0, 1, \dots, p-2\}$ then $a = \log_g b$. More generally we define

$$\log_g : \{b \in \mathbb{Z}; b \not\equiv 0 \pmod{p}\} \rightarrow \{0, 1, \dots, p-2\}$$

by setting

$$\log_g b = \log_g(r_p(b)).$$

Exercise 25.2. Prove that

$$\log_g(bc) \equiv \log_g b + \log_g c \pmod{p-1}$$

for all b, c not divisible by p .

Remark 25.3. No algorithm running in polynomial time is known that computes $\log_g b$ for given b . Any such algorithm would compromise the security of some important public key cryptographic schemes that are in use today.

Exercise 25.4. Prove that for any integer a coprime to a prime $p \neq 2$ we have that

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

Hint: $(a^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$.

Proposition 25.5. Assume $p \neq 2$. Let g be a primitive root mod p and a an integer not divisible by p . Then the following are equivalent:

- 1) The congruence $x^2 \equiv a \pmod{p}$ has a solution;
- 2) $N_p(x^2 = a) = 2$,
- 3) $\log_g a$ is even,
- 4) $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Proof. 1) implies 2) because if c is a solution then $p-c$ is also a solution and $c \not\equiv p-c \pmod{p}$. 2) implies 1) trivially. Now write $a \equiv g^b \pmod{p}$, $x \equiv g^y \pmod{p}$. The congruence

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

is equivalent to

$$g^{2y} \equiv g^b \pmod{p}$$

and hence equivalent to the congruence

$$2y \equiv b \pmod{p-1}.$$

The latter has a solution if and only if $\gcd(2, p-1) | b$ hence if and only if b is even. This proves that 1) and 3) are equivalent. Finally 4) is equivalent to

$$g^{\frac{b(p-1)}{2}} \equiv g^0 \pmod{p}$$

which is equivalent to

$$\frac{b(p-1)}{2} \equiv 0 \pmod{p-1}$$

hence to

$$b(p-1) \equiv 0 \pmod{2(p-1)}$$

hence to $2(p-1) | b(p-1)$ hence to $2 | b$. This proves the equivalence of 3) and 4). \square

Exercise 25.6. Let p be a prime such that $p \equiv 1 \pmod{m}$. Let g be a primitive root mod p and a an integer not divisible by p . Prove that the following are equivalent:

- 1) The congruence $x^m \equiv a \pmod{p}$ has a solution;
- 2) $m \mid \log_g a$,
- 3) $a^{\frac{p-1}{m}} \equiv 1 \pmod{p}$.

Exercise 25.7. Let p be a prime, let $m \geq 1$ be an integer coprime to $p-1$, and let a be any integer. Prove that the congruence $x^m \equiv a \pmod{p}$ has a solution.

Exercise 25.8. Let p be a prime and c be an integer. Prove that there exist integers a, b such that $c \equiv a^2 + b^2 \pmod{p}$. Hint: The set

$$A = \{r_p(a^2); a \in \mathbb{Z}\} \subset S = \{0, \dots, p-1\}$$

has $\frac{p+1}{2}$ elements. Hence the set

$$B = \{r_p(c-x); x \in A\} \subset S$$

also has $\frac{p+1}{2}$ elements. Since $|A| + |B| > |S|$ we must have $A \cap B \neq \emptyset$, so $c - b^2 \equiv a^2 \pmod{p}$ for some a and b .

26. LEGENDRE SYMBOL

Let p be a prime $\neq 2$.

Definition 26.1. If a is any integer define the Legendre symbol

$$\left(\frac{a}{p}\right) = N_p(x^2 = a) - 1,$$

i.e. the Legendre symbol is $-1, 0, 1$ according as $x^2 \equiv a \pmod{p}$ has 2 solutions, one solution (this is the case if and only if $p \mid a$), or no solution respectively.

Exercise 26.2. Prove that

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

Lemma 26.3. (Euler).

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

Proof. This is a reformulation of Proposition 25.5, the equivalence of 2) and 4). (Cf. also Exercise 25.4.) \square

Corollary 26.4. (Euler). $\left(\frac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{4}$.

Lemma 26.5. (Euler) $\left(\frac{2}{p}\right) = 1$ if and only if $p \equiv 1, 7 \pmod{8}$.

Proof. First we claim that $\left(\frac{2}{p}\right) = (-1)^\mu$ where μ is the number of integers in the set $\{2, 4, 6, \dots, p-1\}$ congruent mod p to a negative integer between $-\frac{p}{2}$ and $\frac{p}{2}$. Indeed let $r_1, \dots, r_{\frac{p-1}{2}}$ be the integers between $-\frac{p}{2}$ and $\frac{p}{2}$ that are congruent mod p to $2, 4, 6, \dots, p-1$. Then it is easy to check that

$$\{|r_1|, \dots, |r_{\frac{p-1}{2}}|\} = \{1, 2, 3, \dots, \frac{p-1}{2}\},$$

where $|r|$ is the absolute value of r i.e. r or $-r$ according as r is positive or negative. Taking products we get

$$1 \times 2 \times 3 \times \dots \times \frac{p-1}{2} \equiv (-1)^\mu \times 2^{\frac{p-1}{2}} \times 1 \times 2 \times 3 \times \dots \times \frac{p-1}{2} \pmod{p}$$

which proves our claim.

Now note that if an integer a between $-\frac{p}{2}$ and 0 is congruent mod p to one of the numbers $2, 4, 6, \dots, p-1$ then $2x \equiv a \pmod{p}$ for some $x \in \{1, 2, 3, \dots, \frac{p-1}{2}\}$. Writing $a = 2x + mp$ we get $-\frac{p}{2} < 2x + mp < 0$ hence $\frac{p}{2} < 2x + (m+1)p < p$ which forces $m = -1$ hence $\frac{p}{2} < 2x < p$. Conversely if the latter holds then $a = 2x - p$ is between $-\frac{p}{2}$ and 0 . So if $p = 8k + r$, $0 \leq r < 7$, we have

$$\begin{aligned} \mu &= |\{x \in \mathbb{Z}; \frac{p}{2} < 2x < p\}| \\ &= |\{x \in \mathbb{Z}; \frac{p}{4} < x < \frac{p}{2}\}| \\ &= |\{x \in \mathbb{Z}; 2k + \frac{r}{4} < x < 4k + \frac{r}{2}\}| \\ &= |\{x \in \mathbb{Z}; \frac{r}{4} < x < 2k + \frac{r}{2}\}| \end{aligned}$$

and we conclude by inspecting the values $r = 1, 3, 5, 7$. \square

Exercise 26.6.

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

Hint. The terms equal to 1 in the sum correspond to those a 's whose discrete logarithm is even (cf. Proposition 25.5) while the terms equal to -1 correspond to those a 's whose logarithm is odd. But the number of odd numbers between $0, \dots, p-2$ is equal to that of even numbers.

Exercise 26.7. Let $E(\mathbb{F}_p)$ be the elliptic curve over \mathbb{F}_p attached to the cubic equation $y^2 = x^3 + \bar{a}x + \bar{b}$ where $a, b \in \mathbb{Z}$. Prove that the cardinality (order) of the group $E(\mathbb{F}_p)$ is given by

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p}\right).$$

Prove that if in addition $p|a$ and $p \equiv 2 \pmod{3}$ then $|E(\mathbb{F}_p)| = p + 1$. Hint: for the last statement use Exercise 25.7 to show that the map $f(x) = x^3 + \bar{b}$ is a bijection $\mathbb{F}_p \rightarrow \mathbb{F}_p$. Then use Exercise 26.6.

The main result pertaining to the Legendre symbol is the following theorem of Gauss:

Theorem 26.8. (*Quadratic Reciprocity Law*). For any two distinct primes p and q different from 2 we have

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

This can be proved using integers only but we postpone the proof (and do not use the result) until we introduce algebraic integers.

Theorem 26.8 plus Lemma 26.5 imply:

Corollary 26.9. *If $a \in \mathbb{N}$ and p_1, p_2 are primes such that*

$$p_1 \equiv p_2 \pmod{4a}$$

then

$$N_{p_1}(x^2 = a) = N_{p_2}(x^2 = a).$$

In other words if we fix the polynomial $f(x) = x^2 - a$ then the value of $N_p(f)$ only depends on $r_N(p)$ for an integer N depending on f (in our case $N = 4a$). Such a statement fails, in general, for polynomials f of arbitrary degree (although there are examples of polynomials of higher degree for which such a statement holds).

27. GAUSSIAN INTEGERS

Some results about the integers appear as “shadows” of the arithmetic of more complicated types of (real or even complex) numbers. The first example of this phenomenon is the consideration of Gaussian integers below which leads, in particular, to an elegant proof of the characterization of primes (in \mathbb{Z}) which are sums of two squares (of elements of \mathbb{Z}). This example does not require us to know what real or complex numbers are. Another example to be discussed later involves more general complex numbers called algebraic integers. (For this it really helps to introduce real and complex numbers in full generality.) As a consequence of the introduction of algebraic numbers we will prove the quadratic reciprocity of Gauss (which is, again, a statement about integers in \mathbb{Z}).

Definition 27.1. (Gauss) A Gaussian integer is a pair (a, b) with $a, b \in \mathbb{Z}$. If $u = (a, b)$ and $v = (c, d)$ then define the Gaussian integers $u + v$ and $uv = u \times v$ by

$$\begin{aligned} u + v &= (a + c, b + d) \\ u \times v &= (ac - bd, ad + bc) \end{aligned}$$

Remark 27.2. One checks that

$$(a, b) = (a, 0) + (b, 0) \times (0, 1)$$

for all $a, b \in \mathbb{Z}$. So if we set $(a, 0) = a$ for any integer a and we set $i = (0, 1)$ then $i^2 = -1$ and $(a, b) = a + bi$ for all $a, b \in \mathbb{Z}$. From now on we use the representation $a + bi$ instead of (a, b) . We denote $\mathbb{Z}[i]$ the set of Gaussian integers; then $\mathbb{Z} \subset \mathbb{Z}[i]$.

Exercise 27.3. Prove that $\mathbb{Z}[i]$ is a ring with respect to the operations $+$ and \times .

Definition 27.4. For any $u = a + bi$ the conjugate of u is defined as $\bar{u} = a - bi$ and the norm of u is defined as

$$N(u) = u\bar{u} = a^2 + b^2.$$

Exercise 27.5. Prove that for any $u, v \in \mathbb{Z}[i]$ we have:

- 1) $\overline{u + v} = \bar{u} + \bar{v}$, $\overline{u \times v} = \bar{u} \times \bar{v}$;
- 2) $N(uv) = N(u)N(v)$.

Hint: 1) is an easy computation. 2) follows from 1).

Definition 27.6. $u \in \mathbb{Z}[i]$ is called invertible if there exists $v \in \mathbb{Z}[i]$ such that $uv = 1$.

Proposition 27.7. *The invertible elements in $\mathbb{Z}[i]$ are $1, -1, i, -i$.*

Proof. Clearly $1, -1, i, -i$ are invertible; in fact $i(-i) = 1$. Conversely if u is invertible, hence $uv = 1$ it follows that $N(uv) = N(1) = 1$ hence $N(u)N(v) = 1$ hence $N(u) = 1$ which immediately implies u is one of $1, -1, i, -i$. \square

28. FUNDAMENTAL THEOREM OF ARITHMETIC FOR GAUSSIAN INTEGERS

The following is an analogue of Euclid division:

Proposition 28.1. *For any $u, v \in \mathbb{Z}[i]$ with $v \neq 0$ there exist $w, z \in \mathbb{Z}[i]$ with $u = vw + z$ and $N(z) < N(v)$. (N.B. w, z are not unique.)*

Proof. Define $\mathbb{Q}(i)$ as $\mathbb{Q} \times \mathbb{Q}$ with addition and multiplication given by the same formulae as in the case of $\mathbb{Z}[i]$. Embed $\mathbb{Z}[i]$ into $\mathbb{Q}(i)$. Let $u\bar{v} = a + bi$ and let $t = \frac{a}{N(v)} + \frac{b}{N(v)}i \in \mathbb{Q}(i)$; so $tv = u$ in $\mathbb{Q}(i)$. View the points of $\mathbb{Q}(i) = \mathbb{Q} \times \mathbb{Q}$ as points in the “Euclidean plane”. (The argument that follows can be made, of course, rigorous.) Then $\mathbb{Z}[i]$ can be viewed as the set of points in the plane with integer coordinates. So t will lie inside at least one square of side 1 whose vertices are in $\mathbb{Z}[i]$. There is at least one vertex of this square at distance less than 1 from t . (Any point in a square of side 1 is at distance less than 1 to one of the vertices.) We take that vertex to be w and define $z = uv - w$. Then it follows immediately that $N(z) < N(v)$. \square

Exercise 28.2. Make the above argument rigorous. Hint: the vertices of the square can be defined using integral parts of rational numbers.

Definition 28.3. For $u, v \in \mathbb{Z}[i]$ we say that v divides u if there exists $w \in \mathbb{Z}[i]$ such that $u = vw$. A prime element in $\mathbb{Z}[i]$ is an element $\pi \in \mathbb{Z}[i]$ which is non-zero, non-invertible, and whenever $\pi = uv$ for $u, v \in \mathbb{Z}[i]$ it follows that either u or v is invertible.

The following is an analogue of Euclid’s Lemma:

Proposition 28.4. *If π is a prime element in $\mathbb{Z}[i]$ and $\pi|uv$ with $u, v \in \mathbb{Z}[i]$ then either $\pi|u$ or $\pi|v$.*

Proof. As in the proof of Euclid’s Lemma assume $\pi|uv$, $\pi \nmid u$, $\pi \nmid v$, and seek a contradiction. Consider the set

$$J = \{xu + y\pi; x, y, \in \mathbb{Z}[i]\}$$

and take an element $t \neq 0$ in J whose norm is minimal. We claim that both u and π are divisible by t . This follows by dividing u and π by t with remainders as in Proposition 28.1 and realizing the remainders belong to J hence by the minimality of the norm of t the remainders must be 0. Now since π is prime either t is invertible or t is an invertible element times π . The second case does not occur because it would imply that π divides u . So we conclude that t is invertible. We may assume $t = 1$. Then we can write $1 = xu + y\pi$ with $x, y \in \mathbb{Z}[i]$. In exactly the same way (using v instead of u) we may write $1 = zv + w\pi$ with $z, w \in \mathbb{Z}[i]$. We get

$$1 = (xu + y\pi)(zv + w\pi)$$

and we conclude exactly as in the proof of Euclid’s Lemma. \square

Exercise 28.5. Prove that any element in $\mathbb{Z}[i]$ which is not zero and non-invertible can be written as a product of prime elements in $\mathbb{Z}[i]$. Hint: Assume there are elements that don’t have this property. Pick one of minimal norm and derive a contradiction.

Putting together Proposition 28.4 and Exercise 28.5 we get the following analogue of the Fundamental Theorem of Arithmetic:

Theorem 28.6. Any element u in $\mathbb{Z}[i]$ which is non-zero and non-invertible can be written as a product of prime elements in $\mathbb{Z}[i]$ such that if

$$u = \pi_1 \dots \pi_n = \pi'_1 \dots \pi'_m$$

are two such representations then $n = m$ and (after a permutation of the indices) we have $\pi'_i = \epsilon_i \pi_i$ for some invertible elements ϵ_i .

Exercise 28.7. Write the details of the proof.

29. FACTORING PRIME INTEGERS IN THE GAUSSIAN INTEGERS

Proposition 29.1. Any prime p in \mathbb{Z} with $p \equiv 3 \pmod{4}$ is prime in $\mathbb{Z}[i]$.

Proof. If $p = uv$ then $p^2 = N(p) = N(u)N(v)$ so either $N(u) = p$ or $N(u) = 1$ or $N(v) = 1$. In the last 2 cases we get u or v invertible. The case $N(u) = p$ does not occur because $N(u) = a^2 + b^2$ for integers a, b and we know that a sum of 2 squares in \mathbb{Z} is never $\equiv 3 \pmod{4}$. \square

Proposition 29.2. If p is a prime in \mathbb{Z} with $p \equiv 1 \pmod{4}$ then p is not prime in $\mathbb{Z}[i]$ and in fact can be written as $p = \pi\bar{\pi} = N(\pi)$ with π a prime in $\mathbb{Z}[i]$.

Proof. Recall that since $p \equiv 1 \pmod{4}$ it follows that $p|c^2 + 1$ for some $c \in \mathbb{Z}$. Assume p is prime in $\mathbb{Z}[i]$ and seek a contradiction. Since $c^2 + 1 = (c + i)(c - i)$ it follows by Proposition 28.4 that either $p|c + i$ or $p|c - i$ in $\mathbb{Z}[i]$. But if $p|c + i$ then $c + i = p(a + bi)$ hence $c - i = \overline{c + i} = p(a - bi)$ so adding the last two equalities we get $2c = 2ap$ hence $p|c$, hence $p|1$ a contradiction. In a similar way we get a contradiction assuming $p|c - i$. We proved that p is not prime in $\mathbb{Z}[i]$. Then, by Exercise 28.5 we can write

$$p = \pi_1 \dots \pi_s$$

with $s \geq 2$ and π_i prime. Taking norms we get

$$p^2 = N(p) = N(\pi_1) \dots N(\pi_s).$$

Since the left hand side has only 2 primes in its prime decomposition and none of the factors in the right hand side is 1 it follows that $s = 2$ and $N(\pi_1) = N(\pi_2) = p$. So $p = N(\pi_1) = \pi_1 \bar{\pi}_1$. So $\pi_2 = \bar{\pi}_1$ and we are done. \square

Example 29.3. 5 is not prime in $\mathbb{Z}[i]$ because $5 = (2 + i)(2 - i)$. 7 is prime in $\mathbb{Z}[i]$.

Exercise 29.4. Find the prime factorization in $\mathbb{Z}[i]$ of $29^5 \times 37^3 \times 23^7$.

Exercise 29.5. Prove that $2 + 3i$ is prime in $\mathbb{Z}[i]$.

Exercise 29.6. Find the prime factorization in $\mathbb{Z}[i]$ of the number $12 + 13i$.

Since in Proposition 29.2 $N(\pi)$ is a sum of squares in \mathbb{Z} we obtain a proof of the following:

Theorem 29.7. (Fermat). If p is a prime in \mathbb{Z} with $p \equiv 1 \pmod{4}$ then $p = a^2 + b^2$ for some integers $a, b \in \mathbb{Z}$.

30. REAL AND COMPLEX NUMBERS

Definition 30.1. (Dedekind). A real number is a non-empty subset $u \subset \mathbb{Q}$ of the set of rational numbers with the property that if $x \in u$, $y \in \mathbb{Q}$, and $x \leq y$ then $y \in u$. Denote by \mathbb{R} the set of real numbers.

Example 30.2.

1) Any rational number $x \in \mathbb{Q}$ can be identified with the real number $u_x = \{y \in \mathbb{Q}; x < y\}$. (It is clear that $u_x = u_{x'}$ for $x, x' \in \mathbb{Q}$ implies $x = x'$.) We simply write $x = u_x$. So $\mathbb{Q} \subset \mathbb{R}$.

2) One defines, for instance, for any $n \in \mathbb{N}$, $\sqrt{n} = \{x \in \mathbb{Q}; x \geq 0, x^2 > n\}$.

Definition 30.3. If u and v are real numbers we write $u \leq v$ if and only if $v \subset u$. For $u, v \geq 0$ define

$$\begin{aligned} u + v &= \{x + y; x \in u, y \in v\} \\ u \times v = uv &= \{xy; x \in u, y \in v\}. \end{aligned}$$

Note that this extends addition and multiplication on the non-negative rationals.

Exercise 30.4. Naturally extend the definition of addition $+$ and multiplication \times of real numbers to the case when the numbers are not necessarily ≥ 0 . Prove that \mathbb{R} is a field with respect to $+$ and \times .

Exercise 30.5. Define complex numbers as pairs of real numbers. Define addition $+$ and multiplication \times as in Definition 27.1. Define $i = (0, 1)$ and show one can write any pair of real numbers (a, b) as $a + bi$ where real numbers a are identified with complex numbers $(a, 0)$. Denote by \mathbb{C} the set of complex numbers and prove that \mathbb{C} is a field with respect to $+$ and \times .

Exercise 30.6. Define the sum and the product of a family of real (or complex) numbers indexed by a finite set. Hint: use the already defined concept for integers (and hence for the rationals). Define the value of a polynomial in $\mathbb{Z}[x]$ at a complex number.

Exercise 30.7.

1) Prove that $(\sqrt{n})^2 = n$.

2) Prove that if n is not the square of an integer then $\sqrt{n} \notin \mathbb{Q}$. Hint: Assume the contrary. By 1) we have $n = \frac{a^2}{b^2}$ so $b^2n = a^2$ so $v_p(n) + 2v_p(b) = 2v_p(a)$ so $v_p(n)$ is even for all p so n is a square, a contradiction.

31. ALGEBRAIC INTEGERS

Definition 31.1. A complex number $u \in \mathbb{C}$ is called an algebraic integer if there exists a monic polynomial $F \in \mathbb{Z}[x]$ such that $F(u) = 0$.

Example 31.2. $\sqrt{-7} := \sqrt{7}i \in \mathbb{C}$ is an algebraic integer because it is a root of $F(x) = x^2 + 7$. N.B. Not all algebraic integers can be obtained from rational numbers by iterating the operations of addition, multiplication, and taking radicals of various orders; in order to prove the existence of algebraic integers that cannot be obtained in this way one needs ‘‘Galois theory’’.

Definition 31.3. A subset $\mathcal{O} \subset \mathbb{C}$ is called an order if:

- 1) $1 \in \mathcal{O}$
- 2) $u, v \in \mathcal{O}$ implies $u + v, uv, -u \in \mathcal{O}$;

3) There exist $u_1, \dots, u_n \in \mathcal{O}$ such that

$$\mathcal{O} = \{m_1 u_1 + \dots + m_n u_n; m_1, \dots, m_n \in \mathbb{Z}\}.$$

Remark 31.4. Conditions 1 and 2 imply that \mathcal{O} is a ring with respect to $+$ and \times .

Exercise 31.5. Prove that the sets

$$\mathbb{Z}[i], \{a + 2b\sqrt{-7}; a, b, \in \mathbb{Z}\}, \{a + 2b\sqrt{7}; a, b, \in \mathbb{Z}\}$$

are orders. Draw pictures of these sets.

Proposition 31.6. *A complex number is an algebraic integer if and only if it is contained in an order.*

Proof. (Uses matrices and their determinants!). If u is an algebraic integer, root of a monic polynomial in $\mathbb{Z}[x]$ of degree n then u is contained in the order

$$\mathcal{O} := \{c_0 + c_1 u + \dots + c_{n-1} u^{n-1}; c_0, \dots, c_{n-1} \in \mathbb{Z}\}.$$

Conversely assume u is contained in the order

$$\mathcal{O} = \{m_1 u_1 + \dots + m_n u_n; m_1, \dots, m_n \in \mathbb{Z}\}.$$

Then for all $i = 1, \dots, n$ we can write

$$u u_i = \sum_{j=1}^n m_{ij} u_j$$

with $m_{ij} \in \mathbb{Z}$. Set $a_{ij} = \delta_{ij} u - m_{ij}$ where δ_{ij} is 1 or 0 according as $i = j$ or $i \neq j$. Let $A = (a_{ij})$ be the matrix with entries a_{ij} and let U be the column vector with entries u_i . Since $AU = 0$ and $U \neq 0$ it follows that A is not invertible hence $\det(A) = 0$. But $\det(A)$ is easily seen to have the form

$$\det(A) = u^n + a_1 u^{n-1} + \dots + a_{n-1} u + a_n$$

with $a_k \in \mathbb{Z}$ so u is an algebraic integer and we are done. \square

Proposition 31.7. *If u and v are algebraic integers then $u + v, uv, -u$ are also algebraic integers.*

Proof. Assume u belongs to the order

$$\{a_1 u_1 + \dots + a_n u_n; a_1, \dots, a_n \in \mathbb{Z}\}$$

and v belongs to the order

$$\{b_1 v_1 + \dots + b_m v_m; b_1, \dots, b_m \in \mathbb{Z}\}.$$

Then $u + v, uv, -u$ belong to the set

$$\left\{ \sum_{i=1}^n \sum_{j=1}^m c_{ij} u_i v_j; c_{ij} \in \mathbb{Z} \right\};$$

but this latter set is clearly an order. \square

Definition 31.8. Denote by $\overline{\mathbb{Z}} \subset \mathbb{C}$ be the set of all algebraic integers.

Remark 31.9. By Proposition 31.7 $\overline{\mathbb{Z}}$ is a ring with respect to $+$ and \times .

Proposition 31.10. *A rational number which is also an algebraic integer must be an integer. In other words $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.*

Proof. Assume $\frac{a}{b} \in \mathbb{Q}$ is an algebraic integer,

$$\left(\frac{a}{b}\right)^n + a_1 \left(\frac{a}{b}\right)^{n-1} + \dots + a_n = 0$$

with $a_1, \dots, a_n \in \mathbb{Z}$. Hence

$$a^n + a_1 a^{n-1} b + \dots + a_n b^n = 0.$$

Assume $\frac{a}{b} \notin \mathbb{Z}$. Then there exists a prime $p \in \mathbb{Z}$ with $p|b$ and $p \nmid a$. But by the last equation if $p|b$ then $p|a^n$ hence $p|a$, a contradiction. \square

Exercise 31.11. Find an order containing $\sqrt{3} + \sqrt{7}$. Find a similar example involving cubic roots.

Exercise 31.12. Find a monic polynomial $f(x)$ in $\mathbb{Z}[x]$ such that $f(\sqrt{3} + \sqrt{7}) = 0$. Find a similar example involving cubic roots.

32. NON-UNIQUE FACTORIZATION IN KUMMER INTEGERS

The arithmetic of general orders is much more complicated than that of \mathbb{Z} . This was realized in the 19th century by Kummer, Dedekind, and others. In particular the fundamental theorem of arithmetic may fail in certain orders, as we will see here.

Definition 32.1. An element u in an order \mathcal{O} is called invertible if there exists $v \in \mathcal{O}$ such that $uv = 1$. An element $u \in \mathcal{O}$ is called irreducible if whenever $u = vw$ with $v, w \in \mathcal{O}$ it follows that either v or w is invertible. Two irreducible elements u and v in \mathcal{O} are called associated in divisibility if $u = vw$ with w invertible.

One is tempted to use the word *prime* instead of *irreducible*; but in view of pathologies to be put forward soon one prefers the work *irreducible*.

Exercise 32.2. Prove that in the order $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5}; a, b \in \mathbb{Z}\}$ (called the ring of Kummer integers) the following hold. (Morally the Fundamental Theorem of Arithmetic fails in this order.)

- 1) The only invertible elements in $\mathbb{Z}[\sqrt{-5}]$ are 1 and -1 ;
- 2) The elements $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are irreducible and no two of them are associated in divisibility;
- 3) The element 6 has the following 2 decompositions:

$$6 = 2 \times 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Hint: Define $\overline{a + b\sqrt{-5}} = a - b\sqrt{-5}$ and the norm $N(u) = u\bar{u} = a^2 + 5b^2$ for $u = a + b\sqrt{-5}$. Prove that u is invertible if and only if it has norm 1 which proves 1). To prove 2) assume one of these elements u can be written as $u = vw$ with v, w non-invertible, take norms to get $N(v)N(w)$ is 4, 6, or 9, conclude that $N(v)$ is 2 or 3, and derive a contradiction. 3) is clear.

33. PROOF OF QUADRATIC RECIPROCITY

We prove Theorem 26.8. First we recall its statement:

For any two distinct primes p and q different from 2 we have:

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

Remark 33.1. We will need to know in what follows that there exists a complex number $1 \neq \zeta_p \in \mathbb{C}$ such that $\zeta_p^p = 1$. Note that ζ_p is then an algebraic integer, $\zeta_p \in \overline{\mathbb{Z}}$. Also $\zeta_p^k \neq 1$ for all $1 \leq k \leq p-1$. If the complex exponential function e^z is assumed to be known then one can take

$$\zeta_p = e^{\frac{2\pi i}{p}}.$$

Alternatively, if we assume the Fundamental Theorem of Algebra (saying that any non-constant polynomial with complex coefficients has a complex root) then one can take ζ_p to be any root of the polynomial $x^{p-1} + x^{p-2} + \dots + x + 1$.

Exercise 33.2. Prove that if c is an integer then

$$\sum_{b=1}^{p-1} (\zeta_p^c)^b$$

equals $p-1$ or -1 according as $p|c$ or $p \nmid c$.

Definition 33.3. Define the Gauss sum

$$G = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a \in \overline{\mathbb{Z}}.$$

Lemma 33.4. (*Gauss*).

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

Proof. We have

$$G^2 = \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \left(\frac{ab}{p}\right) \zeta_p^{a+b}.$$

If (a, b) runs through the set of indices of the above sum then clearly $(a, ab \pmod p)$ runs through the same set of indices so substituting a by ab the above sum equals

$$\sum_{a=1}^{p-1} \sum_{b=1}^{p-1} \left(\frac{ab^2}{p}\right) \zeta_p^{ab+b} = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \sum_{b=1}^{p-1} (\zeta_p^{a+1})^b.$$

In view of Exercises 33.2 and 26.6 the above sum equals

$$\left(\frac{-1}{p}\right) (p-1) - \sum_{a=1}^{p-2} \left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right) p$$

and we are done by Lemma 26.3. \square

Definition 33.5. For $u, v \in \overline{\mathbb{Z}}$ and q a prime in \mathbb{Z} let us write $u \equiv v \pmod q$ in $\overline{\mathbb{Z}}$ if there exists $w \in \overline{\mathbb{Z}}$ such that $qw = v - u$.

Exercise 33.6. Prove that if $u \equiv v \pmod q$ in $\overline{\mathbb{Z}}$ and $u, v \in \mathbb{Z}$ then $u \equiv v \pmod q$ in \mathbb{Z} . Hint: this follows directly from Proposition 31.10.

Exercise 33.7. (Freshman's Dream) Prove that

$$(u_1 + \dots + u_n)^p \equiv u_1^p + \dots + u_n^p \pmod p \text{ in } \overline{\mathbb{Z}}$$

for $u_1, \dots, u_n \in \overline{\mathbb{Z}}$ and p a prime in \mathbb{Z} .

Proof of Theorem 26.8. By Lemma 33.4 and then Lemma 26.3

$$G^q = G(G^2)^{\frac{q-1}{2}} = G(-1)^{\frac{p-1}{2} \frac{q-1}{2}} p^{\frac{q-1}{2}} \equiv G(-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right) \pmod{q} \text{ in } \overline{\mathbb{Z}}.$$

On the other hand by “Freshman’s Dream” we get

$$\begin{aligned} G^q &= \left(\sum_{a=1}^{p-1} \binom{a}{p} \zeta_p^a \right)^q \equiv \sum_{a=1}^{p-1} \binom{a}{p}^q \zeta_p^{aq} = \sum_{a=1}^{p-1} \binom{a}{p} \zeta_p^{aq} \\ &= \left(\frac{q}{p}\right) \sum_{a=1}^{p-1} \binom{aq}{p} \zeta_p^{aq} = \left(\frac{q}{p}\right) G \pmod{q} \text{ in } \overline{\mathbb{Z}}. \end{aligned}$$

The two expressions of G^q above give

$$G(-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right) G \pmod{q} \text{ in } \overline{\mathbb{Z}}$$

Assume

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

and let us derive a contradiction. Since the two numbers above are ± 1 we get that one is 1 and the other is -1 so we get

$$G \equiv -G \pmod{q} \text{ in } \overline{\mathbb{Z}}$$

hence

$$2G \equiv 0 \pmod{q} \text{ in } \overline{\mathbb{Z}}$$

Squaring we get

$$4p \equiv 0 \pmod{q} \text{ in } \overline{\mathbb{Z}}$$

and hence, by Exercise 33.6,

$$4p \equiv 0 \pmod{q} \text{ in } \mathbb{Z}$$

which is a contradiction. \square

34. APPENDIX: CRYPTOGRAPHY

Generalities. The aim of cryptography is to devise secure schemes for transfer of information. The simplest setting and general procedure are as follows. One has 3 users A, B, C . The users A and B want to exchange information; they also want to keep this information secret from C . The information is called plaintext. A plaintext is a sequence of letters x_1, x_2, x_3, \dots from an alphabet X and can be understood by anybody who reads it. A cyphertext is a sequence of letters y_1, y_2, y_3, \dots from an alphabet Y and cannot be directly understood by any of the users. X and Y are finite sets usually identified with subsets of \mathbb{Z} (or sometimes with subsets of $\mathbb{Z} \times \mathbb{Z}$, etc.). The transfer of information is performed using a series of sets and maps as follows.

Definition 34.1. A cryptographic system consists of the following data:

- 1) A set X whose elements are called plaintext letters;
- 2) A set Y whose elements are called cyphertext letters;
- 3) A set K_E whose elements are called encryption keys;
- 4) A set K_D whose elements are called decryption keys;
- 5) A map $f : K_D \rightarrow K_E$;
- 6) A map $E : X \times K_E \rightarrow Y$ called the encryption map;

7) A map $D : Y \times K_D \rightarrow X$ called decryption map.

These data are subject to the following condition:

Assumption 34.2. $D(E(x, f(d)), d) = x$ for all $x \in X$, $d \in K_D$.

Then the procedure for the transfer of information from A to B is:

AB1) A transforms the plaintext $x_1, x_2, x_3, \dots \in X$ into a cyphertext $y_1, y_2, y_3, \dots \in Y$ by letting $y_i = E(x_i, e_{AB})$ where $e_{AB} \in K_E$;

AB2) A sends the cyphertext via a channel (a private letter or a public letter in the newspaper) so that B can read it; one should assume that C can have access to the cyphertext (by intercepting the private letter or reading the newspaper).

AB3) B transforms the cyphertext $y_1, y_2, y_3, \dots \in Y$ into the plaintext $x_1, x_2, x_3, \dots \in X$ by letting $x_i = D(y_i, d_{AB})$, where $e_{AB} = f(d_{AB})$.

To transfer information from B back to A :

BA1) B transforms the plaintext $x'_1, x'_2, x'_3, \dots \in X$ into a cyphertext $y'_1, y'_2, y'_3, \dots \in Y$ by letting $y'_i = E(x'_i, e_{BA})$ where $e_{BA} \in K_E$;

BA2) B sends the cyphertext via a channel (a private letter or a public letter in the newspaper) so that A can read it; one should assume that C can have access to the cyphertext (by intercepting the private letter or reading the newspaper).

BA3) A transforms the cyphertext $y'_1, y'_2, y'_3, \dots \in Y$ into the plaintext $x'_1, x'_2, x'_3, \dots \in X$ by letting $x'_i = D(y'_i, d_{BA})$, where $e_{BA} = f(d_{BA})$.

This scheme is based on the following:

Assumption 34.3.

- 1) The maps f , E and D are known to A, B, C .
- 2) $E(x, e)$ is computable in polynomial time from (x, e) .
- 3) $D(y, d)$ is computable in polynomial time from (y, d) .
- 4) e_{AB} is known to (or computable in polynomial time by) A ; e_{BA} is known to (or computable in polynomial time by) B ;
- 5) d_{AB} is known to (or computable in polynomial time by) B ; d_{BA} is known to (or computable in polynomial time by) A .
- 6) d_{AB} and d_{BA} are not known to (or computable in polynomial time by) C . (Otherwise he can decrypt the cyphertexts.)
- 7) C should not be able to impersonate A or B . (This is the case if e_{AB} and e_{BA} are not known to C . In case these numbers are known to C , A and B must have a procedure that allows them to ascertain that messages from each other do not actually come from C ; such a procedure is called a signature scheme.)

Secret key (classical) cryptography. In secret key cryptography A and B choose two numbers $d_{AB} = d_{BA}$ and $e_{AB} = e_{BA}$ such that $f(d_{AB}) = e_{AB}$; these numbers are then known to A and B but they are kept secret from C . The exchange of these numbers between A and B , if unprotected, is the most vulnerable step in the procedure. Since e_{AB} and e_{BA} are not known to C there is no need of a signature scheme. Secret key cryptography requires, in addition to Assumption 34.3, that:

Assumption 34.4. If $e = f(d)$ then either e is computable from d in polynomial time or d is computable from e in polynomial time.

Example 34.5. (Affine cipher). One starts with a prime p . Take

$$\begin{aligned} X &= \{0, 1, \dots, p-1\}, \\ Y &= \{0, 1, \dots, p-1\}, \\ K_D &= \{1, \dots, p-1\} \times \{0, 1, \dots, p-1\}, \\ K_E &= \{1, \dots, p-1\} \times \{0, 1, \dots, p-1\}, \\ f(d_1, d_2) &= (r_p(d'_1), r_p(-d'_1 d_2)), \text{ where } d'_1 \text{ is an inverse of } d_1 \text{ mod } p, \\ E(x, (e_1, e_2)) &= r_p(e_1 x + e_2), \\ D(y, (d_1, d_2)) &= r_p(d_1 x + d_2). \end{aligned}$$

Exercise 34.6. Check that the Assumptions 34.2, 34.3 and 34.4 hold in this example.

Exercise 34.7. Say A wants to transfer to B information consisting of a plaintext that has only one number, 42. Let $p = 691$. Assign values for the keys (small numbers of your choice) and compute the ciphertext. Also show that B can decrypt the ciphertext to reobtain 42.

Example 34.8. (Pohlig-Hellman cipher). One starts with a prime p . Take

$$\begin{aligned} X &= \{1, \dots, p-1\}, \\ Y &= \{1, \dots, p-1\}, \\ K_D &= \{1, \dots, p-1\}, \\ K_E &= \{1, \dots, p-1\}, \\ e = f(d) &= i_{p-1}(d), \text{ the inverse of } d \text{ mod } p-1, \\ E(x, e) &= r_p(x^e), \\ D(y, d) &= r_p(y^d). \end{aligned}$$

Exercise 34.9. Check that the Assumptions 34.2, 34.3, and 34.4 hold in this example.

Exercise 34.10. Say A wants to transfer to B information consisting of a plaintext that has only one number, 42. Let $p = 691$. Assign values for the keys (small numbers of your choice) and compute the ciphertext. Also show that B can decrypt the ciphertext to reobtain 42.

Exercise 34.11. Define a variant of the Pohlig-Hellman cipher in which X is an arbitrary finite group. (This is being done successfully nowadays with $X = E(\mathbb{F}_p)$ the group attached to an elliptic curve.)

Public key cryptography. In public key cryptography each of A and B chooses a number d_A and d_B . The number d_A is only known to A (but not to B or C) and the number d_B is only known to B (but not to A or C). B computes $e_B = f(d_B)$ and publishes e_B in the newspaper. Also A computes $e_A = f(d_A)$ and publishes e_A in the newspaper. Also the ciphertexts y_1, y_2, y_3, \dots created by both A and B are published in the newspaper. Then one applies the general scheme with $e_{AB} = e_B$, $d_{AB} = d_B$ and $e_{BA} = e_A$, $d_{BA} = d_A$. Note that $d_{AB} \neq d_{BA}$ and $e_{AB} \neq e_{BA}$. (The striking feature of public key cryptography is that the encryption keys and the ciphertexts are available to C and indeed to anybody! But since the encryption keys are public one needs a signature scheme.) For public key cryptography to work we need that, in addition to Assumption 34.3 we have:

Assumption 34.12. If $e = f(d)$ then e is computable from d in polynomial time; but it should not be possible to compute d from e in polynomial time.

Example 34.13. (RSA). One takes

$$\begin{aligned} X &= \{0, \dots, M-1\}, \\ Y &= \{0, \dots, N-1\}, N > M, \\ K_D &= \{(p, q); p, q \text{ primes}, \sqrt{M} \leq p < q \leq \sqrt{N}\}, \\ K_E &= \{0, \dots, N-1\} \times \{0, \dots, N-1\} \\ e = f(d) = f(p, q) &= (pq, \epsilon), \epsilon \text{ arbitrary coprime to } \phi(pq), \\ E(x, (m, \epsilon)) &= r_m(x^\epsilon), \\ D(y, (p, q)) &= r_{pq}(y^\delta), \text{ where } \delta = i_{\phi(pq)}(\epsilon), \text{ inverse of } \epsilon \text{ mod } \phi(pq). \end{aligned}$$

For the transfer of information from A to B the signature scheme works as follows. A publishes her nickname $n_A \in X$ in the newspaper and signs the cyphertext with $c_A = D(E(n_A, e_B), d_A)$. Note that the signature involves d_A which only A knows. To ascertain that A is indeed the sender of the message B checks whether $D(E(c_A, e_A), d_B)$ equals n_A . Indeed, if A is the sender then

$$D(E(c_A, e_A), d_B) = D(E(D(E(n_A, e_B), d_A), e_A), d_B) = n_A.$$

Exercise 34.14. In the above computation we used that $E(D(y, d), f(d)) = y$; check this.

Exercise 34.15. Check that the Assumptions 34.2, 34.3, and 34.12 hold in this example. Hint: Note that computing δ requires a priori the knowledge of $\phi(pq) = (p-1)(q-1) = pq - (p+q) + 1$ hence requires the knowledge of $p+q$. Now knowing pq and $p+q$ is equivalent to knowing p and q in polynomial time. But there is no known algorithm that returns p and q from pq in polynomial time. This is evidence that d can't be computed from e in polynomial time.

Exercise 34.16. Say A wants to transfer to B information consisting of a plaintext that has only one number, 42. Assign values for the keys (small numbers of your choice) and compute the ciphertext. Also show that B can decrypt the cyphertext to reobtain 42.

Example 34.17. (El Gamal). Fix a prime p and g a primitive root mod p , both being made public. Take

$$\begin{aligned} X &= \{1, \dots, p-1\}, \\ Y &= \{1, \dots, p-1\} \times \{1, \dots, p-1\}, \\ K_D &= \{2, \dots, p-2\}, \\ K_E &= \{1, \dots, p-1\}, \\ e = f(d) &= r_p(g^d) \\ E(x, e) &= (r_p(g^i), r_p(xe^i)) \\ D((y_1, y_2), d) &= r_p(y_2(y_1^d)^d), \end{aligned}$$

where i is a random integer (that changes for each instance of the computation) and y_1^d is an inverse of y_1 mod p . For the transfer of information from A to B the signature scheme works as follows. A publishes her nickname $n_A \in X$ in the newspaper and signs the cyphertext with

$$(z_A, s_A) := (r_p(g^r), r_{p-1}((n_A - d_A g^r)r'))$$

where r is arbitrary coprime to $p-1$ and r' is an inverse of r mod $p-1$. Note that the signature involves d_A which only A knows. To ascertain that A is indeed the

sender of the message B checks whether $g^{n_A} \bmod p$ equals $z_A^{s_A} e_A^{z_A} \bmod p$. Indeed if A is the sender then

$$z_A^{s_A} e_A^{z_A} \equiv z_A^{s_A} g^{d_A z_A} \equiv (g^r)^{r'(n_A - d_A g^r)} g^{d_A g^r} \equiv g^{n_A - d_A g^r + d_A g^r} \equiv g^{n_A} \bmod p.$$

Exercise 34.18. Check that $E(D((y_1, y_2), d), f(d)) \neq (y_1, y_2)$ in general. (This is why the signature scheme in the El Gamal case cannot be set up in the same style as for RSA.)

Exercise 34.19. Check that the Assumptions 34.2, 34.3, and 34.12 hold in this example. Hint: Computing d from e amounts to computing the discrete logarithm.

Exercise 34.20. Say A wants to transfer to B information consisting of a plaintext that has only one number, 9. Let $p = 17$. Assign values for the keys (small numbers of your choice) and compute the ciphertext. Also show that B can decrypt the ciphertext to reobtain 42.

Exercise 34.21. Define a variant of the El Gamal cipher in which X is an arbitrary finite group. (This is being done successfully nowadays with $X = E(\mathbb{F}_p)$ the group attached to an elliptic curve.)

Remark 34.22. One can use a secret key scheme in which the keys $e_{AB} = e_{BA}$ and $d_{AB} = d_{BA}$ are exchanged via a public key scheme (Diffie-Hellman scheme). In order for this to work one needs a public key scheme that allows A and B to share a number d_{AB} that only A and B know. (Then e_{AB} will be computable in polynomial time.) This can be done as follows. One fixes a prime p and a primitive root $g \bmod p$, both public. A chooses a number d_A which she keeps secret from everybody else and publishes $e_A = r_p(g^{d_A})$ in the newspaper. Similarly B chooses a number d_B which he keeps secret from everybody else and publishes $e_B = r_p(g^{d_B})$ in the newspaper. Then both A and B can compute in polynomial time the number $d_{AB} = r_p(e_A^{d_B}) = r_p(e_B^{d_A})$. This number cannot be computed by anybody else in polynomial time (unless an algorithm in polynomial time is discovered for the computation of the discrete logarithm.)