Algorithmic perspectives of elementary Number Theory & rudimentary abstract algebra

Department of Computer Science
Ariel University

Elad Aigner-Horev

October 26, 2019

Contents

Part I

Preliminaries

Lecture 1

Sets, relations, and functions

We round up various rudimentary definitions and results from set theory that will be used in subsequent parts of the manuscript. In this part of the manuscript we do not delve into proving most of the results mentioned as the purpose of this part of the manuscript is mainly to promote self-containments of subsequent arguments.

§1.1. The notion of a set

Definition 1.1 *An unordered collection of elements with no repetitions is called a* set.

The set $\{a\}$ contains a single element; we refer to such sets as *singletons*. Sets being unordered means that $\{a, b, 1, 4\} = \{1, b, a, 4\}$ as these denote the same set. Having no repetitions means that $\{a, a\} = \{a\}$, $\{a, 1, 2, a\} = \{2, 1, a\}$ and so on. In a set each element can represent a set or a system of sets as can be seen in the set $\{\{a\}, \{a, b, 3\}, 1, \{1, \{2\{3\}\}\}\}$.

Let us conduct some *highly informal* introductions to some well-known sets.

1. The set of natural numbers (i.e., $\{1, 2, \ldots\}$) is denoted by $\mathbb{N}$. A naive way to think of the natural numbers is as dots along an infinite straight line where consecutive dots are separated by one unit of length. Historically the number zero is not considered natural.

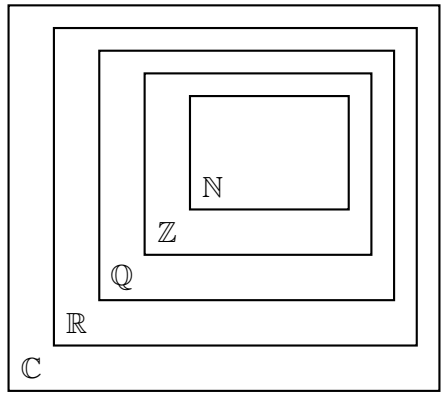
2. The integers is the set $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ and is denoted $\mathbb{Z}$. The integers can be thought of as two copies of the naturals numbers that are disjoint apart from a single common point at zero.

3. The rational numbers denoted $\mathbb{Q}$ are captured by the set $\left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\right\}$. The rationals arose from everyday life necessities of expressing fractions of units of length and amounts. The word *rational* comes from *ratio* and does not mean that these numbers make sense. Another definition is that the rationals are those numbers whose decimal expansion is periodic.

4. The irrational numbers are numbers like $\sqrt{2}$ and π. Often these are defined as those numbers whose decimal expansion is non-periodic. The irrational arise naturally, for instance:

5. $\mathbb{R}$ - the union of the rational and irrational numbers.

The image emerging from he above the definitions is the following.



We write $a \in A$ to denote that the element a belongs to the set A. For instance,

$$\frac{1}{4} \in \left\{ x \in \mathbb{R} : \left| x - \frac{1}{2} \right| < \frac{1}{2} \right\}.$$

We write $a \notin A$ to denote that a is not in A. For instance

$$10 \notin \left\{ x \in \mathbb{R} : \left| x - \frac{1}{2} \right| < \frac{1}{2} \right\}.$$

Example 1.2

1. The set $\{2k : k \in \mathbb{Z}\}$ is the the even integers;
2. the positive even numbers are given by the set $\{2k : k \in \mathbb{N}\}$.
3. Given two integers k and n we write $k \mid n$ to denote that n is divisible by k. The set $\{n \in \mathbb{Z}^+ : 3 \mid n \text{ and } n \leq 10^6\}$ consists of all positive integers that are divisible by 3 not exceeding 10^6.

Definition 1.3 *Let A and B be two sets.*

1. *We write $A \subseteq B$ to denote that every $a \in A$ satisfies $a \in B$. We say that A is* contained *in B and that A is a* subset *of B.*
2. *We write $A \subset B$ to denote that every $a \in A$ satisfies $a \in B$ yet that there exists a $b \in B$ such that $b \notin A$. We say that A is* properly contained *in B and that A is a* proper subset *of B.*

Trivially, for any set A we have $A \subseteq A$ and $A \not\subset A$.

Example 1.4

1. $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
2. $\{x \in \mathbb{Z} : x < 100\} \not\subseteq \{x \in \mathbb{R} : x < 99\}$.

Example 1.5 Let $A = \{1, \{1\}, \{2\}\}$.

$1 \in A$ - true
$2 \in A$ - false
$1 \subseteq A$ - No 1 is not a set
$\{1\} \subseteq A$ - true
$\{2\} \subseteq A$ - false
$\{2\} \in A$ - true
$\{\{2\}\} \in A$ - false
$\{\{2\}\} \subseteq A$ -true

1.1.1 *The Russel paradox*

Consider the set $\mathcal{R} := \{X : X \notin X\}$ comprised of all sets X that are not elements of themselves. This set has been proposed by Bertrand Russel who proceeded to ask whether $\mathcal{R} \in \mathcal{R}$. The issue one encounters here is that if $\mathcal{R} \in \mathcal{R}$ then by definition $\mathcal{R}$ is not an element of itself contradicting the assumption that it is. So the complimentary case asserting $\mathcal{R} \notin \mathcal{R}$ is compelled. In which case $\mathcal{R}$ is not an element of itself, yet $\mathcal{R}$ is define to contain all sets having this property and thus must contain itself as an element; a contradiction.

How to resolve Russel's paradox? Actually, this is the wrong question to ask at this early stage of our exposure to set. Better ask what does one learn from this paradox. The message arising from Russel's paradox is that

merely defining a set does not does not compel its existence;

in very much the same way that we can define *unicorns*, *elves*, and *goblins* and have vast literature about the properties of these yet still not compel these into existence. More importantly, Russel's paradox unveils that

there are properties that do not define sets;

that is, it is not possible to collect all objects satisfying these properties into a single set. One of the main goals of *set theory* then is to accurately describe and characterise those properties that do define sets.

1.1.2 *Axioms*

What are the bare bone 'assumptions' necessary to have any sort of sensible discussion about sets? While we have seen ample examples for sets, Russel's paradox makes us doubt that these even exist. One is then confronted with the certainly primal question: *are there any sets in the world*? Is our universe of discourse not void? Perhaps all attempts to define sets suffer internal fatal contradiction as seen in Russel's argument? We are unable to prove that sets exist. All we can do is postulate their existence.

The axiom of existence: there exists a set which has no elements.

Our discussion so far has identified two core notions that were quite natural to us upon discussing sets. These were captured by the symbols $\in$ and $\subseteq$. We would of course like to be able to determine when two sets X and Y are identical and mark this event by writing $X = Y$ is these are indeed identical. This two we have to postulate.

The axiom of extensionality: if $X \subseteq Y$ and $Y \subseteq X$ then $X = Y$.

Example 1.6 Let
$$A = \{2n+1 : n \in \mathbb{Z}\} \quad B = \{2n+3 : n \in \mathbb{Z}\}.$$
Determine whether $A = B$.

The set A consists of the odd numbers in $\mathbb{Z}$. As every member of B is odd we have that $B \subseteq A$. In order to show that $A \subseteq B$ fix an element $2m+1 \in A$. We show that $2m+1 \in B$. That is we show that there exists an $n \in \mathbb{Z}$ such that $2m+1 = 2n+3$. Let us make this clear. Fixing $2m+1$ in particularly fixes m. Finding n then means that we express n in terms of m. That is n is a function of m: $n = n(m)$.

$$\begin{aligned} 2m+1 &= 2n+3 \\ 2(m-n) &= 2 \\ n &= m-1. \end{aligned}$$

We have just seen that $n = n(m) = m-1$. This completes the proof that $A \subseteq B$.

Example 1.7 Continuing the theme of the previous example let $k_1, k_2 \in \mathbb{Z}$ be odd and set
$$A' = \{2n+k_1 : n \in \mathbb{Z}\} \quad B' = \{2n+k_2 : n \in \mathbb{Z}\}.$$
Is it true that $A' = B'$? The question reduces to whether the following has a solution.
$$\begin{aligned} 2m+k_1 &= 2n+k_2 \\ 2(m-n) &= k_2-k_1. \end{aligned}$$
We see that $2(m-n)$ is an even number and k_2-k_1 is an even number as k_1, k_2 are odd, by assumption. More explicitly, we have that $A' \subseteq B'$ because given an arbitrary element $2m+k_1 \in A'$ this element lies in B' as $2m+k_1 = 2n(m)+k_2$ where $n(m) = m - \frac{k_1-k_2}{2}$. On the other hand we have that $B' \subseteq A'$ because given an arbitrary element $2n+k_2 \in B'$ this element lies in A' as $2n+k_2 = 2m(n)+k_1$ where $m(n) = n + \frac{k_2-k_1}{2}$.

Lemma 1.8 *The exists only one set with no elements.*

Proof. Let A and B be two sets with no elements. Then $A \subseteq B$ and $B \subseteq A$ so that $A = B$ by the Axiom of extensionality. ■

Definition 1.9 *The unique set with no elements is called the empty set and is denoted $\emptyset$.*

We may write, for instance, that
$$\emptyset = \{y : y \neq y\}.$$

Definition 1.10 *Any set containing elements is then said to be* non-empty.

Observation 1.11. *Let A be a set. Then*
(a) $\emptyset \subseteq A$;
(b) if in addition $A \neq \emptyset$ then $\emptyset \subset A$.

Example 1.12

$\emptyset \in \emptyset$ - false
$\emptyset \in \{\emptyset\}$ - true
$\emptyset \subset \emptyset$- false
$\emptyset \subseteq \{\emptyset\}$ - true
$\emptyset \subset \{\emptyset\}$ - true

In a systematic exposition of set theory one should delve at this point to a few other axioms such as the *the axiom schema of comprehension*, *the axiom of pair*, and the *axiom of union*, say. But for our early exposure we skip those for now and alert the interested reader to these certainly important axioms. We choose to continue our brief exposition of fundamental set theory with the notion of *power sets*. The next axiom postulates that all subsets of a given set can be collected into one set.

The axiom of power set: for any set S there exists a set $\mathcal{P}(S)$ such that $X \in \mathcal{P}(S)$ providing $X \subseteq S$.

We refer to $\mathcal{P}(S)$ as the *power set* of S.

Example 1.13

- $\mathcal{P}(\emptyset) = \emptyset$.
- $\mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$.
- $\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

§1.2. Elementary set operations

Definition 1.14 *Let A and B be two sets.*

1. *The* intersection *of A and B is the set denoted $A \cap B$ given by*

$$A \cap B := \{x : x \in A \text{ and } x \in B\}.$$

2. *The* union *of A and B is the set denoted $A \cup B$ given by*

$$A \cup B := \{x : x \in A \text{ or } x \in B\}.$$

Definition 1.15 *Let A and B be two sets. We write $A \setminus B$ to denote the set*

$$A \setminus B := \{x : x \in A \text{ and } x \notin B\}$$

Definition 1.16 *The symmetric difference of two sets A and B is given by*

$$A \Delta B := (A \setminus B) \cup (B \setminus A).$$

Definition 1.17 *Let $\mathcal{U}$ be some universe in which a set A is taken. The* complement *of A is the set $\overline{A} := \mathcal{U} \setminus A$.*

Example 1.18 Let us have $\mathcal{U} = \mathbb{N}$ and let $A = \{2k : k \in \mathbb{N}\}$ so that A is the even natural numbers. Then $\overline{A} = \{2k+1 : k \in \mathbb{N}\}$ is the odd natural numbers.

It is not hard to verify that these operations satisfy

$$\begin{aligned}
\text{Commutativity} \quad & A \cap B = B \cap A \\
& A \cup B = B \cup A \\
\text{Associativity} \quad & (A \cap B) \cap C = A \cap (B \cap C) \\
& (A \cup B) \cup C = A \cup (B \cup C) \\
\text{Distributivity} \quad & A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\
& A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \\
\text{DeMorgan Laws} \quad & C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B) \\
& C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B).
\end{aligned}$$

Example 1.19 Verify the following.

- $A \cap (B \setminus C) = (A \cap B) \setminus C$.
- $A \setminus B = \emptyset \iff A \subseteq B$.
- $A \Delta A = \emptyset$.
- $A \Delta B = B \Delta A$.
- $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.

For any set S there exists a set U such that $x \in U$ if and only if $x \in A$ for some $A \in S$.

The set U is in fact unique and is called the *union of* S; it is denoted by $\bigcup S$. We say that S forms a *system of sets* or a *collection* of sets when we seek to emphasise that the elements of S are sets themselves. The union of a system of sets S is the a set of precisely those x that belong to some set from the system S.

Example 1.20

- For $S := \{\emptyset, \{\emptyset\}\}$; $x \in \bigcup S$ if and only if $x \in A$ for some $A \in S$. In our case it is only if $x \in \emptyset$ or $x \in \{\emptyset\}$. Therefore $x \in \bigcup S$ if and only if $x = \emptyset$ as indeed $\bigcup S = \{\emptyset\}$.
- $\bigcup \emptyset = \emptyset$.

Union revisited. Let M and N be sets. Then $x \in \bigcup\{M, N\}$ if and only if $x \in M$ or $x \in N$. The set $\bigcup\{M, N\}$ is then the union of M and N which have defined to be $M \cup N$ (strictly speaking, in a systematic exposition of set theory the axiom of union has to be defined prior to the operation of union, but we diverge from the norm here).

Intersection revisited. We pursue the same treatment for intersection as we did for union.

Definition 1.21 *Let S be a non-empty set system. Its* intersection *denoted $\bigcap S$ consists of all x satisfying $x \in A$ for all $A \in S$.*

Given two sets A and B, then $\bigcup\{A, B\} = A \cap B$.

Two sets A and B satisfying $A \cap B = \emptyset$ are called *disjoint*.

Definition 1.22 *A set system S is then to be a* system of mutually disjoint sets *if any two distinct members of it are disjoint.*

§1.3. Relations

Let $a \neq b$. The set $\{a, b\}$ is referred to as an *unordered pair* for the order of its elements is insignificant in the sense that $\{a, b\} = \{b, a\}$. When order does matter we write (a, b) instead and stipulate that $(a, b) \neq (b, a)$. In this case, we refer to (a, b) (and to (b, a)) as an *ordered pair*. Put another way for ordered pairs we wish to have the property that

$$(a, b) \neq (b, a) \text{ whenever } a \neq b.$$

We define such pairs as follows.

Definition 1.23 $(a, b) = \{\{a\}, \{a, b\}\}$.

For this definition note that if $a \neq b$ then (a, b) consists of two elements, and that if $a = b$ it has only one.

Lemma 1.24 $(a, b) = (a', b') \iff a = a'$ *and* $b = b'$.

With ordered pairs at our disposal we can define *ordered triples*

$$(a, b, c) := ((a, b), c),$$

ordered quadruples

$$(a, b, c, d) = ((a, b, c), d)$$

and so on to define *ordered k-tuples*. We can also define *ordered* 1*-tuples* as $(a) = a$.

Definition 1.25 *A set R is called a* binary relation *if all its elements are ordered pairs.*

It is customary to write xRy instead of $(x, y) \in R$; we say that x *is in relation R with y* if xRy holds.

At this stage it will be convenient to introduce two shorthands for the two notions that will repeat themselves throughout. We write the *quantifier* $\exists$ to mean *exists* and we write the quantifier $\forall$ to mean *forall*.

Several sets are associated with a binary relation R. The *domain* of R if given by

$$\text{dom } R := \{x : \exists y \text{ s.t. } xRy\}.$$

The *range* of R is given by

$$\text{ran } R := \{y : \exists x \text{ s.t.} xRy\}.$$

If $\text{dom } R \cup \text{ran } R \subseteq X$ we say that R is a relation on X.

The *image* of A under R is defined to be

$$R[A] := \{y \in \text{ran } R : \exists x \in A \text{ s.t. } xRy\}.$$

The *inverse image* of B under R is given by

$$R^{-1}[B] := \{x \in \text{dom } R : \exists y \in B \text{ s.t. } xRy\}.$$

The *inverse* of R is the set

$$R^{-1} := \{z : z = (x, y) \text{ s.t. } (y, x) \in R\}.$$

Lemma 1.26 *The inverse image of B under R is equal to the image of B under R^{-1}.*

Proof. Observe that $\operatorname{dom} R = \operatorname{ran} R^{-1}$. Then, $x \in \operatorname{dom} R$ belongs to the inverse image of B under R if and only if there exists $y \in B$ s.t. $(x, y) \in R$. As $(x, y) \in R$ if and only if $(y, x) \in R^{-1}$ it follows that x lies in the inverse image of B under R if and only if there exists a $y \in B$ such that $(y, x) \in R^{-1}$; that is, if and only if x belongs to the image of B under R^{-1}. ■

Definition 1.27 *Let R and S be binary relations. The* composition *of R and S is the relation*

$$S \circ R := \{(x, z) : \exists y \text{ for which } (x, y) \in R \text{ and } (y, z) \in S\}.$$

That is, $(x, z) \in S \circ R$ means that there exists a y s.t. xRy and ySz.

Definition 1.28 *Let A and B be sets. The set*

$$A \times B := \{(a, b) : a \in A, b \in B\}$$

is called the cartesian product *of A and B.*

Thus, $A \times B$, whenever it exists, forms a relation and so do its subsets. Proving that $A \times B$ always exists is a matter we shall not address as we skipped earlier the axiom required to do so. We define $A^2 := A \times A$. Cartesian products of three sets is defined to as

$$A \times B \times C := (A \times B) \times C;$$

observe that this yields

$$A \times B \times C = \{(a, b, c) : a \in A, b \in B, c \in C\}.$$

In a systematic introduction to set theory generalisations of $A \times B$ to include more factors and thus bring forth with it the notion of *n-tuples* should await the formal definition of the Natural number, which we so far only mentioned in an intuitive manner. In § 1.6 we give a short overview regarding the formal definition of $\mathbb{N}$ but would like to borrow on the readers informal acquaintance with $\mathbb{N}$ in order to put forth generalisations of $A \times B$. With that being said we define

$$A_1 \times \cdots \times A_n := \{(a_1, \ldots, a_n) : a_i \in A_i \forall i \in [n]\}$$

where here $[n] := \{1, \ldots, n\}$ and by $(a_1, \ldots, a_n)$ we mean an *ordered n-tuple*.

§1.4. Functions

Definition 1.29 *A binary relation F is called a* function *or* mapping *if*

$$aFb_1 \text{ and } aFb_2 \implies b_1 = b_2$$

for any a, b_1, and b_2.

Put another way, a binary relation is a function if and only if for every $a \in \operatorname{dom} F$ there is a unique b such that aRb. This unique b is called the *value* of F at a and is denoted $F(a)$. In particular, note that $F(a)$ is undefined if $a \notin \operatorname{dom} F$. If $\operatorname{dom} F = A$ and $\operatorname{ran} F \subseteq B$ it is customary to write $F : A \to B$ and even $A \xrightarrow{F} B$.

Example 1.30 $\alpha : \mathbb{Z} \to \{-1, 1\}$ given by

$$\alpha(n) := \begin{cases} 1, & \text{if } n \text{ is even,} \\ -1, & \text{if } n \text{ is odd.} \end{cases}$$

Application of the axiom of extensionality to functions (viewed as sets) yields the following.

Lemma 1.31 *Let F and G be functions. Then $F = G$ if and only if* dom F = dom G *and $F(x) = G(x)$ for all $x \in$* dom F.

Example 1.32 The functions $x \mapsto x$ and $x \mapsto |x|$ are equal on $\mathbb{R}^+$ but are not equal on $\mathbb{R}$.

Since functions are binary relations, the concepts of domain, range, image, inverse image, inverse, and composition all apply to functions as well. For functions though there are several other notions that are useful.

Definition 1.33 *Let F be a function and let A, B be sets.*

- *If* dom $F = A$, *then F is said to be a function* on A.
- *If* ran $F \subseteq B$, *then F is said to be a function* into B.
- *If* ran $F = B$, *then F is said to be a function* onto B *(*surjective *is also used).*
- *The* restriction *of F to A is the function*

$$F \restriction A := \{(a, b) \in F : a \in A\}$$

Example 1.34 The functions $\mathbb{Z} \to \mathbb{Z}$ given by $x \mapsto x^2$ is not surjective as negative numbers have no pre-image.

The proof of the following is left to the reader.

Theorem 1.35 *Let f and g be functions. Then $g \circ f$ is a function. Moreover,*

$$\dim g \circ d = \text{dom } f \cap f^{-1}[\text{dom } g].$$

and

$$(g \circ f)(x) = g(f(x)), \ \forall x \in \text{dom } (g \circ f).$$

While the operation of function composition is not *commutative* (i.e., $g \circ f$ need not be equal to $f \circ g$) it is however *associative*.

Lemma 1.36 (Associativity of function composition)
Let $f : X \to Y$, $g : Y \to Z$, and $h : Z \to W$. Then $f \circ (g \circ h) = (f \circ g) \circ h$.

Given a function f and an association $f(x) = y$, we called y the image of x under f. We call x the *pre-image of y under f*. The main difference is that unlike x that may have a single image (or none at all), an element $y \in Y$ may have numerous pre-images in X. Moreover, just as an element in X may

have no image, an element in Y need not have a pre-image. If $y \in Y$ has a single pre-image under F then this unique pre-image of Y is denoted by $f^{-1}(y)$. More generally, for $A \subseteq X$ we define the set

$$f(A) := \{y \in Y : f(a) = y, \text{ for some } a \in A\}$$

to denote the *image of A under f*. Note in particular that $f(X) \subseteq Y$ and it need not be the case that $f(X) = Y$. Conversely, given a set $B \subseteq Y$ we define the set

$$f^{-1}(B) := \{x \in X : f(x) \in B\}$$

to the denote the *pre-image of B under f*. If no element of B has a pre-image under f then $f^{-1} = \emptyset$.

Theorem 1.37 *Let $f : X \to Y$ be a function and let $A \subseteq X$ and $B \subseteq Y$. The following holds.*

1. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$;
2. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$;
3. $f(A \cup B) = f(A) \cup f(B)$.

Theorem 1.37 extends to unions and intersections of arbitrarily many sets as follows.

$$f^{-1}\left(\bigcup_\alpha A_\alpha\right) = \bigcup_\alpha f^{-1}(A_\alpha)$$
$$f^{-1}\left(\bigcap_\alpha A_\alpha\right) = \bigcap_\alpha f^{-1}(A_\alpha)$$
$$f\left(\bigcap_\alpha A_\alpha\right) = \bigcup_\alpha f(A_\alpha)$$

However, it is not true that $f(A \cap B) = f(A) \cap f(B)$.

Example 1.38 The rule $x \mapsto x + 1$ defines a function $\mathbb{N} \to \mathbb{N}$. However, the rule $x \mapsto x - 1$ does not as 0 has no image under this rule. However the $x \mapsto x - 1$ does define a function $\mathbb{N} \setminus \{0\} \to \mathbb{N}$; here 0 is not in the domain and can remain undefined.

Example 1.39 (The root function)

How to define the square root function on $\mathbb{R}$? Informally, our goal is to define a function $\sqrt{\ } : \mathbb{R} \to \mathbb{R}$ which sends $x \mapsto \sqrt{x}$. This intuition is very ackward; indeed, the term $\sqrt{x}$ is currently undefined. We overcome this by reverting to the set-theoretic flavour we have for functions. Namely, we would like that the rule specified by $\sqrt{\ }$ would associate pairs $(x, y) \in \mathbb{R}^2$ providing that those satisfy $y^2 = x$.

The first problem we encounter is that negative numbers have no image under this association in $\mathbb{R}$. This can be solved by restricting the domain to $[0, \infty)$. The second problem is that now we have elements in the domain with more than one image, say 4 has 2 and -2 as images. This we can solve by restricting the range to $[0, \infty)$ as well. We end up with a function $\sqrt{\ } : [0, \infty) \to [0, \infty)$ given by the association $x = y^2$; for $x \in [0, \infty)$ we then say that $\sqrt{x}$ is the unique number in $[0, \infty)$ satisfying $x = (\sqrt{x})^2$.

Function definition as seen in Example 1.38 are called *explicit* function definitions. The function definition used in Example 1.39 is called an *implicit* function definition.

Definition 1.40 *Let $f : X \to Y$ be a function. If there exists a $y \in Y$ such that $f(x) = y$ for all $x \in X$ we day that f is constant.*

If f is a function, then its inverse f^{-1} is a relation but it may not be a function. The function f is called *invertible* if f^{-1} is a function. Invertibility can be characterised.

Definition 1.41 *A function f is said to be* one-to-one *or* injective *if*

$$a_1 \in \text{dom } f, a_2 \in \text{dom } f, \text{ and } a_1 \neq a_2 \implies f(a_1) \neq f(a_2).$$

Put another way, a function is injective if it obeys the rule

$$x \neq x' \implies f(x) \neq f(x');$$

equivalently if it obeys

$$f(x) = f(x') \implies x = x'.$$

Example 1.42 The function $\mathbb{Z} \to \mathbb{Z}$ given by $x \to x^2$ is not injective. It becomes so if we restrict the domain to $\mathbb{N}$.

Theorem 1.43 *A function is invertible if and only if it is injective.*

Trivially, if f is invertible then so is f^{-1} so that $(f^{-1})^{-1} = f$ holds.

Definition 1.44 (Bijective/Invertible functions)

Functions that are both injective and surjective are called bijective *or* invertible.

Example 1.45

1. A function $f : X \to X$ sending $x \mapsto x$ is called the *identity* function on X; it is clearly bijective.
2. The function $f : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ given by $f(n) = n + 1$ is bijective. If we replace $\mathbb{N} \setminus \{0\}$ by $\mathbb{N}$ it is no longer bijective.

Example 1.46 The mapping $\alpha : \mathbb{R} \to \mathbb{R}$ given by $\alpha(x) = 2x - 5$ is a bijection. Indeed, if $x_1 \neq x_2$ then $2x_1 - 5 \neq 2x_2 - 5$ so that α is injective. Given $y \in \mathbb{R}$ then $\alpha((y + 5)/2) = y$ implying that α is surjective.

Other names used for bijective functions $x \mapsto f(x)$ are *perfect matchings* and *one-to-one correspondence* which is not to be confused with the term one-to-one function. For a bijection $f : X \to Y$ every $y \in Y$ has a pre-image $f^{-1}(y)$ which in this case is called the *inverse* of y.

The natural numbers are considered to be the "smallest" infinite set. In this notes we will not clarify the notion behind "smallest" with exact terms. Still let us pose the question of: *which set is "larger" the naturals or the natural even numbers?*

Definition 1.47 *Two sets are said to be of* equal cardinality *if there exists a bijection between them.*

Example 1.48 Two sets having equal cardinality does not preclude the option of one properly containing the other. Let X denote the set of even natural numbers. Surely $X \subset \mathbb{N}$. However, the function $f : \mathbb{N} \to X$ given by $f(n) = 2n$ is a bijection.

Definition 1.49 *A set X has size n if there is a bijection from X to $[n] := \{1, \ldots, n\}$.*

§1.5. Equivalences and partitions

Definition 1.50 *Let R be a binary relation in A.*

- *R is called* reflexive *in A if for $a \in A$, aRa.*
- *R is called* symmetric *in A if for $a, b \in A$, aRb implies bRa.*
- *R is called* transitive *in A if for $a, b, c \in A$, aRb and bRc imply aRc.*
- *R is called an* equivalence relation *on A if it is reflexive, symmetric, and transitive in A.*

If E is an equivalence relation on A and $a \in A$, then the *equivalence class of a modulo E* is given by

$$[a]_E := \{x \in A : xEa\}.$$

The members of $[a]_E$ are said to be *equivalent* to a under E. We write $a \equiv_E b$ to denote that a and b are equivalent under E.

Lemma 1.51 *Let E be an equivalence relation on A and let $a, b \in A$.*

- *$a \equiv_E b$ if and only if $[a]_E = [b]_E$.*
- *$a \not\equiv_E b$ if and only if $[a]_E \cap [b]_E = \emptyset$.*

Let E is an equivalence relation on A, then the system of all equivalence classes modulo E is given by

$$A/E := \{[a]_E : a \in E\}$$

and is called the *quotient* of A by E.

A system S of non-empty sets is called *a partition* of A if

- the members of S are mutually disjoint; and
- $\bigcup S = A$.

Theorem 1.52 *If E is an equivalence class then A/E forms a partition of A.*

We have seen that equivalence relations give rise to partitions. The converse is also true. For a partition S of A define the relation

$$E_S := \{(a, b) \in A \times A : \text{ there is a } C \in S \text{ s.t. } a \in C \text{ and } b \in C\}.$$

Theorem 1.53 *If S is a partition of A then E_S is an equivalence relation on A.*

It is not hard to show that if E is an equivalence relation on A and $S = A/E$ then $E_S = E$; and conversely, that is if S is a partition of A then $A/E_S = S$.

A set $X \subseteq A$ is called a set of *representatives* for an equivalence relation E on A if for every class $C \in A/E$, $X \cap C = \{a\}$ for some $a \in C$.

§1.6. The natural numbers: an informal first encounter

Though we are currently not well-equipped to give proper definitions of the sets $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ we include in this section some highlights of how one could go about defining some of these sets.

The definition we provided so far for the natural numbers is that of dots along a line separated by a single unit of length. Almost all of the words just used are undefined. What is a dot really? To expel all these uncertainties we now provide a proper definition for the natural numbers using sets. A technical issue arises now for us due to zero not included in the natural numbers. In the sequel, though, it will be more convenient to have zero be included in the definition. To resolve this, we shall instead define the set $\mathbb{Z}^+ := \{0, 1, 2, \ldots\}$ and work with it instead of $\mathbb{N}$.

The idea behind this definition is exceedingly simple.

- The empty set $\emptyset$ has no elements. This we can identify with 0 in $\mathbb{Z}^+$.
- The set $\{\emptyset\}$ (or more generally $\{a\}$) has a single element which may identify with 1 in $\mathbb{Z}^+$.
- The set $\{\emptyset, \{\emptyset\}\}$ (or more generally $\{a, b\}$) has two elements which we may identify with 2 in $\mathbb{Z}^+$.

A closer look at the above sets reveals the following pattern.

- Define 0 to be the **set** $\emptyset$, i.e., $0 := \emptyset$.
- Next, define $1 := 0 \cup \{\emptyset\} = \emptyset \cup \{\emptyset\} = \{\emptyset\}$.
- $2 := 1 \cup \{1\} = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$.
- $3 := 2 \cup \{2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, and so on.

At this stage note that

$$0 \in 1 \in 2 \in 3.$$

That is we are replacing the natural order of the naturals which we are accustomed to write

$$0 < 1 < 2 < 3$$

using $\in$. Let us make all this precise then. We say that the *successor* of a set X is given by $S(X) := X \cup \{X\}$.

With the above understood, we returning to the natural numbers and define these formally as follows.

Definition 1.54

(N.1) 1 *is natural.*

(N.2) If n is natural then its successor $S(n)$ is natural as well.

Theorem 1.55 *All naturals can be generated through (N.1) and (N.2).*

In fact we would like to argue for something stronger, that $\mathbb{N}$ is in fact "the least set" generated by (N.1) (N.2).However, we choose to avoid the definition of the term "the least set" here.

Successors of finite sets are finite. However, we think of $\mathbb{N}$ as an infinite set. A fair question then is *when does the process captured by (N.1) and (N.2) turns infinite?* In these notes we shall not provide an answer to this. Suffice to say that this is the part where we resort to the following.

Axiom of infinity. Infinite sets exist.

We are unable to prove that infinite sets exist and so at this point the axiom of infinity comes into play.

1.6.1 *The integers*

We observe that the number system $\mathbb{N}$ is somewhat limited. Indeed, $1-2=?$ has no solution in $\mathbb{N}$. This number system is missing additive inverses. The set of the naturals together with their set of inverses is $\mathbb{Z}$. The problem we are faced with now is the following. Given the set $\mathbb{N}$ define the set $\mathbb{Z}$. Ideally, we would have liked to define

$$\mathbb{Z} := \{n-m : n, m \in \mathbb{N}\},$$

as this would capture every element of $\mathbb{Z}$. This however is not well defined as $n-m$ is not well defined in $\mathbb{N}$. We can circumvent this issue by noticing that to denote the integer $n-m$ without using subtraction $\mathbb{N}$ we can simply use the pair (n,m). This approach is also problematic. For instance, $1=2-1=3-2=3-4$ so which pairs of $\{(n,n+1)\}_{n\in\mathbb{N}}$ should we use to represent the integer 1? The answer is all of them! We now make this precise.

Definition 1.56 *We say that pairs $(m,n),(x,y) \in \mathbb{N}\times\mathbb{N}$ are* equivalent *and write $(m,n) \sim (x,y)$ if*

$$x+m = n+y.$$

Why do we ask for $x+m=n+y$? Originally, we would like to write that $x-y=n-m$. However, we cannot do subtraction in $\mathbb{N}$ (and in $\mathbb{Z}^+$). Roughly speaking, in order to define an integer $x \in \mathbb{Z}$ we will round up all pairs $(n,m) \in \mathbb{Z}^+ \times \mathbb{Z}^+$ that are equivalent in the sense that their "subtraction" is equal to x into a single set X and let X represent x. Put another way, the relation $\sim$ defined above forms an equivalence relation on $\mathbb{Z}^+$ and $\mathbb{Z}$ is simply the set of equivalence classes of this relation.

§1.7. Exercises

Exercise 1. For a real number t let $\{t\}$ denote the *fractional part* of t. For instance $\{123.078\} = 0.78$ and $\{\frac{2}{5}\} = \frac{2}{5}$. Next, define $\|t\| := \min(\{t\}, 1-\{t\})$. For instance, $\|\frac{2}{5}\| = \min(\frac{2}{5}, \frac{3}{5}) = \frac{2}{5}$.

1. What is the set $\{x \in \mathbb{R} : \|x\| > \frac{1}{2}\}$ comprised of?
2. What is the set $X_1 = \{x \in \mathbb{R} : \|x\| \leq \frac{1}{10}\}$ comprised of? Describe the set in your own words.
3. Determine the intersection $X_1 \cap X_2$ where $X_2 = \{x \in \mathbb{R} : \|x\| \geq \frac{1}{2} - \frac{1}{10^6}\}$.

Exercise 2. Write the following sets explicitly:

1. $\{n^2 + 2 : n \in \mathbb{Z},\ -3 \leq n \leq 1\}$.
2. $\{2^{2^n} + 1 : n \in \mathbb{Z},\ 1 \leq n \leq 3\}$.
3. $\{\frac{n}{m} : n, m \in \mathbb{Z},\ n^2 < 9,\ |m| \leq n,\ n, m \neq 0\}$.
4. $\{5m + 3n : n, m \in \mathbb{Z},\ 2 \leq n < m \leq 5\}$.

Exercise 3. Let $A = \{\emptyset, \{\emptyset\}, 1, 3, \{\emptyset, 1, 3\}, \{1, 3\}\}$, $B = \{0, 1, \{3\}, \{\emptyset, 3\}\}$, $C = [0, 1] \cap \mathbb{Q}$ and $D = \left\{\frac{1}{2^n} : n \in \mathbb{N}\right\}$. For each statement below determine whether it is true or false.

1. $\{\emptyset\} \subseteq A$.
2. $\emptyset \in A \cap B$.
3. $\emptyset = A \cap B$.
4. $\{\emptyset, 3\} \in B$.
5. $\{\emptyset, 3\} \subseteq B$.
6. $\{1, 3\} \in A$.
7. $\{1, 3\} \subseteq A$.
8. $\frac{1}{2} \in C$.
9. $\frac{1}{3} \in D$.
10. $D \subseteq C$.

Exercise 4. Prove or disprove the following:

1. Let $A \subseteq B$. Then $A \cap B = B$.
2. $A \cap (A \cup B) = A$.
3. $A \cup (A \cap B) = A$.

Exercise 5. Determine which of the following sets are equal.

1. $A_1 = \{2, 5, 7\}$
2. $A_2 = \{x | x \text{ is a prime number and } 2 \leq x \leq 7\}$
3. $A_3 = \{7, 2, 7, 5, 5, 2, 2\}$
4. $A_4 = \{x | k \text{ is an even integer and } x = 2k\}$
5. $A_5 = \{x | k \text{ is an integer and } x = 4k\}$
6. $A_6 = \{x | k \in \mathbb{N} \text{ and } x = 4k\}$

Exercise 6. Let

$$A = \{1, 2, \{2\}, 3, \{2, 3\}\} \text{ and } B = \{2, 3\}.$$

For each statement below determine whether it is true or false.

1. $B \in A$
2. $B \subseteq A$
3. $\{2\} \in B$
4. $\{3\} \in A$
5. $\{2\} \in A$
6. $\{2\} \subseteq A$
7. $\{\{2\}\} \subseteq A$
8. $\varnothing \in A$
9. $\varnothing \subseteq B$
10. $\{2, \{2\}\} \subseteq A$
11. $\{2, 3, 3\} \subseteq B$
12. $\{1\} \subseteq A$
13. $\{2, \{2, 3\}\} \in A$
14. $\{\{2, 3\}\} \subseteq A$

Exercise 7. Determine which of the following sets are equal.

1. $A = \{2m + 1 | m \in \mathbb{Z}\}$
2. $B = \{2n + 3 | n \in \mathbb{Z}\}$
3. $C = \{2p - 3 | p \in \mathbb{Z}\}$
4. $D = \{3r + 1 | r \in \mathbb{Z}\}$
5. $E = \{3s + 2 | s \in \mathbb{Z}\}$
6. $F = \{3t - 2 | t \in \mathbb{Z}\}$

Exercise 8. Determine which of the following sets is non-empty.

1. $A = \{x \in \mathbb{N} \mid 2x + 7 = 3\}$
2. $B = \{x \in \mathbb{Z} \mid 3x + 5 = 9\}$
3. $C = \{x \in \mathbb{Q} \mid x^2 + 4 = 6\}$
4. $D = \{x \in \mathbb{R} \mid x^2 + 4 = 6\}$
5. $E = \{x \in \mathbb{R} \mid x^2 + 3x + 3 = 0\}$

Exercise 9. Prove that
$$\bigcup_\alpha A_\alpha - \bigcup_\alpha B_\alpha \subseteq \bigcup_\alpha (A_\alpha - B_\alpha).$$

Exercise 10. For an $x \in \mathbb{R}$ we write $x = \lfloor x \rfloor + \{x\}$ where $\lfloor x \rfloor$ denotes the integer part of x and $\{x\}$ denotes the fractional part of x.

Consider the function $f : \mathbb{R} \to \mathbb{R}$ given by $x \mapsto \{x\}$.

1. Show that all closed intervals of length 1 in $\mathbb{R}$ have the same image.
   (a) Determine what is that image.
2. Determine the pre-image of the interval $[1/4, 3/4]$.
3. Partition $\mathbb{R}$ into sets that have the same image.

Exercise 11. Let $f : X \to Y$ be a function and let $A \subseteq X$ and $B \subseteq Y$. Prove that the following holds.

1. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$;
2. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$;
3. $f(A \cup B) = f(A) \cup f(B)$.

§1.8. Solutions

Some of the solutions have been written by the TAs in the course and thus have a different style of writing to them. Over time we hope to normalise this part of the text as well.

Solution for Exercise 1.

1. We will prove that the set is empty. To do this, we will prove that for every $a \in \mathbb{R}$, $0 \le \|a\| \le \frac{1}{2}$. Let $a \in \mathbb{R}$. We separate into two cases. In the first case we assume that $\{a\} \le 1 - \{a\}$, which implies $\{a\} \le \frac{1}{2}$, hence, in this case $\|a\| \le \frac{1}{2}$. In the second case we assume that $\{a\} > 1 - \{a\}$, which implies $\{a\} > \frac{1}{2}$ and therefore $1 - \{a\} < \frac{1}{2}$, and so $\|a\| \le \frac{1}{2}$ in this case as well. Therefore $\|a\| \le \frac{1}{2}$ for all $a \in \mathbb{R}$.
2. Let $x \in X_1$. Then by the definition of the set, $\|x\| \le \frac{1}{10}$, therefore $\min(\{x\}, 1 - \{x\}) \le \frac{1}{10}$. We note that only one of the arguments needs to be less than or equal to $\frac{1}{10}$, hence $\{x\} \le \frac{1}{10}$ or $1 - \{x\} \le \frac{1}{10}$, which is implies $\{x\} \le \frac{1}{10}$ or $\{x\} \ge \frac{9}{10}$. We conclude that $\{x\}$ is of distance $\frac{1}{10}$ from either 1 or 0 and therefore $X_1 = \{x \in \mathbb{R} : \{x\} \notin \left(\frac{1}{10}, \frac{9}{10}\right)\}$.
3. We first show that for every $x \in X_2$, the distance of $\{x\}$ from $\frac{1}{2}$ is smaller than $\frac{1}{10^6}$. Let $x \in X_2$, then by the definition of the set, $\|x\| \ge \frac{1}{2} + \frac{1}{10^6}$ therefore $\min(\{x\}, 1 - \{x\}) \ge \frac{1}{2} + \frac{1}{10^6}$. We note that both of the argument must be greater than or equal to $\frac{1}{2} + \frac{1}{10^6}$ since otherwise the statement would not hold, hence $\{x\} \ge \frac{1}{2} + \frac{1}{10^6}$ and $1 - \{x\} \ge \frac{1}{2} + \frac{1}{10^6}$, which implies $\{x\} \ge \frac{1}{2} + \frac{1}{10^6}$ and $\{x\} \le \frac{1}{2} - \frac{1}{10^6}$. Therefore $X_2 = \{x \in \mathbb{R} : \left|\frac{1}{2} - \{x\}\right| \le \frac{1}{10^6}\}$. We conclude with the following observation, for all x such that $\frac{1}{2} - \frac{1}{10^6} \le \{x\}$ it holds that $\frac{1}{10} \le \{x\}$, and since for all x such that $\frac{1}{2} + \frac{1}{10^6} \ge \{x\}$ it holds that $\frac{9}{10} \le \{x\}$, therefore $X_1 \cap X_2 = \emptyset$

Solution for Exercise 2.

1. $\{2, 3, 6, 11\}$.
2. $\{5, 17, 257\}$.
3. $\{-2, -1, 1, 2\}$.
4. $\{21, 26, 31, 29, 34, 37\}$.

Solution for Exercise 3. 1,4,6,7,8,10 are true.

Solution for Exercise 4.

1. The statement is false, for example let $A = \{1, 2\}$ and $B = \{1, 2, 3\}$, then $A \cap B = \{1, 2\} \neq B$
2. The statement is true. We first prove that $A \cap (A \cup B) \subseteq A$. Let $x \in A \cap (A \cup B)$, then $x \in A$ and $x \in A \cup B$, which implies $x \in A$. Therefore $A \cap (A \cup B) \subseteq A$. Next we prove the other direction i.e. $A \subseteq A \cap (A \cup B)$. Let $x \in A$, then $x \in A$ or $x \in B$ and since $x \in A$, this implies that $x \in A \cap (A \cup B)$. Therefore $A \subseteq A \cap (A \cup B)$.
3. The statement is true. We first prove that $A \cup (A \cap B) \subseteq A$. Let $x \in A \cup (A \cap B)$, then $x \in A$ or $x \in A \cap B$. It must hold that $x \in A$ since otherwise $x \notin A \cap B$ which implies $x \notin A \cup (A \cap B)$. Therefore $A \cup (A \cap B) \subseteq A$. Next we prove the other direction i.e. $A \subseteq A \cup (A \cap B)$. Let $x \in A$, then $x \in A$ or $x \in A \cap B$, this implies that $x \in A \cup (A \cap B)$ and therefore $A \subseteq A \cup (A \cap B)$.

Solution for Exercise 5. $A_4 = A_5$, $A_1 = A_3$

Solution for Exercise 6. All but 3,4,8,13 are true.

Solution for Exercise 7. $A = B = C$, $D = F$.

Solution for Exercise 8. all are empty except for D

Solution for Exercise 9. Let $x \in \bigcup_\alpha A_\alpha - \bigcup_\alpha B_\alpha$. We show that it also holds that $x \in \bigcup_\alpha (A_\alpha - B_\alpha)$. Indeed, as $x \in \bigcup_\alpha A_\alpha - \bigcup_\alpha B_\alpha$, it follows that $x \in \bigcup_\alpha A_\alpha$ and that $x \notin \bigcup_\alpha B_\alpha$. Hence there exists β for which $x \in A_\beta$, and for every α it holds that $x \notin B_\alpha$. In particular, it holds that $x \notin B_\alpha$. Therefore $x \in A_\alpha - B_\alpha$, which implies that $x \in \bigcup_\alpha (A_\alpha - B_\alpha)$.

Solution for Exercise 10.

1. We will show that the image of every interval $[a, b]$ of length 1 in $\mathbb{R}$ is $[0, 1)$. We do so by first showing that $f([a, b]) \subseteq [0, 1)$. If a is an integer, then for every $x \in [a, b)$ it holds that
$$f(x) = x - \lfloor x \rfloor = x - a.$$
Since $x < b$ it holds that $f(x) = x - a < b - a = 1$. It also holds that $x \geq a$, hence $x - a \geq 0$, proving that $f(x) \in [0, 1)$. It further holds that
$$f(b) = f(a + 1) = a + 1 - \lfloor a + 1 \rfloor = 0,$$
where the last equality holds since $a \in \mathbb{Z}$. We can now safely assume that a and b are not integers. By Corollary **??** there exists a unique $n \in \mathbb{N}$ such that $n \in [a, b]$. Then for every $x \in [a, n)$, it holds that
$$f(x) = x - \lfloor x \rfloor = x - (n - 1).$$

Since $x < n$ we get that $f(x) = x - n + 1 < 1$. Since n is unique it holds that $x > a \geq n - 1$. Therefore $f(x) = x - n + 1 > n - 1 - n + 1 = 0$. Similarly, for every $x \in [n, b]$ it holds that

$$f(x) = x - \lfloor x \rfloor = x - n.$$

Since $x \geq n$ we get that $f(x) = x - n \geq 0$. Furthermore, it holds that $x \leq b < n + 1$, due to the fact that n is unique, hence $f(x) = x - n < 1$. We conclude that $f([a, b]) \subseteq [0, 1)$.

We next show the opposite direction, i.e., we show that $[0, 1) \subseteq f([a, b])$. Let $y \in [0, 1)$. Then

$$f(n + y) = n + y - \lfloor n + y \rfloor = n + y - n = y,$$

where the second equality is due to the fact that $n + y \leq b \leq n + 1$.

2. We will prove that

$$f^{-1}([1/4, 3/4]) = \{n + \alpha | n \in \mathbb{N} \text{ and } \alpha \in [1/4, 3/4]\}.$$

Let $x \in f^{-1}([1/4, 3/4])$. Then $1/4 \leq x - \lfloor x \rfloor \leq 3/4$, which is equivalent to $1/4 + \lfloor x \rfloor \leq x \leq 3/4 + \lfloor x \rfloor$. Therefore there exists $\alpha \in [1/4, 3/4]$ such that $x = \alpha + \lfloor x \rfloor$. Since $\lfloor x \rfloor$ is a natural number, we get that

$$x \in \{n + \alpha | n \in \mathbb{N} \text{ and } \alpha \in [1/4, 3/4]\}.$$

We now prove the opposite direction. Let $x = n + \alpha$, for some $n \in \mathbb{N}$ and $\alpha \in [1/4, 3/4]$. Then

$$f(x) = f(n + \alpha) = n + \alpha - \lfloor n + \alpha \rfloor = \alpha \in [1/4, 3/4],$$

where the last equality follows from the fact that $\lfloor n + \alpha \rfloor < n$.

3. For $m \in \mathbb{Z}$ let $S_m = \{m + \alpha | \alpha \in [0, 1)\}$. We will first show that $\{S_m\}_{m \in \mathbb{Z}}$ forms a partition of $\mathbb{R}$, that is, we will show that all of the set are pairwise disjoint, and their union is $\mathbb{R}$. Assume towards contradiction that there exists $m \neq k \in \mathbb{Z}$ and $x \in S_m \cap S_k$. Then by definition we get that $m + \alpha = x = k + \beta$, for some α ,$\beta \in [0, 1)$. Assume without loss of generality that $m < k$. Then $\alpha - \beta = k - m \geq 1$, hence $\alpha - \beta \in \mathbb{N}$, in contradiction to the fact that $\alpha - \beta < 1$. We next prove that $\bigcup_{m \in \mathbb{Z}} S_m = \mathbb{R}$. Since every element in S_m is a real number it immediately follows that $\bigcup_{m \in \mathbb{Z}} S_m \subseteq \mathbb{R}$. Let $x \in \mathbb{R}$. Then $x = \lfloor x \rfloor + \{x\}$. Since $\{x\} \in [0, 1)$, it follows that $x \in S_{\lfloor x \rfloor}$. It is left to show that $f(S_m) = f(S_k)$ for every $m, k \in \mathbb{Z}$. Indeed,

$$f(S_m) = \{f(m + \alpha) | \alpha \in [0, 1)\} = \{\alpha | \alpha \in [0, 1)\}.$$

We conclude that $f(S_m) = f(S_k)$.

Solution for Exercise 11.

1. For the first direction we will prove that $f^{-1}(A \cup B) \subseteq f^{-1}(A) \cup f^{-1}(B)$. Let $x \in f^{-1}(A \cup B)$, then $f(x) \in A \cup B$. This implies that either $f(x) \in A$ or $f(x) \in B$. Therefore $x \in f^{-1}(A)$ or $x \in f^{-1}(B)$, hence $x \in f^{-1}(A) \cup f^{-1}(B)$. We next prove the converse, i.e., we prove that $f^{-1}(A) \cup f^{-1}(B) \subseteq f^{-1}(A \cup B)$. Let $x \in f^{-1}(A) \cup f^{-1}(B)$, then either $x \in f^{-1}(A)$ or $x \in f^{-1}(B)$. Therefore $f(x)$ belongs to either A or B, hence $f(x) \in A \cup B$. Therefore $x \in f^{-1}(A \cup B)$.

2. For the first direction we will prove that $f^{-1}(A \cap B) \subseteq f^{-1}(A) \cap f^{-1}(B)$. Let $x \in f^{-1}(A \cap B)$, then $f(x) \in A \cap B$. This implies that $f(x) \in A$ and $f(x) \in B$. Therefore $x \in f^{-1}(A)$ and $x \in f^{-1}(B)$, hence $x \in f^{-1}(A) \cap f^{-1}(B)$. We next prove the converse, i.e., we prove that $f^{-1}(A) \cap f^{-1}(B) \subseteq f^{-1}(A \cap B)$. Let $x \in f^{-1}(A) \cap f^{-1}(B)$, then $x \in f^{-1}(A)$ and $x \in f^{-1}(B)$. Therefore $f(x)$ belongs to both A and B, hence $f(x) \in A \cap B$. Therefore $x \in f^{-1}(A \cap B)$.

3. For the first direction we will prove that $f(A \cup B) \subseteq f(A) \cup f(B)$. Let $y \in f(A \cup B)$, then there exists $x \in A \cup B$ such that $f(x) = y$. Then either $x \in A$ or $x \in B$, hence $f(x)$ belongs to either $f(A)$ or $f(B)$. The claim follows. We next prove the converse, i.e., we prove that $f(A) \cup f(B) \subseteq f(A \cup B)$. Let $y \in f(A) \cup f(B)$. Then either $y \in f(A)$ or $y \in f(B)$. This implies that there exists x in either A or B such that $y = f(x)$. Therefore $x \in A \cup B$, hence $y \in f(A \cup B)$.

Lecture 2

Mathematical induction

The set $\{x \in \mathbb{Q} : x > 0\}$ is non-empty and has no least element. The same can be said for the sets $\{x \in \mathbb{Z} : x \leq 0\}$ and $\{x \in \mathbb{R} : x \geq 0\}$. Unlike the sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, the set of natural numbers, i.e., $\mathbb{N}$, is special.

Well-ordering principle (WOP). *Every non-empty set of $\mathbb{N}$ (alternatively $\mathbb{Z}^+$) has a least element.*

We accept this principle as an *axiom*.

Prior to illustrating a rudimentary application of the WOP, let us introduce a certain piece of notation. Suppose $a_1, a_2, \ldots, a_k$ is a sequence of real numbers. We write

$$\sum_{i=1}^{k} a_i := a_1 + a_2 + a_3 + \cdots + a_k.$$

We could also consider only partial sums by looking at, say

$$\sum_{i=\lfloor k/2 \rfloor}^{k-1} a_i = a_{\lfloor k/2 \rfloor} + a_{\lfloor k/2 \rfloor + 1} + a_{\lfloor k/2 \rfloor + 2} + \cdots + a_{k-1}.$$

If the original sequence consisted of precisely two elements (i.e., $k = 2$) then this partial sum reads as

$$\sum_{i=\lfloor 2/2 \rfloor}^{2-1} a_i = \sum_{i=1}^{1} a_i = a_1$$

If the original sequence had but one element (i.e., $k = 1$) then this partial sum is

$$\sum_{i=\lfloor 1/2 \rfloor}^{1-1} a_i = \sum_{i=0}^{0} a_i = 0$$

as we summed no elements at all. More generally, if we have

$$\sum_{i=j_0}^{j_1} a_i$$

if $j_1 < j_0$ then we sum over no elements and then one usually say that the sum is zero.

As a first illustration for the usefulness of the WOP, we prove the the assertion that

$$\sum_{i=1}^{n}(2i-1) = n^2$$

holds for every $n \in \mathbb{N}$. For suppose that the claim is false. The there exists a non-empty set $S \subseteq \mathbb{N}$ for which the claim is false; i.e.,

$$\sum_{i=1}^{s}(2i-1) \neq s^2$$

for every $s \in S$. By the WOP, the set S has a least element, namely z. Minimality of z implies that every $x < z$ satisfies the claim as long as $x \in \mathbb{N}$. As the claim holds for $n = 1$ it follows that $1 \notin S$ so that $z > 1$. Then, $z - 1 \notin S$ and in addition $z \in \mathbb{N}$. Put another way,

$$\sum_{i=1}^{z-1}(2i-1) \neq (z-1)^2$$

holds. With the aid of the latter we may analyse the sum $\sum_{i=1}^{z}(2i-1)$ and write

$$\sum_{i=1}^{z}(2i-1) = \sum_{i=1}^{z-1}(2i-1) + (2z-1) = (z-1)^2 + (2z-1) = z^2.$$

We have now reached a contradiction; on the one hand $z \in S$ and serves as a counter example to the claim and on the other hand it satisfies it. It follows that $S = \emptyset$ all along.

§2.1. Irrationality of $\sqrt{2}$

In this section, we consider a somewhat more advanced application of the WOP. Taking the existence of the number $\sqrt{2}$ for granted, we now would like to classify to which set of numbers does $\sqrt{2}$ belongs to. We shall use the WOP in order to prove that $\sqrt{2}$ is, in fact, irrational.

Theorem 2.1 *$\sqrt{2}$ is irrational.*

We start with the classical, yet incomplete, proof of this result. Below we provide two additional complete proofs. The first 'proof' we propose requires the following simple fact.

Lemma 2.2 *Let $a \in \mathbb{Z}$. Then, a^2 is odd if and only if a is odd.*

Proof. If a is odd, then we may write $a = 2k + 1$ for some $k \in \mathbb{Z}$. Then,

$$a^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

implying that a^2 is odd.

Conversely, let a^2 be odd; we show that a is odd. For suppose not. Then, a is even and we may write $a = 2k$ for some $k \in \mathbb{Z}$. Then, $a^2 = 4k^2$ and is even; a contradiction. ■

Proof of Theorem 2.1. Assume towards a contradiction that the claim is false. That is, assume that there exists an $x \in \mathbb{Q}$ such that $x = \sqrt{2}$. Write $x = \frac{a}{b}$. We may assume, without loss of generality, that $\frac{a}{b}$ is written in smallest terms. Then, $\frac{a}{b} = \sqrt{2}$ so that $a^2 = 2b^2$, implying that a^2 is even and thus a is even by Lemma 2.2. We may then write $a = 2c$ for some integer c. Then, $a^2 = 2b^2$ becomes $(2c)^2 = 2b^2$ so

that $4c^2 = 2b^2$. It follows that $b^2 = 2c^2$; i.e., b^2 is even and thus b is even, by Lemma 2.2. We have just established that both a and b are even, in contradiction to the assumption that $\frac{a}{b}$ is written in smallest terms. ■

As mentioned, the above proof of Theorem 2.1 is the most known proof of that fact. At this stage we consider it to be incomplete as we did not prove that any member of $\mathbb{Q}$ can be expressed as a fraction in smallest terms. In the preceding proof we assumed this to be true without loss of generality. The next proof we propose for Theorem 2.1 does not omit this detail; in particular it employs the WOP in order to establish the fact that previously we merely assumed to be true. As the next proof is essentially the first major proof encountered in this manuscript, we shall write this proof in an informal manner with an emphasis on the ideas instead on brevity.

Proof of Theorem 2.1. We claim that there exists no $x \in \mathbb{Q}$ such that $x^2 = 2$. We prove this using the WOP. Assume towards a contradiction that there exists an $x \in \mathbb{Q}$ such that $x^2 = 2$. That is $x = \frac{m}{n}$ for some $m, n \in \mathbb{Z}$ and $n \neq 0$ and such that $m^2 = 2n^2$. As $\left(\frac{m}{n}\right)^2 = 2$ we may assume without loss of generality that $m, n \in \mathbb{N}$. It follows that

$$S = \{(m, n) : m^2 = 2n^2, m, n \in \mathbb{N}\} \neq \emptyset$$

We cannot appeal to the WOP with S as S is a set of ordered pairs and not a subset of $\mathbb{N}$. To be able to appeal to the WOP we consider the projection of S namely

$$S' = \{n \in \mathbb{N} : \ \exists m \in \mathbb{N} \text{ s.t. } (m, n) \in S\}.$$

The set S' is non-empty (since S is non-empty) and $S' \subseteq \mathbb{N}$. By the WOP S' has a least element. Let n^* denote this element and let $m^* \in \mathbb{N}$ be a positive integer such that $(m^*, n^*) \in S$. Put another way (m^*, n^*) is a pair in S whose n-part is least amongst all pairs in S (there could be several of those of course as n^* may have many partners; the WOP guarantees us that there is at least one such pair).

To get a contradiction we show that there exists a pair $(p, q) \in S$ such that $q < n^*$. How can we come up with the numbers p and q? As the only restriction we have is on q it is better to start with q. As so far we only know of the existence of n^* and m^* then any attempt at defining q should involve these numbers. There are two "immediate" or natural candidates for q that we can think of; these being $n^* - m^*$ and $m^* - n^*$.

Let us consider $n^* - m^*$. Surely $n^* - m^* < n^*$. However, as $(m^*)^2 = 2(n^*)^2$ we have $n^* < m^*$ so that $n^* - m^* < 0$ and in particular $n^* - m^* \notin \mathbb{N}$ so with such a q we fall out of S. This means that our candidate $n^* - m^*$ cannot be used in order to define q.

The second candidate is $m^* - n^*$. This number is surely positive. But do we have $m^* - n^* < n^*$? Suppose not; then $m^* \geq 2n^*$. Consequently, $(m^*)^2 \geq (2n^*)^2 > 2(n^*)^2$ contradicting the assumption that $(m^*)^2 = 2(n^*)^2$. In particular, we have just established that

$$m^* < 2n^*. \tag{2.3}$$

With q chosen to be $m^* - n^*$ the number p can be determined. This we obtain via the fact that in order for (p, q) to be in S these must satisfy $2q^2 = p^2$; leading us to the following calculation.

$$\begin{aligned} 2q^2 &= 2(m^* - n^*)^2 \\ &= 2(m^*)^2 - 4m^*n^* + 2(n^*)^2 \end{aligned}$$

recall that $2(n^*)^2 = (m^*)^2$ so that

$$\begin{aligned} &= 2 \cdot 2(n^*)^2 - 4m^*n^* + (m^*)^2 \\ &= 4(n^*)^2 - 2(2n^*)(m^*) + (m^*)^2 \\ &= (\underbrace{2n^* - m^*}_{\text{this is } p})^2. \end{aligned}$$

This suggests that we should take $p = 2n^* - m^*$. We can do so providing that $p > 0$. To have the latter we require that $2n^* > m^*$. This we have already seen in (2.3).

We have just seen that the pair $\{p, q\} = \{m^* - n^*, 2n^* - m^*\} \in S$ and $q < n^*$ a contradiction to the choice of $\{m^*, n^*\}$. ■

Here is an alternative proof for Theorem 2.1.

Proof of Theorem 2.1. Assume towards a contradiction that $\sqrt{2} \in \mathbb{Q}$ that is $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ and where $b \neq 0$. Then the set comprised of positive integer multiples of $\sqrt{2}$, namely

$$S = \{k\sqrt{2} \in \mathbb{N} : k \in \mathbb{N}\},$$

indeed, $a = b\sqrt{2}$. By the WOP S admits a least element. Let s denote this element and write $s = t\sqrt{2}$. To reach a contradiction we show that there exists an integer $s' \in S$ such that $s' < s$. We show that $s' = s\sqrt{2} - s = s\sqrt{2} - t\sqrt{2} = (s - t)\sqrt{2}$.

1. We start by showing that $s' \in S$. As $s' = (s - t)\sqrt{2}$ this will be implied once we show that $s' \in \mathbb{N}$.
   (a) To see that s' is in fact an integer note that
   $$\begin{aligned} s' &= s\sqrt{2} - s \\ &= t\sqrt{2}\sqrt{2} - s \\ &= 2t - s \end{aligned}$$
   As $2t \in \mathbb{Z}$ and $s \in \mathbb{Z}$, by assumption, then $2t - s \in \mathbb{Z}$.
   (b) Next, we show that $s' > 0$. Indeed, $s' = s(\sqrt{2} - 1)$. As $\sqrt{2} - 1 > 0$ and $s > 0$, by assumption, we have that $s' > 0$.
2. We have established that $s' \in S$. It remains to show that $s' < s$. Here we note that
   $$s' = 2t - t\sqrt{2} = t(2 - \sqrt{2}) < t\sqrt{2} = s.$$

■

§2.2. Weak Induction

The definition of $\mathbb{N}$ (or $\mathbb{Z}^+$) and the WOP give rise to a powerful proof technique called *mathematical induction*.

Theorem 2.4 (First principle of finite induction)

Let $S \subseteq \mathbb{N}$ be a set satisfying:

(I.1) $1 \in S$; and

(I.2) if $k \in S$ then $k + 1 \in S$.

Then $S = \mathbb{N}$.

Proof. Assume towards a contradiction that the claim is false. Then $T := \mathbb{N} \setminus S$ is non-empty. By the WOP T contains a least element, namely a. As $1 \in S$, it follows that $a > 1$ (recall that $0 \notin \mathbb{N}$). By the minimality of a the number $a - 1 \notin T$ and thus $a - 1 \in S$. By (I.2), we have that $a \in S$ contradicting the assumption that $a \notin S$. ■

A more familiar form of Theorem 2.4 is the following.

Theorem 2.5 (Weak mathematical induction)

Let $S(n)$ denote a mathematical statement that depends on $n \in \mathbb{N}$.

(Base) If $S(1)$ is true; and

(Step) if whenever $S(k)$ is true then $S(k+1)$ is true as well,

then $S(n)$ is true for all $n \in \mathbb{N}$.

A few mathematical jokes are in order. For our first joke let us use induction in order to prove that *all positive integers are small.*

1. **Basis.** Surely 1 is a small number.
2. **Step.** If n is small surely $n+1$ is small.

It follows by induction that all numbers in $\mathbb{N}$ are small. Do you agree?

Here is another joke. Let us use induction to prove that *all horses in the world have the same colour.* Surely in a set consisting of one horse the claim is true. Suppose then that the statement is true for sets of horses of size n. We show it holds for $n+1$. Let our horses be labelled $\{1, \ldots, n, n+1\}$. By the induction hypothesis the n horses labelled $\{1, \ldots, n\}$ are coloured with the same colour. Also, by the induction hypothesis, the n horses labelled $\{2, \ldots, n+1\}$ are coloured with the same colour. It follows that all $n+1$ horses are coloured the same. Do you agree?

Let us now demonstrate the use of Theorems 2.4 and 2.5. In the next lemma we consider the sum

$$\sum_{i=1}^{n}(2i-1).$$

The sequence we are summing over here is

$$2 \cdot 1 - 1, 2 \cdot 2 - 1, 2 \cdot 3 - 1, \ldots, 2 \cdot n - 1$$

which is simply

$$1, 3, 5, 7, \ldots, 2n-1.$$

The last element we cannot produce a number for as that depends on n and here n is a parameter and not a fixed number. This sequence consists of all odd numbers in the set $\{1, 2, 3, \ldots, 2n\}$. A different way of writing the same sum then would be to define $\mathcal{O}$ to be the set consisting of all the odd numbers in the set $\{1, 2, 3, \ldots, 2n\}$ and then write

$$\sum_{a \in \mathcal{O}} a.$$

With the notation regarding sums defined we return to the issue of applying the principle of weak induction. Our first application determines the value of the sum of all members of $\mathcal{O}$.

Lemma 2.6 *For every $n \in \mathbb{N}$:*

$$\sum_{i=1}^{n}(2i-1) = n^2. \tag{2.7}$$

Proof. Let $S \subseteq \mathbb{N}$ denote the set of positive integers satisfying (2.7). We verify that S satisfies both (I.1) and (I.2).

Verifying (I.1) As $2 \cdot 1 - 1 = 1$ we have that $1 \in S$. That is we have verified that S satisfies (I.1).

Verifying (I.2) We seek to prove that S satisfies (I.2). To that end, we have to show that whenever $1 \leq k \in S$ then $k+1 \in S$ as well. The assumption that $k \in S$ means

$$\sum_{i=1}^{k}(2i-1) = k^2.$$

This assumption is then our *induction hypothesis*.

$$\begin{aligned}\sum_{i=1}^{k+1}(2i-1) &= \underbrace{\sum_{i=1}^{k}(2i-1)}_{=k^2 \text{ by I.H.}} + (2(k+1)-1) \\ &= k^2 + 2k + 1 \\ &= (k+1)^2.\end{aligned}$$

As S satisfies both (I.1) and (I.2) we have that $S = \mathbb{N}$, by Theorem 2.4. ■

Returning yet again to the notation of sums set above let us broaden it as follows. Given a function $f : D \to R$ we write

$$\sum_{d \in D} f(d)$$

to denote the summation of the function f over its domain. The next lemma considers the partial sum of squares given by

$$\sum_{i=1}^{n} i^2.$$

Here the function is $f : \mathbb{Z} \to \mathbb{Z}$ given by $m \mapsto m^2$. The sum here is a partial sum as it does not range over the entire domain of the function.

Lemma 2.8 *For every $n \in \mathbb{N}$:*

$$\sum_{i=1}^{n} i^2 = \frac{n(2n+1)(n+1)}{6}. \tag{2.9}$$

Proof. Let $S \subseteq \mathbb{N}$ be the set of positive integers satisfying (2.9). As $1^2 = \frac{1 \cdot (2 \cdot 1+1)(1+1)}{6} = \frac{6}{6}$ we have that $1 \in S$ so that S satisfies (I.1). It remains to verify (I.2). Suppose then that $1 \leq k \in S$, we show that

$$\sum_{i=1}^{k+1} i^2 = \sum_{i=1}^{k} i^2 + (k+1)^2 = \frac{(k+1)(2(k+1)+1)((k+1)+1)}{6} = \frac{(k+1)(2k+3)(k+2)}{6}.$$

By the assumption that $k \in S$ this reduces to showing that

$$\frac{k(2k+1)(k+1)}{6} + (k+1)^2 = \frac{(k+1)(2(k+1)+1)((k+1)+1)}{6}.$$

This is indeed true:

$$\begin{aligned}\frac{k(2k+1)(k+1)}{6}+(k+1)^2 &= (k+1)\left(\frac{k(2k+1)}{6}+(k+1)\right)\\ &= (k+1)\frac{k(2k+1)+6(k+1)}{6}\\ &= (k+1)\left(\frac{2k^2+7k+6}{6}\right)\\ &= (k+1)\left(\frac{(2k+3)(k+2)}{6}\right)\end{aligned}$$

■

The proof of (2.9) was a bit tedious. Indeed, we had to resort to some annoying algebraic manipulations. A weaker statement that would capture the spirit of (2.9) would be that

$$\textit{there exists a } C\in\mathbb{R} \textit{ such that } \sum_{i=1}^{n} i^2 \geq Cn^3 \textit{ for any sufficiently large } n\in\mathbb{Z}^+. \tag{2.10}$$

To see (2.10), let us consider the r.h.s. of (2.9); this is equal to $\frac{n^3}{3}+\frac{n^2}{2}+\frac{n}{6}$. As $n\to\infty$ we see that n^3 becomes the dominant term in $\frac{n^3}{3}+\frac{n^2}{2}+\frac{n}{6}$ allowing us to "neglect" the other terms. We now make this precise.

Lemma 2.11 *For every $\varepsilon>0$ there exists an $n_0=n_0(\varepsilon)$ such that $n^2\leq\varepsilon n^3$ whenever $n\geq n_0$.*

Proof. Given ε we set

$$n_0=\left\lceil\frac{1}{\varepsilon}+1\right\rceil. \tag{2.12}$$

We prove by induction on n that $n^2\leq\varepsilon n^3$ whenever $n\geq n_0$. For the induction basis set $n=n_0$ and note that $n_0^2<\varepsilon n_0^3$. Assuming that the claim holds for $n\geq n_0$ we prove that it holds for $n+1$. That is we prove that $(n+1)^2\leq\varepsilon(n+1)^3$ whenever $n\geq n_0$.

$$\varepsilon(n+1)^3=\varepsilon n^3+3\varepsilon n^2+3\varepsilon n+\varepsilon$$

by the induction hypothesis $\varepsilon n^3\geq n^2$ for $n\geq n_0$ so we may write

$$\geq n^2+3\varepsilon n^2+3\varepsilon n+\varepsilon,$$

neglecting the last two terms we arrive at

$$\geq n^2+3\varepsilon n^2$$

now, as $n\geq n_0\geq\varepsilon^{-1}$ we have that $\varepsilon\geq n^{-1}$ so we may write

$$\begin{aligned}&\geq n^2+\frac{3}{n}n^2,\\ &= n^2+3n\\ &\geq n^2+2n+1\\ &= (n+1)^2,\end{aligned}$$

and the claim follows. ■

In a similar manner we have the following claim proof of which is left to the reader.

Lemma 2.13 *For every $\varepsilon > 0$ there exists an $n_0 = n_0(\varepsilon)$ such that $n \leq \varepsilon n^3$ whenever $n \geq n_0$.*

Lemmas 2.11 and 2.13 imply the following.

Lemma 2.14 *For every $\varepsilon > 0$ there exists an n_0 such that $\varepsilon n^3 \geq n^2 + n$ whenever $n \geq n_0$.*

As a result we have that in the sum $\frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6}$, seen in (2.9), the term $\frac{n^3}{3}$ is the dominant one for n sufficiently large.

Thus far we have verified (2.10) using (2.9). The analysis above serves as a justification as to why C as in (2.10) exists. Suppose now that we had no prior knowledge of (2.9); *how can we come up with C in this case?* Let us try to prove (2.10) directly using induction. Let us start with the induction step. Suppose that the inductive hypothesis is that $\sum_{i=1}^{n} i^2 \geq Cn^3$ where C is yet to be determined whenever $n \geq n_0$ where n_0 is also yet to be determined. The burden of proof in the induction step would then be to show that

$$\underbrace{\sum_{i=1}^{n} i^2}_{\geq Cn^3} + (n+1)^2 \geq C(n+1)^3$$

so that

$$\cancel{Cn^3} + (n+1)^2 \geq \cancel{Cn^3} + 3Cn^2 + 3Cn + C.$$

We see that the term Cn^3 cancels. We are left with

$$n^2 + 2n + 1 \geq 3Cn^2 + 3Cn + C$$

which holds providing that the following three conditions hold for C

$$\begin{aligned} C &\leq \frac{1}{3} \quad \text{(by the } n^2 \text{ term)} \\ C &\leq \frac{2}{3} \quad \text{(by the } n \text{ term)} \\ C &\leq 1 \quad \text{(by the constant term).} \end{aligned}$$

The choice $C = 1/3$ makes sense then in the induction step. It remains to find n_0 from which the claim holds. This is rather easy as we can turn to Lemma 2.14 "feed" it $\varepsilon = 1/3$ and obtain some $n_0 = n_0(1/3)$ from it. Whatever this number will be we can be rest assured that we can use it for (2.10). In particular we can now write the following.

Lemma 2.15 *There exists a $C \in \mathbb{R}$ such that for every n sufficiently large*

$$\sum_{i=1}^{n} i^2 \geq Cn^3$$

holds.

2.2.1 The $n!$ function

Mathematical induction is often used in definitions. For instance, the definition of $n!$ reads as follows.

Definition 2.16 *Let $n \in \mathbb{N}$. Then, $n!$ is given by the following.*
(a) $1! = 1$;
(b) $n! = n \cdot (n-1)!$.

We call such definitions *recursive definition*. A trivial upper bound on $n!$ is the following.

Lemma 2.17 *$n! \leq n^n$ for every $n \in \mathbb{N}$.*

Proof. The proof is by induction on n.

Basis. For $n = 1$ the assertion is true.

Step: Suppose the claim is true for $1 \leq n \in \mathbb{N}$. We show that the assertion also holds for $n+1$.

$$\begin{aligned}(n+1)! &= (n+1) \cdot n! \\ &\leq (n+1)n^n \quad \text{(by the induction hypothesis)} \\ &< (n+1)(n+1)^n \quad (\text{as } n \geq 1) \\ &= (n+1)^{n+1}.\end{aligned}$$

■

To get a sense for the rate of growth of $n!$ let us compare it with the function 2^n. For small values of n we see that 2^n prevails over $n!$:

$$\begin{aligned}1! &= 1 < 2^1 = 2 \\ 2! &= 2 < 2^2 = 4 \\ 3! &= 6 < 2^3 = 8.\end{aligned}$$

But at $n = 4$ we have that $4! = 24 > 2^4 = 16$. This in fact holds for all $n \geq 4$.

Lemma 2.18 *$n! \geq 2^n$ for all $n \geq 4$*

Proof. We prove the assertion by induction on n. The basis of the induction we have already seen above. We proceed to the induction step. Suppose then that the claim is true for $n \geq 4$. We show that it holds for $n+1$.

$$\begin{aligned}(n+1)! &= n!(n+1) \\ &\geq 2^n(n+1) \quad \text{(by I.H.)} \\ &\geq 2^n \cdot 2 \quad (n \geq 4 \implies n+1 \geq 2) \\ &\geq 2^{n+1}.\end{aligned}$$

■

2.2.2 Powers of 2

The function 2^n is a fast growing function. Can we quantify "fast"? We will now show that this function grows so fast that 2^n is larger than the sum of all the powers of 2 preceding it.

Lemma 2.19 *For all $n \in \mathbb{N}$*

$$\sum_{i=1}^{n} 2^i \leq 2^{n+1} \tag{2.20}$$

holds.

Proof. The proof is by induction on n. For $n = 1$ the assertion holds. Assume then that the claim holds for $n \geq 1$. We show that it holds for $n + 1$. That is, we show that $\sum_{i=1}^{n+1} 2^i \leq 2^{n+2}$. This is indeed true as

$$\sum_{i=1}^{n+1} 2^i = \underbrace{\sum_{i=1}^{n} 2^i}_{\leq 2^{n+1}} + 2^{n+1} \leq 2 \cdot 2^{n+1} = 2^{n+2}.$$

■

2.2.3 *Stronger assertions*

The following lemma demonstrates an important principle. This being the fact that sometimes one has to prove a stronger assertion than the one intended. Let us consider the sum of the reciprocals of the first n squares, namely $\sum_{i=1}^{n} \frac{1}{i^2}$ and let us try to prove that

$$\sum_{i=1}^{n} \frac{1}{i^2} \leq 2.$$

A naive attempt would be to have the latter as our induction hypothesis. However this will clearly end in failure. Indeed, in the induction step we would have to prove that

$$\underbrace{\sum_{i=1}^{n} \frac{1}{i^2}}_{\leq 2} + \frac{1}{(n+1)^2} \leq 2.$$

We see that the inductive hypothesis is simply too weak. The problem is that we did not make room for $\frac{1}{(n+1)^2}$ in the inductive hypothesis.

Lemma 2.21 *For every $n \in \mathbb{N}$*

$$\sum_{i=1}^{n} \frac{1}{i^2} \leq 2$$

holds.

Proof. We will prove a stronger assertion. Namely that for every $n \in \mathbb{N}$

$$\sum_{i=1}^{n} \frac{1}{i^2} \leq 2 - \frac{1}{n} \tag{2.22}$$

holds.

We prove (2.22) by induction on n. For $n = 1$ note that $\frac{1}{1} = 1 \leq 2 - \frac{1}{1} = 2 - 1 = 1$. Assume then that (2.22) holds for n, we show it holds for $n + 1$. By the induction hypothesis we have

$$\sum_{i=1}^{n} \frac{1}{i^2} + \frac{1}{(n+1)^2} \leq 2 - \frac{1}{n} + \frac{1}{(n+1)^2}.$$

To conclude it remains to show that $2 - \frac{1}{n} + \frac{1}{(n+1)^2} \leq 2 - \frac{1}{n+1}$. That is, $\frac{1}{(n+1)^2} + \frac{1}{n+1} = \frac{n+2}{(n+1)^2} \leq \frac{1}{n}$. Note now that $n(n+2) = n^2 + 2n$ while $(n+1)^2 = n^2 + 2n + 1$. The claim then follows. ■

How did we come up with 2 in Lemma 2.21? Can we replace it with a smaller number? What about 1? Let us try to prove that

$$\sum_{i=1}^{n} \frac{1}{i^2} \leq 1 - \frac{1}{n}.$$

For the induction step we have

$$\sum_{i=1}^{n} \frac{1}{i^2} + \frac{1}{(n+1)^2} \leq 1 - \frac{1}{n} + \frac{1}{(n+1)^2} \leq 1 - \frac{1}{(n+1)^2}.$$

So at this point we might be inclined to believe that replacing 2 with 1 is possible. However, the fact that we can prove the induction step is meaningless unless we can find some n from which we can start. Here, there cannot be such an n. Indeed, for every $n \in \mathbb{N}$ we have $\sum_{i=1}^{n} \frac{1}{i^2} \geq 1$ as the first element in the sum is 1. On the other hand $1 - \frac{1}{n} < 1$ for every $n \in \mathbb{N}$

2.2.4 *Versatility of induction*

So far we we used induction to prove inequalities. Inductions are much more versatile than this.

Lemma 2.23 *For all $n \in \mathbb{N}$: $3 \mid n^3 + 2n$.*

Proof. The proof is by induction on n. For the induction basis let us note that for $n = 1$ we have that $1^3 + 2 \cdot 1 = 3$ and so the claim holds for $n = 1$. We proceed to the induction step. Suppose then that $3 \mid n^3 + 2n$ and we seek to show that $3 \mid (n+1)^3 + 2(n+1)$. Expand $(n+1)^3$ to $n^3 + 3n^2 + 3n + 1$ and obtain

$$(n+1)^3 + 2(n+1) = n^3 + 3n^2 + 5n + 3 = (n^3 + 2n) + (3n^2 + 3n + 3).$$

Surely $3 \mid 3(n^2 + n + 1)$. Furthermore, $3 \mid (n^3 + 2n)$ by the induction hypothesis. The claim follows. ■

2.2.5 *Power sets*

In all of the examples so far we always invoked the inductive hypothesis only once. In fact, we are allowed to invoke it more than once. Here is an example of that. For a set X let $\mathcal{P}(X)$ denote the set comprised of all subsets of X, that is

$$\mathcal{P}(X) = \{Y : Y \subseteq X\};$$

another notation of $\mathcal{P}(X)$ is 2^X. We refer to $\mathcal{P}(X)$ as the *power set* of X. For instance, if $X = \{1, 2\}$ then $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. For now let us postpone the question of whether for every set X the set $\mathcal{P}(X)$ actually exists to§ 2.2.5.1; for now let us assume $\mathcal{P}(X)$ exists for every X and prove the following

Lemma 2.24 *Let X be a finite set of size n. Then $|\mathcal{P}(X)| = 2^n$.*

Proof. The proof is by induction on n. For any set of size 1, say $\{1\}$ we have that $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$. Hence $|\mathcal{P}(\{1\})| = 2^1$. Assume then that $|\mathcal{P}(\{1, \ldots, n\})| = 2^n$. We show that the claim holds for $n + 1$. The subsets of $\{1, \ldots, n, n+1\}$ can be partitioned into two types. Those that contain $n + 1$ and those that do not. Any subset not containing $n + 1$ is a subset of $\{1, \ldots, n\}$. Hence, there are 2^n sets of

this type, by the induction hypothesis. Any subset containing $n+1$ has the form $A \cup \{n+1\}$ where $A \subseteq \{1, \ldots, n\}$. The number of choices for A then is 2^n, by the inductive hypothesis. Altogether the number of subsets we have accounted for is $2^n + 2^n = 2^{n+1}$. ■

2.2.5.1 Existence of power sets

Above we considered power sets of finite sets; existence of which is trivial. Do power sets of infinite sets exist as well? Given two sets X and Y we write Y^X to denote the set of all functions $X \to Y$. We are unable to prove that the latter sets exists for any two sets; hence the following.

Power set axiom: *For any two sets X and Y the set Y^X exists.*

Given a set X each subset $S \subseteq X$ can be viewed as a boolean function on X denoted $\mathbf{1}_S : X \to \{0, 1\}$ where $\mathbf{1}_S(x) = 1$ if $x \in S$ and is zero otherwise.

Proposition 2.25 *For every set X the set $\mathcal{P}(X)$ exists.*

Proof. By the power set axiom the set $\{0,1\}^X$ exists. Given $f \in \{0,1\}^X$ we have $S_f = \{x : f(x) = 1\} \subseteq X$. The so called *replacement axiom* (which we do not mention in these notes) ensures that the replacement of each such $f \in \{0,1\}^X$ with S_f generates all subsets of X precisely. ■

We choose not delete into more details regarding this partial proof as it would entail delving into more details in pure set theory. The main point one should grasp from the above partial proof is that there is a bijection between $\mathcal{P}(X)$ and $\{0,1\}^X$.

2.2.6 *Infinitude of the natural numbers*

Given a function $f : X \to Y$ and a subset $S \subseteq X$ we write $f|_S$ to denote the function $S \to Y$ given by $f|_S(s) := f(s)$ for every $s \in S$. We say that $f|_S$ is the *restriction* of f to S.

Lemma 2.26 *Let n be a positive natural number and let $f : [n] \to \mathbb{N}$. Then there exists a positive natural number M such that $f(i) \leq M$ for every $i \in [n]$.*

Proof. The proof is by induction on n. For $n = 1$ we consider functions $\{1\} \to \mathbb{N}$ and we can choose $M = f(1)$. Assume then that the claim holds for n and consider a function $f : [n+1] \to \mathbb{N}$. By the induction hypothesis applied to $f|_{[n]}$ there exists a natural number M' such that $f|_{[n]}(i) \leq M'$ for every $i \in [n]$. As $f(n+1) \leq M' + f(n+1)$ choosing $M = M' + f(n+1)$ completes the induction step and thus the proof. ■

Theorem 2.27 *There are infinitely many natural numbers.*

Proof. Assume for the sake of contradiction that the set $\mathbb{N}$ is finite so that there exists a natural number n for which there exists a bijection from $f : [n] \to \mathbb{N}$. By Lemma 2.26, there exists a natural number M such that $f(i) \leq M$ for all $i \in \mathbb{N}$. But then $M + 1$ is a natural number that is not equal to any of the images $f(i)$ contradicting the assumption that f is a bijection. ■

The observant reader may now be confused. In the discussion following Theorem 1.55 we argued that we cannot prove that any infinite sets exist and that to do so one requires the so called axiom of infinity. So how come we just proved that the set $\mathbb{N}$ is infinite? The observant reader may now also notice that we are using induction to do so of which we learned through the WOP which we also took for granted. So the proof seen here is under the assumption that the WOP is correct.

§2.3. Strong/complete induction

The step of a weak induction has the form $S(n) \implies S(n+1)$ where $S(n)$ is assumed to be true (see Theorems 2.4 and 2.5). There is an additional type of induction which allows us to assume $S(1), \ldots, S(n)$ and using all of these (or perhaps just a part of them) prove that $S(n+1)$ is true. This form of induction is called *strong* or *complete* induction. We have the following two analogous versions of Theorems 2.4 and 2.5.

Theorem 2.28 (The second principle of finite induction)
Let $S \subseteq \mathbb{Z}^+$ be a set satisfying:

(S.1) $0 \in S$*; and*

(S.2) if $\{0, 1, \ldots, n\} \subseteq S$ *then* $n+1 \in S$.

Then $S = \mathbb{Z}^+$.

Theorem 2.29 (Strong/Complete mathematical induction) *Let $S(n)$ denote a mathematical statement that depends on $n \in \mathbb{Z}^+$. In addition, let $n_0, n_1 \in \mathbb{Z}^+$ satisfy $n_0 \leq n_1$.*

(Base) If $S(n_0), S(n_0+1), \ldots, S(n_1)$ are all true; and

(Step) if whenever $S(n_0), S(n_0+1), \ldots, S(k-1), S(k)$ are true then $S(k+1)$ is true as well,

then $S(n)$ is true for all $n \geq n_0$.

(Strong Base) It is a bit difficult to motivate at this stage why the basis of this induction has this specific form. Below we shall consider examples that will clarify this point.

Sets satisfying (I.1) and (I.2) clearly satisfy (S.1) and (S.2); consequently the principle of strong induction implies the principal of weak induction. The converse also holds.

Theorem 2.30 *The principle of weak induction implies the principle of strong induction.*

Proof. Let S be a set satisfying (S.1) and (S.2) and define

$$Q := \{n \in \mathbb{N} : k \in S \text{ for all } k < n\} \cup \{1\}.$$

If Q coincides with the naturals then so does S. Indeed, fix $n \in \mathbb{N}$ as $n \in Q$ then $\{1, \ldots, n-1\} \subseteq S$ so that $n \in S$ by (S.2); this implies that $\mathbb{N} \subseteq S$.

It remains to prove that $Q = \mathbb{N}$. This we do with the aid of weak induction. By definition Q satisfies (I.1). To see that it satisfies (I.2) let $n \in Q$ (we may assume $n > 1$); we prove that $n+1 \in Q$. The assumption that $n \in Q$ implies that $\{1, \ldots, n-1\} \subseteq S$ so that $n \in S$ by (S.2). Consequently $\{1, \ldots, n\} \subseteq S$ implying that $n+1 \in Q$. ■

The principles of weak and strong induction are then equivalent. In fact these are both equivalent to the WOP.

Theorem 2.31 *The WOP and the principles of weak induction and strong induction are all equivalent.*

To establish Theorem 2.31 it suffices to prove the following.

Lemma 2.32 *The principle of strong induction (i.e., Theorem 2.28) implies the WOP.*

Proof. Assume towards a contradiction that there exists a set $S \subseteq \mathbb{N}$ admitting no least element. We show that the set $T = \mathbb{N} \setminus S$, i.e., the complement of S satisfies both (S.1) and (S.2); this would then mean that $T = \mathbb{N}$, by Theorem 2.28, which in turn implies that $S = \emptyset$.

As 1 is the least element in $\mathbb{N}$ it follows that $1 \notin S$ as S is assumed to not have a least element. Then $1 \in T$ verifying (S.1) for T. To verify (S.2) for T we have to show that if $\{1, \ldots, n\} \subseteq T$ then $n+1 \in T$. The assumption that $\{1, \ldots, n\} \subseteq T$ means that $i \notin S$ for every $i \in [n]$. So if $n+1 \in S$ that would mean that $n+1$ is the least element in S. As S is assumed to not have a least element $n+1 \notin S$ so that $n+1 \in T$. We have thus verified (S.2) for T. ■

2.3.1 *Cauchy's inequality*

One of the most heavily used inequalities in mathematics is the Cauchy-Schwartz inequality. This inequality for real sequences reads as follows.

Lemma 2.33 *Let $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ be two sequences of real numbers. Then*

$$\left(\sum_{i=1}^{n} a_i b_i\right)^2 \leq \sum_{i=1}^{n} a_i^2 \cdot \sum_{i=1}^{n} b_i^2$$

Proof. The proof is by induction on n. For $n = 1$ the assertion is trivial formally this is enough. However, for pedagogical reasons we consider $n = 2$. Here we need to show that

$$(a_1 b_1 + a_2 b_2)^2 \leq (a_1^2 + a_2^2)(b_1^2 + b_2^2). \tag{2.34}$$

Expand both sides to obtain

$$\cancel{(a_1 b_1)^2} + 2a_1 a_2 b_1 b_2 + \cancel{(a_2 b_2)^2} \leq \cancel{(a_1 b_1)^2} + (a_1 b_2)^2 + (a_2 b_1)^2 + \cancel{(a_2 b_2)^2}$$

which is equivalent to

$$0 \leq (a_1 b_2)^2 - 2a_1 a_2 b_1 b_2 + (a_2 b_1)^2 = (a_1 b_2)^2 - 2(a_1 b_2)(a_2 b_1) + (a_2 b_2)^2 = (a_1 b_2 - a_2 b_1)^2$$

The term $(a_1 b_2 - a_2 b_1)^2$ is clearly non-negative due to the square. This completes the basis of the induction.

We proceed to the induction step. For $n \in \mathbb{Z}^+$ let $H(n)$ denote the assertion that Cauchy's inequality is true for sequences of length n. Assuming that $H(1), \ldots, H(n)$ hold, we show that $H(n+1)$ follows. In fact, we will show that $H(2)$ and $H(n)$ imply $H(n+1)$. By $H(n)$ we have that

$$\sum_{i=1}^{n} a_i b_i + a_{n+1} b_{n+1} \leq \sqrt{\sum_{i=1}^{n} a_i^2} \sqrt{\sum_{i=1}^{n} b_i^2} + a_{n+1} b_{n+1} \tag{2.35}$$

Put $\alpha := \sqrt{\sum_{i=1}^{n} a_i^2}$ and $\beta := \sqrt{\sum_{i=1}^{n} b_i^2}$ so that the r.h.s. of (2.35) becomes $\alpha\beta + a_{n+1} b_{n+1}$. By (2.34) we have

$$\alpha\beta + a_{n+1} b_{n+1} \leq (\alpha^2 + a_{n+1}^2)^{1/2} (\beta^2 + b_{n+1}^2)^{1/2}$$

and the claim follows. ■

2.3.2 *Lucas numbers*

The *Lucas numbers* are given by the sequence

$$1, 3, 4, 7, 11, 18, 29, 47, 76, \ldots.$$

Alternatively, these can be defined recursively as follows.

Definition 2.36 *The* Lucas numbers ℓ_n *are given by*

$$\begin{aligned} \ell_1 &= 1 \\ \ell_2 &= 3 \\ \ell_n &= \ell_{n-1} + \ell_{n-2}, \quad \forall n \geq 3. \end{aligned}$$

Lemma 2.37 *For all* $n \in \mathbb{Z}^+$

$$\ell_n < \left(\frac{7}{4}\right)^n$$

holds.

Proof. The proof is by induction on n. For $n = 1, 2$ the assertion holds. (In fact we must insist on verifying the induction basis for both $n = 1$ and $n = 2$). This is because in the induction step we shall invoke the hypothesis once for ℓ_{n-1} and once for ℓ_{n-2}. This is the point that we raised in *(Strong Base)*.

Assume then that for $n \geq 3$ we have that $\ell_{n-1} < \left(\frac{7}{4}\right)^{n-1}$ and $\ell_{n-2} < \left(\frac{7}{4}\right)^{n-2}$. Then

$$\begin{aligned} \ell_n = \ell_{n-1} + \ell_{n-2} &< \left(\frac{7}{4}\right)^{n-1} + \left(\frac{7}{4}\right)^{n-2} \\ &= \left(\frac{7}{4}\right)^{n-2} \left(1 + \frac{7}{4}\right) \\ &= \left(\frac{7}{4}\right)^{n-2} \left(\frac{11}{4}\right). \end{aligned}$$

Note now that $\frac{11}{4} < \left(\frac{7}{4}\right)^2$ (indeed, $16 \cdot 11 < 49 \times 4$) and so we have

$$< \left(\frac{7}{4}\right)^n$$

and the claim follows. ■

It the sequel it will be convenient to have ℓ_0 also defined.

Definition 2.38 *The* extended Lucas numbers L_n *are given by*

$$\begin{aligned} L_0 &= 2 \\ L_1 &= 1 \\ L_n &= L_{n-1} + L_{n-2}, \quad \forall n \geq 2. \end{aligned}$$

2.3.3 *Fibonacci numbers*

Perhaps the most famous recursively defined sequence is that of Fibonacci that first appeared in Fibonacci's book *Liber Abaci* in 1202. Fibonacci was faced with the following problem involving rabbits. Suppose one places a pair of rabbits one of each sex on an island. Assuming that rabbits do not breed until these are two months old, and assuming that each pair produces another pair each month, how many pairs of rabbits does one have after n months?

Let f_n denote the number of pairs of rabbits on the island after n months. Then $f_1 = 1$ and also $f_2 = 1$ as we have to wait two months for the first breeding. On the third month we have two pairs so $f_3 = 2$. More generally, $f_n = f_{n-1} + f_{n-2}$ because for each newly born pair we must wait two months.

Definition 2.39 *The* Fibonacci *sequence is defined as follows.*

$$\begin{aligned} f_1 &= 1 \\ f_2 &= 1 \\ f_n &= f_{n-1} + f_{n-2}, \quad \forall n \geq 3. \end{aligned}$$

With this definition we have

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144$$

as the first twelve numbers of the Fibonacci sequence.

We notice that apart from their initialisations the Lucas sequence (see § 2.3.2) and the Fibonacci sequence have the same definition. Indeed, it was Lucas who named the Fibonacci sequence after Fibonacci and discovered many of its properties. To clarify the connection between these sequences let us first extend the Fibonacci sequence to have f_0 defined.

Definition 2.40 *The* extended Fibonacci *sequence is defined as follows.*

$$\begin{aligned} F_0 &= 0 \\ F_1 &= 1 \\ F_n &= F_{n-1} + F_{n-2}, \quad \forall n \geq 2. \end{aligned}$$

Lemma 2.41 *For all $n \in \mathbb{Z}^+$*

$$L_n = F_{n-1} + F_{n+1}$$

holds.

Proof. The proof is by induction on n. For the induction base note that

$$\begin{aligned} L_1 &= 1 = 0 + 1 = F_0 + F_2 = F_{1-1} + F_{1+1} \\ L_2 &= 3 = 1 + 2 = F_1 + F_3 = F_{2-1} + F_{2+1} \end{aligned}$$

so the claim holds for both $n = 1, 2$ (recall *(Strong Base)*).

Suppose then that $L_n = L_{n-1} + L_{n+1}$ for $n = 1, \ldots, k-1, k$, $k \geq 2$, and let us consider L_{k+1}.

$$L_{k+1} = L_k + L_{k-1}$$

so by the induction hypothesis

$$= (F_{k-1} + F_{k+1}) + (F_{k-2} + F_k)$$

rearranging we get

$$\begin{aligned} &= (F_{k-2} + F_{k-1}) + (F_k + F_{k+1}) \\ &= F_k + F_{k+2} \end{aligned}$$

and the claim follows. ■

2.3.4 Growth of Fibonacci numbers

How fast does the Fibonacci sequence grow? In § 2.2.2 we have seen that the function 2^n grows in the sense that $\sum_{i=1}^{n} 2^i \leq 2^{n+1}$. For the Fibonacci sequence a similar phenomenon occurs.

Lemma 2.42 *For all $n \in \mathbb{Z}^+$*

$$\sum_{i=1}^{n} f_i = f_{n+2} - 1$$

holds.

Proof. The proof is by induction on n (a non-inductive proof will be presented in the practical session). For $n = 1$ note that $f_1 = 1$ and that $f_{1+2} - 1 = f_3 - 1 = 2 - 1 = 1$.

Assume then that the claim holds for $n \geq 1$, that is

$$\sum_{i=1}^{n} f_i = f_{n+2} - 1;$$

we show that it holds for $n + 1$, that is

$$\sum_{i=1}^{n+1} f_i = f_{n+3} - 1.$$

Indeed, we have

$$\underbrace{\sum_{i=1}^{n} f_i}_{\text{I.H.}} + f_{n+1} = f_{n+2} - 1 + f_{n+1} = f_{n+3} - 1$$

and the claim follows. ■

With Lemma 2.42 we might begin to suspect that f_n and 2^n are rather close. This is misleading. Lemma 2.42 is somewhat superficial and with it we cannot really estimate the rate of growth of f_n. The next lemma does.

Lemma 2.43 *Let $\alpha = (1 + \sqrt{5})/2 \approx 1.61803398875$.*

$$f_n > \alpha^{n-2}$$

for all $n \geq 3$.

Proof. The proof is by induction on n. For the induction basis we verify the claim for $n = 3$ and $n = 4$. Indeed, here we see that $\alpha^{3-2} = \alpha < 2 = f_3$ and that $\alpha^{4-2} = \alpha^2 \approx 2.61803398875 < 3 = f_4$.

Let $n > 4$ and assume that $f_k > \alpha^{k-2}$ for all $3 \leq k < n$. We consider f_n, and by the induction hypothesis we have

$$f_n = f_{n-1} + f_{n-2} > \alpha^{n-3} + \alpha^{n-4}.$$

We seek to show that $\alpha^{n-3} + \alpha^{n-4} \geq \alpha^{n-2}$. To that end note that

$$\alpha^{n-3} + \alpha^{n-4} = (\alpha + 1)\alpha^{n-4}$$

Next, we note that $\alpha + 1 = \alpha^2$. Indeed, α is a solution to $x^2 - x - 1 = 0$ (or put another way, $x^2 = x + 1$) and so we have that

$$(\alpha + 1)\alpha^{n-4} = \alpha^2\alpha^{n-4} = \alpha^{n-2}$$

and the claim follows. ■

To distinguish f_n from 2^n we prove the following.

Lemma 2.44 *For all $n \geq 11$*

$$f_n < 2^{n-4}$$

holds

Proof. The proof is by induction on n. For the induction basis we consider $n = 11$ and $n = 12$. Indeed here we see that $2^{11-4} = 128 > 89 = f_{11}$ and that $2^{12-4} = 256 > 144 = f_{12}$.

Let $n \geq 13$ and assume that $f_k < 2^{k-4}$ for all $11 \leq k \leq n - 1$. For f_n we have

$$\begin{aligned} f_n &= f_{n-1} + f_{n-2} \\ &< 2^{n-5} + 2^{n-6} \\ &= 2^{n-6} \cdot (2 + 1) \\ &< 2^{n-6} \cdot 2^2 \\ &= 2^{n-4}. \end{aligned}$$

The claim follows. ■

So far we were able to completely distinguish f_n from 2^n as follows.

Corollary 2.45 *For all $n \geq 11$*

$$\alpha^{n-2} < f_n < 2^{n-4}$$

holds.

In fact much more is known. Let $\beta = (1 - \sqrt{5})/2$.

Theorem 2.46 *For all $n \in \mathbb{Z}^+$*

$$f_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$$

holds.

§2.4. Exercises

Exercise 1. Recall that the Fibonacci numbers are defined by $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for $n \geq 2$. Prove that f_n is even if and only if $3 \mid n$

Exercise 2. In this exercise you will prove the so called AM-GM theorem relating the arithmetic means with the geometric mean.

1. Let $a > 1$ an $b < 1$ be two real numbers. Prove that
$$a + b > ab + 1$$

2. Let $n \geq 1$ be a positive integer and let $a_1, \ldots, a_n$ be a sequence of non-negative real numbers. Prove that if $\prod_{i=1}^{n} a_i = a_1 \cdot a_2 \cdots a_n = 1$ then $\sum_{i=1}^{n} a_i \geq n$.

3. Let $n \geq 1$ be a positive integer and let $a_1, \ldots, a_n$ be a sequence of non-negative real numbers. Prove that
$$\left(\prod_{i=1}^{n} a_i\right)^{1/n} = (a_1 \cdot a_2 \cdots a_n)^{1/n} \leq \frac{\sum_{i=1}^{n} a_i}{n} \tag{2.47}$$
This is the full version of the AM-GM theorem.

Exercise 3. In this exercise you will prove the so called Bernoulli's inequality that we have used in one of the practical sessions without proof.

Let $x > -1$. Prove that $(1 + x)^n \geq 1 + nx$ for every $n \in \mathbb{N}$.

Exercise 4. Prove that every $N \in \mathbb{N}$ is either a perfect square or $\sqrt{N}$ is irrational.

Exercise 5. Prove that $8 \mid n^2 - 1$ for every odd $n \in \mathbb{Z}^+$.

Exercise 6. Prove that $3 \mid 4^n + 5$ for every $n \in \mathbb{Z}^+$.

Exercise 7. Prove that $13 \mid 2^{4n+2} + 3^{n+2}$ for every $n \in \mathbb{N}$.

Hint: Write 2^{4n+2} as $13 \cdot 2^{4n-2} + 3 \cdot 2^{4n-2}$.

Exercise 8. Prove that $9 \mid 4^n + 15n - 1$ for every $n \in \mathbb{Z}^+$.

Hint: Exercise 6.

Recall that the Fibonacci numbers are defined by $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for $n \geq 2$.

Exercise 9. Prove that $f_n = 5f_{n-4} + 3f_{n-5}$. holds for every $n > 5$.

Exercise 10. Prove that $5 \mid f_n$ whenever $5 \mid n$.

Exercise 11. Define $a_0 = 1, \quad a_n = 5a_{n-1} + 4,$ for $n \geq 1$. Prove that $a_n \leq 5^{n+1}$.

Hint: Prove that $a_n \leq 5^{n+1} - 1$.

Exercise 12. Define $b_0 = 1, \quad b_n = 4b_{n-1} - 1,$ for $n \geq 1$. Prove that $b_n \geq 4^{n-1}$.

Exercise 13. Define $c_0 = 0, \quad c_n = 2c_{n-1} + n,$ for $n \geq 1$. Prove that $c_n \leq 2^{n+2}$.

Exercise 14. Prove that $n^3 < 2^n$ for every integer $n \geq 10$.

Exercise 15. Prove that $\left|\sin nx\right| \leq n\left|sinx\right|$ for all $n \in \mathbb{N}$ and $x \in \mathbb{R}$.

Exercise 16. Let
$$a_1 = 11, \quad a_2 = 21, \quad a_n = 3a_{n-1} - 2a_{n-2},\ n \geq 3.$$

Prove that $a_n = 5 \cdot 2^n + 1$ for every $n \geq 1$.

Exercise 17. Prove by induction the following equalities:

1. $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, for every $n \in \mathbb{Z}^+$.
2. $\sum_{i=n}^{2n-1} \frac{1}{i(i+1)} = \frac{1}{2n}$, for every $n \in \mathbb{Z}^+$.
3. $\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$, for every $n \in \mathbb{Z}^+$.
4. $\sum_{i=0}^{n} ar^i = \frac{a(r^{n+1}-1)}{r-1}$, for every $n \in \mathbb{N}$, $a, r \in \mathbb{R}$, $r \neq 1$.

Exercise 18. Without using the closed formula for $\sum_{i=1}^{n} i$ prove directly that $\sum_{i=1}^{n} i \geq \frac{n^2}{2}$ for every $n \in \mathbb{N}$.

Exercise 19. Prove by induction the following inequalities:

1. $(1+a)^n \geq 1 + na$, for every $n \in \mathbb{Z}^+$, $a > -1$.
2. $2 \cdot 5^n \leq 4^n + 6^n$, for every $n \in \mathbb{N}$.

Exercise 20.

1. Define the sequence $a_1 = 1$, $a_2 = 2$, $a_{n+2} = a_n + 1$, for every $n \in \mathbb{Z}^+$. Prove that $a_n = \frac{1}{2}(n+1) + \frac{1}{4}(1 + (-1)^n)$, for every $n \in \mathbb{Z}^+$.
2. Define the sequence $b_0 = 1$, $b_1 = 2$, $b_2 = 3$, $b_{n+3} = b_{n+2} + b_{n+1} + b_n$, for every $n \in \mathbb{Z}^+$. Prove that $b_n \leq 2^n$, for every $n \in \mathbb{N}$.
3. Define the Fibonacci sequence $f_0 = 0$, $f_1 = 1$, $f_n = f_{n-1} + f_{n-2}$, for every $n \in \mathbb{Z}^+$, $n \geq 2$. Prove that $f_n \geq \left(\frac{3}{2}\right)^{n-2}$ for every $n \in \mathbb{Z}^+$.

Exercise 21. Given two integers k and n, we write $k \mid n$ to denote that k divides n (i.e., that n is a multiple of k). Prove by induction the following divisibility statements:

1. $6 \mid (2n^3 + 3n^2 + n)$, for every $n \in \mathbb{N}$.
2. $6 \mid (n^3 + 5n)$, for every $n \in \mathbb{N}$.
3. $16 \mid n^4 + 4n^2 + 11$, for every odd $n \in \mathbb{Z}^+$.

Exercise 22. This exercise is in anticipation of § 5.2.3. Prove that for every $k \geq 1$,

$$\frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \cdots - 1 = \sum_{i=0}^{2^k - 1} (-1)^i x^{2^k - 1 - i}.$$

In your proof you are not to use long division of polynomials; instead you are to provide an inductive proof of this fact.

§2.5. Solutions

Some of the solutions have been written by the TAs in the course and thus have a different style of writing to them. Over time we hope to normalise this part of the text as well.

Solution for Exercise 1. As the assertion involves an if and only if statement it is not enough to show that $2 \mid f_{3n}$ for every $n \geq 1$. We must also show that any Fibonacci number f_i such that $3 \not| i$ is not even. The following claim establishes this.

Claim 2.48. *For every integer $n \geq 1$ it holds that f_{3n} is even and both f_{3n-1} and f_{3n-2} are odd.*

Proof. The proof is by induction on n. For the induction basis we consider $n = 1$. Here we have that $f_{3\cdot 1-2} = f_1 = 1$, $f_{3\cdot 1-1} = f_2 = 1$, and $f_{3\cdot 1} = f_3 = 2$.

We proceed to the induction step. Assume the claim holds for $n \geq 0$. That is, we assume that f_{3n} is even and that both f_{3n-1} and f_{3n-2} are odd. We show that the claim holds for $n+1$. We consider three cases.

(a) By the definition of Fibonacci numbers we have that $f_{3(n+1)-2} = f_{3n+1} = f_{3n} + f_{3n-1}$. By the induction hypothesis f_{3n} is even and f_{3n-1} is odd; so that $f_{3(n+1)-2}$ is odd.

(b) Next, we consider $f_{3(n+1)-1}$. Here we have $f_{3(n+1)-1} = f_{3n+2} = f_{3n+1} + f_{3n}$. By the induction hypothesis f_{3n} is even. In case (a) we have shown that f_{3n+1} is odd. It then follows that $f_{3(n+1)-1} = f_{3n+2}$ is odd.

(c) Finally, we consider $f_{3(n+1)}$. In this case we have that $f_{3(n+1)} = f_{3n+3} = f_{3n+2} + f_{3n+1}$. In case (a) we have shown that f_{3n+1} is odd and in case (b) we proved that f_{3n+2} is odd. It follows that f_{3n+3} is even.

■

Solution for Exercise 2.

1. Consider the inequality $a > 1$ which is given to us. Multiplying both sides of this inequality with $1 - b > 0$ yields
$$a - ab > 1 - b$$
which implies the claim.

2. The proof is by induction on n. For $n = 1$ the claim is trivial and is left to the reader to verify. Assume then that the claim holds for sequences of length $n - 1$ and let us consider a sequence $\mathcal{A} = (a_1, \ldots, a_n)$ of length n satisfying $\prod_i a_i = 1$. We may arrange the sequence $\mathcal{A}$ so that $a_{n-1} = \min \mathcal{A}$ and $a_n = \max \mathcal{A}$.

   (a) We may assume $a_n > 1$. To see this note that if $a_n = \max \mathcal{A} < 1$ then $\prod_i a_i < 1$ contradicting the assumption. Next, if $a_n = 1$ then $\prod_{i=1}^{n-1} a_i = 1$. In which case the induction hypothesis applied to $(a_1, \ldots, a_{n-1})$ yields $\sum_{i=1}^{n-1} a_i \geq n - 1$; so that $\sum_{i=1}^{n} a_i \geq n$ as $a_n = 1$ is assumed. It follows then that $a_n > 1$.

   (b) We may assume that $a_{n-1} < 1$. Assuming $a_{n-1} = \min \mathcal{A} > 1$ negates the assumption that $\prod_i a_i = 1$. Assuming $a_{n-1} = \min \mathcal{A} = 1$ together with the assumption $\prod_i a_i = 1$ implies that $a_i = 1$ for every $i \in [n]$ in which case the claim is trivially true (alternatively it negates our assumption that $a_n > 1$).

We have thus established that

$$a_n > 1 \text{ and } a_{n-1} < 1. \tag{2.49}$$

Define now the sequence $\mathcal{B} = (b_1, \ldots, b_{n-1})$ of length $n-1$ where the latter is given by

$$\begin{aligned} b_i &= a_i, \quad 0 \le i \le n-2, \\ b_{n-1} &= a_{n-1} \cdot a_n. \end{aligned}$$

As $\prod_i b_i = \prod_i a_i = 1$ the induction hypothesis can be applied to the sequence $\mathcal{B}$ as to attain.

$$\sum_{i=1}^{n-1} b_i = \sum_{i=1}^{n-2} a_i + a_{n-1} \cdot a_n \ge n-1.$$

If $a_{n-1} \cdot a_n \ge 1$ the claim follows so assume the contrary i.e., that $a_{n-1} \cdot a_n < 1$. By the claim appearing in the first part of the question we then have $a_{n-1} + a_n > a_{n-1}a_n + 1$. It then follows that

$$\sum_{i=1}^{n-2} a_i + (a_{n-1} + a_n) > \sum_{i=1}^{n-2} a_i + a_{n-1}a_n + 1 \ge n$$

concluding the proof.

3. Given the sequence $a_1, \ldots, a_n$ define the sequence $b_1, \ldots, b_n$ given by

$$b_i := \frac{a_n}{(a_1 \cdot a_2 \cdots a_n)^{1/n}}.$$

Then $\prod_i b_i = 1$ so that $\sum_i b_i \ge n$, by the claim proved in the second section of this question. The assertion now follows.

Solution for Exercise 3. The proof is by induction on n. For $n = 1$ we have equality hold. Assume then Bernoulli's inequality holds for n and let us consider $n+1$.

$$\begin{aligned} (1+x)^{n+1} &= (1+x)^n(1+x) \\ &\ge (1+nx)(1+x) \\ &= 1 + (n+1)x + nx^2 \\ &\ge 1 + (n+1)x; \end{aligned}$$

where the second inequality is due to the induction hypothesis.

Solution for Exercise 4. Suppose N is not a perfect square and that $\sqrt{N} \in \mathbb{Q}$. This implies that we may write

$$\sqrt{N} = a + \frac{b}{c} \tag{2.50}$$

where $a, b, c \in \mathbb{N}$ and $\frac{b}{c}$ is in lowest terms, i.e., $b < c$. Of all options to write $\sqrt{N}$ as in (2.50) choose a, b, c so that for any other alternative a', b', c' satisfying $\sqrt{N} = a' + \frac{b'}{c'}$ the fraction $\frac{b'}{c'}$ does not appear in lower terms than $\frac{b}{c}$; in particular it means that we cannot have $b' \le b$ and $c' < c$ hold together. By the well-ordering principle this is possible (see the proof we had for $\sqrt{2}$; there we essentially do this process using the sets S and S').

Write $c\sqrt{N} = ac + b$. Then

$$c^2 N = (ac+b)^2 = c^2a^2 2cab + b^2.$$

Then

$$b^2 = c^2N - c^2a^2 - 2cab = c(cN - ca^2 - 2ab).$$

Set $d := cN - ca^2 - 2ab$ and write $c = b^2/d$. Substituting this into (2.50) we arrive at

$$\sqrt{N} = a + \frac{b}{c} = a + \frac{d}{b}$$

As $b < c$ we will reach a contradiction if we prove that in addition $d \leq b$; as then $\frac{d}{b}$ is written in lower terms than $\frac{b}{c}$. Assume then that $d > b$. Then $cd > b^2$ as $c > b$ and $d > b$. Hence we reach a contradiction.

Solution for Exercise 5. The proof is by induction on n. For the induction basis we consider $n = 1$. Here we have that $8 \mid 1^2 - 1 = 0$ holds. We proceed to the induction step. Suppose the claim holds for an odd integer $n \geq 1$, that is we assume that $8 \mid n^2 - 1$. We prove that the claim holds for the next odd integer i.e. $8 \mid (n+2)^2 - 1$. Since n is odd there exists $m \in \mathbb{Z}$ such that $n = 2m - 1$, therefore $(n+2)^2 - 1 = n^2 + 4n + 4 - 1 = n^2 - 1 + 4(2m-1) + 4 = n^2 - 1 + 8m$. By the induction hypothesis $8 \mid n^2 - 1$, therefore $8 \mid n^2 - 1 + 8m$, which implies $8 \mid (n+2)^2 - 1$.

Solution for Exercise 6. The proof is by induction on n. For the induction basis we consider $n = 1$. Here we have that $3 \mid 4^1 + 5 = 9$ holds. We proceed to the induction step. Suppose the claim holds for $n \geq 1$, that is we assume that $3 \mid 4^n + 5$. We prove that the claim holds for $n+1$ i.e. $3 \mid 4^{n+1} + 5$. $4^{n+1} + 5 = 4 \cdot 4^n + 5 = 4^n + 5 + 3 \cdot 4^n$. By the induction hypothesis $3 \mid 4^n + 5$ and since $3 \mid 3 \cdot 4^n$ it also holds that $3 \mid 4^n + 5 + 3 \cdot 4^n$.

Solution for Exercise 7. The proof is by induction on n. For the induction basis we consider $n = 0$. Here we have that $13 \mid 2^2 + 3^2 = 13$ holds. We proceed to the induction step. Suppose the claim holds for $n \geq 0$, that is we assume that $13 \mid 2^{4n+2} + 3^{n+2}$. We prove that the claim holds for $n+1$ i.e. $13 \mid 2^{4(n+1)+2} + 3^{(n+1)+2}$. $2^{4(n+1)+2} + 3^{(n+1)+2} = 2^{4n+6} + 3^{n+3} = 16 \cdot 2^{4n+2} + 3 \cdot 3^{n+2} = 13 \cdot 2^{4n+2} + 3 \cdot (2^{4n+2} + 3^{n+2})$. By the induction hypothesis $13 \mid 2^{4n+2} + 3^{n+2}$ hence $13 \mid 3 \cdot (2^{4n+2} + 3^{n+2})$ and since $13 \mid 13 \cdot 2^{4n+2}$ it also holds that $13 \mid 13 \cdot 2^{4n+2} + 3 \cdot (2^{4n+2} + 3^{n+2})$.

Solution for Exercise 8. The proof is by induction on n. For the induction basis we consider $n = 1$. Here we have that $9 \mid 4^0 - 1 = 0$ holds. We proceed to the induction step. Suppose the claim holds for $n \geq 1$, that is we assume that $9 \mid 4^n + 15n - 1$. We prove that the claim holds for $n+1$ i.e. $9 \mid 4^{n+1} + 15(n+1) - 1$. $4^{n+1} + 15(n+1) - 1 = 4 \cdot 4^n + 15n + 15 - 1 = 4^n + 15n - 1 + 3(4^n + 5)$. By the induction hypothesis $9 \mid 4^n + 15n - 1$. By Exercise 6 $3 \mid 4^n + 5$ and therefore $9 \mid 3(4^n + 5)$, hence $9 \mid 4^n + 15n - 1 + 3(4^n + 5)$.

Solution for Exercise 9.

$$f_n = f_{n-1} + f_{n-2} = 2f_{n-2} + f_{n-3} = 3f_{n-3} + 2f_{n-4} = 5f_{n-4} + 3f_{n-5}$$

Solution for Exercise 10. The proof is by induction on n. For the induction basis we consider $n \in \{0, 1, 2, 3, 4\}$. Here we have that $5 \mid f_0$ and $5 \nmid f_1, f_2 = 1, f_3 = 2, f_4 = 3$ holds. We proceed to the induction step. Suppose the claim holds for $n \geq 1$, that is we assume that $5 \mid f_k$ if and only if $5 \mid k$, for every $k \leq n$. We prove that the claim holds for $n+1$ i.e. $5 \mid f_{n+1}$ if and only if $5 \mid n+1$. As this is an if and only if statement, it is not enough to show that if $5 \mid f_{n+1}$ then $5 \mid n+1$. We also need to prove the other direction, if $5 \mid n+1$ then $5 \mid f_{n+1}$. Assume that $5 \mid f_{n+1}$. By the previous part

$f_{n+1} = 5f_{n-3} + 3f_{n-4}$, hence $5 \mid 3f_{n-4}$. Since 5 and 3 are relatively prime we get $5 \mid f_{n-4}$, so by the induction hypothesis, $5 \mid (n-4)$, therefore $5 \mid (n+1)$. We now prove the second direction. Assume that $5 \mid (n+1)$. By Exercise 9 $f_{n+1} = 5f_{n-3} + 3f_{n-4}$. Since $5 \mid (n+1)$ it also holds that $5 \mid (n-4)$, therefore by the induction hypothesis $5 \mid f_{n-4}$, hence $5 \mid f_{n+1}$.

Solution for Exercise 11. We will prove a stronger claim: $a_n \leq 5^{n+1} - 1$ for every $n \in \mathbb{N}$. The proof is by induction on n. For the induction basis we consider $n = 0$. Here we have that $1 \leq 5^1 - 1 = 4$ holds. We proceed to the induction step. Suppose the claim holds for $n \geq 0$, that is we assume that $a_n \leq 5^{n+1} - 1$. We prove that the claim holds for $n+1$ i.e. $a_{n+1} \leq 5^{n+2} - 1$. $a_{n+1} = 5a_n + 4 \leq 5 \cdot (5^{n+1} - 1) + 4 = 5^{n+2} - 1$, where the inequality is by the induction hypothesis.

Solution for Exercise 12. First we note that $b_0 = 1 \geq 4^{-1}$. For $n \geq 1$ we will prove a stronger claim: $b_n \geq 4^{n-1} + 1$. The proof is by induction on n. For the induction basis we consider $n = 1$. Here we have that $4b_0 - 1 = 3 \geq 2 = 4^0 + 1$ holds. We proceed to the induction step. Suppose the claim holds for $n \geq 1$, that is we assume that $b_n \geq 4^{n-1} + 1$. We prove that the claim holds for $n+1$ i.e. $b_{n+1} \geq 4^n + 1$. $b_{n+1} = 4b_n - 1 \geq 4 \cdot (4^{n-1} + 1) - 1 = 4^n + 3 \geq 4^n + 1$, where the first inequality is by the induction hypothesis.

Solution for Exercise 13. First we note that $c_0 = 0 \leq 2^2$, $c_1 = 1 \leq 2^3$, $c_2 = 4 \leq 2^4$. For $n \geq 3$ we will prove a stronger claim: $c_n \leq 2^{n+2} - 2n$. The proof is by induction on n. For the induction basis we consider $n = 3$. Here we have that $c_3 = 2c_2 + 3 = 11 \leq 2^5$ holds. We proceed to the induction step. Suppose the claim holds for $n \geq 3$, that is we assume that $c_n \leq 2^{n+2} - 2n$. We prove that the claim holds for $n+1$ i.e. $c_{n+1} \leq 2^{n+3} - 2(n+1)$. $c_{n+1} = 2c_n + n + 1 \leq 2 \cdot (2^{n+2} - 2n) + n + 1 = 2^{n+3} - 3n + 1 \leq 2^{n+3} - 2(n+1)$, where the first inequality is by the induction hypothesis and the last one hold for every $n \geq 3$.

Solution for Exercise 14. The proof is by induction on n. For the induction basis we consider $n = 10$. Here we have that $10^3 = 1000 < 1024 = 2^{10}$ holds. We proceed to the induction step. Suppose the claim holds for $n \geq 10$, that is we assume that $n^3 < 2^n$. We prove that the claim holds for $n+1$ i.e. $(n+1)^3 < 2^{n+1}$. $(n+1)^3 = n^3 + 3n^2 + 3n + 1 < n^3 + 3n^2 + 3n^2 + n^2 = n^3 + 7n^2 < n^3 + n \cdot n^2 = 2n^3 < 2 \cdot 2^n = 2^{n+1}$, Where the second inequality is since $n > 7$ and the last inequality is by the induction hypothesis.

Solution for Exercise 15. The proof is by induction on n. For $n = 1$ the claim is an identity. Assume the claim is true for n and consider $n+1$.

$$\begin{aligned} \big|\sin(n+1)x\big| &= \big|\sin(nx + x)\big| \\ &= \big|\sin nx \cos x + \cos nx \sin x\big|; \end{aligned}$$

the triangle inequality then yields

$$\leq \big|\sin nx\big|\big|\cos x\big| + \big|\cos nx\big|\big|\sin x\big|;$$

as $\big|\cos y\big| \leq 1$ for all $y \in \mathbb{R}$ we arrive at

$$\big|\sin(n+1)x\big| \leq \big|\sin nx\big| + \big|\sin x\big|;$$

by the induction hypothesis we have

$$\begin{aligned} &\leq n\big|\sin x\big| + \big|\sin x\big| \\ &= (n+1)\big|\sin x\big|. \end{aligned}$$

Solution for Exercise 16. The proof is by induction on n. For the induction basis we consider $n = 1, 2$. Here we note that

$$a_1 = 5 \cdot 2 + 1 = 11,$$
$$a_2 = 5 \cdot 2^2 + 1 = 21.$$

We proceed to the induction hypothesis. Assume that the claim holds for all positive integers up to k. That is, $a_i = 5 \cdot 2^i + 1$ for all $i \in [1, k]$. We prove the same equality for $k + 1$.

$$\begin{aligned} a_{k+1} &= 3 \cdot a_k - 2 \cdot a_{k-1} \\ &= 3(5 \cdot 2^k + 1) - 2(5 \cdot 2^{k-1} + 1) \\ &= 10 \cdot 2^k + 1 \\ &= 5 \cdot 2 \cdot 2^k + 1 \\ &= 5 \cdot 2^{k+1} + 1 \end{aligned}$$

Solution for Exercise 17.

1. The proof is by induction on n. For the induction basis we consider $n = 1$. Here we have that $1 = \frac{1 \cdot 2}{2}$ holds. We proceed to the induction step. Assume the claim holds for $n \geq 1$, that is we assume that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. We prove that the claim holds for $n + 1$.

$$\begin{aligned} \sum_{i=1}^{n+1} i &= \sum_{i=1}^{n} i + n + 1 \\ &= \frac{n(n+1)}{2} + n + 1 \\ &= \frac{n^2 + 3n + 2}{2} \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

2. The proof is by induction on n. For the induction basis we consider $n = 1$. Here we have that $\frac{1}{1 \cdot 2} = \frac{1}{2}$ holds. We proceed to the induction step. Assume the claim holds for $n \geq 1$, that is we

assume that $\sum_{i=n}^{2n-1} \frac{1}{i(i+1)} = \frac{1}{2n}$. We prove that the claim holds for $n+1$.

$$\begin{aligned}
\sum_{i=n+1}^{2n+1} \frac{1}{i(i+1)} &= \sum_{i=n}^{2n-1} \frac{1}{i(i+1)} - \frac{1}{n(n+1)} \\
&+ \frac{1}{2n(2n+1)} + \frac{1}{(2n+1)(2n+2)} \\
&= \frac{1}{2n} - \frac{2n+1}{2n(2n+1)(n+1)} \\
&= \frac{(2n+1)(n+1) - 2n - 1}{2n(n+1)(2n+1)} \\
&= \frac{2n^2+n}{2n(n+1)(2n+1)} \\
&= \frac{1}{2(n+1)}.
\end{aligned}$$

3. The proof is by induction on n. For the induction basis we consider $n = 1$. Here we have that $1^3 = \left(\frac{1\cdot 2}{2}\right)^2$ holds. We proceed to the induction step. Assume the claim holds for $n \geq 1$, that is we assume that $\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$. We prove that the claim holds for $n+1$.

$$\begin{aligned}
\sum_{i=1}^{n+1} i^3 &= \sum_{i=n}^{n} i^3 + (n+1)^3 \\
&= \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 \\
&= (n+1)^2 \left(\frac{n^2}{4} + n + 1\right) \\
&= (n+1)^2 \left(\frac{n^2+4n+4}{4}\right) \\
&= \frac{(n+1)^2(n+2)^2}{4}.
\end{aligned}$$

4. The proof is by induction on n. For the induction basis we consider $n = 0$. Here we have that $ar^0 = \frac{a(r^1-1)}{r-1}$ holds. We proceed to the induction step. Assume the claim holds for $n \geq 0$, that is we assume that $\sum_{i=0}^{n} ar^i = \frac{a(r^{n+1}-1)}{r-1}$. We prove that the claim holds for $n+1$.

$$\begin{aligned}
\sum_{i=0}^{n+1} ar^i &= \sum_{i=0}^{n} ar^i + ar^{n+1} \\
&= \frac{a(r^{n+1}-1)}{r-1} + ar^{n+1} \\
&= \frac{a(r^{n+1} - 1 + r^{n+1}(r-1))}{r-1} \\
&= \frac{a(r^{n+2}-1)}{r-1}.
\end{aligned}$$

Solution for Exercise 18. The proof is by induction on n. For the induction basis we consider

$n = 1$. Here we have that $1 \geq \frac{1}{2}$ holds. We proceed to the induction step. Suppose the claim holds for $n \geq 1$, that is we assume that $\sum_{i=1}^{n} i \geq \frac{n^2}{2}$. We prove that the claim holds for $n+1$ i.e. $\sum_{i=1}^{n+1} i \geq \frac{(n+1)^2}{2}$. $\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + n + 1 \geq \frac{n^2}{2} + n + 1 = \frac{n^2+2n+2}{2} > \frac{n^2+2n+1}{2} = \frac{(n+1)^2}{2}$, where the first inequality is by the induction hypothesis.

Solution for Exercise 19.

1. The proof is by induction on n. For the induction basis we consider $n = 1$. Here we have that $(1+a)^1 \geq 1 + a$ holds. We proceed to the induction step. Assume the claim holds for $n \geq 1$, that is we assume that $(1+a)^n \geq 1 + na$. We prove that the claim holds for $n+1$.

$$\begin{aligned}(1+a)^{n+1} &= (1+a)(1+a)^n \\ &\geq (1+a)(1+na) = 1 + (n+1)a + na^2 \\ &\geq 1 + (n+1)a.\end{aligned}$$

2. The proof is by induction on n. For the induction basis we consider $n = 0$. Here we have that $2 \cdot 5^0 \leq 4^0 + 6^0$ holds. We proceed to the induction step. Assume the claim holds for $n \geq 0$, that is we assume that $2 \cdot 5^n \leq 4^n + 6^n$. We prove that the claim holds for $n+1$.

$$\begin{aligned}2 \cdot 5^{n+1} &= 5 \cdot (2 \cdot 5^n) \leq 5 \cdot (4^n + 6^n) \\ &= 4 \cdot 4^n + 4^n + 6 \cdot 6^n - 6^n \\ &= 4^{n+1} + 6^{n+1} + 4^n - 6^n \\ &\leq 4^{n+1} + 6^{n+1}.\end{aligned}$$

Solution for Exercise 20.

1. The proof is by induction on n. For the induction basis we consider $n = 2$. Here we have that $a_1 = 1$ and $a_2 = 2 = \frac{1}{2}(2+1) + \frac{1}{4}(1+1)$ holds. We proceed to the induction step. Assume the claim holds for every integer $k \leq n$, for $n \geq 1$, that is we assume that $a_k = \frac{1}{2}(k+1) + \frac{1}{4}\left(1 + (-1)^k\right)$. We prove that the claim holds for $n+1$.

$$\begin{aligned}a_{n+2} &= a_n + 1 \\ &= \frac{1}{2}(n+1) + \frac{1}{4}\left(1 + (-1)^n\right) + 1 \\ &= \frac{1}{2}(n+3-2) + \frac{1}{4}\left(1 + (-1)^{n+2}\right) + 1 \\ &= \frac{1}{2}(n+3) + \frac{1}{4}\left(1 + (-1)^{n+2}\right).\end{aligned}$$

2. The proof is by induction on n. For the induction basis we consider $n = 0, 1, 2$. Here we have that $b_0 = 1 \leq 2^0$, $b_1 = 2 \leq 2^1$ and $b_2 = 3 \leq 2^2$ holds. We proceed to the induction step. Assume the claim holds for every integer $k \leq n$, for $n \geq 1$, that is we assume that $b_k \leq 2^k$. We prove that the claim holds for $n+1$.

$$\begin{aligned}b_{n+1} &= b_n + b_{n-1} + b_{n-2} \\ &\leq 2^n + 2^{n-1} + 2^{n-2} \\ &= 4 \cdot 2^{n-2} + 2 \cdot 2^{n-2} + 2^{n-2} \\ &= 2^{n+1}.\end{aligned}$$

3. The proof is by induction on n. For the induction basis we consider $n = 1, 2$. Here we have that $f_1 = f_2 = 1 \geq \frac{2}{3}$ holds. We proceed to the induction step. Assume the claim holds for every integer $k \leq n$, for $n \geq 1$, that is we assume that $f_k \geq \left(\frac{3}{2}\right)^{k-2}$. We prove that the claim holds for $n+1$.

$$\begin{aligned} f_n &= f_{n-1} + f_{n-2} \\ &\geq \left(\frac{3}{2}\right)^{n-3} + \left(\frac{3}{2}\right)^{n-4} \\ &= \frac{2}{3}\left(\frac{3}{2}\right)^{n-2} + \frac{4}{9}\left(\frac{3}{2}\right)^{n-2} \\ &= \frac{10}{9}\left(\frac{3}{2}\right)^{n-2} \\ &\geq \left(\frac{3}{2}\right)^{n-2}. \end{aligned}$$

Solution for Exercise 21.

1. The proof is by induction on n. For the induction basis we consider $n = 0$. Here we have that $6 \mid 0$ holds. We proceed to the induction step. Assume the claim holds for $n \geq 0$, that is we assume that $6 \mid (2n^3 + 3n^2 + n)$. We prove that the claim holds for $n+1$.

$$\begin{aligned} &2(n+1)^3 + 3(n+1)^2 + (n+1) = \\ &2n^3 + 6n^2 + 6n + 2 + 3n^2 + 6n + 3 + n + 1 = \\ &2n^3 + 3n^2 + n + 6(n^2 + 2n + 1). \end{aligned}$$

By the induction assumption $6 \mid 2n^3 + 3n^2 + n$, and since $6 \mid 6(n^2 + 2n + 1)$ it also holds that $6 \mid 2(n+1)^3 + 3(n+1)^2 + (n+1)$.

2. The proof is by induction on n. For the induction basis we consider $n = 0$. Here we have that $6 \mid 0$ holds. We proceed to the induction step. Assume the claim holds for $n \geq 0$, that is we assume that $6 \mid (n^3 + 5n)$. We prove that the claim holds for $n+1$.

$$\begin{aligned} &(n+1)^3 + 5(n+1) = n^3 + 3n^2 + 3n + 1 + 5n + 5 \\ &= n^3 + 5n + 3n^2 + 3n + 6 \\ &= n^3 + 5n + 3(n^2 + n + 2) \\ &= n^3 + 5n + 3(2 + n(n+1)). \end{aligned}$$

By the induction assumption $6 \mid n^3 + 5n$. $2 \mid n(n+1)$, therefore $2 \mid (2 + n(n+1))$. Then $6 \mid 3(2 + n(n+1))$. We conclude that $6 \mid (n+1)^3 + 5(n+1)$.

3. The proof is by induction on n. For the induction basis we consider $n = 1$. Here we have that $16 \mid 1 + 4 + 11$ holds. We proceed to the induction step. Assume the claim holds for $n \geq 1$, that is we assume that $16 \mid n^4 + 4n^2 + 11$. We prove that the claim holds for next odd integer i.e. $n+2$.

Since n is odd there exists $m \in \mathbb{Z}$ such that $n = 2m - 1$. Therefore:

$$\begin{aligned}
&(n+2)^4 + 4(n+2)^2 + 11 = (2m+1)^4 + 4(2m+1)^2 + 11 \\
&= (2m-1+2)^4 + 4(2m-1+2)^2 + 11 \\
&= (2m-1)^4 + 8(2m-1)^3 + 24(2m-1)^2 \\
&+ 32(2m-1) + 16 + 4(2m-1)^2 + 16(2m-1) + 16 + 11 \\
&= (2m-1)^4 + 4(2m-1)^2 + 11 + 8(2m-1)^3 + 24(2m-1)^2 \\
&+ 48(2m-1) + 32 \\
&= (2m-1)^4 + 4(2m-1)^2 + 11 + (2m-1)^2(8(2m-1)+24) \\
&+ 48(2m-1) + 32 \\
&= (2m-1)^4 + 4(2m-1)^2 + 11 + 16(2m-1)^2(m+1) \\
&+ 48(2m-1) + 32.
\end{aligned}$$

By the induction assumption $16 \mid (2m-1)^4 + 4(2m-1)^2 + 11$ and since $16 \mid 16(2m-1)^2(m+1) + 48(2m-1) + 32$, we conclude that $16 \mid (n+2)^4 + 4(n+2)^2 + 11$.

Solution for Exercise 22. The proof is by induction on k. For $k = 1$, the claim is essentially self-evident as

$$\frac{x^2 - 1}{x+1} = \frac{(x-1)(x+1)}{x+1} = x - 1.$$

Prior to considering the general case, we find it instructive to linger on the $k = 2$ case. Here, we may write

$$\frac{x^{2^2} - 1}{x+1} = \frac{(x^2-1)(x^2+1)}{x+1} = \frac{(x-1)(x+1)(x^2+1)}{x+1} = (x-1)(x^2+1).$$

Progressing on to the general case, lets us assume the claim holds for some $k \geq 1$ and consider $k+1$. Following the illuminating argument shown for $k = 2$, we write

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

The I.H. asserts that $x + 1 \big| x^{2^k} - 1$. The claim follows.

Lecture 3

Binomial coefficients

§3.1. Counting subsets

In Lemma 2.24 we proved that a set consisting of n elements has 2^n subsets. Let us now focus on the following more complicated problem.

$$\text{How many } k\text{-subsets does a set of size } n \text{ have?} \tag{3.1}$$

where by *k-subset* we mean a subset of size k. The approach taken here to handle Problem (3.1) uses sequences.

Observation 3.2. *The number of sequences of length n composed of k elements is k^n.*

This observation can easily be generalised as follows.

Observation 3.3. *Let $n \in \mathbb{Z}^+$, let $\{k_i \in \mathbb{Z}^+ : i \in [n]\}$, and let $\mathcal{A} = \{A_1, \ldots, A_n\}$ be a collection*[1] *of sets where $|A_i| = k_i$ for every $i \in [n]$. Then the number of sequences of length n in which the ith entry is taken from the set A_i is $\prod_{i=1}^{n} k_i$.*

A special type of sequences of interest to us are *permutations*. Given a collection of n elements, any ordered list of these n elements is called a*permutation*. For instance, if $A = \{a, b, c\}$ then $(a, b, c), (c, b, a), (b, c, a)$ are all permutations of A.

Observation 3.4. *The number of permutations of a set of order n is $n!$.*

This last observation generalises easily as follows.

Observation 3.5. *The number of permutations of k-subsets taken from a set of order n is*

$$n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!}$$

We are now in a position to solve Problem 3.1.

Theorem 3.6 *The number of subsets of order k of a set of order n is $\frac{n!}{k!(n-k)!}$*

Proof. By Observation 3.5 the number of k-tuples in our set is $\frac{n!}{(n-k)!}$. Let $\mathcal{A}$ denote the set of k-tuples of our set. That is, $\mathcal{A}$ consists of all permutations of all k-subsets of our set. By Observation 3.4 each

[1] In collections repetitions are allowed.

k-subset of our set has $k!$ permutations of it found in $\mathcal{A}$. Consequently, the number of k-subsets is $|\mathcal{A}|/k! = \frac{n!}{k!(n-k)!}$ as required. ■

Definition 3.7 *Given $k \leq n \in \mathbb{N}$ we write*

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

Let us consider some special values of $\binom{n}{k}$.

1. Every set has a single subset of size zero which is the empty set; indeed $\binom{n}{0} = 1$.
2. Every set of size n has a single subset of size n, i.e., itself. Indeed, $\binom{n}{n} = 1$.
3. Trivially there are n ways to choose singletons out of n elements; indeed, $\binom{n}{1} = n$. The act of throwing one element out from a set of n is the same as picking one element out of the set. As we have n ways to throw one element out of a set of size n it follows that there are n subsets of size $n-1$ on a set of order n. Indeed, $\binom{n}{n-1} = n$.
4. The number of pairs in a set of size n is $\binom{n}{2} = n(n-1)/2$. A more revealing way to write this is $n^2/2 - n/2$. Despite the fact that we already proved Theorem 3.6 let us repeat its proof for the case $k = 2$ but in a slightly different manner.

   The question then is how can we reason about $n(n-1)/2$ being the number of pairs in a set of size n? The number of ordered pairs arising from a set of order n is n^2, by Observation 3.2. Amongst these pairs we count pairs of the form (a, a) comprised of the same element repeating it self. There are n such pairs. It follows then that the number of ordered pairs comprised of distinct elements is then $n^2 - n$. A subset $\{a, b\}$ with $a \neq b$ gives rise to the ordered pairs (a, b) and (b, a). Hence $n^2 - n$ is equal to twice the number of 2-subsets in our set of order n.

Example 3.8 In view of Theorem 3.6, the quantity $\binom{n}{k}k$ is then number of ways to choose a single element from a k-subset of a set of size n, say $[n]$. We can think of this counting exercises as the number of ways to choose a chairperson from a board of directors for a company of size n. We can think of this chairperson "election" counting process in a different way. First we can choose the chairperson for the board (there are n options to do so) and after the chairperson is chosen (and thus fixed) then we can choose the remaining $k-1$ members of the board (and there are $\binom{n-1}{k-1}$ ways to do so. We have just prove that

$$\binom{n}{k}k = n\binom{n-1}{k-1}. \tag{3.9}$$

Example 3.10 (subset of a subset)
Let $0 \leq k \leq m \leq n$. How many ways are there to choose a k-subset out of an m-subset of the set $[n]$? If we first choose the m-subset and from it the k-subset then we arrive at the quantity $\binom{n}{m}\binom{m}{k}$. Alternatively, we can first choose the k-subset and then complete it into an m-subset yielding the quantity $\binom{n}{k}\binom{n-k}{m-k}$. We have just established that

$$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}.$$

§3.2. The binomial theorem

Binomial coefficients have the word *coefficient* in their names due to the following result.

Theorem 3.11 (The binomial theorem)
The coefficient of the term $x^{n-k}y^k$ in the expansion of $(x+y)^n$ is $\binom{n}{k}$. That is,

$$(x+y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n}y^n. \tag{3.12}$$

Biome is the Greek word for an expression with two terms; hence the word *binomial*.

Prior to proving the binomial theorem we require the following identity by Pascal.

Lemma 3.13 (Pascal's identity)
Let $0 \le k \le n \in \mathbb{N}$. Then

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k} \tag{3.14}$$

Proof. Suffices to prove that

$$\frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!} = \frac{n!}{k!(n-k)!}$$

Multiplying all terms by $\frac{(k-1)!(n-k-1)!}{(n-1)!}$ gives

$$\frac{1}{n-k} + \frac{1}{k} = \frac{n}{k(n-k)}$$

which is easily seen to be true. ■

The proof supplied above for Pascal's identity was an algebraic proof. Here is an alternative combinatorial proof of the same identity.

Proof of Lemma 3.13. Let A be a set consisting of n elements and fix $a \in A$. Then the number of k-subsets in A which is equal to $\binom{n}{k}$ satisfies

$$\binom{n}{k} = |\mathcal{A}_1| + |\mathcal{A}_2|,$$

where $\mathcal{A}_1$ denotes all the k-subsets of A containing a and $\mathcal{A}_2$ consists of all k-subsets of A not containing a. By Theorem 3.6 we have that $|\mathcal{A}_1| = \binom{n-1}{k-1}$ and $|\mathcal{A}_2| = \binom{n-1}{k}$. Pascal's identity is thus established. ■

We are now in position to prove the binomial theorem.

Proof of Theorem 3.11. The proof is by induction on n. For $n = 1$ we see that

$$\sum_{k=0}^{1} \binom{1}{k} x^{1-k}y^k = \binom{1}{0}x^1y^0 + \binom{1}{1}x^0y^1 = x + y$$

so that the claim holds for $n = 1$.

Assume then that the claim holds for $n \ge 1$ and let us consider $n+1$. Write

$$(x+y)^{n+1} = x(x+y)^n + y(x+y)^n.$$

By the induction hypothesis

$$\begin{aligned} x(x+y)^n &= x\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k \\ &= \sum_{k=0}^{n}\binom{n}{k}x^{n-k+1}y^k \\ &= x^{n+1}+\sum_{k=1}^{n}\binom{n}{k}x^{n-k+1}y^k. \end{aligned} \tag{3.15}$$

In a similar manner we have

$$\begin{aligned} y(x+y)^n &= y\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k \\ &= \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^{k+1} \\ &= y^{n+1}+\sum_{j=1}^{n}\binom{n}{j-1}x^{n-j+1}y^j. \end{aligned} \tag{3.16}$$

Adding the (3.15) and (3.16) we arrive at

$$\begin{aligned} (x+y)^{n+1} &= x^{n+1}+\sum_{k=1}^{n}\binom{n}{k}x^{n-k+1}y^k+y^{n+1}+\sum_{j=1}^{n}\binom{n}{j-1}x^{n-j+1}y^j \\ &= x^{n+1}+\sum_{k=1}^{n}\left(\binom{n}{k}+\binom{n}{k-1}\right)x^{n+1-k}y^k+y^{n+1}; \end{aligned}$$

By Lemma 3.13 we may then write

$$\begin{aligned} &= x^{n+1}+\sum_{k=1}^{n}\binom{n+1}{k}x^{n+1-k}y^k+y^{n+1} \\ &= \sum_{k=0}^{n+1}\binom{n+1}{k}x^{n+1-k}y^k; \end{aligned}$$

concluding the induction step. ■

As the term $(1+x)^n$ is encountered quite often the following is convenient to note for future reference.

Corollary 3.17

$$(1+x)^n = \sum_{k=0}^{n}\binom{n}{k}x^k.$$

§3.3. Symmetry of binomial coefficients

The first aspect of symmetry for binomial coefficients can be seen through the following result.

Theorem 3.18 *Let $k \leq n \in \mathbb{N}$. Then*

$$\binom{n}{k} = \binom{n}{n-k} \tag{3.19}$$

Proof. Let S be a set of size n, let $\mathcal{A}$ denote the k-subsets of S, and let $\mathcal{B}$ denote the $(n-k)$-subsets of S. Define a mapping $\mathcal{A} \to \mathcal{B}$ given by mapping each k-subset of S (i.e., a member of $\mathcal{A}$) to its complement (which is a member of $\mathcal{B}$). As the resulting mapping is a bijection it follows that $|\mathcal{A}| = |\mathcal{B}|$. The claim follows by noting that $|\mathcal{A}| = \binom{n}{k}$ and that $|\mathcal{B}| = \binom{n}{n-k}$. ■

The proof we have just seen is simply an overcomplicated way to say that the number of ways to choose sets of size k is equal to the number of ways to choose their complements; indeed, once the complement of a set is determined so is the set.

The symmetry seen in Theorem 3.19 implies that

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0; \tag{3.20}$$

For suppose that n is odd. Then for an even k the number $n-k$ is odd and for an odd k the number $n-k$ is even. This means that given a fixed k then in the sum appearing on the right hand side of (3.19) we have that the coefficients of $\binom{n}{k}$ and $\binom{n}{n-k}$ always have different signs, i.e., we always have $(-1)^k = -(-1)^{n-k}$. By (3.19) then, these two terms cancel each other out. However, this is still not enough in order to claim that this sum in fact vanishes. For indeed, we still have to argue that we can couple the terms appearing in this sum into pairs that cancel one another. As n is odd $n+1$ is even. The sum in (3.20) consists of $n+1$ terms so the coupling of terms discussed above is possible and this sum must then vanish.

Suppose next that n is even. The argument we have seen above for an odd n fails. Already for $k = 0$ and $n - k = n$ we note that $(-1)^k = (-1)^{n-k} = 1$ so the sum of these two terms (i.e., the first and the last term) would result in 2 and not in 0 as we had in the odd case. Moreover, the sum consists now of an odd number of terms and not an even number of terms so this is another hardship we have to face for an even n that did not occur for an odd n.

Consider now (3.12) with $x = 1$ and $y = -1$ and note that

$$0 = (1-1)^n = \sum_{k=0}^{n} (-1)^k \binom{n}{k}.$$

So the binomial theorem establishes (3.20) in "one stroke" sort of speak for both even and odd n. This convinces us that (3.20) is indeed true but applying to the binomial theorem here hides from us what is truly going on here. Let us then prove (3.20) this time without using the binomial theorem. In the sum

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n \binom{n}{n}$$

we may replace $\binom{n}{0}$ with $\binom{n-1}{0}$ as both are equal to 1. By (3.14) we may replace $\binom{n}{1}$ with $\binom{n-1}{0} + \binom{n-1}{1}$. We can repeat this for $\binom{n}{2}$ and replace it with $\binom{n-1}{1} + \binom{n-1}{2}$. If we keep doing so we arrive at the sum

$$\binom{n-1}{0} - \left[\binom{n-1}{0} + \binom{n-1}{1}\right] + \left[\binom{n-1}{1} + \binom{n-1}{2}\right] - \\ \cdots + (-1)^{n-1}\left[\binom{n-1}{n-2} + \binom{n-1}{n-1}\right] + (-1)^n \binom{n-1}{n-1}.$$

This sum is clearly zero as the first term in each pair cancels with the second term in the preceding pair. Observe

$$\cancel{\binom{n-1}{0}} - \left[\cancel{\binom{n-1}{0}} + \cancel{\binom{n-1}{1}}\right] + \left[\cancel{\binom{n-1}{1}} + \binom{n-1}{2}\right] - \\ \cdots + (-1)^{n-1}\left[\binom{n-1}{n-2} + \cancel{\binom{n-1}{n-1}}\right] + \cancel{(-1)^n\binom{n-1}{n-1}}.$$

This last proof of (3.20) gives us more than a mere proof of an identity we already knew is true. For suppose we are interested in the following

$$\sum_{i=0}^{k}(-1)^i\binom{n}{i} \tag{3.21}$$

for some prescribed integer $0 \leq k \leq n$. Here the binomial theorem is useless. However, if we repeat our last proof of (3.20) using substitutions we can write

$$\sum_{i=0}^{k}(-1)^i\binom{n}{i} = \binom{n-1}{0} - \left[\binom{n-1}{0} + \binom{n-1}{1}\right] + \\ \left[\binom{n-1}{1} + \binom{n-1}{2}\right] - \cdots + (-1)^k\left[\binom{n-1}{k-1} + \binom{n-1}{k}\right]$$

Repeating the cancellation pattern we have seen before we arrive at the following.

Lemma 3.22 *Let $0 \leq k \leq n$ be integers. Then*

$$\sum_{i=0}^{k}(-1)^i\binom{n}{i} = (-1)^k\binom{n-1}{k}. \tag{3.23}$$

By Lemma 2.24 we conclude the following.

Corollary 3.24

$$\sum_{i=0}^{n}\binom{n}{i} = 2^n. \tag{3.25}$$

Alternatively, we could attain a proof of (3.25) through (3.12) noticing that

$$2^n = (1+1)^n = \sum_{i=0}^{n}\binom{n}{i}.$$

Above we have shown how we could obtain a closed formula for partial sums of (3.20) and obtain (3.23). Can we do the same for (3.25)? That is, can we attain a closed form for the sum

$$\sum_{i=0}^{k}\binom{n}{i},$$

where $0 \leq k \leq n$. Such an achievement would be of significant interest as no such closed form is currently known.

§3.4. Pascal's triangle

Let us arrange the binomial coefficients as follows.

$$\begin{array}{ccccccccccccccc}
 & & & & & & & \binom{0}{0} & & & & & & & \\
 & & & & & & \binom{1}{0} & & \binom{1}{1} & & & & & & \\
 & & & & & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & & & & & \\
 & & & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & & & & \\
 & & & \binom{4}{0} & & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & & \binom{4}{4} & & & \\
 & & \binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5} & & \\
 & \binom{6}{0} & & \binom{6}{1} & & \binom{6}{2} & & \binom{6}{3} & & \binom{6}{4} & & \binom{6}{5} & & \binom{6}{6} & \\
\binom{7}{0} & & \binom{7}{1} & & \binom{7}{2} & & \binom{7}{3} & & \binom{7}{4} & & \binom{7}{5} & & \binom{7}{6} & & \binom{7}{7}
\end{array}$$

If we replace the binomial coefficients with their numerical values we get the following illustration.

$$\begin{array}{ccccccccccccccc}
 & & & & & & & 1 & & & & & & & \\
 & & & & & & 1 & & 1 & & & & & & \\
 & & & & & 1 & & 2 & & 1 & & & & & \\
 & & & & 1 & & 3 & & 3 & & 1 & & & & \\
 & & & 1 & & 4 & & 6 & & 4 & & 1 & & & \\
 & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & \\
 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & \\
1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1
\end{array}$$

. These illustrations are commonly referred to as *Pascal's triangle*. This triangle is symmetric with respect to the vertical line passing through its apex; this we learn from (3.19). Moreover, (3.14) informs us how to deduce one row of the Pascal triangle from its predecessor. Figure **??** illustrates the relation between the pascal triangle and the binomial theorem.

$$1$$
$$x+1$$
$$x^2+2x+1$$
$$x^3+3x^2+3x+1$$
$$x^4+4x^3+6x^2+4x+1$$
$$x^5+5x^4+10x^3+10x^2+5x+1$$
$$x^6+6x^5+15x^4+20x^3+15x^2+6x+1$$
$$x^7+7x^6+21x^5+35x^4+35x^3+21x^2+7x+1$$

Figure 3.1: Polynomials in Pascal's triangle

The identity (3.25) is then the summation of a single row of the Pascal triangle and is thus referred to the the *row sum property of the Pascal triangle*. "Geometrically" or "visually" one may have a problem identifying columns and diagonals in the Pascal triangle.

n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$	$\binom{n}{7}$	$\binom{n}{8}$	Σ
0	1									1
1	1	1								2
2	1	2	1							4
3	1	3	3	1						8
4	1	4	6	4	1					16
5	1	5	10	10	5	1				32
6	1	6	15	20	15	6	1			64
7	1	7	21	35	35	21	7	1		128
8	1	8	28	56	70	56	28	8	1	256

Figure 3.2: Pascal triangle in table form.

Nevertheless, we still think of this triangle as though it is a rectangular table and assign to it notions of column and diagonals of all sorts. For instance here is what we perceive to be a column.

n	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$
2		1	
3		3	
4		6	
5		10	
6		15	
7			35

Summing up a column leads to the following identity.

Lemma 3.26 (Column property of the Pascal triangle)
Let $0 \le c \le n$ be integers. Then

$$\sum_{k=0}^{n} \binom{k}{c} = \binom{n+1}{c+1} \tag{3.27}$$

Proof. The proof is by induction on n. For $n = 0$ we have $c = 0$ and the assertion is trivial. Assume then that

$$\sum_{k=0}^{n-1} \binom{k}{c} = \binom{n}{c+1},$$

and consider the sum $\sum_{k=0}^{n} \binom{k}{c}$. We may write

$$\begin{aligned}\sum_{k=0}^{n} \binom{k}{c} &= \sum_{k=0}^{n-1} \binom{k}{c} + \binom{n}{c} \\ &= \binom{n}{c+1} + \binom{n}{c} \\ &= \binom{n+1}{c+1}.\end{aligned}$$

Here, the second equality is due to the induction hypothesis and the third equality is due to Pascal's identity (3.14). ■

One may now trace the sum appearing on the left hand side of (3.27) and unveil the meaning of a column in the Pascal triangle. This next lemma considers summation along the *south-east diagonal of the Pascal triangle* illustrated here.

n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$
2	1				
3		3			
4			6		
5				10	
6					15
7					35

Lemma 3.28 *Let $0 \le r \le n$. Then*

$$\sum_{k=0}^{n} \binom{r+k}{k} = \sum_{k=0}^{n} \binom{r+k}{r}.$$

Proof.

$$\begin{aligned}\sum_{k=0}^{n} \binom{r+k}{k} &\overset{(3.19)}{=} \sum_{k=0}^{n} \binom{r+k}{r} \\ &\overset{(3.27)}{=} \binom{r+n+1}{r+1} \\ &\overset{(3.19)}{=} \binom{r+n+1}{n}.\end{aligned}$$

■

§3.5. Squares of binomial coefficients

Definition 3.29 *For a positive integer n we write $[n]$ to denote the set $\{1, \ldots, n\}$.*

Let $0 \le k \le n$ be positive integers. Let $S_{n,k}$ denote the number of n-subsets of $[2n]$ with precisely k elements from $[n]$. We can express $S_{n,k}$ as follows. There are $\binom{n}{k}$ ways to choose the k elements which we insist must come from $[n]$. There are $\binom{n}{n-k}$ ways to choose the remaining $n-k$ elements that have to come from $\{n-1, \ldots, 2n\}$. That is

$$S_{n,k} = \binom{n}{k}\binom{n}{n-k} \overset{(3.19)}{=} \binom{n}{k}^2.$$

The total number of n-subsets of $[2n]$ is then given by $\sum_{k=0}^{n} S_{n,k}$ leading to the following.

Lemma 3.30

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}. \tag{3.31}$$

§3.6. Growth and decay of binomial coefficients

Fix a positive integer n. Letting k range over $[0, n] := \{0\} \cup [n]$ we may view $\binom{n}{k}$ as a function $\binom{n}{\cdot} : [n] \to \mathbb{N}$. A typical calculus question would then be: *what does $\binom{n}{\cdot}$ look like?* Let us consider $\binom{n}{k}$ and $\binom{n}{k+1}$ and try to determine '<?>' in the following expression:

$$\binom{n}{k} <?> \binom{n}{k+1};$$

here '<?>' acts as a place holder for one of the symbols $<, =, >$. The aim now is to determine which symbol to replace '<?>' with as k ranges over $[0, n]$.

$$\frac{n!}{k!(n-k)!} <?> \frac{n!}{(k+1)!(n-(k+1))!}.$$

Cancelling common terms we get

$$\frac{1}{n-k} <?> \frac{1}{k+1}$$

rearranging this we get

$$k+1 <?> n-k$$

this is simply

$$k <?> \frac{n-1}{2};$$

which then yields the following.

Proposition 3.32 *Let $0 \leq k \leq n$ be integers. Then:*

1. *if $k < (n-1)/2$ then $\binom{n}{k} < \binom{n}{k+1}$;*
2. *if $k > (n-1)/2$ then $\binom{n}{k} > \binom{n}{k+1}$;*
3. *in the case that n is odd and $k = (n-1)/2$ then $\binom{n}{k} = \binom{n}{k+1}$.*

Put another way, up to the "middle" of the Pascal triangle the function $\binom{n}{\cdot}$ strictly increases; from the "middle" of the Pascal triangle the function $\binom{n}{\cdot}$ strictly decreases. We can capture this behaviour by looking at the quotient

$$\binom{n}{k+1}\binom{n}{k}^{-1} = \frac{n-k}{k+1}.$$

For $k < (n-1)/2$ this ratio is > 1 for $k < (n-1)/2$ this ratio is < 1. If n permits $k = (n-1)/2$ then this ration is equal to 1.

Example 3.33 Suppose n is even. Then $\binom{n}{n/2}$ is the largest binomial coefficient with respect to n. *How large is it?* Trivially we have

$$\binom{n}{n/2} \leq \sum_{i=0}^{n} \binom{n}{i} \overset{(3.25)}{=} 2^n.$$

On the other hand

$$\binom{n}{n/2} \geq \frac{\sum_{i=0}^{n} \binom{n}{i}}{n+1} = \frac{2^n}{n+1}.$$

§3.7. Vandermonde convolution

Let n, m be nonnegative integers, and let A be a set of size $n+m$. Suppose that $A = A_1 \uplus A_2$ (where $\uplus$ denotes disjoint union) where $|A_1| = n$ and $|A_2| = m$. Given a nonnegative integer k in how many ways can we pick k elements from A? The fast answer is $\binom{n+m}{k}$. We could go about this question in a different route. We can first choose j elements from, say A_1, and then complete them into k elements by choosing $k-j$ elements from A_2. For a fixed j the number of ways to do that is $\binom{n}{j}\binom{m}{k-j}$. Going over all possibilities for j we arrive at the quantity $\sum_{j=0}^{k} \binom{n}{j}\binom{m}{k-j}$. Note that letting j range all the way to n does not alter this sum as only zeros would be thus introduced. So we arrive at the sum $\sum_{j=0}^{n} \binom{n}{j}\binom{m}{k-j}$.

The *Vandermonde convolution* is defined to be the quantity $\sum_{j=0}^{n} \binom{n}{j}\binom{m}{k-j}$. We have just established (in a combinatorial manner) that

$$\sum_{j=0}^{n} \binom{n}{j}\binom{m}{k-j} = \binom{n+m}{k} \tag{3.34}$$

Let us now prove (3.34) using the binomial theorem. In the polynomial $(1+x)^{m+n}$ the coefficient of the monomial x^k is $\binom{n+m}{k}$. Consider next the polynomial $(1+x)^n(1+x)^m$. In this polynomial the coefficient of x^k is $\sum_{j=0}^{n}\binom{n}{j}\binom{m}{k-j}$. Now as $(1+x)^m(1+x)^n = (1+x)^{m+n}$ it in particular implies that the coefficient of x_k in both these polynomials must be equal yielding (3.34).

§3.8. Parity of binomial coefficients

Is $\binom{165}{93}$ odd or is it even? Can one answer this without any calculations? The parity of the binomial coefficients was studied by James Glassier (1848-1928).

Theorem 3.35 *Let $0 \le k \le n$ be integers. If n is even and k is odd then $\binom{n}{k}$ is even. Otherwise it has the same parity as $\binom{\lfloor n/2\rfloor}{\lfloor k/2\rfloor}$.*

Proof. We distinguish between four cases depending on the parity of n and k.

1. *n is even and k is odd.* By (3.9)
$$k\binom{n}{k} = n\binom{n-1}{k-1};$$
n being even means that $k\binom{n}{k}$ must then be even; k being odd means that $\binom{n}{k}$ must then be even.

2. *n is even and k is even.* Write
$$\binom{n}{k} = \frac{n^{\underline{k}}}{k!} = \frac{(n-1)(n-3)\cdots(n-(k-1))}{1\cdot 3\cdot 5\cdots(k-1)}\cdot\frac{n(n-2)(n-4)\cdots(n-(k-2))}{2\cdot 4\cdot 6\cdots k}$$
Consider the quotient involving only even numbers. As k is even there are $k/2$ terms in the denominator and numerator of this quotient. We may thus write
$$\begin{aligned}\binom{n}{k} &= \frac{(n-1)(n-3)\cdots(n-(k-1))}{1\cdot 3\cdot 5\cdots(k-1)}\cdot\frac{\cancel{2^{k/2}}\frac{n}{2}\left(\frac{n}{2}-1\right)\cdots\left(\frac{n}{2}-\frac{k}{2}+1\right)}{\cancel{2^{k/2}}\cdot 1\cdot 3\cdots\frac{k}{2}}\\ &= \frac{(n-1)(n-3)\cdots(n-(k-1))}{1\cdot 3\cdot 5\cdots(k-1)}\cdot\binom{n/2}{k/2}.\end{aligned}$$
Rearranging we arrive at
$$1\cdot 3\cdot 5\cdots(k-1)\binom{n}{k} = (n-1)(n-3)\cdots(n-(k-1))\binom{n/2}{k/2}.$$
As n and k are both even in this case, $n/2 = \lfloor n/2\rfloor$ and $k/2 = \lfloor k/2\rfloor$ so that
$$1\cdot 3\cdot 5\cdots(k-1)\binom{n}{k} = (n-1)(n-3)\cdots(n-(k-1))\binom{\lfloor n/2\rfloor}{\lfloor k/2\rfloor}.$$
Multiplying an integer by an odd number does not change its parity. Implying that the parity of the quantities appearing on both sides are determined solely by $\binom{n}{k}$ on the left and $\binom{\lfloor n/2\rfloor}{\lfloor k/2\rfloor}$ on the right. Equality here then implies that these numbers must have the same parity.

3. *n is odd and k is odd.* Appealing to (3.9) again (as in the first case) yields
$$k\binom{n}{k} = n\binom{n-1}{k-1};$$

as k and n are both odd, $\binom{n}{k}$ and $\binom{n-1}{k-1}$ are of the same parity. As both $n-1$ and $k-1$ are even we revert to the second case and argue that $\binom{n-1}{k-1}$ has the same parity as $\binom{\lfloor (n-1)/2 \rfloor}{\lfloor (k-1)/2 \rfloor}$. As n and k are both odd, we have that $\lfloor n/2 \rfloor = (n-1)/2 = \lfloor (n-1)/2 \rfloor$ and $\lfloor k/2 \rfloor = (k-1)/2 = \lfloor (k-1)/2 \rfloor$ and the claim follows in this case.

4. *n is odd and k is even.* By (6.61) we may write

$$(n-k)\binom{n}{k} = (n-k)\binom{n}{n-k} \text{ and } n\binom{n-1}{n-k-1} = n\binom{n-1}{k}.$$

Next, by (3.9) we note that

$$(n-k)\binom{n}{n-k} = n\binom{n-1}{n-k-1};$$

so that

$$(n-k)\binom{n}{k} = n\binom{n-1}{k}.$$

As $n-k$ and n are both odd then (by the third case) we have that $\binom{n}{k}$ and $\binom{\lfloor (n-1)/2 \rfloor}{\lfloor k/2 \rfloor}$ have the same parity. As n is odd $\lfloor (n-1)/2 \rfloor = \lfloor n/2 \rfloor$ and the claim follows in this case as well.

■

§3.9. Exercises

Exercise 1. Prove that $\sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n$.

Exercise 2. Given $n \geq 0$ in $\mathbb{N}$ let A denote the even members of the set $[n]$ and let B denote the odd members of the set $[n]$. Prove that

$$\sum_{k \in A} \binom{n}{k} = 2^{n-1} = \sum_{k \in B} \binom{n}{k}.$$

Exercise 3. For $n \geq 2$ prove that

$$\sum_{k=2}^{n} \binom{k}{2} = \binom{n+1}{3}.$$

Exercise 4. Let f_n denote the nth Fibonacci number. Prove that

$$\sum_{k=0}^{n} \binom{n-k}{k} = f_{n+1} \tag{3.36}$$

Exercise 5. Let n be an even positive integer. Prove that

$$\sum_{k=0}^{n/2} \left(\binom{n}{k}^2 + \binom{n}{k-1}^2 \right) = \sum_{k=0}^{n} \binom{n}{k}^2$$

Exercise 6. Let n be a positive even number. Prove that the coefficient of x^{n-1} in the polynomial $(x+1)^{2n}$ is given by

$$2\sum_{k=0}^{n/2} \binom{n}{k}\binom{n}{k-1}$$

Exercise 7. Prove that for any positive integer

$$\binom{2n}{n} - \binom{2n}{n-1} = \binom{2n}{n}\left(1 - \frac{n}{n+1}\right).$$

Exercise 8. Let n be an even positive integer. Prove that

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \left(\binom{n}{k} - \binom{n}{k-1}\right)^2 = \frac{1}{n+1}\binom{2n}{n}.$$

Exercise 9.

1. Suppose $f : \mathbb{N} \to \mathbb{Z}$ satisfies $f(1) = 2$ and $f(n+1) = 2f(n)$ for every $n \geq 1$. Prove that $f(n) = 2^n$.
2. Prove that
$$\sum_{k=0}^{n} \binom{n+k}{k} \frac{1}{2^k} = 2^n$$

Exercise 10. Prove that

$$\sum_{k=1}^{n} k \binom{n}{k}^2 = n\binom{2n-1}{n-1}.$$

Exercise 11. Prove that $\binom{n}{k} \leq \frac{n^k}{k!}$.

Exercise 12.

1. Let $0 < m < k \leq n$. Prove that $\frac{n}{k} \leq \frac{n-m}{k-m}$.
2. Prove that $\binom{n}{k} \geq \left(\frac{n}{k}\right)^k$.

Exercise 13. Exercises 11 and 12 has left us with the estimates

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \frac{n^k}{k!}.$$

In this exercise we "tidy up" the upper bound as to yield

$$\left(\frac{n}{k}\right)^k \leq \binom{n}{k} \leq \left(\frac{e \cdot n}{k}\right)^k, \tag{3.37}$$

where here e is Euler's constant.

In § 17.1 (below) we give a brief explanation as to why

$$e^k = \sum_{n=0}^{\infty} \frac{k^n}{n!}$$

holds (though a full proof of this lies beyond the scope of these lecture notes). Use this equality in order to establish the upper bound seen in (3.37).

§3.10. Solutions

Some of the solutions have been written by the TAs in the course and thus have a different style of writing to them. Over time we hope to normalise this part of the text as well.

Solution for Exercise 1. In the Binomial theorem set $x = 1$ and $y = 2$ to get that $3^n = (x+y)^n$. The claim follows immediately from the Binomial identity in that theorem upon substituting $x = 1$ and $y = 2$.

Solution for Exercise 2. Recall

$$2^n = \sum_{k=0}^{n} \binom{n}{k} \text{ and } 0 = \sum_{k=0}^{n} (-1)^k \binom{n}{k}.$$

We first consider the sum $\sum_{k\in A} \binom{n}{k}$. We distinguish between two cases. If n is even, then we may write

$$2^n = 2^n + 0 = \sum_{k=0}^{n} \binom{n}{k} + \sum_{k=0}^{n} (-1)^k \binom{n}{k} = 2 \sum_{k\in A} \binom{n}{k}.$$

In the second case that n is odd then the last term of the sum $\sum_{k=0}^{n} (-1)^k \binom{n}{k}$ is $-\binom{n}{n}$. In which case we have

$$2^n = \sum_{k=0}^{n} \binom{n}{k} + \sum_{k=0}^{n} (-1)^k \binom{n}{k} = 2\left(\binom{n}{0} + \binom{n}{2} + \cdots + \binom{n}{n-1}\right);$$

the latter sum is again precisely $\sum_{k\in A} \binom{n}{k}$ in the case that n is odd.

We proceed to the sum $\sum_{k\in B} \binom{n}{k}$. In a similar manner to we considered $\sum_{k\in A} \binom{n}{k}$ you should argue now that

$$2 \cdot \sum_{k\in B} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} - \sum_{k=0}^{n} (-1)^n \binom{n}{k} = 2^n.$$

Details are left to the reader.

Solution for Exercise 3. The proof is by induction on n. For $n = 2$ the claim holds as $\binom{2}{2} = 1 = \binom{2+1}{3}$. Assume the claim holds for n and consider the claim for $n+1$.

$$\begin{aligned}
\sum_{k=2}^{n+1} \binom{k}{2} &= \sum_{k=2}^{n} \binom{k}{2} + \binom{n+1}{2} \\
&= \binom{n+1}{3} + \binom{n+1}{2} \\
&= \binom{n+2}{3},
\end{aligned}$$

where here second equality is due to the induction hypothesis and the third equality is due to Pascal's identity.

Solution for Exercise 4. The proof is by induction on n. For $n = 0$ and $n = 1$ one may note that (3.36) holds true. Let $n \geq 2$ and assume that

$$\sum_{k=0}^{n-1} \binom{n-1-k}{k} = f_n \text{ and } \sum_{k=0}^{n-2} \binom{n-2-k}{k} = f_{n-1}.$$

We may now write

$$\begin{aligned}\sum_{k=0}^{n}\binom{n-k}{k} &\overset{(3.14)}{=} \sum_{k=0}^{n}\binom{n-1-k}{k-1}+\sum_{k=0}^{n}\binom{n-1-k}{k}\\ &= \sum_{j=0}^{n-2}\binom{n-j-2}{j}+\sum_{k=0}^{n-1}\binom{n-k-1}{k}\\ &= f_{n-1}+f_n\\ &= f_{n+1}\end{aligned}$$

where the next to last equality is due to the induction hypothesis. The last equality is due to the definition of f_{n+1}.

Solution for Exercise 5. Write $(x+1)^{2n}=(x+1)^n(x+1)^n$. By the binomial theorem

$$(x+1)^n=\sum_{k=0}^{n}\binom{n}{k}x^k.$$

Let C_r denote the coefficient of x^r in $(x+1)^n(x+1)^n$ for $0\le r\le n$. Then as n is even

$$\begin{aligned}C_n &= 2\sum_{k=0}^{n/2-1}C_k\cdot C_{n-k}+C_{n/2}\\ &= 2\sum_{k=0}^{n/2-1}\binom{n}{k}\cdot\binom{n}{n-k}+\binom{n}{n/2}^2\\ &\overset{(3.19)}{=} 2\sum_{k=0}^{n/2-1}\binom{n}{k}^2+\binom{n}{n/2}^2.\end{aligned}$$

To see this write

$$(x+1)^n(x+1)^n=(C_0x^0+\cdots C_{n/2}x^{n/2}+\cdots C_nx^n)\cdot(C_0x^0+\cdots C_{n/2}x^{n/2}+\cdots C_nx^n).$$

To attain the monomial x^n in the cross multiplication here we pair up coefficients of x^k with x^{n-k} as k ranges from 0 to $n/2$. However, note that in this cross multiplication the monomial $x^{n/2}$ from the left term and the same monomial from the right term are taken precisely once while all other pairs $(k,n-k)$ with $k<n/2$ are taken twice.

More concisely we may write

$$C_n=\sum_{k=0}^{n/2}\binom{n}{k}^2+\sum_{k=0}^{n/2}\binom{n}{k-1}^2$$

with the understanding that $\binom{n}{-1}=0$. Note that $\binom{n}{n/2}^2$ appears once in this summation overall. This simplifies to

$$C_n=\sum_{k=0}^{n/2}\left(\binom{n}{k}^2+\binom{n}{k-1}^2\right).$$

On the other hand we have from the binomial theorem that $(x+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} x^k$ so that

$$C_n = \binom{2n}{n} \overset{(3.31)}{=} \sum_{k=0}^{n} \binom{n}{k}^2.$$

The claim follows.

Solution for Exercise 6. Referring to the solution proposed for Exercise 5 we note that

$$C_{n-1} = 2\Big(\underbrace{C_{-1}}_{=0} \cdot C_n + C_0 \cdot C_{n-1} + C_1 \cdot C_{n-2} + \cdots + C_{n/2-1} \cdot C_{n-n/2}\Big)$$

which we may write more concisely as

$$\begin{aligned} C_{n-1} &= 2\sum_{k=0}^{n/2} C_{k-1} \cdot C_{n-k} \\ &= 2\sum_{k=0}^{n/2} \binom{n}{k-1}\binom{n}{n-k} \\ &\overset{(3.19)}{=} 2\sum_{k=0}^{n/2} \binom{n}{k-1}\binom{n}{k} \end{aligned}$$

and the claim follows.

Solution for Exercise 7.

$$\begin{aligned} \binom{2n}{n} - \binom{2n}{n-1} &= \binom{2n}{n} - \binom{2n}{n-1}\frac{n}{n} \\ &= \frac{(2n)!}{(2n-n)!n!} - \frac{n \cdot (2n)!}{(2n-(n-1))!n!} = \\ &= \frac{(2n)!}{n!n!} - \frac{n \cdot (2n)!}{(n+1)!n!} \\ &= \frac{(2n)!}{n!n!}\left(1 - \frac{n}{n+1}\right) \\ &= \frac{(2n)!}{(2n-n)!n!}\left(1 - \frac{n}{n+1}\right) \\ &= \binom{2n}{n}\left(1 - \frac{n}{n+1}\right). \end{aligned}$$

Solution for Exercise 8. One must show that

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \left(\binom{n}{k}^2 + \binom{n}{k-1}^2\right) - 2\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{k}\binom{n}{k-1} = \frac{1}{n+1}\binom{2n}{n}.$$

In Exercise 5 we have see that

$$\sum_{k=0}^{n/2} \left(\binom{n}{k}^2 + \binom{n}{k-1}^2\right) = \sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

In Exercise 6 we have seen that the coefficient of x^{n-1} in the polynomial $(x+1)^{2n}$ is given by

$$2\sum_{k=0}^{n/2}\binom{n}{k}\binom{n}{k-1}.$$

For the latter we also know that this coefficient is also equal to $\binom{2n}{n-1}$ by the binomial theorem. Hence

$$\begin{aligned}\sum_{k=0}^{\lfloor n/2\rfloor}\left(\binom{n}{k}^2+\binom{n}{k-1}^2\right)-2\sum_{k=0}^{\lfloor n/2\rfloor}\binom{n}{k}\binom{n}{k-1} &= \binom{2n}{n}-\binom{2n}{n-1}\\ &= \frac{1}{n+1}\binom{2n}{n}\end{aligned}$$

where the last equality is due to Exercise 7.

Solution for Exercise 9.

1. The proof is by induction on n. For $n=1$ the claim is true by assumption. Assume then that $f(n)=2^n$ and consider $n+1$. By assumption $f(n+1)=2f(n)$; the induction hypothesis then yields $f(n+1)=2\cdot 2^n=2^{n+1}$ and the claim follows.

2. Set $f(n):=\sum_{k=0}^{n}\binom{n+k}{k}\frac{1}{2^k}$. Then $f(1)=2$. We show that $f(n+1)=2f(n)$ for every $n>1$ implying that $f(n)=2^n$ for every $n\geq 1$ by the first part of this exercise and thus completing this proof.

$$\begin{aligned}f(n+1) &= \sum_{k=0}^{n+1}\binom{n+1+k}{k}\frac{1}{2^k} \overset{(3.14)}{=} \sum_{k=0}^{n+1}\binom{n+k}{k}\frac{1}{2^k}+\sum_{k=0}^{n+1}\binom{n+k}{k-1}\frac{1}{2^k}\\ &= f(n)+\binom{2n+1}{n+1}\frac{1}{2^{n+1}}+\sum_{k=0}^{n+1}\binom{n+k}{k-1}\frac{1}{2^k}\\ &= f(n)+\binom{2n+1}{n+1}\frac{1}{2^{n+1}}+\frac{1}{2}\sum_{k=1}^{n+2}\binom{n+1+k-1}{k-1}\frac{1}{2^{k-1}}-\binom{2n+2}{n+1}\frac{1}{2^{n+2}}\\ &= f(n)+\frac{1}{2}\left(\binom{2n+1}{n+1}\frac{1}{2^n}+\sum_{k=1}^{n+2}\binom{n+1+k-1}{k-1}\frac{1}{2^{k-1}}-\binom{2n+2}{n+1}\frac{1}{2^{n+1}}\right)\\ &= f(n)+\frac{1}{2}f(n+1)\end{aligned}$$

so that $f(n+1)=2f(n)$ as required.

Solution for Exercise 10. By the binomial theorem, the term $n\binom{2n-1}{n-1}$ is simply the coefficient of x^{n-1} the polynomial $n(1+x)^{2n-1}$. In order to get a closed form of this coefficient we study two polynomial $(1+x)^n$ and $n(1+x)^{n-1}$. The product of these two polynomials is $n(1+x)^{2n-1}$. By the binomial theorem

$$(1+x)^n=\sum_{k=0}^{n}\binom{n}{k}x^k=1+x\binom{n}{1}+x^2\binom{n}{2}+\cdots.$$

Note that $n(1+x)^{n-1}$ is the derivative of $(1+x)^n$. Then

$$n(1+x)^{n-1}=\sum_{j=1}^{n}j\binom{n}{j}x^{j-1}=\binom{n}{1}+2\binom{n}{2}x+3\binom{n}{3}x^2+\cdots.$$

It then follows that

$$n(1+x)^{2n-1} = \left(\sum_{k=0}^{n}\binom{n}{k}x^k\right)\cdot\left(\sum_{j=1}^{n} j\binom{n}{j}x^{j-1}\right).$$

It remains to evaluate the coefficient of x^{n-1} on the right hand side of the last equation. To that end we seek to consider pairs of indices k and j summing up to n as then $x^k \cdot x^{j-1} = x^n$. This leads to the following expression for the coefficient:

$$\sum_{k=0}^{n}\binom{n}{k}\underbrace{(n-k)}_{=j}\binom{n}{n-k} \overset{(3.19)}{=} \sum_{k=0}^{n}(n-k)\binom{n}{n-k}^2 \overset{(3.19)}{=} \sum_{k=0}^{n} k\binom{n}{k}^2$$

Solution for Exercise 11.

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} \leq \frac{n^k}{k!}.$$

Solution for Exercise 12.

1. As $\frac{m}{n} \leq \frac{m}{k}$ then $1-\frac{m}{n} \leq 1-\frac{m}{k}$. This we may rewrite as $\frac{k-m}{k} \leq \frac{n-m}{n}$. This last inequality we can rewrite as $\frac{n}{k} \leq \frac{n-m}{k-m}$.

2. The argument for $k=1$ and $k>1$ differs and so we distinguish between the two cases. For $k=1$ the claim is easily seen to be true. If $k>1$ we note that

$$\left(\frac{n}{k}\right)^k = \underbrace{\frac{n}{k}\cdots\frac{n}{k}}_{k \text{ times}}$$

By the first part of this exercise, for each $0 < m \leq k-1$ we have that $\frac{n-m}{k-m}$. Consequently we may write

$$\left(\frac{n}{k}\right)^k = \underbrace{\frac{n}{k}\cdots\frac{n}{k}}_{k \text{ times}} \leq \frac{n}{k}\cdot\frac{n-1}{k-1}\cdot\frac{n-2}{k-2}\cdots\frac{n-k+1}{1} = \binom{n}{k};$$

note that we never divide by zero in any of the terms as m ranges over $[1, k-1]$ so that $k-m>0$ always.

Solution for Exercise 13. The equality $e^k = \sum_{n=0}^{\infty}\frac{k^n}{n!}$ implies that $e^k \geq \frac{k^k}{k!}$ which is the kth term in this (infinite) sum. Then $\frac{1}{k!} \leq \left(\frac{e}{k}\right)^k$. Hence,

$$\frac{n^k}{k!} \leq \left(\frac{e\cdot n}{k}\right)^k$$

and the claim follows.

Part II

Elementary Number theory

Lecture 4

Divisibility in $\mathbb{Z}$

§4.1. The division theorem

Given two integers a and b, $b \neq 0$, one is often accustomed to having $a/b \in \mathbb{R}$. In these notes however we take a different approach. We will mandate that $a/b \in \mathbb{Z}$. We say that a *divides* b, and write $a \mid b$, if there exists an integer c such that $b = ac$. Otherwise we write $a \nmid b$.

The main result of this section reads as follows.

Theorem 4.1 (The division theorem)
If a and b are integers such that $b > 0$ then there are unique integers q and r such that $a = bq + r$ with $0 \leq r \leq b - 1$.

Proof. The proof is split into two claims. The first is that q, the *quotient* and r, the *remainder*, exist. The second is that these are in fact unique.

Existence. To prove existence of q and r we shall appeal to the WOP. To that end let

$$S = \{a - bk : k \in \mathbb{Z} \text{ and } a - bk \geq 0\}.$$

Note that S is non-empty. Indeed setting $k = -|a| - 1$ gives $a - (-|a| - 1)b = a + |a|b + b \geq a + |a| + 1 \geq 0$, as $b > 0$. The set S has a least element, by the WOP. Let $r = a - bq$ denote this element. The existence of q is then established. It remains to show that $0 \leq r < b$. Indeed, $r \geq 0$ by definition of S. To see that $r < b$, assume towards a contradiction that $r \geq b$. Then

$$r > r - b = a - bq - b = a - b(q + 1) \geq 0,$$

where the first inequality is due to the assumption that $b > 0$. We now have that $r - b \in S$ and $r - b < r$ contradicting the minimality of r. Existence of r and q is then established.

Uniqueness. Suppose that there exist q_1, q_2, r_1, r_2 satisfying

$$bq_1 + r_1 = a = bq_2 + r_2$$

such that $0 \leq r_i < b$ for $i \in \{1, 2\}$. We show that it must be that $q_1 = q_2$ and that $r_1 = r_2$. Indeed, subtracting the second equation from the first we have

$$0 = b(q_1 - q_2) + (r_1 - r_2)$$

so that $r_2 - r_1 = b(q_1 - q_2)$. This means that $b \mid (r_2 - r_1)$. Now, as $r_1, r_2 \in [0, b)$ it follows that $-b < r_2 - r_1 < b$. This in turn implies that to have $b \mid (r_2 - r_1)$ we must have that $r_2 - r_1 = 0$, i.e., $r_1 = r_2$. This in turn implies that $q_1 = q_2$. ■

In Theorem 4.1 we assume that $b > 0$. Where did we use this in the proof? We used it in the part where we claim that S is non-empty. Indeed we reasoned that $a - (-|a| - 1)b = a + |a|b + b \geq a + |a| + 1 > 0$ in which we use the fact that $b \geq 1$.

Suppose we were to make a weaker assumption; namely that $b \neq 0$ (instead of $b > 0$). How would this effect the proof? We see that the argument for S being non-empty will be effected. Any other places? In the proof above we took a least element $r \in S$ and then considered $r - b$ and relied on the fact that $r - b < r$. With b allowed to be negative we in fact may have that $r - b > r$.

Corollary 4.2 *If a and b are integers such that $b \neq 0$ then there are unique integers q and r such that $a = bq + r$ with $0 \leq r < |b|$.*

Proof. We may assume that $b < 0$ for otherwise the assertion follows by Theorem 4.1. Now, applying Theorem 4.1 for a and $|b|$ we get a unique q and r satisfying $a = \ell|b| + r$ such that $0 \leq r < |b|$. As $b < 0$, by assumption $|b| = -b$ so that $a = \ell(-b) + r = (-\ell)b + r$ and the assertion follows with $q = -\ell$ and r. ■

Definition 4.3 *For $a, b \in \mathbb{Z}$ let $a = bq + r$ be the unique representation of a according to the Division theorem. We write $a \mod b$ to denote r.*

Example 4.4 The division theorem for $a = 17$ and $b = -7$:

$$17 = (-2)(-7) + 3$$

yields $q = -2$ and $r = 3$. That is $17 \mod (-7) = 3$.

Example 4.5 Let a be an integer. Then $3 \mid a^3 - a$. To see this, first let us note that

$$a^3 - a = a(a^2 - 1) = (a - 1)a(a + 1).$$

By the division theorem (see Theorems 4.1 and 4.2) we have that $a = 3k$ or $a = 3k+1$ or $a = 3k+2$. We consider all three cases.

1. If $a = 3k$ we have that $a^3 - a = a(a^2 - 1) = 3k(a^2 - 1)$ which is clearly divisible by 3.
2. If $a = 3k + 1$ then $a - 1 = 3k$ so that $3 \mid a^3 - a$.
3. If $a = 3k + 2$ then $a + 1 = 3k + 3 = 3(k + 1)$ and the claim again holds.

In Example 4.5 we have proved the following.

Observation 4.6. *Amongst any three consecutive numbers at least one is a multiple of 3.*

This could easily be generalised to any positive integer.

Proposition 4.7 *Let $b \in \mathbb{Z}^+$. Amongst any b consecutive numbers at least one is a multiple of b.*

The next set of examples demonstrates the power of the Division theorem in determining the forms of numbers that are of special interest to us. For instance, if $a = 2k$ is an even number then a^2 must clearly be a multiple of 4. This was easy enough. What could we say about the squares of odd numbers? We shall investigate the forms of squares of odd numbers through two perspectives: "through the eyes of the number 4" and through the "eyes of the number 2". We now make this precise.

Example 4.8 We are accustomed to thinking of the even integers as the set $\{2k : k \in \mathbb{Z}\}$ and consequently of the odd numbers as the set $\{2k + 1 : k \in \mathbb{Z}\}$. These representation of, say, the odd numbers we get by applying the division theorem to the odd numbers with a our target odd number and $b = 2$. We can get an alternative description of the odd numbers if we apply to them the division theorem with $b = 4$, say. This would yield that every odd number can either be written

as $4k+1$ or as $4k+3$. That is,

$$\{2k+1 : k \in \mathbb{Z}\} = \{4k+1 : k \in \mathbb{Z}\} \cup \{4k+3 : k \in \mathbb{Z}\}.$$

At this point we have two representations for the odd numbers we can use these to explore the form of the squares of odd numbers.

Example 4.9 The fact that every odd square comes in either the form $(4k+1)^2$ or the form $(4k+3)^2$ means that the squares of odd numbers can only have one form which is $8n+1$.

$$(4k+1)^2 = 16k^2 + 8k + 1 = 8\underbrace{(2k^2+k)}_{n} + 1$$

$$(4k+3)^2 = 16k^2 + 24k + 9 = 16k^2 + 24k + 8 + 1 = 8\underbrace{(2k^2+3k+1)}_{n} + 1$$

in both cases the form we got is $8n+1$.

Let us reiterate Example 4.9. We have proved two claims.

Claim (a) $\forall k \in \mathbb{Z}\, \exists n \in \mathbb{Z}$ *such that* $(4k+1)^2 = 8n+1$.

Claim (b) $\forall k \in \mathbb{Z}\, \exists n \in \mathbb{Z}$ *such that* $(4k+3)^2 = 8n+1$.

Each of these claims were very easy to prove as we only had to deal with some quadratic form. Let us now revisit the task of proving that the square of every odd number has the form $8n+1$. However, this time we shall use the $2k+1$ representation for odd numbers. The difference now is that here we will have only one case and two cases as we had when we used representations of odd numbers through the number 4. This will result in a more complicated proof as it has to account for both cases in one stroke.

Example 4.10 Let a be an odd integer so that a has the form $2t+1$. Hence, $a^2 = (2t+1)^2 = 4t^2 + 4t + 1 = 4t(t+1) + 1$. At this point we appeal to Proposition 4.7 (with $b = 2$) and deduce from that that at least one of t and $t+1$ must be even. To define n we now have to consider two cases.

1. If t is even then $t = 2k$ for some integer k so that

$$a = 4(2k)(2k+1) + 1 = 8k(2k+1) + 1$$

   so we may take $n = k(2k+1)$.

2. If $t+1$ is even, then we leave the details of defining n in this case to the reader.

Example 4.11 Let a be an integer. Then $x = \frac{a(a^2+2)}{3}$ is an integer. We consider three cases.

1. $a = 3k$. In this case $x = k(a^2+2)$ and we are done.

2. $a = 3k + 1$. Here we have

$$\begin{aligned} x &= \frac{(3k+1)((3k+1)^2+2)}{3} \\ &= \frac{(3k+1)(9k^2+6k+1+2)}{3} \\ &= \frac{(3k+1)(9k^2+6k+3)}{3}. \end{aligned}$$

As $3 \mid 9k^2 + 6k + 3$ we are done.

3. $a = 3k + 2$. We leave the details of this case to the reader.

Definition 4.12 *For a real number x we write $\lfloor x \rfloor$ to denote the largest integer not exceeding x.*

Example 4.13

$$\lfloor 2/5 \rfloor = 0, \quad \lfloor 5.706 \rfloor = 5, \quad \lfloor -6.456 \rfloor = -7.$$

Lemma 4.14 *For every positive real x and positive integer d we have*

$$|\{y \in \mathbb{Z}^+ : d \mid y \text{ and } 0 < y \leq x\}| = \lfloor x/d \rfloor.$$

Proof. All positive integers divisible by d have the form kd with $k > 0$. The claim follows. ■

Example 4.15 How many integers between 100 and 1000 are divisible by 49?

$$[1000/49] - [100/49] = 20 - 2 = 18.$$

§4.2. Integer representation

We are accustomed to write out numbers (i.e., represent them) in the decimal base (i.e., base 10) in that we write

$$8912 = 8 \cdot 10^3 + 9 \cdot 10^2 + 1 \cdot 10^1 + 2 \cdot 10^0.$$

We are also accustomed to the fact that this representation of 8912 is unique. This phenomenon is not restricted to the decimal representation as the following theorem asserts.

Theorem 4.16 *Let $1 < b \in \mathbb{Z}$. Then every $N \in \mathbb{Z}^+$ can be written uniquely as*

$$N = a_k \cdot b^k + a_{k-1} b^{k-1} + \cdots + a_0 \cdot b^0 \tag{4.17}$$

where $k \in \mathbb{Z}^+$ and $a_j \in [0, b-1]$ for each $j \in [0, k]$.

Proof. (Sketch only!) As the idea behind this proof is exceedingly simple while its formal presentation is somewhat tedious we shall make do with a sketch of the argument here.

Existence. We start by arguing the existence of the representation (4.17) for N. This representation is attained by successive applications of the division algorithm. We start off by expressing

$$N = b \cdot q_0 + a_0,$$

where $a_0 \in [0, b-1]$. If $q_0 = 0$ we are done. Otherwise, we apply the Division algorithm again this time for b and q_0 as to obtain

$$q_0 = bq_1 + a_1,$$

where $a_1 \in [0, b-1]$. If we substitute this expression for q_1 in the expression for n we attain

$$N = b \cdot (bq_1 + a_1) + a_0 = b^2 \cdot q_1 + b \cdot a_1 + a_0.$$

If $q_1 = 0$ we are done. Otherwise we apply the division algorithm yet again.

More generally, these successive applications of the division algorithm generate the following equations

$$\begin{aligned} N &= b \cdot q_0 + a_0 \\ q_0 &= b \cdot q_1 + a_1 \\ q_1 &= b \cdots q_2 + a_2 \\ &\cdots \\ q_{k-2} &= b \cdot q_{k-1} + a_{k-1} \\ q_{k-1} &= b \cdot 0 + a_k \end{aligned}$$

The key point here is that this process must terminate as a strictly decreasing sequence of integers of the form $N > q_0 > q_1 > q_2 > \cdots > q_{k-1} > \cdots > 0$ must be finite. This establishes the existence of the representation (4.17).

Uniqueness. We omit here the argument that this representation is unique. ■

The essential feature here is that N (per Theorem 4.16) is completely determined by the integers $a_k, \ldots, a_0$. In particular, we use the notation $(a_k a_{k-1} \cdots a_1 a_0)_b$ to denote the *expansion* or *representation* namely $N = a_k \cdot b^k + a_{k-1} b^{k-1} + \cdots + a_0$ and call this representation the *expansion of N to the base b*.

Example 4.18

$$\begin{aligned} (000)_2 &= 0 \\ (001)_2 &= 1 \cdot 2^0 = 1 \\ (010)_2 &= 1 \cdots 2^1 = 2 \\ (011)_2 &= 1 \cdot 2^1 + 1 \cdot 2^0 = 3 \\ (100)_2 &= 1 \cdot 2^2 = 4 \\ (101)_2 &= 1 \cdot 2^2 + 1 \cdot 2^0 = 5. \end{aligned}$$

The proof of Theorem 4.16 (the existence part that is) provides us with an algorithm for finding the representation of any integer in any given base b.

Example 4.19 Find the binary expansion of 116. We repeatedly apply the division algorithm until we reach 0 for the coefficient of 2 as follows.

$$\begin{aligned} 116 &= 2 \cdot 58 + 0 \\ 58 &= 2 \cdot 29 + 0 \\ 29 &= 2 \cdot 14 + 1 \\ 14 &= 2 \cdot 7 + 0 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 2 \cdot 0 + 1. \end{aligned}$$

So that $(1110100)_2 = 116$.

Example 4.20 Find the binary expansion of 110. We repeatedly apply the division algorithm until we reach 0 for the coefficient of 2 as follows:

$$\begin{aligned} 110 &= 2 \cdot 55 + 0 \\ 55 &= 2 \cdot 27 + 1 \\ 27 &= 2 \cdot 13 + 1 \\ 13 &= 2 \cdot 6 + 1 \\ 6 &= 2 \cdot 3 + 0 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 2 \cdot 0 + 1 \end{aligned}$$

So that $110 = (1101110)_2$.

4.2.1 *Size of binary representation*

Given an integer $n \geq 0$ how large is its binary expansion? That is, how many bits do we require in order to represent n? We need to estimate the number of iterations that our conversion algorithm (see previous section) would require.

After applying the division algorithm to n and 2 the first time we get that q_1 (see proof of Theorem 4.16) either $n/2$ or $(n-1)/2$. Indeed, if n is even $q_0 = n/2$ and if n is odd then $q_0 = (n-1)/2$ (indeed $n = 2(n-1)/2 + 1$). If $q_0 \neq 0$ we repeat this and obtain $q_1 \in \{q_0/2, (q_0-1)/2\}$ and so on. In particular this algorithm stops once

$$\frac{n}{2^i} \leq 1$$

as then the corresponding q_i would be zero. Isolating for i:

$$\begin{aligned} n &\leq 2^i \\ \log_2 n &\leq \log_2 2^i \\ \log_2 n &\leq i \log_2 2 \\ \log_2 n &\leq i. \end{aligned}$$

This shows that to represent any integer n we require at least $\log_2 n$ bits. A more careful analysis would show that in fact we always need at most $\log_2 n + 1$ bits. We omit this analysis.

Proposition 4.21 *Let $a \in \mathbb{Z}$. Then $\Theta(\log a)$ bits are required to represent a as a binary string.*

4.2.2 *Binary expansion of negative numbers*

Theorem 4.16 concerns the representation of positive numbers. In this section we shall consider an approach for the representation of negative numbers in base 2; this technique is referred to as *one's complement*.

In this approach we reserve the left most bit to represent the sign of the number: 0 indicates positive and 1 indicates negative. For positive integers the remaining bits remain identical to those obtained through Theorem 4.16. For negative numbers the remaining bits are obtained as follows. First we find the binary representation of the absolute value of the integer using Theorem 4.16. Second, we "flip" each bit.

Example 4.22 To represent all numbers between -7 to 7 we shall require 4 bits. Recall that we need to reserve a bit for the sign of the number. Let us start with the number 0. Here $0 = (0000)_2$. But in one's complement we also have -0 which is (1111). A more conventional example would be 5. Here $5 = (0101)_2$. In one's complement $-5 = (1010)$. More generally we have the following:

Number	Positive	Negative
0	0000	1111
1	0001	1110
2	0010	1101
3	0011	1100
4	0100	1011
5	0101	1010
6	0110	1001
7	0111	1000

§4.3. Greatest common divisors

In this section we introduce two algorithms. The first is called *Euclid's algorithm* and the second is called the *extended Euclidean algorithm.* The focal point of both these algorithms is the following definition.

Definition 4.23 *Let $a, b \in \mathbb{Z}$ not both zero. The* greatest common divisor *(gcd, hereafter) of a and b is the largest integer d satisfying $d \mid a$ and $d \mid b$.*

It is also useful to keep the following definition in mind that spells out the term *largest* in the previous definition. Indeed, in proofs we shall actually be using the following definition.

Definition 4.24 *Let $a, b \in \mathbb{Z}$. We say that $d \in \mathbb{Z}$ is the* greatest common divisor *of a and b if that satisfies:*

1. *$d \mid a$ and $d \mid b$, and*
2. *whenever we have an integer c such that $c \mid a$ and $c \mid b$ then $c \leq d$.*

The gcd of a and b is denoted $gcd(a, b)$ or simply (a, b). For $n \in \mathbb{Z}$ we write $D(n)$ to denote the set of divisors of n. That is

$$D(n) = \{m \in \mathbb{Z} : m \mid n\}.$$

This set is clearly finite. The set of common divisors of $n, m \in \mathbb{Z}$ is then given by $D(n) \cap D(m)$, and $(m, n) \in D(n) \cap D(m)$, in particular. In fact,

$$(m, n) = \max D(n) \cap D(m).$$

In what follows we shall only focus on (a, b) for positive a and b. Indeed, the divisors of a and $-a$ are the same.

Example 4.25

$$D(6) = \{1, 2, 3, 6\}$$
$$D(12) = \{1, 2, 3, 4, 6, 12\}$$

Then $D(6) \cap D(12) = D(6)$ so that $(12, 6) = 6$.

Definition 4.26 *Integers a and b are called* relatively prime *or* co-prime *if* $(a, b) = 1$.

Example 4.27

$$(25, 6) = 1$$
$$(102, 103) = 1.$$

4.3.1 *Fundamental properties of the gcd*

Throughout this section $a, b > 0$ is assumed.

Lemma 4.28 *Let a, b be integers with $d = (a, b)$. Then $(a/d, b/d) = 1$. That is, a/d and b/d are relatively prime.*

Proof. Let $e > 0$ be a common divisor of a/d and b/d. Then $a = edk$ and $b = ed\ell$ for some two integers k and ℓ. It follows that ed is a common divisor of a and b and thus must satisfy $ed \leq d$, as d is the gcd of a and b. It follows that $e = 1$. ■

By *linear combination* of two integers a and b we mean is a sum of the form $ma + nb$ where $m, n \in \mathbb{Z}$.

Lemma 4.29 (Bézout's identity) *For any two integers a and b, (a, b) can be expressed as a linear combination of a and b.*

We now proceed to prove Bézout's identity. Define

$$\mathcal{L}(a, b) := \{ma + nb : m, n \in \mathbb{Z}\}.$$

Bézout's identity asserts that $(a, b) \in \mathcal{L}(a, b)$. Surely $\mathcal{L}(a, b) \cap \mathbb{Z}^+$ is non-empty, and as such admits a minimal element by the WOP.

Proposition 4.30 *(a, b) is the least element in $\mathcal{L}(a, b) \cap \mathbb{Z}^+$.*

Proof. Let $0 < d = ma + nb$ be the least element in $\mathcal{L}(a, b) \cap \mathbb{Z}^+$. We show that $d \in D(a) \cap D(b)$. By the division algorithm (see Theorem 4.1) $a = dq + r$ where $0 \leq r < d$. If $r = 0$ then $d \mid a$. Assume for the sake of contradiction then that $r > 0$. Then

$$0 < r = a - qd = a - q(ma + nb) = (1 - qm)a - qnb.$$

We see that $r \in \mathcal{L}(a, b) \cap \mathbb{Z}^+$ and that $r < d$ in contradiction to the minimality of d. This establishes that $d \mid A$. A similar argument shows that for $d \mid b$.

Let c be a(ny) common divisor of a and b. As $d = ma + nb$ it follows that $c|d$ so that $d \geq c$. ■

Corollary 4.31 *If $c \in D(a) \cap D(b)$ Then $c \mid (a, b)$.*

Let us remark at this point that Corollary 4.31 does not stem directly from Definition 4.24. We are now in a position to have the following theorem that often doubles as the definition for the gcd.

Theorem 4.32 *Let $a, b \in \mathbb{Z}$ not both zero. Then $d = (a, b)$ if and only if*

1. *$d \mid a$ and $d \mid b$ and*
2. *whenever $c \mid a$ and $c \mid b$ then $c \mid d$.*

In fact, the whole structure of $\mathcal{L}(a, b)$ is determined by (a, b).

Proposition 4.33

$$\mathcal{L}(a, b) = \{k(a, b) : k \in \mathbb{Z}\}.$$

Proof. We start by proving that $\mathcal{L}(a, b) \subseteq \{k(a, b) : k \in \mathbb{Z}\}$. That is we show that for every $m, n \in \mathbb{Z}$ there exists a $k \in \mathbb{Z}$ such that $ma + nb = k(a, b)$. Indeed, as (a, b) is a common divisor of a and b then $(a, b) \mid ma + nb$ for any $m, n \in \mathbb{Z}$. This implies the existence of k.

For the converse direction (i.e., that $\{k(a, b) : k \in \mathbb{Z}\} \subseteq \mathcal{L}(a, b)$) fix a multiple of (a, b) namely $k(a, b)$, $k \in \mathbb{Z}$. By Proposition 4.30, $(a, b) \in \mathcal{L}(a, b)$ so that $(a, b) = ra + sb$ for some $r, s \in \mathbb{Z}$. Multiplying both side by k we arrive at $k(a, b) = (kr)a + (ks)b \in \mathcal{L}(a, b)$. ■

Example 4.34 Determine the set $X = \{9m + 15n : m, n \in \mathbb{Z}\}$. To answer this we first note that $(9, 15) = 3$. Then, by Proposition 4.33, we have that

$$X = \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$$

Corollary 4.35 *If a and b are relatively prime then $1 \in \mathcal{L}(a, b)$, that is, there exist integers m and n satisfying $ma + nb = 1$.*

Here are two applications of Corollary 4.35. If $a \mid c$ and $b \mid c$ then $ab \mid c$ is not necessarily true. Indeed, we may have that $ab > c$; for instance $6 \mid 24$ and $12 \mid 24$ but $6 \cdot 12 \nmid 24$. For relatively prime numbers a and b this cannot happen.

Proposition 4.36 *If $a \mid c$ and $b \mid c$ and $(a, b) = 1$ then $ab \mid c$.*

Proof. Having both a and b divisors of c there exist integers k_1 and k_2 such that

$$ak_1 = c = bk_2.$$

As $(a, b) = 1$ we have that $1 = ax + by$ for some integers x and y, by Corollary 4.35. Then

$$c = c \cdot 1 = c(ax + by) = acx + bcy = abk_2x + bak_1y = ab(k_2x + k_1y)$$

so that $ab \mid c$. ■

It is not generally true that if $a \mid bc$ then $a \mid b$ or $a \mid c$; for instance, $4 \mid 6 \cdot 2$ yet $4 \nmid 6$ and $4 \nmid 2$. Here is a partial converse to 4.36.

Lemma 4.37 (Euclid's lemma)
If $a \mid bc$ and $(a, b) = 1$ then $a \mid c$.

Proof. There exist x, y such that $1 = ax + by$. Next let us note that

$$c = c \cdot 1 = c(ax + by) = cax + cby$$

Trivially, $a \mid acx$ and $a \mid cby$ as $a \mid bc$ by assumption. It follows that $a \mid c$ and consequently $a \mid bc$. ■

Example 4.38 100 and 99 are co-prime. The least positive integer that can be expressed as a linear combination of 100 and 99 is $100 - 99 = 1$. In fact for any positive integer a we have that $(a+1, a) = 1$ as $(a+1, a) \leq (a+1) - a$.

Corollary 4.39 *Let $a, b > 0$ and let $c \in \mathbb{Z}^+$. Then $(ca, ab) = c(a, b)$.*

Proof. Let $d = (a, b)$. By Proposition 4.33, d is the smallest positive integer of the form $am + bn$. Therefore, cd is the smallest positive integer of the form $c(am + bn)$. But this latter expression equals $(ca)m + (cb)n$. Hence, again by Proposition 4.33, $cd = (ca, cb)$. ■

Above we considered cases in which we can assume whether an integer c divides an integer b if $c \mid ab$ is known for some integer a. We conclude this section by addressing sums. Naturally, if $c \mid a + b$, it need not be true that $c \mid a$ or $c \mid b$. For instance,

$$5 \mid 25 = 24 + 1$$
$$5 \mid 25 = 19 + 6,$$

and so on. We do observe the following though.

Lemma 4.40 *If $c \mid a + b$ and $c \mid a$ then $c \mid b$.*

Proof. We may write $a + b = kc$ for some $k \in \mathbb{Z}$ and that $a = \ell c$ for some $\ell \in \mathbb{Z}$. Then, $\ell c + b = kc$ so that $b = (k - \ell)c$ and the claim follows. ■

4.3.1.1 GCD of multiple numbers

So far we considered the common divisors of pairs of numbers. We now consider the common divisors of several numbers.

Definition 4.41 *The* greatest common divisor *of integers $a_1, \ldots, a_n$ (not all zero) is the largest number d satisfying $d \mid a_i$ for every $i \in [n]$. We denote this number by $(a_1, \ldots, a_n)$.*

Lemma 4.42 *Let $a_1, \ldots, a_n$ be integers not all zero. Then*

$$(a_1, \ldots, a_n) = (a_1, \ldots, a_{n-2}, (a_{n-1}, a_n)).$$

Proof. A common divisor of $a_1, \ldots, a_n$ is in particular a divisor of a_{n-1} and a_n and thus of (a_{n-1}, a_n), by Corollary 4.31.

Conversely, a common divisor of $a_1, \ldots, a_{n-2}$ and (a_{n-1}, a_n) must divide a_{n-1} and a_n as (a_{n-1}, a_n) does. ■

Example 4.43 $(15, 21, 35) = (15, (21, 35)) = (15, 7) = 1$.

§4.4. The Euclidean algorithm

The greatest common divisor problem is formulated as follows.

Definition 4.44 (The GCD problem)

Instance: two positive integers $a \geq b > 0$.

Output: (a, b).

In this section we shall present an algorithm due to Euclid that given two integers finds their gcd.

Definition 4.45 *By* algorithm *we mean a self-contained step-by-step set of operations to be performed.*

Prior to formally stating Euclid's algorithm we first present the *engine* behind Euclid's algorithm.

Lemma 4.46 *For any three integers* $a, b,$ *and* c *we have* $(a + cb, b) = (a, b)$.

Proof. Suffice to show that the set of common divisors of a and b is the same as that of $a + cb$ and b. On the one hand we have that if e is a common divisor of a and b then $e \mid a + cb$ so that e is a common divisor of $a + cb$ and b as well. On the other hand, if f is a common divisor of $a + bc$ and b then $f \mid (a + cb) - cb$ so that f is a common divisor of a and b. ■

For $a > b \geq 1$ we have that $\lfloor a/b \rfloor \geq 1$. The Division Theorem (Theorem 4.1) then asserts that $a \bmod b = a - \lfloor a/b \rfloor b$. Setting $c = -\lfloor a/b \rfloor$ in Lemma 4.46 delivers the following.

Corollary 4.47 *Let* $a > b \geq 1$. *Then*

$$(a, b) = (b, a \bmod b). \tag{4.48}$$

Example 4.49 Let us calculate $(72, 30)$. In this example we in fact "running" Euclid's algorithm.

1. For the first iteration we:
   (a) use the division theorem (Theorem 4.1) to write $72 = 30 \cdot 2 + 12$.
   (b) By Lemma 4.46 $(72, 30) = (72 - 2 \cdot 30, 30) = (30, 12)$.
2. For the second iteration we:
   (a) use the division theorem to write $30 = 2 \cdot 12 + 6$.
   (b) By Lemma 4.46 $(30, 12) = (12, 30 - 2 \cdot 12) = (12, 6)$.
3. For the third iteration we:
   (a) use the division theorem to write $12 = 2 \cdot 6 + 0$.
   (b) By Lemma 4.46 $(12, 6) = (6, 12 - 2 \cdot 6) = (6, 0)$.

Here the algorithm stops. We found out that $(72, 30) = (6, 0) = 6$.

Example 4.50 Let us calculate $(252, 198)$. This time we do our calculations in a more concise

manner where we only emphasise the applications of the division theorem.

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 \\ 198 &= 3 \cdot 54 + 36 \\ 54 &= 1 \cdot 36 + 18 \\ 36 &= 2 \cdot 18 + 0 \end{aligned}$$

We see that $(252, 198) = (18, 0) = 18$.

We conclude this section with a demonstration for the usefulness of Lemma 4.46.

Lemma 4.51 *Let t, m, n be a positive integers. Then*

$$(t^n - 1, t^m - 1) = t^{(n,m)} - 1$$

Proof. The proof is by induction on $\max\{m, n\}$. If $\max\{m, n\} = 1$ or if $m = n$ then the claim is trivial. Assume then that $m < n$. We appeal to Lemma 4.46 using the identity

$$(t^n - 1) - t^{n-m}(t^m - 1) = t^{n-m} - 1$$

and we intend to using by letting $a = t^n - 1$, $b = t^m - 1$, and $c = t^{n-m}$ in that lemma. We write as follows.

$$\begin{aligned} (t^n - 1, t^m - 1) &= ((t^n - 1) - t^{n-m}(t^m - 1), t^m - 1) \\ &= (t^m - 1, t^{n-m} - 1) \\ &\overset{\text{I.H.}}{=} t^{(m,n-m)} - 1 \\ &= t^{(n,m)} - 1 \end{aligned}$$

where the second and last equalities follow by Lemma 4.46. ■

Lemma 4.51 is quite powerful as it reduces the calculation of the gcd of 'big' numbers to the calculation of the gcd of 'small' numbers.

Example 4.52 Lemma 4.51 asserts that

$$(2^{15} - 1, 2^{20} - 1) = 2^5 - 1 = 31.$$

This fact would not have been obvious if we had written

$$2^{15} - 1 = 32767 \text{ and } 2^{20} - 1 = 1048575.$$

4.4.1 *Recursive vs. iterative algorithms*

We detail two implementations of Euclid's algorithm. The first of which is an *iterative* algorithm; that is to say that it operates via the iteration of some loop control structure in which the algorithm repeats a set of operations until the condition for continuation of the loop is broken.

Euclid's algorithm: (iterative implementation)

Input: two integers $a \geq b > 0$.
Output: (a, b)

1. Set $r_0 = a$, $r_1 = b$, $n = 1$.
2. While $r_n \neq 0$ do:
   (a) Apply the division theorem to r_n and r_{n-1} to obtain numbers q and r_{n+1} satisfying $r_{n-1} = qr_n + r_{n+1}$
   (b) Set $n = n + 1$
3. Return r_{n-1}.

A single algorithm may have numerous implementation. For instance, in the case of Euclid's algorithm its *recursive* formulation is of great appeal due to its brevity.

EUCLID(a,b)
1. if $b = 0$ return a.
2. else return EUCLID(b, a mod b).

From the syntax used to detail procedure EUCLID we see that this procedure does not proceed by the means of a loop control structure. Instead it keeps invoking itself on different instances of the GCD problem. The observant reader may also note that in fact the input of EUCLID and the input on which this procedure invokes itself again are tied through (4.48). In the next section we shall see that EUCLID proceeds inductively (which is yet another term often used instead of recursively) in order to calculate (a, b). Roughly speaking, the procedure continues to generate instances of the GCD problem whose *size* is monotonically decreasing (as one would do in an inductive process). In the next section the notion *size of an instance* will be defined.

For algorithms we usually care about two features: correctness and computational complexity. The latter we address in the next section. Correctness has to do with proving that if the algorithm (ever) stops then it outputs/returns the desired output. Does EUCLID(a, b) ever stop? Suffice to show that the EUCLID procedure generates a call to itself with the second argument equal to zero. Observing the second argument in a chain of recursive calls made by EUCLID(a, b) we see

$$b, a \bmod b, b \bmod (a \bmod b), (a \bmod b) \bmod (b \bmod (a \bmod b)) \ldots.$$

It is not at all clear that this sequence ever descend to zero. But due to the fact that we carry out all our divisions here in the integers means that this sequence eventually does vanish.

Lemma 4.53 *Let $a \geq b > 0$ be integers. Then EUCLID(a, b) stops.*

Proof. Let a_i be the ith element in the sequence

$$b, a \bmod b, b \bmod (a \bmod b), (a \bmod b) \bmod (b \bmod (a \bmod b)) \ldots$$

defined above. An alternative way to define this sequence is by setting $a_1 := b$ and then $a_2 := a \bmod b$ and $a_{i+1} := a_{i-1} \bmod a_i$. Then by induction $a_i \leq b - (i - 1)$ for every $i \geq 2$. Indeed $a_2 \leq a_1 - 1 = b - 1$. Assume this holds for a_i and consider a_{i+1}. Then by the definition of a_{i+1} we have $a_{i+1} \leq a_i - 1$ then the induction hypothesis yields

$$a_{i+1} \leq a_i - 1 \leq b - (i - 1) - 1 = b - i$$

and the claim follows. It now follows that $a_b \leq 0$ implying that a call of EUCLID with the second argument being zero is generated causing the algorithm to halt. ■

Lemma 4.54 *Let $a \geq b > 0$ be integers. Then $(a, b) = EUCLID(a, b)$.*

Proof. By Lemma 4.53 EUCLID(a, b) halts. Let d be the value returned by the algorithm. Let $(a_1, b_1), \ldots, (a_k, b_k)$ be the sequence of inputs ever considered by the invocation of EUCLID(a, B). Then $d = (a_k, b_k)$ by definition. However, by (4.48), $(a, b) = (a_i, b_i)$ for every $i \in [k]$. The claim follows. ■

4.4.2 *Computational complexity of the Euclidean algorithm*

Given an algorithm we seek to know how much "time" and how much "space" is required in order to execute it. If either of these is too large then the algorithm will either not practical as it may conclude after all of humanity is long gone or require an amount of storage space that we cannot provide. We are then interested in defining the *time complexity* and *space complexity* of an algorithm.

To define time complexity we first have to agree on what should be considered as a *single computational step* that would form the basis of our measurement tools. As with other types of measurement there is a rich array of options to choose from. For instance for algorithms that sort arrays of numbers we might want to count the number of comparisons these make in order to sort the array.

In the case of Euclid's algorithm a prime candidate to act as a measure of its complexity is the number of recursive calls that an invocation of this algorithm performs for a given instance, namely an (ordered) pair a, b. For different pairs though we can get different number of recursive calls. This implies that the computational complexity of an algorithm is a *function of its input*.

If we make do with counting recursive calls we in fact miss a certain aspect of the time complexity involved in executing Euclid's algorithm. In modern computers the inputs a and b to Euclid's algorithm would be encoded as *binary* strings consisting of 0/1 bits. Calculations would then be carried out on these strings. We would like to factor in the amount of time required to manipulate these strings in order to attain the final result. Computers often have different hardware architecture. It could very well be that one computer can perform binary addition of two, say, 32 bit integers much faster than another computer. To avoid having to consider computer architecture in our running time analysis of an algorithm we will simply count the number of *single bit operations* that an algorithm has to perform. That is the collective number of times it has to set a bit to 0 or 1. This number is then an invariant of the algorithm independent of the architecture of the computer on which this algorithm would be executed.

To execute Euclid's algorithm on the inputs a and b one has to first write a and b as binary strings in the memory of computational device only once this is done can we execute the algorithm. Surely it takes time to write the binary representation of a and b into memory. However, in the running time analysis of any algorithm we ignore this as it is not relevant (or even part) of the algorithm. We start the running time analysis under the assumption that the input is has already been written. Moreover, we also do not count the number of bits required to write a and b into memory as part of the space that the algorithm requires. We only take into account the additional space (beyond that required to represent the input) that the algorithm would require in order to carry out its instructions.

Two questions have to be addressed now.

1. Given an integer a how many bits are required to write a as a binary string? An answer is provided by Proposition 4.21.

2. Given two numbers a and b each represented by a binary string of length n. How many bit operations does it take to get the binary representation of $a + b, a - b, a * b$, and a/b?

4.4.2.1 Size of the input

Every problem that we seek to solve algorithmically specifies a relation between the valid inputs to the algorithms and its outputs. That is given an instance of the problem (i.e., the input) what should the algorithm output for the given instance. In the case of the GCD problem given as instance the (ordered) pair a, b the output associated with this instance is (a, b); the gcd of a and b.

The *computational complexity* is a measure taken with respect to the *size of the input or the instance* of the algorithm.

Definition 4.55 *The* size of the input *of an algorithm is the number of bits required to describe all the input.*

4.4.2.2 Counting recursive calls in Euclid's algorithm

Let us defer any concrete definitions regarding notions of computational complexity of algorithms. For now let us focus on the recursive formulation of Euclid's algorithm and develop some metrics by which we can get a measure of what would be the "price" of executing this algorithm. The first metric we shall consider is the number of recursive calls Euclid's algorithm can make. Let F_n denote the extended Fibonacci number (see Definition 2.40).

Lemma 4.56 *Let $a > b \geq 1$ be integers and suppose Euclid's algorithm performed k recursive calls on input (a, b). Then $a \geq F_{k+2}$ and $b \geq F_{k+1}$.*

Proof. The proof is by induction on k. Let us first note that $b > a \bmod b$ hence in each recursive call we may assume that the first parameter, namely a, and the second parameter, namely b, satisfy $a > b$.

For $k = 1$ we have that $b \geq 1 = F_2$ and $a > b$ implies $a \geq 2 = F_3$. Assume the claim is true for $k - 1$ and suppose that k recursive calls had been made. As $k > 0$, the initial call EUCLID(a,b) invokes EUCLID(b, $a \bmod b$) which by assumption generates $k - 1$ recursive calls. By the induction hypothesis for $k - 1$ we then have that $b \geq F_{k-1+2} = F_{k+1}$ and $a \bmod b \geq F_{k-1+1} = F_k$. It remains to prove that $a \geq F_{k+2}$. As $a > b > 0$, then $\lfloor a/b \rfloor \geq 1$. Consequently,

$$\underbrace{a \geq b + (a - \lfloor a/b \rfloor\, b)}_{\lfloor a/b \rfloor \geq 1} \geq F_{k+1} + F_k = F_{k+2}.$$

■

Corollary 4.57 *Let $k \geq 1$ be an integer. If $a > b \geq 1$ and $b < F_{k+1}$ then EUCLID(a,b) performs $< k$ recursive calls.*

Corollary 4.57 is best possible in the sense that allowing $b \geq F_{k+1}$ mandates that Euclid's algorithm would perform $\geq k$ iterations. To see this let us consider EUCLID(F_{k+2},F_{k+1}). For $n \geq 3$,

$$\lfloor F_{n+1}/F_n \rfloor = \lfloor (F_n + F_{n-1})/F_n \rfloor = 1.$$

Then

$$\begin{aligned} F_{n+1} \bmod F_n &= F_{n+1} - \underbrace{\lfloor F_{n+1}/F_n \rfloor}_{=1} F_n \\ &= F_{n+1} - F_n \\ &= F_{n-1}. \end{aligned} \tag{4.58}$$

Then

$$(F_{n+1}, F_n) \overset{(4.48)}{=} (F_n, F_{n+1} \bmod F_n) \overset{(4.58)}{=} (F_n, F_{n-1}).$$

This implies that EUCLID(F_{k+2},F_{k+1}) would generate k recursive calls (note that the instance $(F_1, F_0 = 0)$ does not generate a call).

By Theorem 2.46

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}$$

where $\alpha = \left(1 + \sqrt{5}\right)/2$ and $\beta = \left(1 - \sqrt{5}\right)/2$. We use this fact in order to prove the following.

Theorem 4.59 *Let $a > b > 1$ be integers. The EUCLID(a,b) generates $O(\log a)$ recursive calls.*

We require some preparation.

Lemma 4.60 *Let $m > 1$ be an integer such that $m \geq F_n$ then $n < c \log m$ for some $c = c(\alpha)$.*

Proof. As $-1 < |\beta| < 1$ we may write

$$m \geq \frac{\alpha^n - \beta^n}{\sqrt{5}} > \frac{\alpha^n - 1}{\sqrt{5}}$$

so that

$$\begin{aligned} n \log_2 \alpha &< \log_2 \left(1 + m\sqrt{5}\right) \\ &= \log_2 \left(m\sqrt{5}\right) + \log_2 \left(1 + 1/m\sqrt{5}\right) \\ &\leq \log_2 m + \log_2 \sqrt{5} + \log_2(1 + 1/\sqrt{5}) \end{aligned}$$

and the claim follows. ■

We are now in a position to prove Theorem 4.59.

Proof of Theorem 4.59. Given $a > b > 1$, set

$$n := \lceil c \log b \rceil + 1$$

where c are is as in Lemma 4.60. Then $b < F_n \leq F_{n+1}$ by the same lemma. By Corollary 4.57 EUCLID(a,b) generates at most n recursive calls. The claim follows. ■

4.4.2.3 Counting bit operations

When performing basic arithmetics with numbers in base 2 we count the number of bits that need to be changed, written, and read in order to obtain the result as let this number denote the computational complexity or running time of that basic step.

Proposition 4.61 *Let $a, b \in \mathbb{Z}$.*

1. *Performing $a + b$ requires at most $\log a + \log b$ bit operations.*
2. *Performing $a - b$ requires at most $\log a + \log b$ bit operations.*
3. *Performing $a * b$ requires at most $(\log a)(\log b)$ bit operations.*
4. *Performing a/b requires at most $(\log a)(\log b)$ bit operations.*

For multiplication and division there are faster algorithms than the one stated here. There is an algorithm that is capable of multiplying two k-bit numbers performing only $O(k^{\log 3})$ bit operations. For instance, given $a \in \mathbb{Z}$ such an algorithm can calculate a^2 in $(\log a)^{\log 3}$. Note that $\log 3 \approx 1.5$. This was improved later still by Schönage and Strassen.

Theorem 4.62 (Schönage and Strassen)
Two k-bits numbers can be multiplied in time $O(k \log k \log \log k)$.

Note that all running times stated are always a function of the input; more accurately, it is a function of the size of the input.

An algorithm is said to be *polynomial* if its running time can be bounded by a polynomial in the size of its input. We make this precise.

Definition 4.63 *An algorithm is said to be* polynomial *if there exists a constant $0 < k \in \mathbb{R}$ if given input of size n it performs $O(n^k)$ bit operations.*

Definition 4.64 *An algorithm is said to be* exponential *if given input of size n it performs $O(2^n)$ bit operations.*

Note that when considering the running time of algorithms we let the worst-case analysis take over. Note that we did not say that an algorithm is exponential if given n sufficiently large then the number of bit operations required is $\Omega(2^n)$. In that sense, then, all polynomial time algorithm are also exponential; yet for the former we have a worst case analysis which is polynomial while for the latter this need not be the case.

Example 4.65 Suppose an algorithm performs $O(n)$ bit operations when its input is an integer $n \in \mathbb{Z}$. Such an algorithm has exponential running time. Indeed, the size of the input is $\log n$ (and not n).

We are now in position to give an estimation for the running time of Euclid's algorithm.

Theorem 4.66 *Let $a > b > 0$ be integers. Then EUCLID(a,b) performs $O((\log a)^3)$ bit operations.*

Proof. Per recursive call, Euclid's algorithm has to calculate $a \bmod b$ for the current instance a, b. This involves calculating $a - \lfloor a/b \rfloor b$. Ignoring the flooring operation here, this involves one multiplication, one division, and one subtraction. All of which require $O((\log a)^2)$ bit operations. As there are $O(\log a)$ recursive calls, by Theorem 4.59, the claim follows. ■

4.4.3 *The extended Euclidean algorithm*

By Bézout's identity, (a, b) can be uniquely expressed as a linear combination of a and b, namely $(a, b) = am + bn$. In what follows we adapt Euclid's algorithm to find such m and n.

Definition 4.67 (The extended Euclidean problem)

Instance: $a \geq b > 0$ integers.

Output: a triple (d, x, y) of integers such that

$$d = (a, b) = ax + by.$$

Let us return to Example 4.50 in which we calculated $(252, 198)$. The calculation there was the following.

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 \\ 198 &= 3 \cdot 54 + 36 \\ 54 &= 1 \cdot 36 + 18 \\ 36 &= 2 \cdot 18 + 0 \end{aligned}$$

Working backwards from the next to last equation we see that

$$\begin{aligned} 18 &= 54 - 1 \cdot 36 \\ 36 &= 198 - 3 \cdot 54 \\ 54 &= 252 - 1 \cdot 198. \end{aligned}$$

Substituting the second equation here into the first we obtain that

$$18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198.$$

Substituting the third equation in to this last equation yields

$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198.$$

The algorithm we just applied is called the *extended Euclidean algorithm.*

4.4.3.1 Recursive implementation

Here is a recursive formulation of the extended Euclidean algorithm.

EXT-EUCLID(a,b)

1. if $b = 0$ then return $(a, 1, 0)$.
2. $(d', x', y') = EXT - EUCLID(b, a \bmod b)$.
3. $(d, x, y) = (d', y', x' - \lfloor a/b \rfloor y')$.
4. return (d, x, y).

Theorem 4.68 *The running time of procedure EXT-EUCLID(a, b) is the same as the running time of EUCLID(a, b) within a constant factor.*

§4.5. Least common multiple

Let us now consider a concept analogous somewhat to that of the gcd. We say that c is a *common multiple* of non-zero integers a and b if $a \mid c$ and $b \mid c$. Clearly $-ab$, 0, and ab are all common multiples. Such are all trivial ones. The WOP implies that there are non-trivial ones. Indeed, for a and b consider the set

$$S = \{c : a \mid c,\ b \mid c,\ c > 0\}$$

of positive common multiples of a and b. As $ab \in S$ this set is non-empty and thus admits a least element by the WOP. We refer to this element as the *least common multiple* of a and b. Trivially we have that

$$lcm(a, b) \leq |ab|.$$

Definition 4.69 *The* least common multiple *of two non-zero integers a and b, denoted $lcm(a, b)$, is the positive integer m satisfying:*

1. *$a \mid m$ and $b \mid m$, and*
2. *whenever $a \mid \ell$ and $b \mid \ell$ then $m \leq \ell$.*

Example 4.70 The positive common multiples of -12 and 30 are

$$60, 120, 180, \ldots$$

and $lcm(-12, 30) = 60$.

Theorem 4.71 *For positive integers a and b*

$$(a, b)lcm(a, b) = ab$$

Proof. Let $d = (a, b)$ so that $a = dk_1$ and $b = dk_2$ for some two integers k_1 and k_2. Put $m = \frac{ab}{d}$. We verify that m satisfies the conditions of Definition 4.69.

Note that $m = \frac{adk_2}{d} = ak_2$ and $m = \frac{dk_1b}{d} = bk_1$ so that $a \mid m$ and $b \mid m$ and m satisfies the first condition of Definition 4.69.

We turn to the second condition of that definition. Let c be a common multiple of a and b so that $av = c = bu$ for some two integers v and u. In addition, we may write $d = ax + by$ for some two integers x and y, by Bézout's identity. We now show that not only is it that $m \leq c$ but also that $m \mid c$.

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax + by)}{ab} = \frac{c}{b}x + \frac{c}{a}y = ux + vy,$$

and we are done. ■

From the proof of Theorem 4.71 we have learned that the lcm has a similar property as the gcd (see Corollary 4.31) in that

every common multiple of a and b is a multiple of $lcm(a, b)$.

This gives rise to the following alternative definition of the lcm.

Definition 4.72 *The* least common multiple *of two non-zero integers a and b, denoted $lcm(a, b)$, is the positive integer m satisfying:*

1. *$a \mid m$ and $b \mid m$, and*
2. *whenever $a \mid \ell$ and $b \mid \ell$ then $m \mid \ell$.*

Corollary 4.73 *For relatively prime integers a and b we have*

$$lcm(a, b) = ab. \tag{4.74}$$

As in the case of the gcd, here too, we shall be interested in the lcm of multiple integers.

Definition 4.75 *The* least common multiple *of k non-zero integers $m_1, \ldots, m_k$, denoted $lcm(m_1, \ldots, m_k)$, is the positive integer m satisfying:*

1. *$m_i \mid m$ for every $i \in [k]$, and*
2. *whenever $m_i \mid \ell$ for every $i \in [k]$ then $m \mid \ell$.*

In general Theorem 4.71 does not extend to more than two numbers. Indeed, one cannot attain the value of $lcm(a, b, c)$ using only the values of $a \cdot b \cdot c$ and (a, b, c). For instance, $(1, 2, 2) = (1, 1, 4) = 1$ and $1 \cdot 2 \cdot 2 = 1 \cdot 1 \cdot 4 = 4$ but $lcm(1, 2, 2) = 2$ and $lcm(1, 1, 4) = 4$. The generalisation of Theorem 4.71 for, say, three numbers is in fact

$$(ab, ac, bc) \cdot lcm(a, b, c) = a \cdot b \cdot c.$$

To prove this one needs either the *principle of inclusion-exclusion* which we do not cover in these notes or the fundamental theorem of arithmetics (Theorem 5.2) which we did not yet cover. Nevertheless, Corollary 4.73 does extend verbatim to more than two numbers.

Lemma 4.76 *Let $a_1, \ldots, a_n$ be relatively prime to one another. Then*

$$lcm(a_1, \ldots, a_n) = a_1 \cdot a_2 \cdots a_n.$$

We postpone the proof of this result until § 5.1.2.2.

§4.6. The (linear) Diophantine equation $ax + by = c$

Given three integers a, b, c one is often interested whether a formula of the following form

$$ax + by = c \tag{4.77}$$

has a solution in $\mathbb{Z}$. Such an equation is called a *linear Diophantine equation*. Some linear equations such as $3x + 6y = 18$ have several solutions:

$$\begin{aligned} 3 \cdot 4 + 6 \cdot 1 &= 18 \\ 3 \cdot (-6) + 6 \cdot 6 &= 18 \\ 3 \cdot 10 + 6 \cdot (-2) &= 18. \end{aligned}$$

However, the equation $2x + 10y = 17$ has no solution. Indeed, the left hand side of this equation is always even while the right side is odd. The following lemma characterises the linear equations for which at least one solution exists.

Lemma 4.78 *The equation $ax + by = c$ has a solution in $\mathbb{Z}$ if and only if $(a, b) \mid c$.*

Proof. Let $d = (a, b)$. There exist integers r and s such that $a = dr$ and $b = ds$. Suppose now that a solution (x_0, y_0) to (4.77) exists. Then

$$c = ax_0 + by_0 = drx_0 + dsy_0 = d(rx_0 + sy_0)$$

which simply asserts that $d \mid c$.

Conversely, suppose that that $d \mid c$ so that $c = dt$ for some integer t. Now, by Bézout's identity there are integers x_1 and y_1 satisfying $d = ax_1 + by_1$. We thus have that

$$c = dt = (ax_1 + by_1)t = a(tx_1) + b(ty_1)$$

so that (tx_1, ty_1) is a solution to (4.77). ■

Corollary 4.79 *Determining whether (4.77) has any solutions requires $O((\max\{\log a, \log b\})^3 \cdot \log c)$.*

For linear equations such as (4.77) it is sufficient to find a single solution. Indeed, given one solution we can find them all as the next lemma asserts.

Lemma 4.80 *Suppose that (x_0, y_0) is a solution of (4.77). Then any other solution (x, y) to (4.77) has the form*

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

where $d = (a, b)$ and $t \in \mathbb{Z}$ is arbitrary.

Proof. To establish the second assertion of the lemma, let us suppose that a solution x_0, y_0 of the given equation is known. If x', y' is any other solution, then

$$ax_0 + by_0 = c = ax' + by'$$

which is equivalent to

$$a(x' - x_0) = b(y_0 - y')$$

There exist relatively prime integers r and s such that $a = dr$, $b = ds$. Substituting these values into the last equation and canceling the common factor d, we find that

$$r(x' - x_0) = s(y_0 - y')$$

The situation is now this: $r \mid s(y_0 - y')$, with $gcd(r, s) = 1$. Using Euclid's lemma, it must be the case that $r \mid (y_0 - y')$; or, in other words, $y_0 - y' = rt$ for some t. Substituting, we obtain

$$x' - x_0 = st$$

This leads us to the formulas

$$x' = x_0 + st = x_0 + \left(\frac{b}{d}\right) t$$
$$y' = y_0 - rt = y_0 - \left(\frac{a}{d}\right) t$$

It is easy to see that these values satisfy the Diophantine equation, regardless of the choice of the integer t; for

$$\begin{aligned} ax' + by' &= a\left(x_0 + \left(\frac{b}{d}\right)t\right) + b(y_0 - (\frac{a}{d})t) \\ &= (ax_0 + by_0) + \left(\frac{ab}{d} - \frac{ab}{d}\right)t \\ &= c + 0 \cdot t \\ &= c \end{aligned}$$

Thus, there is an infinite number of solutions of the given equation, one for each value of t. ■

Lemma 4.80 delivers an interesting message

$$ax + by = c \text{ has either no solution or infinitely many solutions.}$$

The problem then boils down to finding some solution for a soluble equation of the form (4.77). For this we will use the extended Euclidean algorithm. Here is the general template to find a solution for $ax + by = c$.

1. Apply the extended Euclidean algorithm to find m and n satisfying $am + bn = (a, b)$.
2. Multiply what you got by c:
$$acm + bcn = (a, b)c.$$
3. Divide by (a, b):
$$a\left(\frac{cm}{(a,b)}\right) + b\left(\frac{cn}{(a,b)}\right) = c$$

If $x_0 = \frac{cm}{(a,b)}$ and $y_0 = \frac{cn}{(a,b)}$ are both integers we are done.

Corollary 4.81 *Solving an equation of the form $ax + by = c$ requires $O(\max\{\log a, \log b, \log c\}^3)$ bit operations.*

Example 4.82 Let us consider $56x + 72y = 40$. Using the extended Euclidean algorithm we find out that $(56, 72) = 8 = 4 \cdot 56 + (-3) \cdot 72$. Then we have

$$x_0 = \frac{4 \cdot 40}{8}, \quad y_0 = \frac{(-3) \cdot 40}{8},$$

which are clearly integers.

The fact that both x_0 and y_0 are multiples of c implies that to solve $ax + by = c$ we must first solve $ax + by = 1$. Find suggestions for solutions $x_0' = x_0/c$ and $y_0' = y_0/c$ and from those we can extract x_0 and y_0.

Example 4.83 Find $x, y \in \mathbb{Z}$ such that $172x + 20y = 1000$. Applying the Euclidean Algorithm to the evaluation of $gcd(172, 20)$, we find that

$$\begin{aligned} 172 &= 8 \cdot 20 + 12 \\ 20 &= 1 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 \end{aligned}$$

whence $(172, 20) = 4$. Because $4 \mid 1000$, a solution to this equation exists.

Applying the extended Euclidean algorithm we work backwards through the previous calculations, and get that

$$4 = -17 \cdot 20 + 2 \cdot 172.$$

Then we have $x = \dfrac{2 \cdot 1000}{4} = 500$ and $y = \dfrac{-17 \cdot 1000}{4} = -4250$.

§4.7. Exercises

Exercise 1. We have seen an implementation of Euclid's algorithm that for input $a > b > 0$ integers has running time $O((\log a)^3)$. In this exercise you are to give an implementation of this algorithm that has running time $O(\log a \cdot \log b)$.

Let $u_0 = a$ and $u_1 = b$. The Euclidean algorithm implicitly generates the following system of equations.

$$\begin{aligned} u_0 &= q_0 u_1 + u_2 \\ u_1 &= q_1 u_2 + u_3 \\ &\dots \\ u_{n-2} &= q_{n-2} u_{n-1} + u_n \\ u_{n-1} &= q_{n-1} u_n \end{aligned}$$

where $q_i = \left\lfloor \frac{u_i}{u_{i+1}} \right\rfloor$, $u_n = (a, b)$ (which is the number returned by the algorithm), and the number of iterations/recursive calls the algorithm performs is $n = O(\log a)$ (as proved in the lecture notes). Taking a more global point of view, the running time of the Euclidean algorithm is determined by the time it takes to calculate the series of quotients $(q_i)_{i=0}^{n-1}$ (the time to calculate all additions and multiplications will be "swallowed" by the time to evaluate this series.

Assuming each q_i can be calculated in $O(\log q_i \log u_{i+1})$ time, use this assumption and the first part of this exercise to prove that the running time of the Euclidean algorithm is bounded by $O(\log a \log b)$.

Hint.

$$\sum_{0 \le i \le n-1} \log q_i \log u_{i+1}.$$

Exercise 2. The following algorithm is proposed as a non-Euclidean method for calculating the gcd of two numbers. The input of the algorithm are two integers $a, b > 0$.

1. $g = 1$, $u = a$, $v = b$.
2. while u is even and v is even do
   (a) $u = u/2$
   (b) $v = v/2$
   (c) $g = 2g$
3. while $u \neq 0$ do
   (a) if u is even then $u = u/2$.
   (b) else if v is even then $v = v/2$.
   (c) else:

i. $t = |u - v|/2$.
ii. if $u \geq v$ then $u = t$.
iii. else $v = t$

4. return $g \cdot v$.

(a) Prove that this algorithm stops. Consider the quantity uv captured by the variables u and v and show that this quantity reduces by a factor of at least 2 after each iteration of the first while loop and after each iteration of the second while loop.

(b) Use Exercise 18 below to prove that the above algorithm (also known as the binary gcd algorithm) returns (a, b).

(c) (i) Let an integer m be given in its binary representation. Prove that the binary representation of $m/2$ can be attained by simply shifting the binary representation of m one bit to the right (and thus incurring a 0 bit in the most significant bit).

(ii) Prove that the running time of this algorithm is $O((\log ab)^2)$.

Exercise 3. Show that if a, b, c are non-zero integers then $a \mid b$ if and only if $ac \mid bc$.

Exercise 4. Prove that the product of any three consecutive integers is divisible by 6.

Exercise 5. Use the Euclidean gcd and Extended Euclidean algorithm for the following pairs:

1. 4116, 21609.
2. 84, 1124.
3. 899, 1914.

Exercise 6. Solve the equation $105x + 121y = 3$ for $x, y \in \mathbb{Z}$.

Exercise 7.

1. Let $1 \leq b \leq a$ be integers. Prove that $a \bmod b < \frac{a}{2}$.
2. Suppose that we apply the Euclidean algorithm on two integers a, b satisfying $1 \leq b \leq a \leq 2^{100}$. Give an upper bound on the number of iterations of the algorithm.

   Hint: Use the part 1 of this question.

Exercise 8. Let a, b be integers. Prove that $a \mid b$ if and only if $a \mid -b$.

Exercise 9. Let a, b, c be integers. Prove that if $a \mid b$ and $b \mid c$ then $a \mid c$.

Exercise 10. Let a, b, c be integers. Prove that if $a \mid b$ and $a \mid c$ then $a \mid (b \pm c)$.

Exercise 11. Let a, b, c, d be integers such that $a \mid b$ and $c \mid d$. Prove that $ac \mid bd$.

Exercise 12. Let a, b be two positive odd integers such that $b \nmid a$. Show that there exist integers q

and p such that $a = bq + p$ where p is odd and $|p| < b$.

Exercise 13. Find the number of integers not exceeding 1000 that are not divisible by 3 or by 5

Exercise 14. Show that the fourth power of every odd integer has the form $16k + 1$.

Exercise 15. For any three consecutive natural numbers $(n-1)$, n, and $(n+1)$ prove the following properties:

1. $(n, n-1) = (n, n+1) = 1$.
2. $(n-1, n+1) \leq 2$.
3. $(n, (n-1)(n+1)) = 1$.

Exercise 16.

1. Let $a, b, c \in \mathbb{N}$ and $c \geq 1$. Prove that $(a, b)c = (ac, bc)$.
2. Let $a, b, c \in \mathbb{N}$, $(a, b) = 1$ and $c|(a + b)$. Prove that $(c, b) = (c, a) = 1$.

Exercise 17. Let a and b be relatively prime integers not both zero. Show that $(a^2+b^2, a+b) \in \{1, 2\}$.

Exercise 18. Prove the following properties of the gcd.

1. Let $a, b > 0$ be even integers. Prove that
$$(a, b) = 2\big(a/2, b/2\big). \tag{4.84}$$
2. Let $a, b > 0$ be integers such that a is even and b is odd. Prove that
$$(a, b) = (a/2, b). \tag{4.85}$$
3. Let $a, b > 0$ be odd integers. Prove that
$$(a, b) = \big(|a - b|/2, b\big). \tag{4.86}$$

Exercise 19. Find the binary expansion of 110

§4.8. Solutions

Some of the solutions have been written by the TAs in the course and thus have a different style of writing to them. Over time we hope to normalise this part of the text as well.

Solution for Exercise 1. We start by noticing that

$$\begin{aligned}
\prod_{i=0}^{n-1} q_i &\leq \prod_{i=0}^{n-1} \frac{u_i}{u_{i+1}} \\
&= \frac{u_0}{u_1} \cdot \frac{u_1}{u_2} \cdots \frac{u_{n-2}}{u_{n-1}} \frac{u_{n-1}}{u_n} \\
&= \frac{u_0}{u_n} \\
&= \frac{a}{u_n} \\
&\leq a.
\end{aligned} \tag{4.87}$$

The running time of Euclid's algorithm under the given assumption is $\sum_{0\le i\le n-1}\log q_i \log u_{i+1}$. Then

$$\begin{aligned}\sum_{0\le i\le n-1}\log q_i\log u_{i+1} &\le \log b\sum_{0\le i\le n-1}\log q_i\\ &= \log b\log\Bigg(\underbrace{\prod_{0\le i\le n-1} q_i}_{\le a \text{ by } (4.87)}\Bigg)\end{aligned}$$

and the claim follows.

Solution for Exercise 2.

(a) The algorithm stops as the quantity uv captured by the variables u and v reduces by a factor of at least 2 after each iteration of the first while loop and after each iteration of the second while loop.

  (i) In each iteration of the first while loop the quantity uv is reduced by a factor of 2. Indeed, in the first while loop both u and v are even and are both divided by 2.

  (ii) In each iteration of the second while loop either one of u and v is even, or both are odd. In the former case the even of the even of the pair is divided by 2 so that uv is diminished by a factor of 2. In the latter the larger of the two is replaced by $|u-v|/2$. Let u' and v' be the values of the variables u and v after such a replacement. Assuming without loss of generality that $u\ge v$ we have that $u'v'\le |u-v|v/2 = uv/2 - v^2/2 \le uv/2$.

(b) As long as $u\ne 0$ the algorithm maintains the invariant that $(a,b)=g(u,v)$.

  (i) This identity surely holds when in line 1.

  (ii) At the beginning of each iteration of the while loop starting at line 2 we have $(a,b)=g(u,v)$ due to (4.84).

  (iii) After the first while loop terminates the variable g holds power of 2 in the prime power factorisation of (a,b).

  (iv) At the beginning of each iteration of the while loop starting at line 6 for which $u>0$ still holds we have $(a,b)=g(u,v)$ due to (4.85) and (4.86).

  Finally, the variable u is set to 0 in the second while loop only if $t=0$ which happens only if $u=v$. At this moment $(a,b)=g(u,v)=g(v,v)=gv$. The algorithm return gv.

(c) (i) Let

$$m = a_k2^k + a_{k-1}2^{k-1} + \dots a_12^1 + a_0.$$

  Shifting the representation $(a_k, a_{k-1},\dots,a_1,a_0)$ generates the representation $(0,a_k,a_{k-1},\dots,a_1)$ and thus the number

$$a_k2^{k-1} + a_{k-1}2^{k-2} + \dots a_1.$$

  which is precisely $m/2$.

  (ii) As the quantity uv reduces by a factor of at least 2 after each iteration of either of the while loops, both while loops make $O(\log ab)$ iterations combined. Each division by 2 of either u or v require $O(\log uv)$ time (as we need only shift the representation one bit to the right). Also, any calculation $|u-v|$ also require $O(\log uv)$ time. The claim follows.

Solution for Exercise 3. Since this is an *if and only if* statement it's not enough to show that if $a \mid b$ then $ac \mid bc$, we also need to prove the other direction i.e. if $ac \mid bc$ than $a \mid b$. We start by showing that if $a \mid b$ then $ac \mid bc$. Assume that $a \mid b$. Then there exists some $k \in \mathbb{Z}$ such that $b = ak$. Therefore $(bc) = (ac)k$, hence $ac \mid bc$. Next we show that if $ac \mid bc$ than $a \mid b$. Assume $ac \mid bc$. Then there exists some $k \in \mathbb{Z}$ such that $(bc) = (ac)k$. Therefore $b = ak$, hence $a \mid b$.

Solution for Exercise 4. Let $n \in \mathbb{Z}$. We prove that $6 \mid (n-1)n(n+1)$. Recall that $3 \mid (n-1)n(n+1)$. If $2 \mid n$ then $2 \mid (n-1)n(n+1)$, and therefore by Proposition 2.12 of the lecture notes since 2 and 3 are relatively prime it holds that $6 \mid (n-1)n(n+1)$. If $2 \nmid n$ then $2 \mid (n-1), (n+1)$ hence $2 \mid (n-1)n(n+1)$. Since 2 and 3 are relatively prime it holds that $6 \mid (n-1)n(n+1)$.

Solution for Exercise 5.

1. gcd:

$$\begin{aligned} 21609 &= 5 \cdot 4116 + 1029 \\ 4116 &= 4 \cdot 1029. \end{aligned}$$

   therefore $gcd(21609, 4116) = 1029$.
   Extended Euclidean algorithm: $1029 = 21609 - 5 \cdot 4116$

2. Euclidean Algorithm:

$$\begin{aligned} 1124 &= 13 \cdot 84 + 32 \\ 84 &= 2 \cdot 32 + 20 \\ 32 &= 1 \cdot 20 + 12 \\ 20 &= 1 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4. \end{aligned}$$

   therefore $gcd(1124, 84) = 4$.
   Extended Euclidean algorithm:
   By the fifth equality of the Euclid Algorithm, $4 = 12 - 8$. Since $20 = 12 + 8$ we can write $4 = 12 - (20 - 12) = 12 \cdot 2 - 20$. By the third equality $12 = 32 - 20$ and therefore $4 = (32 - 20) \cdot 2 - 20 = 32 \cdot 2 - 20 \cdot 3$. By the second equlity $20 = 84 - 2 \cdot 32$, hence $4 = 32 \cdot 2 - (84 - 32 \cdot 2) \cdot 3 = 32 \cdot 8 - 84 \cdot 3$. Finally $32 = 1124 - 13 \cdot 84$ and so $4 = (1124 - 84 \cdot 13) \cdot 8 - 84 \cdot 3 = 1124 \cdot 8 - 84 \cdot 107$.

3. Euclid Algorithm:

$$\begin{aligned} 1914 &= 2 \cdot 899 + 116 \\ 899 &= 7 \cdot 116 + 87 \\ 116 &= 1 \cdot 87 + 29 \\ 87 &= 3 \cdot 29. \end{aligned}$$

   therefore $gcd(1914, 899) = 29$.
   Extended Euclidean algorithm:

$$\begin{aligned} &29 = \\ &116 - 87 = 116 - (899 - 7 \cdot 116) = \\ &116 \cdot 8 - 899 = (1914 - 2 \cdot 899) \cdot 8 - 20 = \\ &8 \cdot 1914 - 17 \cdot 8993. \end{aligned}$$

Solution for Exercise 6. We will use the Extended Euclidean algorithm for 105 and 121. First we use the Euclidean Algorithm.

$$\begin{aligned}
&121 = 1 \cdot 105 + 16.\\
&105 = 6 \cdot 16 + 9\\
&16 = 1 \cdot 9 + 7\\
&9 = 1 \cdot 7 + 2\\
&7 = 3 \cdot 2 + 1\\
&2 = 2 \cdot 1
\end{aligned}$$

Therefore by the Extended Euclidean Algorithm:

$$\begin{aligned}
&1 =\\
&7 - 3 \cdot 2 = 7 - 3 \cdot (9 - 7) =\\
&4 \cdot 7 - 3 \cdot 9 = 4 \cdot (16 - 9) - 3 \cdot 9 =\\
&4 \cdot 16 - 7 \cdot 9 = 4 \cdot 16 - 7 \cdot (105 - 6 \cdot 16) =\\
&46 \cdot 16 - 7 \cdot 105 = 46 \cdot (121 - 105) - 7 \cdot 105 =\\
&-53 \cdot 105 + 46 \cdot 121
\end{aligned}$$

Therefore $-159 \cdot 105 + 138 \cdot 121 = 3$ and thus the set of solutions is $\{(-159 + 121t, 138 - 105t) : t \in \mathbb{Z}\}$.

Solution for Exercise 7.

1. Let $a = bk + r$ by the division algorithm and assume towards a contradiction that $r \geq a/2$. As $r = a - bk$ it follows now that $a - bk \geq a/2$ so that $2a - 2bk \geq a$ leading to $a \geq 2bk$. As $a = bk + r$ we reach $bk + r = a \geq 2bk$. As $r \leq b - 1$ this is a contradiction.

   Here is an alternative proof. Let $a = bk + r$ by the division algorithm and consider two cases: either $b < a/2$ or $b \geq a/2$. In the former case $r \leq b - 1 < a/2 - 1$ and we are done. Suppose then that $b \geq a/2$. In this case either $k = 0$ or $k = 1$. In the former case $a = r < b$ contradicting the assumption that $b \leq a$. In the latter case $a = b + r$ and thus $r = a - b < a/2$ as required. .

2. Let n be the number of iterations the Euclidean algorithm performs. To make the definition of this number clear set $r_0 := a$ and for every $i \in \{1 \ldots, n\}$ define r_i to be the residue obtained in the i-th iteration. The algorithm receives r_0 as input generates $(r_i)_{i=1}^n$ and stops when it encounters $r_{n+1} = 0$ and does not perform another iteration. That is we assume $r_n > 0$. We claim that $2^{\frac{n-1}{2}} \cdot r_{n-1} \leq r_0$ or $2^{\frac{n}{2}} \cdot r_n \leq r_0$. By the previous part of this exercise we get that $r_{i+1} = r_{i-1} \bmod r_i \leq \frac{r_{i-1}}{2}$. Therefore, depending on the parity of n, we get that either $2^{\frac{n}{2}} \cdot r_n \leq r_0$ or $2^{\frac{n-1}{2}} \cdot r_{n-1} \leq r_0$. As $0 = r_{n+1} < r_n \leq r_{n-1}$ and $r_n \neq 0$ it follows that $1 \leq r_n, r_{n-1}$; hence $2^{\frac{n-1}{2}} \leq r_0 = a \leq 2^{100}$ or $2^{\frac{n}{2}} \leq r_0 = a \leq 2^{100}$. By solving the equation we get that the number of iterations is at most 200 or 201.

Solution for Exercise 8. As $a \mid b$ then $b = ak$ for some integer k. Multiplying the equation by -1 yields $-b = -ak = a(-k)$. The claim follows.

Solution for Exercise 9. If $b \mid c$ then $c = bt$ for an integer t. In addition, $a \mid bt$, as $a \mid b$. The claim follows.

Solution for Exercise 10. As $a \mid b$ and $a \mid c$, there exist integers s and t such that $b = as$ and $c = at$. Then $(b \pm c) = a(s \pm t)$. Note that $(s \pm t)$ is an integer; consequently $a|(b \pm c)$.

Solution for Exercise 11. Let t, s be integers such that $at = b$ and $cs = d$. We write this as $\frac{b}{t} = a$ and $\frac{d}{s} = c$. So $\dfrac{bd}{ts} = ac$. Now, ts is an integer, since t and s are integers. It follows that $ac \mid bd$.

Solution for Exercise 12. By the division algorithm we may write $a = bs + t$ for some integers s and t, with $0 \leq t < b$. As $b \not| a$ we may in fact assume that $t > 0$. If t is odd we are done as we may take $q = s$ and $p = t$. Suppose then that t is even. As b is odd, by assumption, then $t - b$ is odd and negative, in particular $t - b < b$ (as $t < b$). We nay then write

$$a = bs + t = b(s + 1) - b + t = b(s + 1) + (t - b)$$

and set $q = s + 1$ and $p = t - b$. The claim follows.

Solution for Exercise 13. $1000 - \lfloor 1000/3 \rfloor - \lfloor 1000/5 \rfloor + \lfloor 1000/15 \rfloor = 533$.

Solution for Exercise 14. Every odd integer has the form $4k + 1$ or $4k + 3$. Observe that

$$(4k + 1)^4 = 16^2k^4 + 4(4k)^3 + 6(4k)^2 + 4(4k) + 1 = 16(16k^4 + 16k^3 + 6k^2 + k) + 1,$$

and that

$$(4k + 3)^4 = (4k)^4 + 12(4k)^3 + 54(4k)^2 + 108(4k) + 3^4 = 16(16k^4 + 48k^3 + 54k^2 + 27k + 5) + 1.$$

Solution for Exercise 15.

1. Let $(n, n - 1) = d$, $d \mid n$ and $d \mid n - 1$. We have that also $d \mid (n - 1) - n$ or $d \mid -1$. If $d \mid -1$, then also $d \mid 1$. We obtain $(n, n - 1) = d = 1$.

   For the second equality $d \mid n$ and $d \mid n + 1$. We have that also $d \mid (n + 1) - n$. We obtain $d \mid 1$ and $(n, n + 1) = d = 1$.

2. Let $(n + 1, n - 1) = d$. $d \mid n + 1$ and $d \mid n - 1$. So $d \mid (n + 1) - (n - 1)$ or $d \mid 2$. If $d \mid 2$, it can be only 1 or 2.

3. Let $(n, (n - 1)(n + 1)) = d$.
   $d \mid n$, therefore $d \mid n^2$. In addition $d \mid (n - 1)(n + 1)$ or $d \mid n^2 - 1$.
   $d \mid n^2 - (n^2 - 1)$. In this way $d \mid 1$.

Solution for Exercise 16.

1. We have seen that (a, b) is the least element of a linear combination $d = ax + by$. For $c \geq 1$ we have $cd = cax + cby$. We will prove that cd is the least element. Suppose that there exist x' and y' such that $0 < acx' + cby' < acx + cby \Rightarrow 0 < ax' + by' < ax + by$. We got a contradiction, because $ax + by = d$ must be the least element.

2. If $(a, b) = 1$, there exist integers m and n such that $1 = ma + nb$. Because $c|(a + b)$ we know that there exists $k \in \mathbb{Z}$ such that $a + b = kc$.
   $b = kc - a$
   $1 = ma + n(kc - a) = a(m - n) + nkc$. By definition $(a, c) = 1$. By the same way we can prove that $(c, b) = 1$.

Solution for Exercise 17. Let c be a prime satisfying $c \mid (a^2 + b^2, a + b)$. Then $c \mid a^2 + b^2$ and $c \mid a + b$ so that $c \mid (a + b)^2 - (a^2 + b^2) = 2ab$. We may assume that

$$c \not| a \text{ and that } c \not| b. \tag{4.88}$$

To see (4.88) suppose, without loss of generality, that $c \mid a$. Then as $c \mid a + b$ it follows that $c \mid b$. For otherwise we may write $b = k_1c + r$, $0 \leq r < c$, by the Division Theorem, and $a = k_2c$ by our assumption. Then $a + b = (k_1 + k_2)c + r$ which is its unique representation by the Division Theorem; contradicting the assumption that $c \mid a + b$. Pressing on, as $(a, b) = 1$ and as c is a common divisor of a and b it follows that $c = 1$ in this case. That is, we have just shown that any divisor of $(a^2 + b^2, a + b)$ (under the assumption that $c \mid a$) can only be 1 implying that $(a^2 + b^2, a + b) = 1$ and the claim follows in this case. This establishes (4.88).

Now, (4.88) together with $c \mid 2ab$ implies that $c \mid 2$ as c is prime. As 2 is prime we must have that $c \in \{1, 2\}$. In particular we have shown then that the sole divisors of $(a^2 + b^2, a + b)$ are either 1 or 2 (or both). This means that $(a^2 + b^2, a + b) \in \{1, 2\}$.

Solution for Exercise 18.

1. The identity $(ca, cb) = c(a, b)$ is proved in Corollary 4.39.

2. We prove that $D(a) \cap D(b) = D(a/2) \cap D(b)$. The inclusion $D(a/2) \cap D(b) \subseteq D(a) \cap D(b)$ being trivial we proceed to prove $D(a) \cap D(b) \subseteq D(a/2) \cap D(b)$. Let $c \in D(a) \cap D(b)$; b being odd implies that $c \neq 2$. As $1 \in D(a/2) \cap D(b)$ we may as well assume $c \neq 1$ co that $c > 2$. Let $a = 2m$, then $c \mid 2m$. As $(c, 2) = 1$ it follows that $c \mid m$ (see Euclid's theorem). As $c \mid b$ by definition the inclusion in this direction follows.

3. Surely $|a - b|$ is even; then by the second part of this exercise $(|a - b|, b) = (|a - b|/2, b)$. As $a > b$, $(|a - b|, b) = (a - b, b) = (a, b)$ where the last equality is owing to the identity $(a + cb, b) = (a, b)$ whenever $c \in \mathbb{Z}$.

Solution for Exercise 19. We repeatedly apply the division algorithm until we reach 0 for the coefficient of 2 as follows:

$$\begin{aligned}
110 &= 2 \cdot 55 + 0 \\
55 &= 2 \cdot 27 + 1 \\
27 &= 2 \cdot 13 + 1 \\
13 &= 2 \cdot 6 + 1 \\
6 &= 2 \cdot 3 + 0 \\
3 &= 2 \cdot 1 + 1 \\
1 &= 2 \cdot 0 + 1
\end{aligned}$$

So that $110 = (1101110)_2$.

Primes

§5.1. Unique factorisation in $\mathbb{Z}$

Definition 5.1 *A* prime *is a positive integer greater than* 1 *divisible by no positive integer other than* 1 *and itself.*

Positive integers that are not prime are called *composite*. That is, a positive integer n is composite if $n = a \cdot b$ for some $2 \leq a, b < n$. The following theorem asserts that the primes are the building blocks of number theory.

The main result of this section is the following.

Theorem 5.2 (The fundamental theorem of arithmetics)
Every integer greater than 1 *can be uniquely written as a product of primes up to the order of the primes involved.*

Corollary 5.3 *Any integer $n > 1$ can be written uniquely in a canonical form*

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k},$$

where for each $i \in [k]$ we have that $a_i > 0$, each p_i is prime, and $p_1 < p_2 < \cdots < p_k$.

The act of decomposing a number to prime numbers in such a way is called *factorisation*. We distinguish between two types of factorisations.

Example 5.4

$$\begin{aligned} 240 &= \underbrace{2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5}_{\text{prime factorisation}} = \underbrace{2^4 \cdot 3 \cdot 5}_{prime-power\,factorisation} \\ 289 &= 17 \cdot 17 = 17^2; \\ 1001 &= 7 \cdot 11 \cdot 13. \end{aligned}$$

Definition 5.5 *The distinct primes appearing in the prime-power factorisation of a number are called its* prime factors.

Prior to proving Theorem 5.2 let us prove something significantly more naive in order to be convinced that primes and in fact Theorem 5.2 are of interest.

Lemma 5.6 *Every positive integer greater than* 1 *has a prime divisor.*

Proof. Assume towards a contradiction that the claim is false. Then there are positive integers that form a counter example to this claim. Let n be the least counter example to the claim (we appeal here to the WOP). We may assume that n is not a prime as then n is not a counter example. Hence, n is composite and we may write $n = ab$ for some two integers $2 \leq a, b < n$. By the choice of n the number a is not a counter example to the claim. Hence, a has a prime divisor; and consequently so does n; contradiction. ■

Actually, we can do much better than Lemma 5.6.

Theorem 5.7 *If n is composite then it has a prime factor not exceeding $\sqrt{n}$.*

Proof. We may write $n = ab$ where $1 < a \leq b < n$. We may also assume that $a \leq \sqrt{n}$ for otherwise $ab > n$. By Lemma 5.6 a has a prime divisor and the claim follows. ■

An immediate corollary of Lemma 4.37 is the following.

Corollary 5.8 *If p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$.*

Proof. If $p \mid a$ we are done, so assume that $p \nmid a$ implying that $(p, a) = 1$ (indeed, as p is prime $(p, a) \in \{1, p\}$; having $p \nmid a$ implies that $(p, a) = 1$). The claim then follows by Lemma 4.37. ■

Note that Corollary 5.8 is unique to prime numbers. For instance $4 \cdot 6 = 24$ and $12 \mid 4 \cdot 6$. However, $12 \nmid 4$ and $12 \nmid 6$. Corollary 5.8 extends to products of more than two integers.

Corollary 5.9 *If a prime p satisfies $p \mid a_1 \cdots a_n$, where a_i is a positive integer for every $i \in [n]$, then there exists a $j \in [n]$ such that $p \mid a_j$.*

Proof. The proof is by induction on n. For $n = 1$ the claim is trivial (Corollary 5.8 handles $n = 2$) . Suppose then that the claim is true for $n \geq 1$ and consider a product of $n + 1$ numbers $a_1 \cdots a_n a_{n+1}$ that is divisible by p. Either $p \mid a_1 \cdot a_2 \cdots a_n$ or $p \nmid a_1 \cdot a_2 \cdots a_n$. In the former case the claim follows by the induction hypothesis. In the latter case $p \mid a_{n+1}$ by Corollary 5.8. ■

Taking all of the a_i, $i \in [n]$, to be prime in Corollary 5.9 yields the following.

Corollary 5.10 *Let $p, q_1, \ldots, q_n$ be prime. If $p \mid q_1 \cdot q_2 \cdots q_n$, then there exists a $k \in [n]$ such that $p = q_k$.*

We are now in a position to prove Theorem 5.2.

Proof of Theorem 5.2. The argument consists of two parts. First we will show that for every positive integer there exists at least one way to express the number as a product of primes. Second, we will show that this expression is in fact unique.

Existence. Assume towards a contradiction that the claim is false and that there are positive integers that cannot be written as a product of primes. Let n be the least[1] integer amongst these counter examples (which are all positive integers). We now analyse this counter example n. Surely, n is not a prime or n is not a counter example to the statement. We may assume that n is composite then and thus may write $n = ab$ for some integers $2 \leq a, b < n$. Each of a and b do not constitute a counter example to the statement, by the choice of n. Hence, both a and b can be expressed as a product of primes and consequently n as well; a contradiction.

Uniqueness. Suppose that there exists an integer n for which two factorisations exist; that is

$$n = p_1 \cdots p_s = q_1 \cdots q_\ell.$$

Amongst all numbers with at least two representations choose n such that its two representations share no common elements (put another way, reduce common primes in the original representations). Then $p_1 \mid q_1 \cdots q_\ell$ (as $p_1 \cdot (p_2 \cdots p_s) = q_1 \cdots q_\ell$), and consequently there exists a $j \in [\ell]$ such that $p_1 = q_j$, by Corollary 5.10; contradiction. ■

[1] Here we appeal to the WOP.

5.1.1 *Inductive proof of the fundamental theorem of arithmetics*

In the proof of Existence we used the proof technique of minimal counter example. We mentioned before that this is just another way to do induction. Let us translate this proof to the induction framework.

Proposition 5.11 *Every integer $n > 1$ is either prime or can be written as a product of primes.*

Proof. The proof is by induction on n. The claim is true for $n = 2$. Assume the claim holds true for all integers $< n$. If n is prime we are done. Suppose then that n is composite, that is $n = ab$ for some two integers $2 \leq a, b < n$. By the induction hypothesis both a and b are either primes or can be written as a product of primes. The claim follows. ■

Next we give an alternative proof of Theorem 5.2 using induction as follows.

Proof of Theorem 5.2 (Alternative proof). The proof is by induction on n. For $n = 2$ the claim holds. Assume then that the claim is true for all integers $1 < k < n$. We may assume that n is composite and that n can be written as a product of primes, by Proposition 5.11. It remains to prove the uniqueness of the factorisation for n. Assume towards a contradiction that n has two distinct prime factorisations, that is

$$n = p_1 \cdots p_s = q_1 \cdots q_t.$$

We show that $s = t$ and that these two factorisations are comprised of the same primes appearing the same number of times.

As $p_1 \cdot (p_2 \cdots p_s) = q_1 \cdots q_t$ we have that $p_1 \mid q_1 \cdots q_t$. Then, by Corollary 5.9, there exists a q_j satisfying $p_1 = q_j$. Without loss of generality we may assume that $j = 1$. Cancelling $p_1 = q_1$ on both sides we obtain

$$\frac{n}{p_1} = p_2 \cdots p_s = q_2 \cdots q_t$$

As n is composite we have that $s > 1$ (and $t > 1$ as well) and thus $1 < n/p_1 < n$. The induction hypothesis for n/p_1 asserts that this number has a unique prime factorisation. Therefore $s = t$ and the factorisation of n is unique. ■

5.1.2 *Applications*

Message: $d \mid n$ if and only if:

1. the prime factors of d are amongst the prime factors of n.
2. Every prime factor of d that is also a prime factor of n has its power in the factorisation of d bounded by its power in the factorisation of n.

Example 5.12 List all divisors of 120. We start of by finding the prime factorisation of 120. Here we have that $120 = 2^3 \cdot 3 \cdot 5$. The number 1 we list automatically. To produce all the others we go over all options to choose prime factors from this factorisation where 2 can be chosen at most 3 times in each combination. We leave the details to the reader.

Proposition 5.13 *The set of divisors of* $n = \prod_{i=1}^{r} p_i^{a_i}$ *is given by*

$$\left\{ \prod_{i=1}^{r} p_i^{c_i} : 0 \leq c_i \leq a_i \right\}.$$

Example 5.14 We can use prime factorisation to find the gcd of numbers. For instance, what is $(720, 2100)$? First let us note that $720 = 2^4 \cdot 3^2 \cdot 5$ and that $2100 = 2^2 \cdot 3 \cdot 5^2 \cdot 7$. Recall the Message we had above. Any common divisor of 720 and 2100 will be comprised of prime factors that are common to both these numbers. We get the gcd if we pick as many common factors as we can. Here the common prime factors are $2, 3, 5$. Then $(720, 2100) = 2^2 \cdot 3 \cdot 5$.

Let us make this last example more general.

Proposition 5.15 *Let* a *and* b *be positive integers with factorisations*

$$a = p_1^{a_1} \cdots p_n^{a_n} \text{ and } a = p_1^{b_1} \cdots p_n^{b_n},$$

then

$$(a, b) = p_1^{\min\{a_1, b_1\}} \cdots p_n^{\min\{a_n, b_n\}} \tag{5.16}$$

5.1.2.1 $\sqrt{p}$ is irrational

In this section we use the fundamental theorem of arithmetics to provide yet another proof to the fact that$\sqrt{2}$ is irrational.

Theorem 5.17 $\sqrt{2}$ *is irrational.*

Proof. Suppose, to the contrary, that $\sqrt{2}$ is rational, say, $\sqrt{2} = a/b$, where a and b are both integers with $gcd(a, b) = 1$. Squaring, we get $a^2 = 2b^2$, so that $b \mid a^2$. If $b > 1$, then the Fundamental Theorem of Arithmetic guarantees the existence of a prime p such that $p \mid b$. It follows that $p \mid a^2$ and by theorem "if p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$" , that is $p \mid a$. Hence, $gcd(a, b) \geq p$. We therefore arrive at a contradiction unless $b = 1$. But if this is the case, then $a^2 = 2$, which is impossible when a is a integer. Therefore, our assumption upon which $\sqrt{2}$ is a rational is not tenable. ■

The integer 2 is by no means special in this respect as the following suggests.

Theorem 5.18 $\sqrt{p}$ *is irrational for every prime* p.

Proof. Suppose, to the contrary, that $\sqrt{p}$ is a rational number. Then there exist $a, b \in \mathbb{Z}$ with $b \neq 0$ such that $\sqrt{p} = a/b$. Without loss of generality, we may assume that $(a, b) = 1$. Then $p^2 = a^2/b^2$, or equivalently $a^2 = pb^2$, implying $p \mid a^2$ so that $p \mid a$. Hence, there exists $k \in \mathbb{Z}$ such that $a = pk$. If so $a^2 = p^2k^2 = pb^2$ so that $pk^2 = b^2$ implying $p \mid b^2$ and then $p \mid b$. It now follows that p is a common divisor of a and b contradiction to the assumption that $(a, b) = 1$. ■

5.1.2.2 The lcm of multiple pairwise co-prime numbers

Let us be reminded of Lemma 4.76 asserting that if $a_1, \ldots, a_n$ be pairwise co-prime Then

$$lcm(a_1, \ldots, a_n) = a_1 \cdot a_2 \cdots a_n. \tag{5.19}$$

In this section we prove this result. We require some preparation.

For a positive integer a let

$$\mathcal{D}_a = \{n \in \mathbb{Z}^+ : a \mid n\},$$

that is $\mathcal{D}_a$ consist of all numbers divisible by a.

Lemma 5.20 *Let a and b be two positive integers.*

$$\mathcal{D}_a = \mathcal{D}_b \text{ if and only if } a = b.$$

Proof. We consider only the non-trivial direction, that is that if $\mathcal{D}_a = \mathcal{D}_b$ then $a = b$. Assume towards contradiction that the premise of this direction hold yet $a \neq b$ and assume without loss of generality that $a < b$. Surely $a \in \mathcal{D}_a$ and $a \notin \mathcal{D}_b$; contradiction. ■

Lemma 5.21 $lcm(a_1, \ldots, a_n) = lcm(lcm(a_1, \ldots, a_{n-1}), a_n)$.

Proof. Let $\alpha = lcm(a_1, \ldots, a_n)$ and let $\beta = lcm(lcm(a_1, \ldots, a_{n-1}), a_n)$. We show that $\mathcal{D}_\alpha = \mathcal{D}_\beta$ so that $\alpha = \beta$ by Lemma 5.20. Let $m \in \mathcal{D}_\alpha$. Then $\alpha \mid m$ and as $a_i \mid \alpha$ it follows that $a_i \mid m$ for every $i \in [n]$. Then $\gamma = lcm(a_1, \ldots, a_{n-1}) \mid m$ and $a_n \mid m$ implying that $\beta \mid m$. This then shows that $\mathcal{D}_\alpha \subseteq \mathcal{D}_\beta$. Conversely, let $m \in \mathcal{D}_\beta$ so that $\beta \mid m$. This in turn implies that $a_n \mid m$ and that $\gamma \mid m$. The latter also implies that $a_i \mid m$ for every $i \in [n-1]$. It now follows that $a_i \mid m$ for every $i \in [n]$ so that $\alpha \mid m$ and thus $m \in \mathcal{D}_\alpha$. We have thus shown that $\mathcal{D}_\beta \subseteq \mathcal{D}_\alpha$ and the claim follows. ■

We are now in position to prove Lemma 4.76.

Proof of Lemma 4.76. The proof is by induction on n. The holds true for $n = 2$, by (4.74). Assume then that the claim holds true for $n \geq 2$ and consider the claim for $n + 1$. By Lemma 5.21 we have that

$$lcm(a_1, \ldots, a_n, a_{n+1}) = lcm(lcm(a_1, \ldots, a_n), a_{n+1}).$$

By the induction hypothesis

$$lcm(a_1, \ldots, a_n) = a_1 \cdot a_2 \cdots a_n.$$

As, by assumption, none of the a_i's share any common prime factors it follows that

$$(a_1 \cdot a_2 \cdots a_n, a_{n+1}) = 1.$$

Then by (4.74)

$$lcm(a_1, \ldots, a_n) = a_1 \cdot a_2 \cdots a_n \cdot a_{n+1}.$$

■

We record the following for future use.

Corollary 5.22 *Let $n_1, \ldots, n_r$ be pairwise relatively prime and let m be an integer such that $n_i \mid m$ for every $i \in [r]$. Then $n_1 \cdot n_2 \cdots n_r \mid m$.*

§5.2. Infinitude of primes

For the infinitude of $\mathbb{N}$ we had two responses. The first was to appeal to the axiom of infinity (asserting that infinite sets exist). The second more rigorous approach can be seen in § 2.2.6. In this section we consider the question regarding the infinitude of primes.

5.2.1 *Euclid's proof*

Perhaps the most known proof that this set is infinite is that of Euclid presented next.

Theorem 5.23 (Euclid)
There are infinitely many primes.

Proof. Assume towards a contradiction that there are finitely many primes. Let $p_1, \ldots, p_n$ denote these primes. Put

$$Q := p_1 p_2 \cdots p_n + 1.$$

By Lemma 5.6 the number Q has at least one prime divisor, namely q. We show that q is not amongst the primes $p_1, \ldots, p_n$ and thus attain a contradiction. Suppose that $q = p_j$ for some $j \in [n]$. Then $q \mid Q - p_1 p_2 \cdots p_n$. As $Q - p_1 p_2 \cdots p_n = 1$ this implies that $q \mid 1$ which is impossible as $q \geq 2$. It follows that $q \neq p_j$ for every $j \in [n]$; contradiction. ■

Remarks.

1. The proof above uses Lemma 5.6 to deduce the existence of q. We could in fact have used Theorem 5.2 to that end. Notice that Lemma 5.6 is much more naive than Theorem 5.2.

2. The proof we have seen here discovers a new prime q. The proof however does not reveal a *method* to finding q. It just shows it exists. In math we distinguish between *non-constructive* or *existential* proofs (like the one we have here) and *constructive* proofs.

5.2.2 *The Hardy-Wright argument*

Let us prepare for yet another proof of the infinitude of primes. The following notion assumes a key rôle in this new approach.

Definition 5.24 *An integer is said to be square-free if it is divisible by no square of any prime.*

The factorisation of any square-free number m has the form $m = p_{i_1} p_{i_2} \cdots p_{i_k}$. If all these factors of m are $\leq p_j$ (i.e., the jth prime) for some j then we can write

$$m = 2^{b_1} 3^{b_2} \cdots p_j^{b_j}$$

where each $b_i \in \{0, 1\}$. Any integer n can be expressed as

$$n = n_1^2 m$$

with $n \in \mathbb{Z}$ and m square-free.

Definition 5.25 *For a integers $x, j > 0$ let*

$$N(x,j) := \{n \in \mathbb{Z}^+ : n \leq x \text{ and } p \not| n, \ \forall \text{ primes } p > p_j\}.$$

An upper bound for $|N(x,j)|$ is as follows.

Lemma 5.26 *Let $x, j > 0$ be integers. Then $|N(x,j)| \leq 2^j\sqrt{x}$.*

Proof. Any integer $n \in N(x,j)$ has the form $n = n_1^2 m$ with m being square-free so that $m = 2^{b_1}3^{b_2}\cdots p_j^{b_j}$, where each $b_i \in \{0,1\}$, as $p \not| n$ for all primes $p > p_j$. An upper bound for $|N(x,j)|$ follows from the number of ways to choose m times the number of ways to choose n_1. There are $\leq 2^j$ way to construct m. Next as $n_1 \leq \sqrt{n} \leq \sqrt{x}$ there are $\leq \sqrt{x}$ ways to choose n_1. Hence $|N(x,j)| \leq 2^j\sqrt{x}$. ■

Let us now give an alternative proof for the infinitude of primes.

Proof of Theorem 5.23. Assume for the sake of contradiction that there are only finitely many primes, namely $2, 3, \ldots, p_j$. Then trivially, $|N(x,j)| = x$ for every x. Then

$$x = |N(x,j)| \leq 2^j\sqrt{x}$$

by Lemma 5.26, implying that

$$x \leq 2^{2j}$$

for every x. The integer $2^{2j} + 1$ contradicts this. ■

5.2.3 *Fermat primes*

For $n \in \mathbb{N}$, set

$$\mathcal{F}_n := 2^{2^n} + 1.$$

Number of the form $\mathcal{F}_n$ are called *Fermat numbers*. The prime members this sequence are called *Fermat primes*. Fermat conjectured that numbers of the form $\mathcal{F}_n$ are all prime. And indeed, the first four elements in this sequence, namely,

$$\begin{aligned}
\mathcal{F}_1 &= 2^{2^1} + 1 = 5 \\
\mathcal{F}_2 &= 2^{2^2} + 1 = 17 \\
\mathcal{F}_3 &= 2^{2^3} + 1 = 257 \\
\mathcal{F}_4 &= 2^{2^4} + 1 = 65537
\end{aligned}$$

are all prime. The fifth element in this sequence is

$$\mathcal{F}_5 = 2^{2^5} + 1 = 4294967297.$$

It was Euler, who in 1732 unveiled that $\mathcal{F}_5$ is composite; indeed $\mathcal{F}_5 = 641 \cdot 6700417$ holds. Hardy and Wright report of the following argument by Coxeter for establishing this fact. Coxeter's starting point was the observation that

$$641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$$

and with this could trivially write

$$641 | 2^{28}(5^4 + 2^4) = 5^4 \cdot 2^{28} + 2^{32}.$$

This 'strange' choice of numbers is motivated by a special case of Exercise 22 asserting that $x+1\big|x^4-1$. More explicitly, take $x=5\cdot 2^7$ as to attain

$$641=\underbrace{5\cdot 2^7}_{x}+1\Big|\underbrace{(5\cdot 2^7)^4}_{x^4}-1.$$

Then,

$$641\big|(5^4\cdot 2^{28}+2^{32})-\big((5\cdot 2^7)^4-1\big)=2^{32}+1=2^{2^5}+1=\mathcal{F}_5.$$

In 1880, Landry proved that $\mathcal{F}_6$ is composite. Later it was discovered that $\mathcal{F}_n$ is composite for $7\le n\le 16$ and also for

$$n=18,19,21,23,36,38,39,55,63,73.$$

As far as we know, at the time of writing these notes, no prime beyond $\mathcal{F}_4$ has been found.

Conjecture 5.27
The number of Fermat primes is finite.

One of the main results of this section is an alternative proof establishing the infinitude of primes employing Fermat primes. The core observation propelling the latter reads as follows.

Lemma 5.28 *Any two distinct Fermat numbers are coprime.*

Proof. For suppose that $\mathcal{F}_n$ and $\mathcal{F}_{n+k}$, $k\ge 1$, are such that there exists an m such that

$$m\big|\mathcal{F}_n \text{ and } m\big|\mathcal{F}_{n+k}.$$

With Exercise 22 on our mind, we write

$$\frac{\mathcal{F}_{n+k}-2}{\mathcal{F}_n}=\frac{2^{2^{n+k}}+1-2}{2^{2^n}+1}=\frac{2^{2^{n+k}}-1}{2^{2^n}+1}=\frac{\left(2^{2^n}\right)^{2^k}-1}{2^{2^n}+1}.$$

Setting $x=2^{2^n}$ in Exercise 22 we arrive that the last expression has the form $\frac{x^{2^k}-1}{x+1}$ and from that exercise it is known that $x+1\big|x^{2^k}-1$. Consequently, we may write $\mathcal{F}_n\big|\mathcal{F}_{n+k}-2$.

Then $m\big|\mathcal{F}_n\big|\mathcal{F}_{n+k}-2$ as well as $m\big|\mathcal{F}_{n+k}$. It follows that $m\big|2$ mandating that $m=2$. This, however, is a contradiction as all Fermat numbers are odd. ■

We are now ready to give an alternative proof of Theorem 5.23 asserting that there are infinitely many primes.

Proof of Theorem 5.23. By Lemma 5.28, the members of the sequence $(\mathcal{F}_n)_{n\in\mathbb{N}}$ are pairwise coprime; i.e., each has a unique (odd) prime factor not appearing in any other member. The claim follows. ■

5.2.4 *Mersenne primes*

If Conjecture 5.27 is true, then the number of primes of the form 2^n+1 is finite as well.

Proposition 5.29 *Let $a\ge 2$. If a^n+1 is prime, then a is even and n is a power of two.*

PROOF. If a is odd, then, $a^n + 1$ is even and $a \geq 2$ then implies that $a^n + 1$ is not prime negating the premise. This establishes the first part of the proposition. To see that the second part holds, suppose n has an odd prime factor $k \geq 3$ and write $n = k\ell$. Polynomial long division coupled with $k \geq 3$ yield that

$$\frac{a^{k\ell} + 1}{a^\ell + 1} = a^{(k-1)\ell} - a^{(k-2)\ell} + \cdots + 1;$$

note that for $k = 2$ this division fails. Then, for $k \geq 3$, $a^\ell + 1 \big| a^{k\ell} + 1$ implying that $a^{k\ell} + 1$ is not a prime contradicting the premise. ■

COROLLARY 5.30 *Any prime number of the form $2^k + 1$ is a Fermat prime.*

If Conjecture 5.27, then Corollary 5.30 asserts that all primes of the form $2^k + 1$ (which must be Fermat primes) form a finite set.

Numbers of the form $2^n - 1$ are called *Mersenne numbers* and *Mersenne primes* if these are prime. It is known that not all Mersenne numbers are primes and we forgo the rather long history of the pursuit of Mersenne primes.

CONJECTURE 5.31
There are infinitely many Mersenne primes.

Perhaps the most known result regarding Mersenne numbers is that of Mersenne himself.

THEOREM 5.32 (Mersenne) *Let $a, n \in \mathbb{N}$. If $a^n - 1$ is prime then $a = 2$ and n is prime. In particular if a Mersenne number $2^n - 1$ is prime, then n is prime.*

PROOF. If $a \geq 3$, then $a - 1 \big| a^n - 1$; primality of $a^n - 1$ mandates that $a = 2$ then. If $n = k\ell$ is composite with $2 \leq k, \ell < n$, then $2^k - 1 \big| 2^n - 1$; a contradiction with the assumption that $a^n - 1$ is prime. It follows that if $2^n - 1$ is prime then n is prime. ■

The infinitude of primes can also be established using Mersenne numbers. The driving observation in this derivation would be that for Mersenne numbers we have

$$(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1$$

which follows from Lemma 4.51.

PROOF OF THEOREM 5.23. Let $P := \{p_1 = 2, \ldots, p_n\}$ be a finite set of primes. Then, owing to Lemma 4.51,

$$(2^{p_1} - 1, 2^{p_j} - 1) = 2^{(p_1, p_j)} - 1 = 1$$

holds. For each $i \in [n]$, $2^{p_i} - 1$ is odd and hence does not have 2 as a factor. It follows that the numbers $2^{p_1} - 1, \ldots, 2^{p_n} - 1$ are pairwise coprime and thus collectively induce a set of n distinct odd primes. As P contains only $n - 1$ odd primes, it follows that there is a prime not in P. ■

5.2.4.1 Perfect numbers

DEFINITION 5.33 *A natural number is said to be* perfect *if it coincides with the sum of its proper divisors. That is, n is perfect if*

$$n = \sum_{d|n, d \geq 1, d \neq n} d$$

Example 5.34

$$6 = 1 + 2 + 3$$
$$28 = 1 + 2 + 4 + 7 + 14.$$

Both 6 and 28 are perfect numbers.

For an integer n, we write $\sigma(n)$ to denote the sum of its positive divisors,

$$\sigma(n) := \sum_{d|n, d\geq 1} .$$

Observation 5.35. *n is perfect if and only if $\sigma(n) = 2n$.*

Theorem 5.36 (Euclid) *If $2^m - 1$ is (a Mersenne) prime, then $2^{m-1}(2^m - 1)$ is perfect.*

Proof. Let $q := 2^m - 1$; recall that we assume q is prime. The factorisation of n has the concise form $2^{m-1}q$; of which all divisors of n can be read off. Then,

$$\begin{aligned}\sigma(n) &= 1 + 2 + \cdots + 2^{m-1} + q + 2q + \cdots + 2^{m-1}q \\ &= (q+1)\underbrace{(1 + 2 + \cdots + 2^{m-1})}_{=2^m-1=q} \\ &= 2^m q \\ &= 2(2^{m-1}q) \\ &= 2n.\end{aligned}$$

The claim follows. ■

Theorem 5.36 is due to Euclid and indeed numbers of the form $2^{m-1}(2^m - 1)$ with $2^m - 1$ prime are called *Euclid numbers*. Euclid in fact proved that for every Mersenne prime there is a corresponding a perfect number. On the other hand, if $n = 2^k u$ is perfect, then

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

yielding $u = 2^{k+1} - 1$. This means that for any perfect number of the form $2^k u$ there is a corresponding Mersenne prime. Much more can be said as the next result of Euler suggests.

Theorem 5.37 (Euler) *If $n \geq 2$ is perfect and even, then $n = 2^{m-1}(2^m - 1)$ and $2^m - 1$ is (a Mersenne) prime.*

Proof. Let n be perfect. We may write $n = 2^t u$ with u odd. The divisors of n have the form $2^s m$ where $0 \leq s \leq t$ and $m \mid u$. For a fixed s, the contribution of the divisors of u to the sum $\sigma(n)$ is $2^s\sigma(u)$. Consequently,

$$\sigma(n) = (1 + 2 + \cdots + 2^t)\sigma(u) = (2^{t+1} - 1)\sigma(u). \tag{5.38}$$

Owing to n being perfect we have $\sigma(n) = 2n$ yielding

$$2^{t+1}u = (2^{t+1} - 1)\sigma(u). \tag{5.39}$$

Noting that, being consecutive, $2^{t+1}-1$ and 2^{t+1} are coprime; we appeal to Euclid's lemma, namely Lemma 4.37 as follows. As $2^{t+1}\big|(2^{t+1}-1)\sigma(u)$ it follows that $2^{t+1}\big|\sigma(u)$, by Lemma 4.37. In a similar manner, we have that $2^{t+1}-1\big|2^{t+1}u$ implying, again via Lemma 4.37, that $(2^{t+1}-1)\big|u$. This allows us to write

$$u=(2^{t+1}-1)k \text{ and } \sigma(u)=2^{t+1}k'$$

for some integers k and k'. However, we may insist that k and k' coincide. To see this, rewrite (5.39) as

$$\frac{u}{\sigma(u)}=\frac{2^{t+1}-1}{2^{t+1}};$$

and then upon substitution attain

$$\frac{(2^{t+1}-1)k}{2^{t+1}k'}=\frac{2^{t+1}-1}{2^{t+1}}.$$

This equality coupled with the fact that the fraction on the r.h.s. is in lowest terms (i.e., $(2^{t+1},2^{t+1}-1)=1$) mandates that $k=k'$. Hence, we may now write that

$$u=(2^{t+1}-1)c \text{ and } \sigma(u)=2^{t+1}c \tag{5.40}$$

for some integer c.

If $c>1$, then $u,c,1$ are distinct divisors of u. In which case we may write

$$\sigma(u)\geq u+c+1=(2^{t+1}-1)c+c+1=2^{t+1}c+1>2^{t+1}c=\sigma(u);$$

a contradiction. We may assume that $c=1$. In which case, $n=2^tu=2^t(2^{t+1}-1)$, by definition and (5.40), yielding the desired form for n.

It remains to prove that subject to $c=1$, that $2^{t+1}-1$ is (a Mersenne) prime. For suppose this is not the case so that $2^{t+1}-1$ admits divisors other than 1 and itself. Then,

$$\sigma(2^{t+1}-1)\geq(2^{t+1}-1)+d+1>2^{t+1},$$

where here d is any divisor of $2^{t+1}-1$ not coinciding with 1 or $2^{t+1}-1$; such a d is now assumed to exist. Recall however that for $c=1$, we have $u=2^{t+1}-1$ and consequently $\sigma(2^{t+1}-1)=2^{t+1}$, by (5.40). This is a contradiction completing the proof. ■

§5.3. The sieve of Eratosthenes

Given an integer n consider the process of listing all integers 2 to n and then for each prime $p\leq\sqrt{n}$ erasing all multiples of p from the list, i.e., delete $2p,3p,4p,\ldots$ and so on. The remaining integers - i.e., those who did not fall through the *sieve* - are all prime. Such is the *sieve of Eratosthenes*.

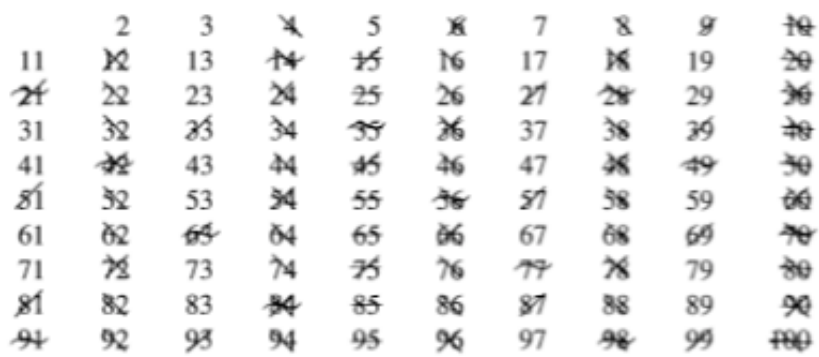


Figure 5.1: Finding all primes ≤ 100 using the sieve of Eratosthenes.

Example 5.41 Figure 5.1 shows that $\pi(100) = 25$.

We can mimic the list mentioned above using an array $A[2 \cdots n]$ of boolean variables and implement the sieve of Eratosthenes as follows.

SIEVE(n):

1. for $k = 2$ to n do: $A[k] = 1$.
2. MAIN LOOP: for $k = 2$ to $\lfloor \sqrt{n} \rfloor$ do:
   (a) if $A[k] = 1$ then:
      i. $i = 2k$.
      ii. while $i \leq n$ do:
         A. $A[i] = 0$
         B. $i = i + k$.

Theorem 5.42 *When the algorithm finishes, $A[k] = 1$ if and only if k is prime.*

Theorem 5.42 stems directly from the following loop invariant.

Lemma 5.43 *For each $k \in [2, \lfloor \sqrt{n} \rfloor + 1]$ we have that at the beginning of the kth iteration of the MAIN LOOP $A[i] = 0$ holds for $i \in [2, n]$ if and only if there exists a prime $p < k$ dividing i.*

Proof. The proof is by induction on k. For $k = 2$ the claim holds trivially; indeed at the beginning of the first iteration $A[i] = 1$ for all $i \in [2, n]$ and indeed there are no primes less than 2 dividing any such i.

Consider $k + 1$ and assume the claim holds for all $2 \leq j < k + 1$. Fix $i \in [2, n]$. Suppose first that $A[i] = 0$ at the beginning of the $(k + 1)$st iteration. Then either $A[i]$ was zero at the beginning of the kth iteration already or it was zeroed during the kth iteration. If the former holds then i is divisible by a prime less than k by the induction hypothesis and thus divisible by a prime less than $k + 1$ and the claim in this direction follows in this case. In the latter case, that $A[i]$ is zeroed during the kth iteration, it means that i is divisible by k and that $A[k] = 1$ at the beginning of the kth iteration and thus not divisible by any prime less than k by the induction hypothesis and hence k is prime. It again follows that i is divisible by a prime less than $k + 1$.

Suppose, second, that i is divisible by a prime less than $k + 1$. Let p be such a prime. Then at the beginning of the pth iteration $A[p] = 1$ by the induction hypothesis. During the pth iteration $A[i]$ is zeroed. ■

We proceed to analysing the running time of the sieve of Eratosthenes. We immediately see that counting bit operations here is a bit tedious. We use this algorithm to introduce yet another convention in computer science where we assume all arithmetic operations require $O(1)$ time and instead of counting bit operations we count the number of basic arithmetic operations instead and thus avoid the tedious bit counting. Naturally, given the number of elementary arithmetic operations retrieving the number of bit operations is straightforward.

The inner (while) loop of the algorithm makes $O(n/k)$ steps in order to clear the entries of A indexed by multiples of k. One estimate here would be to bound the total number of steps performed by the main loop would be $O(n \cdot \sum_{k \leq \sqrt{n}} 1/k)$. Approximating the sum by an integral[2] we have

$$\sum_{k=1}^{\sqrt{n}} 1/k = \int_1^{\sqrt{n}} \frac{\mathrm{d}\, y}{y} + O(1) \asymp \log n.$$

[2]Recall the techniques of § **??**; though here we need a tool not mentioned in these notes.

This brings the running time to $O(n \log n)$. This is clearly an exponential running time estimate.

This running time analysis is rather crude. In particular, the inner (while) loop is executed only for prime values of k. This means that the running time can in fact be bounded by $O(n \sum_{p \leq \sqrt{n}} 1/p)$.

$$\sum_{p \leq \sqrt{n}} 1/p = \log \log \sqrt{n} + O(1) = O(\log \log n),$$

by Theorem 17.16. This yields a running time of $O(n \log \log n)$ for the sieve of Eratosthenes. This is an exponential improvement over our previous estimate; however this too gives an exponential running time for the algorithm.

Another limitation of the sieve of Eratosthenes is that it requires enormous amounts of space. Indeed, it requires space exponential in the binary representation of n. This severely limits the range of numbers we can apply this algorithm to (let alone the exponential running time we have here).

§5.4. Early observations pertaining to the distribution of primes

For $n \in \mathbb{N}$ let p_n denote the nth prime number. For $x \in \mathbb{R}$ let $\pi(x) := \sum_{p \leq x} 1$ denote the number of primes $\leq x$. In this section we develop estimates for p_n and $\pi(x)$. Our first result comes from Euclid's proof of Theorem 5.23. There we established that the number $p_1 \cdot p_2 \cdots p_n + 1$ has at least one prime divisor that is not amongst $\{p_1, \ldots, p_n\}$. If there are several then p_{n+1} cannot exceed the least of these.

Proposition 5.44 *For every $n \geq 1$*

$$p_{n+1} < p_1 \cdot p_2 \cdots p_n + 1$$

holds.

The estimate provided by Proposition 5.44 is rather crude as can be seen here:

$$p_5 = 11 \leq 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 210.$$

A better estimate is that of Bonse.

Theorem 5.45 (Bonse)

$$p_{n+1}^2 < p_1 \cdot p_2 \cdots p_n, \text{ whenever } n \geq 5.$$

We omit the proof of Bonse's result. Suffices to note that

$$p_5 = 11 < \sqrt{2 \cdot 3 \cdot 5 \cdot 7} = \sqrt{210} \approx 14.491.$$

A fairly trivial estimates for p_n arises from Fermat numbers and in particular Lemma 5.28. For any $n \in \mathbb{N}$, each of the numbers $\mathcal{F}_1, \ldots, \mathcal{F}_n$ has its own unique odd prime factor not shared with any other. Hence, there are at least n odd primes not exceeding $\mathcal{F}_n$ for every $n \in \mathbb{N}$. Consequently, we attain the bound

$$p_n < \mathcal{F}_n = 2^{2^n} + 1.$$

A rudimentary inductive arguments produces this bound as well.

Theorem 5.46 $p_n \leq 2^{2^n}$.

Proof. The proof is by induction on n. For $n = 1$ the claim is trivial. Let then $n > 1$ and assume the claim holds true for all integers $\leq n$. We prove the claim for $n + 1$. By Proposition 5.44 we have that

$$p_{n+1} < p_1 \cdot p_2 \cdots p_n + 1.$$

Applying the induction hypothesis to each p_i we arrive at

$$\begin{aligned} &\leq 2 \cdot 2^2 \cdots 2^{2^n} + 1 \\ &= 2^{1+2+2^2+\cdots+2^n} + 1. \end{aligned}$$

In the induction lecture we proved that $\sum_{i=1}^{k} 2^i \leq 2^{k+1}$, for every $k \geq 1$. In fact, one can prove (by induction) that $\sum_{i=1}^{k} 2^i \leq 2^{k+1} - 1$. Applying this inequality to the exponent here we arrive at

$$\begin{aligned} &\leq 2^{2^{n+1}-1} + 1 \\ &\leq 2 \cdot 2^{2^{n+1}-1} \\ &= 2^{2^{n+1}}. \end{aligned}$$

■

Corollary 5.47 *For $n \geq 1$ there are at least $n + 1$ primes less than 2^{2^n}.*

Proof. By Theorem 5.46 the primes $p_1, p_2 \ldots, p_{n+1}$ all do not exceed 2^{2^n}. ■

Corollary 5.48 $\pi(x) = \Omega(\log \log x)$.

Proof. Let us consider $\mathbb{R}$ in intervals of $[2^{2^n}, 2^{2^{n+1}}]$ and show that whenever we pick $x \in [2^{2^n}, 2^{2^{n+1}}$ then $\pi(x) \geq \log \log x$. Indeed, notice that

$$\pi(x) \geq \underbrace{\pi\left(2^{2^n}\right) \geq \pi(p_n)}_{\text{Theorem 5.46}} = n \geq \log \log x.$$

■

We can do much better than Theorem 5.46 using the so called *Bertrand's postulate*.

Theorem 5.49 (Bertrand's postulate)
For $n \geq 2$ the interval $(n, 2n)$ contains at least one prime. (In fact, $\pi(2n) - \pi(n) = \Omega(n/logn)$).

Bertrand conjectured Theorem 5.49 in 1845. It was then proved by Tchebycheff in 1852 and much later by Erdős who gave rise to the limerick: *Tchebycheff proved it, I proved it again; there is always a prime between $2n$ and n.*

A trivial conclusion of Bertrand's postulate is that

$$p_{n+1} < 2p_n,$$

which one should compare with, say, Bonse's result. We use Bertrand's postulate together with a mathematical induction to produce the following.

Corollary 5.50 *For $n \geq 2$ we have that $p_n < 2^n$.*

Proof. The proof is by induction on n. For $n = 2$ we have that $p_2 = 3 \leq 2^2$. Assume then that the claim holds for n, i.e., that $p_n < 2^n$. We prove the assertion for $n+1$. By Bertrand's postulate there exists a prime p satisfying $2^n < p < 2^{n+1}$. In particular, $p_n < p$, by the induction hypothesis. Consequently, $p_{n+1} < p$ as well and the first part of the claim follows. ■

Bertrand's postulate has given us a significant "boost"; we are now capable in giving an exponential improvement to Corollary 5.48 using Corollary 5.50

Corollary 5.51 $\pi(x) = \Omega(\log x)$.

Proof. We show that for every interval $[2^n, 2^{n+1}]$ it holds that whenever x is taken from such an interval $\pi(x) \geq \log x$ holds.

$$\pi(x) \geq \underbrace{\pi\left(2^n\right) \geq \pi(p_n)}_{\text{Corollary 5.50}} = n \geq \log x.$$

■

§5.5. Primes in arithmetic progressions

We have seen that there are infinitely many primes of which only 2 is even the rest are clearly odd. The odd integers are of the form $4n+1$ or $4n+3$. The infinitude of primes does not imply directly that we have infinitely many primes of the form $4n+1$ and of the form $4n+3$; it only implies that at least one of these forms sees infinitely many primes. Could it be for instance that there are infinitely many primes of the form $4n+1$ and only finitely many of the form $4n+3$? Perhaps the other way around? In this section we answer these questions. We start with an observation.

Observation 5.52. *The product of two numbers of the form $4k+1$ is also of the form $4k+1$.*

Proof.

$$\begin{aligned}(4n+1)(4m+1) &= 16mn + 4n + 4m + 1 \\ &= 4 \cdot 4mn + 4(m+n) + 1 \\ &= 4 \cdot \underbrace{(4 \cdot mn + m + n)}_{\text{Integer}} + 1\end{aligned}$$

■

Proposition 5.53 *There are infinitely many primes of the form $4n+3$.*

Prior to proving Proposition 5.53 let us consider the following failed attempt to prove this proposition. Assume towards a contradiction that there are only finitely many primes of the form $4n+3$ and let p be the largest such prime. Put

$$N := 4 \cdot (3 \cdot 7 \cdots p) + 3,$$

where $3 \cdot 7 \cdots p$ contains all primes of the form $4n+3$ (which we now assume a finite number of them). The advantage of such a definition is that N cannot be prime as it has the form $4n+3$ (and we have used all other such primes to define N in particular $N > p$). By Lemma 5.6 N has a prime divisor q. We wish to say that q is of the form $4n+3$ in order to replicate our argument from Theorem 5.23 in that q is not amongst the list of primes of this form that we assumed is finite.

Other than the prime 2 all primes are odd and consequently of the form $4n+1$ or of the form $4n+3$. As N is odd $2 \nmid N$. In addition, it cannot be that all prime factors of N are of the form $4n+1$, by Observation 5.52. It follows then that N has a prime factor q of the form $4n+3$. At this point we would have liked to reach a contradiction but we fail. Indeed, q could be equal to 3. This attempt failed but we are not far.

Let us try yet again to prove Proposition 5.53. Assume towards a contradiction that there are only finitely many primes of the form $4n+3$. Let S denote the (finite) set of such primes and let p be the largest prime in S. Put

$$N := 4 \cdot (3 \cdot 7 \cdots p - 1) + 3,$$

where $3 \cdot 7 \cdots p$ contains all primes of the form $4n+3$. As in the previous attempt N cannot be prime and it must have a prime divisor of the form $4n+3$. We wish to argue that $q \notin S$ but it seems we are stuck; in particular the "trick" we used in Euclid's result (i.e., Theorem 5.23) does not seem applicable here. So at this point it is not clear how to continue. This does not mean that this approach cannot lead to a proof it just means that our choice of N makes it difficult to see how to end it gracefully.

At this point we make the following observation

$$\{4n-1 : n \in \mathbb{Z}\} = \{4n+3 : n \in \mathbb{Z}\}.$$

So instead of proving Proposition 5.53 we could instead prove the following.

Proposition 5.54 *There are infinitely many primes of the form $4n-1$.*

Proof. Assume towards a contradiction that there are only finitely many primes of the form $4n-1$. Let S denote the (finite) set of such primes and let p be the largest prime in S. Put

$$N := 4 \cdot (3 \cdot 7 \cdots p) - 1,$$

where $3 \cdot 7 \cdots p$ contains all primes of the form $4n-1$. Note that N cannot be prime as it has the form $4n-1$. It cannot be that all of its prime factors are of the form $4n+1$, by Observation 5.52, and as N is odd we have that $2 \nmid N$. It follows then that N has a prime factor q of the form $4n-1$. If $q \in S$ then $q \mid 3 \cdot 7 \cdots p$ implying that $q \mid N - 4 \cdot (3 \cdot 7 \cdots p)$. As $N - 4 \cdot (3 \cdot 7 \cdots p) = 1$ and $q \geq 3$ (recall that q is odd) this is impossible; contradiction. ■

Returning to our original question, we are still left with the problem of determining whether there are infinitely many primes of the form $4n+1$. While the proof of Proposition 5.53 was fairly easy, we are currently not equipped to prove the same assertion for $4n+1$.

Proposition 5.55 *There are infinitely many primes of the form $4n+1$.*

It was Dirichlet that proved the following seminal result. Proof of which lies beyond the scope of these notes.

Theorem 5.56 (Dirichlet's theorem)
If a and b are co-prime integers then the arithmetic progression $an+b$ contains infinitely many primes.

5.5.1 *Primes along polynomials*

The results we have encountered thus far, essentially all stem from a rather naïve question in which one seeks to find a 'simple' function f such that $f(n)$ is prime for all $n \in \mathbb{N}$. In § 5.2.3) and § 5.2.4 we have encountered proposals by Fermat and Mersenne, respectively, towards such a question. This ended with us having to mitigate our expectations somewhat severely by making do with having $f(n)$ be prime infinitely often. Dirichlet's theorem can also be cast in this light; Dirichlet's function is even simpler than those proposed by Fermat's and Mersenne; indeed, Dirichlet's function is polynomial and in fact linear having the form $an + b$. What sets Dirichlet's result apart from those of Fermat's and Mersenne's is that in this case we can also supply a justification for Dirichlet's result only supplying infinitely many prime of the form $an + b$ and proving that in this case an improvement is impossible.

Proposition 5.57 *No polynomial $f(n)$ with integral coefficients, not a constant, can be prime for all n, or for all sufficiently large n.*

Proof. W.l.o.g. the leading coefficient of $f(n)$ is positive so that $\lim_{n\to\infty} f(n) = \infty$ and $f(n) > 1$ for $n \geq n_0$ for some n_0. Let $x > n_0$ and write

$$f(x) = a_0 x^k + \cdots = y > 1.$$

Then,

$$y \big| f(ry + x) = a_0(ry + x)^k + \cdots$$

for every integral r. Moreover, $\lim_{r\to\infty} f(ry + x) = \infty$. Hence, there are infinitely many composite values of $f(n)$. ■

5.5.2 *The Tao-Green Theorem: progressions in the primes*

In the previous section we considered the presence of prime numbers along arithmetic progressions. The following result by Green and Tao establishes something even more astonishing.

Theorem 5.58 (Green-Tao theorem, abridged)
The primes contain arbitrarily long arithmetic progressions.

Let us make this last theorem precise. For $n \in \mathbb{Z}^+$, let $\mathcal{P}_n$ denote the first n prime numbers.

Theorem 5.59 (Green-Tao theorem, abridged)
For every integer $k \geq 3$ there exists an $n_0 = n_0(k)$ such that for all $n \geq n_0$ the set P_n contains a k-term arithmetic progression.

Theorem 5.59 is best possible in the sense that there cannot be an infinite arithmetic progression in the primes. For if there were, that would imply that the gap between every two consecutive primes is bounded by some constant. This is easily negated.

Theorem 5.60 *The gap between two consecutive primes can be arbitrarily large.*

Proof. We show that for every $n \in \mathbb{Z}^+$ there exist two consecutive primes separated by at least $n - 1$ consecutive composite numbers. Indeed, given n the numbers

$$n! + 2, n! + 3, \ldots, n! + n$$

is such an interval of composite numbers. ■

§5.6. Exercises

Exercise 1. Let $N \geq 1$ be an integer. Prove that the interval $[1, 2^N]$ contains at least N primes.

Exercise 2. Let $x \in \mathbb{R}$. Prove $\prod_{p \leq x} p < 4^x$.

Exercise 3. An integer n is said to be a *perfect square* if there exists an $a \in \mathbb{Z}$ such that $n = a^2$. An integer n is called *quad-free* if other than 1 there exists no $b \in \mathbb{Z}$ such that $b^2 \mid n$.

1. Let $a = q_1 \cdots q_t$ where q_i is prime for every $i \in [t]$ and such that $q_i \neq q_j$ for every $1 \leq i < j \leq t$. Is it necessarily the case that a is always quad-free? Prove your answer.

2. Prove or disprove the following claim. Every positive integer $n \geq 1$ can be expressed as $n = a \cdot b$ where a is quad-free and b is a perfect square.

Exercise 4. Prove or disprove the following claim. Every positive integer n can be written in the form $n = p + a^2$ where p is either prime or 1 and $a \geq 0$.

Exercise 5. Determine all (distinct) prime factors of 1000!. Generalise your answer to all n.

Exercise 6. Prove or disprove that there exists an n_0 such that every integer $n \geq n_0$ can be written as the sum of two composite numbers.

Exercise 7. We say that a number n is *prime square divisible* if whenever $p \mid n$, p prime, then $p^2 \mid n$. An integer n is said to be a *perfect cube* if there exists an $a \in \mathbb{Z}$ such that $n = a^3$.

Prove or disprove the following claim. Every prime square divisible integer n satisfies $n = a \cdot b$ where a is a perfect square and b is a perfect cube.

Exercise 8. In this exercise you are asked to provide two distinct proofs for the infinitude of primes using factorials. For the first proof, you are to take the road with the view, sort of speak; for the first proof you are to alter Euclid's proof (see Theorem 5.23) for the infinitude of primes by setting the number Q defined in Euclid's argument to $Q := n! + 1$ for some suitable $n \in \mathbb{Z}^+$.

For the second proof, you are to utilise Exercise 5 above.

Exercise 9. In Proposition 5.53 we have shown that there are infinitely many primes of the form $4n + 3$. The argument presented resorted to saying that as $-1 \equiv 3 \pmod 4$ it is sufficient to prove that there are infinitely many primes of the form $4n - 1$ and consequently we defined $Q = 4 \cdot (\prod_{p \in S} p) - 1$ where S denoted the set of all primes of the form $4n - 1$ (which we assumed towards contradiction is finite).

Revisit this proof and alter it by defining Q to be of the form $4n + 3$ and do not use the fact that $-1 \equiv 3 \pmod 4$.

Exercise 10. Let p_n denote the nth prime. Prove that

$$p_{n+3}^2 < p_n p_{n+1} p_{n+2}$$

for every $n \geq 3$.

Exercise 11. Prove each of the assertions below

1. Any prime of the form $3n + 1$ is also of the form $6m + 1$.

2. Each integer of the form $3n + 2$ has a prime factor of this form.

3. The only prime of the form $n^3 - 1$ is 7. Hint : $n^3 - 1 = (n-1)(n^2+n+1)$.

Exercise 12. Let n be a positive integer and p the least prime such that $p \mid n$. Prove the following assertion: If $n^{1/3} < p$ then either $n/p = 1$ or n/p is a prime.

Exercise 13. Prove the following assertion: For every prime greater than 3, at least one of the following numbers is not prime : $p+2$, $p+4$.

Exercise 14. Prove that if $(a,b) = 1$ and $ab = s^2$ then there exist some natural integers k and t such that $a = k^2$ and $b = t^2$.

§5.7. Solutions

Some of the solutions have been written by the TAs in the course and thus have a different style of writing to them. Over time we hope to normalise this part of the text as well.

Solution for Exercise 1. Write

$$[2^{N-1}, 2^N] = (1,2] \cup (2,4] \cup (4,8] \cup \cdots \cup (2^{N-1}, 2^N].$$

By Bertrand's postulate (i.e., Theorem 17.37) each such interval contains at least one prime number.

Solution for Exercise 2. Suffice to prove

$$\vartheta(x) = \log\left(\prod_{p \le x} p\right) = \sum_{p \le x} \log p < x \log 4 = 2x;$$

this we already established in Exercise 3.

Solution for Exercise 3.

1. The claim is true. For suppose that $b^2 \mid a$ for some $1 < b \in \mathbb{Z}$. Let $b = p_1^{a_1} \cdots p_k^{a_k}$ so that $b^2 = p_1^{2a_1} \cdots p_k^{2a_k}$. Note that every divisor of a has every one of its prime factors appearing in its factorisation with power equal to 1 precisely. From the prime factorisation of b^2 we see that b^2 does not satisfy this property.

2. The claim is true. Let the prime power factorisation of n be given by

$$n = (p_1^{a_1} \cdots p_k^{a_k}) \cdot (q_1^{b_1} \cdots q_t^{b_t})$$

where a_i is even for every $i \in [k]$ and b_i is odd for every $i \in [t]$. Then $a_i = 2a_i'$ for every $i \in [k]$ and $b_i = 2b_i' + 1$ for every $i \in [t]$. Then

$$\begin{aligned} n &= (p_1^{2a_1'} \cdots p_k^{2a_k'}) \cdot (q_1^{2b_1'+1} \cdots q_t^{2b_t'+1}) \\ &= (p_1^{a_1'} \cdots p_k^{a_k'} q_1^{b_1'} \cdots q_t^{b_t'})^2 \cdot (q_1 \cdots q_t). \end{aligned}$$

The claim follows by the first part of the question.

Solution for Exercise 4. The claim is false. The short answer here is to simply present an n for which this claim fails. For instance $n = 25$. Let us however discuss how one can reach 25 as being a counter example. This discussion is not a part of the answer but is instructive nonetheless. Indeed,

when faced with such a problem the brute force approach is not recommended in case that the property fails starting at some large integer.

Let us show that the claim fails for n being a perfect square, i.e., $n = k^2$ for some positive integer k. Why show failure for squares? The reason we gravitate towards this case is that we will then be trying to prove that for every $k \in \mathbb{Z}^+$ there exists an a as above such that $k^2 - a^2$ is prime. As $k^2 - a^2 = (k-a)(k+a)$ requiring that this is prime seems problematic or for the very least challenging. In particular for this to be prime one must insist on $k - a = 1$ or $k + a = 1$, for if both of these terms are ≥ 2 then we get a composite number (by definition). As we expect $k^2 - a^2 = p > 0$ it should be the case that $k - a = 1$ and $k + a$ prime.

To have this form impose more structure let us take $k = q$ where q is some prime > 2. In this case, for the claim to be true two conditions must be satisfied: (i) $q - a = 1$ and (ii) $q + a$ is prime. From (i) we have $a = q - 1$ substituting this in (ii) yields $q + a = 2q - 1$. Consequently, these two conditions suggest that $2q - 1$ must also be prime.

At this point we know for certain that something is wrong with this stipulation. For if this claim is true then it also holds for squares of primes q^2 and if it holds for square of primes then we get that if q is prime then so is $2q - 1$. This cannot be true as the gaps between consecutive primes can be arbitrarily large; moreover we recall that the larger gaps came as we "drifted" away towards infinity. So it makes sense to let q have some "size" to it. That is taking q to be 2 or 3 should not be the place for a counter example.

Indeed, for $q = 3$ (i.e., $n = q^2 = 9$) we have that we can take $a = 2$ (by (i)) and (ii) is true as $3 + 2 = 5$ is prime, and indeed, $9 = 5 + 2^2$. If we take one step further, say, take $q = 5$ (i.e., $n = q^2 = 25$) then we have $a = 4$ and $5 + a = 5 + 4 = 9$ which is not prime and we are done with our search.

Solution for Exercise 5. Let p be a prime factor of 1000!. Then $p \mid 1 \cdot 2 \cdot 3 \cdots 1000$. As p is prime it follows that there exists at least one integer ℓ appearing in the product defining 1000! such that $p \mid \ell$. As $\ell \leq 1000$ it follows that $p \leq 1000$. This, in particular, shows that all prime factors of 1000! do not exceed 1000.

On the other hand, all primes not exceeding 1000 appear in the product defining 1000!; it follows that the prime factors of 1000! are all the primes not exceeding 1000. One can substitute 1000 with any positive integer n.

Solution for Exercise 6. We consider two cases. Either n is even or n is odd. In the former case, we may write $n = 2k$ for some $k \in \mathbb{Z}$. Note that

$$\begin{aligned} n = 2k &= 2(k-1) + 2 \text{ (2 is prime - not good)} \\ &= 2(k-2) + 4, \end{aligned}$$

so that n is a sum of the composite number 4 and the number $2(k-2)$. For $k \geq 4$ we have that $2(k-2)$ is composite. That is we have that if n is even and $n \geq 8$ then it can be expressed as a sum of two composite numbers.

We consider the complimentary case that $n = 2k + 1$ is odd. Here we note that

$$\begin{aligned} n = 2k + 1 &= 2(k-1) + 3, \text{ 3 is prime -not good} \\ &= 2(k-2) + 5, \text{ 5 is prime -not good} \\ &= 2(k-3) + 7, \text{ 7 is prime -not good} \\ &= 2(k-4) + 9, \end{aligned}$$

so that n is a sum of the composite number 9 and $2(k-4)$. The latter is composite for $k \geq 6$. That is, we have shown that for if n is odd and $n \geq 13$ then it is a sum of two composite numbers.

The claim then holds with $n_0 = 13$.

Solution for Exercise 7. The claim is true. Let $p_1, \ldots, p_k$ be the prime factors of n that have an even power in the factorisation of n. Let $q_1, \ldots, q_t$ be the prime factors of n that have an odd power in the factorisation of n. As n is prime square divisible the power of each factor q_i, $i \in [t]$, is at least 3. Consequently, the powers of these odd exponents must be of the form $2a + 3$ (and not $2a + 1$). Hence,

$$\begin{aligned} n &= p_1^{2a_1} \cdots p_k^{2a_k} q_1^{2b_1+3} \cdots q_t^{2b_t+3} \\ &= (p_1^{a_1} \cdots p_1^{a_k} q_1^{b_1} \cdots q_t^{b_t})^2 \cdot (q_1 \cdots q_t)^3, \end{aligned}$$

and the claim follows.

Solution for Exercise 8. For the first proof, we follow Euclid's proof (i.e., Theorem 5.23) very closely. Assume then towards a contradiction, that there are only finitely many primes; and let S denote the set of all prime numbers. Let $p \in S$ be its largest member, and let $N > p$ be an integer. Define

$$Q = N! + 1.$$

As $N > p \geq 2$ it follows that $N \geq 3$ so that $Q > 1$. Then, Q has a prime factorisation. Let $q \geq 2$ be a prime factor of Q. We show that $q \notin S$. For suppose that $q \in S$. Then, $q \mid Q - N!$. As $Q - N! = 1$ and $q \geq 2$; we reach a contradiction.

For the second proof, we utilise the claim implicit in Exercise 5 asserting that *for all positive integers n, the prime factors of $n!$ are all primes not exceeding n.* For every positive integer $n > 1$, let q_n be the least prime dividing $n! + 1$. As $(n!, n! + 1) = 1$, $n!$ and $n! + 1$ share no common factors. The fact that all prime factors of $n!$ do not exceed n then implies that q_n exceeds the largest prime not exceeding n. This in particular means that $q_n > n$. It follows that for every n there is a prime exceeding it. The infinitude of primes follows.

Solution for Exercise 9. Assume the claim is false and that there are finitely many such primes. Let S denote the set of such primes so that there exists a $t \in \mathbb{Z}^+$ such that $S = \{q_1 = 3, q_2 \ldots, q_t\}$. Put $Q = 4\prod_{i=2}^{t} q_i + 3$. Note that $q_1 = 3$ does not participate in $\prod_{i=2}^{t} q_i$.

Show now (as we did in class) that Q has a prime divisor of the form $4n + 3$. We consider two cases. Either $q = 3$ or $q > 3$. In the former case $q \mid Q - 3 = 4\prod_{i=2}^{t} q_i$ which is a contradiction. Indeed, $(3, 4) = 1$ and 3 does not participate in $\prod_{i=2}^{t} q_i$ (which is comprised solely of primes). If $q > 3$ then $q \in S \setminus \{3\}$ and participates in $\prod_{i=2}^{t} q_i$ so that $q \mid \prod_{i=2}^{t} q_i$ implying that $2 \leq q \mid (Q - \prod_{i=2}^{t} q_i) = 1$ which is a contradiction.

Solution for Exercise 10. For $n = 3, 4, 5$ one can verify the claim by "hand". Let us assume then that $n \geq 5$. By Bertrand's postulate in we have that $p_{n+3} < 2p_{n+2}$. Then

$$p_{n+3}^2 < 4p_{n+2}^2 = 4p_{n+2} \cdot p_{n+2} < 4p_{n+2}(2p_{n+1}) = 8p_{n+1}p_{n+2},$$

where the last inequality is again due to Bertrand's postulate. Note now that $p_5 = 11$ so that $8p_{n+1}p_{n+2} < p_5 p_{n+1} p_{n+2}$. Surely $p_n \geq p_5$ for every $n \geq 5$ so that $p_5 p_{n+1} p_{n+2} \leq p_n p_{n+1} p_{n+2}$ for every $n \geq 5$. The claim follows.

Solution for Exercise 11.

1. Let us define $p = 3n+1$. Any integer can only be of the form $6m, 6m+1, 6m+2, 6m+3, 6m+4, 6m+5$. If p is a prime, it cannot be of the form $6m, 6m + 2 = 2(3m + 1), 6m + 3 = 3(2m + 1), 6m + 4 = 2(3m + 2)$. It leaves us with $6m + 1$ and $6m + 5$.

Let us assume that p is of the form $6m+5$. Then $3n+1 = 6m+5$, hence $3n-6m = 3(n-2m) = 4$ or equivalently $n-2m = 4/3$ which is impossible since $n-2m$ is an integer. It leaves with the only possible form : $6m+1$.

2. Let us prove that each integer of the form $N = 3n+2$ has a prime factor of the form $3k+2$. Suppose, to the contrary, that $3n+2$ has no prime factor of the form $p = 3k+2$. Then all prime factors must have the form $3k+1$.
   Let us show that the product of two numbers of the form $3k+1$ is also of the form $3k+1$: $(3k+1)(3m+1) = 9mk+3k+3m+1 = 3(3mk+k+m)+1$, by contradiction to the fact that N is of the form $3n+2$.

3. Let $p = n^3-1 = (n-1)(n^2+n+1)$. Therefore, p is a product of two numbers. It is composite unless $n-1 = 1$ which leads to $n = 2$, and $p = 2^3-1 = 7$.

Solution for Exercise 12. By assumption, p is a prime, therefore $p > 1$. Moreover, $n^{1/3} < p$ hence $n < p^3$. We will show that if $n \neq p$ then there exists a prime k such that $n = kp$. Suppose, to the contrary, that k is composite, hence there exist p_1, k_1 such that $k = p_1k_1$ where p_1 is a prime. Therefore $n = p_1k_1p$, that is p_1 is a divisor of n. By assumption, p is the least prime divisor of n therefore $p \leq p_1$.

If k_1 is prime, then it is also a prime divisor of n, therefore $p \leq k_1$. As a conclusion $p \leq p_1$ and $p \leq k_1$. Altogether, $p^3 \leq pp_1k_1 = n$ by contradiction to the assumption.

If k_1 is composite, there exists a prime p_2 such that $k_1 = p_2k_2$ where p_2 is a prime and $p \leq p_2 < k_1$. In addition to the fact that $p \leq p1$, we get $p^3 \leq pp_1k_1 = n$ by contradiction to the assumption.

As a conclusion, $k_1 = 1$, the only number which is neither prime and nor composite. Hence, $k = p_1$ therefore k is prime.

Solution for Exercise 13. Let p any prime greater than 3. p is either of the form $3n+1$ or $3n+2$. If $p = 3n+1$ then $p+2 = 3n+3 = 3(n+1)$ is composite. If $p = 3n+2$ then $p+4 = 3n+6 = 3(n+2)$ is composite.

Solution for Exercise 14. Let $s = p_1^{a_1}p_2^{a_2}...p_k^{a_k}$ be the factorisation of s. Then $s^2 = p_1^{2a_1}p_2^{2a_2}...p_k^{2a_k}$. By assumption, $gcd(a,b) = 1$, so these numbers have no common prime factors. Consequently, the prime factors of s^2 (and thus of s) split into two disjoint sets between a and b. Say $a = p_{i_1}^{2a_{i_1}} \cdots p_{i_\ell}^{2a_{i_\ell}}$ and $b = p_{j_1}^{2a_{j_1}} \cdots p_{j_m}^{2a_{j_m}}$ with $\ell + m = k$ and $i_r, j_r \in [1,k]$. The claim then follows.

Lecture 6

Congruences

§6.1. Congruence classes

Definition 6.1 *Let $m \in \mathbb{Z}^+$ and let $a, b \in \mathbb{Z}$. We say that a is* congruent to b modulo m, *and write $a \equiv b \pmod{m}$ if $m \mid a - b$. If $m \nmid a - b$ then we say that a is* incongruent to b modulo m *and we write $a \not\equiv b \pmod{m}$.*

When $m = 1$ we get a triviality as $1 \mid a - b$ for any $a, b \in \mathbb{Z}$.

Example 6.2

$$\begin{aligned} 1 &\equiv -1 \pmod{2} \text{ as } 2 \mid 1 - (-1) \\ 5 &\equiv 1 \pmod{2} \text{ as } 2 \mid 5 - 1 \\ (n-1) &\equiv -1 \pmod{n} \text{ as } n \mid (n-1) - (-1) \\ n - 2 &\equiv -2 \pmod{n} \text{ as } n \mid (n-2) - (-2) \\ n - i &\equiv -i \pmod{n} \text{ as } n \mid (n-i) - (-i) \end{aligned}$$

Theorem 6.3 *Let $m \in \mathbb{Z}^+$. If $a, b \in \mathbb{Z}$ then $a \equiv b \pmod{m}$ if and only if $a = b + km$ for some $k \in \mathbb{Z}$.*

Proof. If $a \equiv b \pmod{m}$ then $m \mid a - b$ so that $km = a - b$ for some $k \in \mathbb{Z}$ and the claim follows in this direction. Conversely, if $a = b + km$ for some $k \in \mathbb{Z}$ then $a - b = km$ so that $m \mid a - b$ and the claim follows in this direction. ■

Theorem 6.4 *Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then $a \equiv b \pmod{m}$ if and only if $a = km + r$ and $b = k'm + r$ for some $k, k' \in \mathbb{Z}$ and $0 \leq r < m$. That is, both a and b have the same remainder after division by m.*

Proof. If $a \equiv b \pmod{m}$ then $a = b + km$ for some $k \in \mathbb{Z}$ by Theorem 6.3. In addition, by the division algorithm $b = k'm + r$ for some $k' \in \mathbb{Z}$ and $0 \leq r < m$. Then

$$a = b + km = k'm + r + km = (k' + k)m + r$$

and the first direction is complete.

Conversely, suppose that $a = km + r$ and $b = k'm + r$ for some $k, k' \in \mathbb{Z}$. Then $a - b = (k - k')m$ so that $m \mid a - b$ and the claim follows. ■

Given $m \in \mathbb{Z}^+$ we have just defined a relation on the members of $\mathbb{Z}$, namely,

$$\mathcal{R}_m := \{(a, b) \in \mathbb{Z}^2 : a \equiv b \pmod{m}\}.$$

Theorem 6.5 asserts that this relation is an *equivalence relation*[1] on $\mathbb{Z}$.

Theorem 6.5 *Let $m \in \mathbb{Z}^+$. Congruences modulo m satisfy the following properties.*

1. *Reflexive property: $a \equiv a \pmod{m}$ for every $a \in \mathbb{Z}$.*
2. *Symmetric property: If $a, b \in \mathbb{Z}$ then $a \equiv b \pmod{m} \iff b \equiv a \pmod{m}$.*
3. *Transitive property: If $a, b, c \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.*

Proof. The reflexive property follows from the fact that $m \mid a - a$ for every $a \in \mathbb{Z}$. The symmetric property follows from the observation that $m \mid a - b$ if and only if $m \mid b - a$. Finally, the transitive property follows from the fact that if $m \mid a - b$ and $m \mid b - c$ then $a = b + k_1 m$ and $b = c + k_2 m$. Then $a - c = b + k_1 m - (b - k_2 m) = (k_1 + k_2)m$ so that $m \mid a - c$. ■

The relation $\mathcal{R}_m$ partitions $\mathbb{Z}$ into disjoint sets given by its equivalence classes to which we refer as the *congruence classes of m*. Given $a \in \mathbb{Z}$ we may write $a = km + r$ with $0 \le r < m$. The number r is referred to as the *least non-negative residue of a modulo m*. We say that r is the result of *reducing a modulo m*. A commonly used notation is $a \bmod m = r$. In fact, we have that $a \equiv r \pmod{m}$. The uniqueness of the presentation $a = km + r$ assures us that every integer $a \in \mathbb{Z}$ is congruent to precisely one of the numbers $\{0, 1, \ldots, m - 1\}$. The latter are pairwise incongruent giving rise to the following definition.

Definition 6.6 A complete system of residues modulo m *is a set of integers such that every $a \in \mathbb{Z}$ is congruent to precisely one member of the set modulo m.*

The Division Algorithm then asserts that for $m \in \mathbb{Z}^+$ the set $\{0, 1 \ldots, m - 1\}$ is a complete system of residues modulo m. Each member of this set is a representative of the equivalence class of $\mathcal{R}_m$ containing it. For instance 0 represents all integers divisible by m, 1 represents all integers divisible by m with residue 1 and so on. One often write

$$0 \pmod{m}, 1 \pmod{m}, \ldots, (m - 1) \pmod{m}.$$

to denote all the congruence classes modulo m; so that in particular $0 \in 0 \pmod{m}$ and in fact all integers divisible by m are members of the set $0 \pmod{m}$. Additional more concise notation for these classes is

$$[0]_m, [1]_m, \ldots, [m - 1]_m$$

where the subscript m is dropped if m is clear from the context.

$$\overline{0}_m, \overline{1}_m, \ldots, \overline{m - 1}_m$$

is also a common notation in use by the community, and again the subscript m is dropped if the latter is clear from the context.

[1] A relation is said to be an equivalence relation if it is reflexive, symmetric, and transitive.

Definition 6.7 *Given $m \in \mathbb{Z}^+$ and $x \in \mathbb{Z}$ we write $[x]_m$ or $\overline{x}_m$ to denote the congruence class of m containing x.*

The set $\{0, 1, \ldots, m-1\}$ is certainly the canonical choice for a complete system of residues modulo m as it arises naturally from the Division Theorem. $\mathcal{R}_m$ being an equivalence relation means though that we could change the names of the representative we take based on our notational convenience. For instance, if m is odd one often uses the set

$$-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2}$$

as a complete system of residues modulo m.

Proposition 6.8 *Let $m \in \mathbb{Z}^+$. A(ny) set of m incongruent integers forms a complete set of residues modulo m.*

Proof. For a set S of size m we have that each $s \in S$ satisfies $s = k_s m + r_s$, by the division algorithm. Put $R := \{r_s : s \in S\}$. Suppose now towards contradiction that S consists of incongruent integers and yet does not form a complete set of residues modulo m. Then $|R| \leq m-1$ so that there exist $s, s' \in S$ with $s \neq s'$ such that $r_s = r_{s'}$, by the pigeonhole principle. Then s and s' are congruent modulo m; contradiction. ■

This last result is an outcome of the following core principle.
The pigeonhole principle. *if n pigeons are distributed into at most $n-1$ pigeonholes then after the distribution there would be a pigeonhole with at least two pigeons in it.*

The following result defines the arithmetics of congruence classes.

Theorem 6.9 (Modular arithmetics)
Let $a, b, c \in \mathbb{Z}$ and let $m \in \mathbb{Z}^+$ such that $a \equiv b \pmod{m}$. Then the following holds.

1. *Addition.* $a + c \equiv b + c \pmod{m}$.
2. *Subtraction.* $a - c \equiv b - c \pmod{m}$.
3. *Multiplication.* $ac \equiv bc \pmod{m}$.

Proof.

1. As $m \mid a - b$ and $a - b = (a + c) - (b + c)$ we have that $m \mid ((a + c) - (b + c))$ and the addition property follows.
2. The subtraction property is proved is a similar manner using the identity $a - b = (a - c) - (b - c)$.
3. For the multiplication property note that $ac - bc = c(a - b)$. As $m \mid a - b$ it follows that $m \mid c(b - a)$ and the claim follows.

■

Theorem 6.10 (Modular arithmetics)
Let $a, b, c, d \in \mathbb{Z}$ and let $m \in \mathbb{Z}^+$ such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then:

1. *Addition.* $a + c \equiv b + d \pmod{m}$.
2. *Subtraction.* $a - c \equiv b - d \pmod{m}$.

3. Multiplication. $ac \equiv bd \pmod{m}$.

PROOF. By assumption we have that

$$a - b = km \quad \text{and} \quad c - d = \ell m. \tag{6.11}$$

1. Note that $a + c - (b + d) = (a - b) + (c - d)$; the claim follows by (6.11).
2. Note that $a - c - (b - d) = (a - b) - (c - d)$; the claim follows by (6.11).
3. Here we note that

$$ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) = kmc + \ell mb = m(kc + b\ell);$$

and the claim follows.

■

EXAMPLE 6.12 As $13 \equiv 3 \pmod{5}$ and $7 \equiv 2 \mod 5$ then $13 + 7 \equiv 3 + 2 \pmod{5}$.

Note that division (in its traditional sense) is an operation that is not supported by congruences classes. For instance we have that $14 \equiv 8 \pmod{6}$ as $6 \mid 14 - 8$. Rewriting this we have that $7 \cdot 2 \equiv 4 \cdot 2 \pmod{6}$. The common factor 2 cannot be reduced, however. Indeed, $7 \not\equiv 4 \pmod{6}$.

THEOREM 6.13 *Let $a, b, c \in \mathbb{Z}$, let $m \in \mathbb{Z}^+$, and let $d = (c, m)$. Then $ac \equiv bc \pmod{m}$ if and only if $a \equiv b \pmod{m/d}$.*

PROOF. Assume first that $ac \equiv bc \pmod{m}$; i.e., that $m \mid c(a - b)$ so that $ca - cb = km$ for some $k \in \mathbb{Z}$. We may write $c = dr$ and $m = ds$ where $(s, r) = 1$[2]. Substituting we get $r(a - b) = ks$. That is $s \mid r(a - b)$. As $(s, r) = 1$, it follows that $s \mid (a - b)$. As $s = m/d$ the claim follows.

For the converse direction we simply note that we can 'reverse' the first direction. Let s be as above, i.e., $s = m/d$ and assume $a \equiv b \pmod{s}$ so that $s \mid a - b$. Consequently, $s \mid k(a - b)$ for any $k \in \mathbb{Z}$. For the rôle of k we can in particular choose $k = r$ where $c = dr$ as to have $s \mid r(a - b)$. We may then write $r(a - b) = k's$ for some $k' \in \mathbb{Z}$. Multiplying both sides by d we arrive at $dr(a - b) = k'ds$. Recalling that $c = dr$ and that $m = ds$ we get $c(a - b) = k'm$ as required. ■

In Theorem 6.13 suppose that $c \equiv 0 \pmod{m}$ so that $c = km$ for some $k \in \mathbb{Z}$. Then $(c, m) = m$. The assertion of Theorem 6.13 in this case would be that $a \equiv b \pmod{1}$ which is a triviality.

EXAMPLE 6.14 Rewrite $50 \equiv 20 \pmod{15}$ as $10 \cdot 5 \equiv 2 \cdot 10 \pmod{15}$. As $(15, 10) = 5$ we have that $5 \equiv 2 \pmod{3}$.

Theorem 6.13 becomes very powerful when $(c, m) = 1$ as then there is no change in the modulus.

COROLLARY 6.15 *Let $a, b, c \in \mathbb{Z}$ and let $m \in \mathbb{Z}^+$ such that $(c, m) = 1$. If $ac \equiv bc \pmod{m}$ then $a \equiv b \pmod{m}$.*

Another corollary of interest in the venue of Theorem 6.13 is the case that $m = p$ is prime. In which case $(c, p) = 1$ is equivalent to $p \not| c$.

[2] $d(s, r)$ is a common divisor of m and c which will be greater than d if $(s, r) > 1$.

Corollary 6.16 *Let $a, b, c \in \mathbb{Z}$ and let p be prime such that $p \nmid c$. Then if $ac \equiv bc \pmod{p}$ then $a \equiv b \pmod{p}$.*

Example 6.17 It is trivial that if $a \equiv 0 \pmod{m}$ and $b \equiv 0 \pmod{m}$ then $ab \equiv 0 \pmod{m}$. Indeed, this is implied by the multiplication property in Theorem 6.10 (below) or more simply from the fact that the product of two numbers divisible by m results in a number divisible by m. Suppose now that $a \not\equiv 0 \pmod{m}$ and that $b \not\equiv 0 \pmod{m}$. Is it true that $ab \not\equiv 0 \pmod{m}$? Not necessarily. For instance $5 \not\equiv 0 \pmod{25}$ yet $5 \cdot 5 \equiv 0 \pmod{25}$.

Corollary 6.18 *Let $a, b \in \mathbb{Z}$ and let $m \in \mathbb{Z}^+$. If $ab \equiv 0 \pmod{m}$ and $(a, m) = 1$ then $b \equiv 0 \pmod{m}$.*

Proof. Surely $ab \equiv a \cdot 0 \pmod{m}$. As $(a, m) = 1$ we have by Corollary 6.15 that $b \equiv 0 \pmod{m}$. ■

Corollary 6.19 *Let $a, b \in \mathbb{Z}$ and let p be prime. If $ab \equiv 0 \pmod{p}$ then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.*

Proof. Suppose that $a \not\equiv 0 \pmod{p}$. Then $(a, p) = 1$ and $b \equiv 0 \pmod{p}$ by Corollary 6.18. ■

We conclude this section with the operation of raising congruence classes to a power. The polynomial factoring identity

$$a^2 - b^2 = (a - b)(a + b)$$

is known to us from high school. This identity generalises as follows for $k \geq 2$.

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + ab^{k-2} + b^{k-1}). \tag{6.20}$$

The following asserts that congruence is preserved if both sides are raised to the power of the same positive integer.

Theorem 6.21 *Let $a, b \in \mathbb{Z}$ and let $k, m \in \mathbb{Z}^+$. If $a \equiv b \pmod{m}$ then $a^k \equiv b^k \pmod{m}$.*

Proof. By (6.20) we have that $(a-b) \mid (a^k - b^k)$. As $m \mid a-b$, by assumption, it follows that $m \mid a^k - b^k$. An alternative proof would be to simply apply the multiplication property seen in Theorem 6.10 k times with a on the left and b on the right. ■

The following example shows that the converse of Theorem 6.21 is false.

Example 6.22 Suppose that $a^2 \equiv b^2 \pmod{m}$. Does that imply that $a \equiv b \pmod{m}$? Not necessarily. Note that $5^2 \equiv 4^2 \pmod{3}$ as $25 - 16 = 9$. However, $5 \not\equiv 4 \pmod{3}$.

Given a finite set $X = \{x_1, \ldots, x_k\} \subseteq \mathbb{Z}$, the set

$$aX + b := \{ax_1 + b, \ldots, ax_k + b\}$$

is called a *generalised arithmetic progression*.

Proposition 6.23 *Let R be a complete set of residues modulo m, and let $a \in \mathbb{Z}$ such that $(a, m) = 1$. Then the generalised arithmetic progressions $aR + b$ is a complete set of residues modulo m for every $b \in \mathbb{Z}$.*

Proof. Fix $b \in \mathbb{Z}$. By Proposition 6.8, it suffices to show that the members of $a + bR$ are incongruent modulo m. To that end, fix $r, r' \in R$ such that $r \neq r$ and consider $ar + b$ and $ar' + b$ and assume towards a contradiction that

$$ar + b \equiv ar' + b \pmod{m}.$$

Then, by the addition property (see Theorem 6.9),

$$ar \equiv ar' \pmod{m}.$$

By Theorem 6.13 then we have that

$$r \equiv r' \pmod{m};$$

contradiction to the assumption that r and r' are incongruent. ■

§6.2. Linear congruences

An equation of the form

$$ax \equiv b \pmod{m} \tag{6.24}$$

with x unknown is called a *linear congruence*. If $x_0 \in \mathbb{Z}$ is a solution, i.e., $ax_0 \equiv b \pmod{m}$ and $x_1 \equiv x_0 \pmod{m}$, i.e., $x_1 \in [x_0]_m$, then $b \equiv ax_1 \equiv ax_0 \pmod{m}$ so that x_1 is a solution to the equation as well.

Observation 6.25. *If $x_0 \in \mathbb{Z}$ is a solution to (6.24) then every member of $[x_0]_m$ is a solution to (6.24) as well.*

Due to this observation our attention now shifts to the number of incongruent solutions Equation (6.24) has.

Owing to Theorem 6.3 linear congruences are equivalent to solving linear Diophantine equations (see § 4.6 for details). For indeed, by Theorem 6.3, $ax \equiv b \pmod{m}$ if and only if $ax = b + ym$ for some $y \in \mathbb{Z}$. In order to solve (6.24) then, we need only solve the linear Diophantine equation

$$ax - my = b, \tag{6.26}$$

where x and y are the variables we seek in $\mathbb{Z}$. By Lemma 4.78

$$\text{(6.26) has a solution if and only if } (a, m) \mid b. \tag{6.27}$$

By Lemma 4.80, if (6.26) has a solution then it has infinitely many solutions given by

$$x = x_0 + \left(\frac{m}{(a, m)}\right) t, \quad y = y_0 + \left(\frac{a}{(a, m)}\right) t, \ t \in \mathbb{Z}$$

where $x = x_0$ and $y = y_0$ is a particular solution to the equation. The following theorem asserts that these infinitely many solutions can be arranged in precisely (a, m) congruence classes modulo m. Moreover, the proof of this theorem will reveal that in order to find these congruence classes modulo m into which the solutions fit it suffices to consider a complete set of residues modulo (a, m) (see (6.79) below for details).

Theorem 6.28 *Let $a, b \in \mathbb{Z}$, let $m \in \mathbb{Z}^+$, and put $d = (a, m)$.*

1. *If $d \nmid b$ then (6.24) has no solutions.*
2. *Otherwise (6.24) has d incongruent solutions modulo m.*

Proof. By (6.26) the equation $ax \equiv b \pmod{m}$ has no solutions if $d \nmid b$. If on the other hand $d \mid b$ then the diophantine equation $ax - my = b$ has infinitely many solutions of the form

$$x = x_0 + \left(\frac{m}{d}\right) t, \quad y = y_0 + \left(\frac{a}{d}\right) t, \ t \in \mathbb{Z}$$

where $x = x_0$ and $y = y_0$ is a particular solution to the equation. The values of x given by $x = x_0 + \left(\frac{m}{d}\right) t$ are all solutions to $ax \equiv b \pmod{b}$.

It remains to show that these infinitely many solutions are partitioned into precisely d congruence classes modulo m. To that end we find a condition in order to determine when two solutions for x are congruent modulo m. In particular we show the following. Let $x_1 = x_0 + \left(\frac{m}{d}\right) t_1$ and $x_2 = x_0 + \left(\frac{m}{d}\right) t_2$ be two solutions for x.

$$x_1 \equiv x_2 \pmod{m} \text{ if and only if } t_1 \equiv t_2 \pmod{d}. \tag{6.29}$$

This in turn implies that if we let t range over a complete set of residues modulo d then this will produce a set of size d of values for x that are all incongruent modulo m. As a complete set of residues modulo d has size d this in particular shows that one cannot generate more than d incongruent values for x that are incongruent modulo m.

It remains to prove (6.79). We show one direction as one can note that the proof can easily be reversed to yield the other direction. Suppose that

$$x_0 + \left(\frac{m}{d}\right) t_1 \equiv x_0 + \left(\frac{m}{d}\right) t_2 \pmod{m}.$$

Then by Theorem 6.9 we may cancel x_0 so that

$$\left(\frac{m}{d}\right) t_1 \equiv \left(\frac{m}{d}\right) t_2 \pmod{m}.$$

By Theorem 6.13

$$t_1 \equiv t_2 \pmod{\frac{m}{D}},$$

where $D = (m, m/d)$. As $\frac{m}{d} \mid m$ we have that $D = m/d$ so that

$$t_1 \equiv t_2 \pmod{d},$$

and (6.79) follows and thus concluding the proof of the theorem. ■

The following is implied by Corollary 4.81.

Corollary 6.30 *Solving an equation of the form $ax \equiv b \pmod{m}$ requires $O(\max\{\log a, \log b, \log m\}^3)$ bit operations.*

Example 6.31 Find all incongruent solutions to the equation $2x \equiv 1 \pmod{2}$. Here we have that $(2, 2) = 2 \nmid 1$ so the are no solutions to this equation. More generally, $mx \equiv 1 \pmod{m}$ has no solutions for the same reason.

Example 6.32 Find all solutions to the equation $9x \equiv 12 \pmod{15}$. We start by noting that $(15, 9) = 3 \mid 12$ so that there are three incongruent solutions modulo 15, by Theorem 6.28. From the proof of this theorem we know that the solutions have the form

$$x = x_0 + (15/3) \cdot t, \ t \in \mathbb{Z}.$$

We are missing x_0. To find x_0 we consider the linear diophantine equation $9x - 15y = 12$. We have learned how to solve such equations in the lecture on Divisibility. We are now looking for some solution to this diophantine equation the x-part of which we will use as x_0.

We apply the extended Euclid's algorithm. Euclid's algorithm for $(15, 9)$; the first phase of which is to generate the equation of Euclid's algorithm for $(15, 9)$:

$$\begin{aligned} 15 &= 1 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

Using these equations we express $3 = (15, 9)$ as a linear combination of 15 and 9.

$$3 = 9 - 6 = 9 - (15 - 9) = (-1) \cdot 15 + 2 \cdot 9.$$

As $3 \cdot 4 = 12$ then $((-1) \cdot 15 + 2 \cdot 9) \cdot 4 = 12$ so that

$$9 \cdot 8 + 15 \cdot (-4) = 12.$$

The value $x_0 = 8$ and $y_0 = -4$ form a solution to the linear diophantine equation $9x + 15y = 12$. We use $x_0 = 8$ to generate all solution to the linear congruence $9x \equiv 12 \pmod{15}$:

$$x = 8 + (15/3)t = 8 + 5t, \ t \in \mathbb{Z}.$$

This infinite set of solutions is partitioned into precisely three congruences classes modulo 15. To discover which classes are those it is sufficient to let t range over a complete set of residues modulo 3. The canonical choice is naturally $\{0, 1, 2\}$. This gives us that the solutions to $9x \equiv 12 \pmod{15}$ are partitioned amongst the congruence classes $8 \pmod{15}$, $13 \pmod{15}$, and $18 \pmod{15}$, where the latter is equivalent to $3 \pmod{15}$.

Corollary 6.33 *If in (6.24) we have $(a, m) = 1$ then (6.24) has a unique solution modulo m.*

That is, if $(a, m) = 1$ in (6.24) then there are infinitely many solutions in the integers but they all fall into a single congruence class modulo m.

6.2.1 *Modular inverse*

Of special interest to us are equations of the form

$$ax \equiv 1 \pmod{m}; \tag{6.34}$$

such equations have a unique solution modulo m if and only if $(a, m) = 1$ giving rise to the following definition.

Definition 6.35 *Let $a \in \mathbb{Z}$ and let $m \in \mathbb{Z}^+$ such that $(a, m) = 1$. The (unique) solution modulo m to (6.34) is called the* inverse *of a modulo m.*

An alternative way to define the inverse relation is to say that two integers a and $\tilde{a}$ are called *inverses of one another modulo m* if $\tilde{a}a \equiv 1 \pmod{m}$.

There is a subtle point hidden in the phrase *inverse of modulo m*. By inverse of a modulo m we in fact mean an inverse of $[a]_m$ and not of a as a simple integer. We learn of the inverse of $[a]_m$ by taking a as its representative and solving the appropriate linear congruence in the integers finding a solution say $\tilde{a} \in \mathbb{Z}$ and then claim that $[\tilde{a}]_m$ is the inverse of $[a]_m$.

Example 6.36 What is the inverse of 7 modulo 31? We start with the equation $7x \equiv 1 \pmod{31}$. Solving this linear congruence we find that all solutions x to this equation must satisfy $x \equiv 9 \pmod{31}$. This means that the inverse of the class $7 \pmod{31}$ is the class $9 \pmod{31}$. It is not the case that 7 is the inverse of 9 in the integers.

Example 6.37 As $(5, 10) \neq 1$, 5 has no inverse modulo 10.

The following example demonstrates the usefulness of modular inverses.

Example 6.38 Solve $16x \equiv 9 \pmod{35}$ for x. We start by finding the modular inverse of $[16]_{35}$. As $(35, 16) = 1$, then $\overline{16}$ has an inverse modulo 35. The first two iterations of the Euclidean algorithm yield

$$35 = 2 \cdot 16 + 3 \text{ and } 16 = 5 \cdot 3 + 1.$$

Then

$$1 = 16 - 5 \cdot 3 = 16 - 5 \cdot (35 - 2 \cdot 16) = 11 \cdot 16 - 5 \cdot 35.$$

Then

$$11 \cdot 16 \equiv 1 + 5 \cdot 35 \equiv 1 \pmod{35}$$

implying that $[11]_{35}$ is the inverse of $[16]_{35}$.

Now that we have the modular inverse of $[16]_{35}$ we return to the modular equation $16x \equiv 9 \pmod{35}$. Multiplying both sides by 11 we arrive at

$$11 \cdot 16x \equiv 9 \cdot 11 \equiv 29 \pmod{35}$$

which we can write as

$$x \equiv 29 \pmod{35}$$

Generalising the last example, consider the equation $ax \equiv b \pmod{m}$ and multiply both of its sides with the inverse of a modulo m, namely $\tilde{a}$, and assuming one exists. We then get $\tilde{a}(ax) \equiv (\tilde{a}a)x \equiv \tilde{a}b \pmod{m}$ so that $x \equiv \tilde{a}b \pmod{m}$.

A corollary of Theorem 6.28 is the following.

Corollary 6.39 *Let p be a prime. Then for every $a \in [1, p-1]$ has an inverse modulo p.*

In Definition 6.35 we do not require that $a \neq \tilde{a}$. According to this definition if $a^2 \equiv 1 \pmod{m}$ then a is its own inverse modulo m. Consider for instance the integer 6 which satisfies $6 \equiv 1 \pmod{5}$. Note that $36 = 7 \cdot 5 + 1$ so that $36 \equiv 1 \pmod{5}$. We reach that 6 is its own inverse modulo 5. The following lemma aids in classifying when an integer is its own inverse.

The following lemma asserts that only 1 and $p - 1$ are their own inverses modulo p where p is a prime.

Lemma 6.40 *Let $a \in \mathbb{Z}$ and let p be a prime. Then a is its own inverse modulo p if and only if $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.*

Proof. Assume first that $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$. Then $a^2 \equiv 1 \pmod{p}$ in both cases so that a is its own inverse modulo p by definition. Assume second that a is its own inverse modulo p. Then $a^2 \equiv 1 \pmod{p}$ so that $p \mid a^2 - 1$. As $a^2 - 1 = (a-1)(a+1)$ we have that $p \mid a - 1$ or $p \mid a + 1$. In the former case $a \equiv 1 \pmod{m}$. In the latter case $a \equiv -1 \pmod{m}$. ■

In this last proof note that if $p = 1$ then $2 \mid a - 1$ and $2 \mid a + 1$ can occur simultaneously. The proof is remains intact as $-1 =\equiv 1 \pmod{2}$ so in fact there is a single case for $p = 2$. The following result shows that the behaviour seen in Lemma 6.40 persists also for powers of primes p^k as long as $p > 2$.

Lemma 6.41 *Let $p \geq 3$ be prime, let $k \in \mathbb{Z}^+$, and let $a \in \mathbb{Z}$. Then a is its own inverse modulo p^k if and only if $a \equiv \pm 1 \pmod{p^k}$.*

Proof. Instead of proving an *if and only if* statement in the traditional sense (as we did in Lemma 6.40) let us phrase the problem as a congruence problem. This comes in the following form. We seek all the numbers x satisfying $x^2 \equiv 1 \mod p^k$. We will show that this quadratic congruence has precisely two solutions, namely $x \equiv \pm 1 \pmod{p^k}$.

If $x^2 \equiv 1 \pmod{p^k}$ then $p^k \mid x^2 - 1 = (x-1)(x+1)$. As the difference between $x + 1$ and $x - 1$ is 2 and as $p \geq 3$ then p, and consequently p^k, can divide precisely one of these terms (recall that amongst 3 consecutive numbers only one is a multiple of 3)[3]. If $p^k \mid x - 1$ we have that $x \equiv 1 \pmod{p}$. If $p^k \mid x + 1$ we have that $x \equiv -1 \pmod{p}$. ■

Lemma 6.41 left the case of $p = 2$ unanswered. We shall deal with this case below.

Example 6.42

1. Inverses modulo 3:

Class	0 (mod 3)	1 (mod 3)	2 (mod 3)
Inverse	None	1 (mod 3)	2 (mod 3)

2. Inverses modulo 5:

Class	0 (mod 5)	1 (mod 5)	2 (mod 5)	3 (mod 5)	4 (mod 5)
Inverse	None	1 (mod 5)	3 (mod 5)	2 (mod 5)	4 (mod 5)

3. Inverses modulo 7:

Class	0 (mod 7)	1 (mod 7)	2 (mod 7)	3 (mod 7)	4 (mod 7)	5 (mod 7)	6 (mod 7)
Inverse	None	1 (mod 7)	4 (mod 7)	5 (mod 7)	2 (mod 7)	3 (mod 7)	6 (mod 7)

At this stage we are only capable in determining the inverse of an $a \in [1, p-1]$ modulo a prime p by solving the related linear congruence. In the sequel we shall prove the so called *Euler's theorem* a corollary of which is that for an odd prime p

$$a \cdot a^{p-2} \equiv 1 \pmod{p} \tag{6.43}$$

holds for every $a \in [1, p-1]$. That is a^{p-2} is the inverse of a modulo p.

[3] This is precisely the point where the proof fails for $p = 2$ as for $p = 2$ we may have $p \mid x - 1$ and $p \mid x + 1$ simultaneously.

Example 6.44 What is the inverse of 3 (mod 11)? We seek $3^{11-2} \equiv 3^9 \pmod{11}$. We start by noticing that $27 = 3^3 \equiv 5 \pmod{11}$. Then:

$$\begin{aligned}
3^4 &\equiv 5 \cdot 3 \equiv 15 \equiv 4 \pmod{11} \\
3^5 &\equiv 3 \cdot 4 \equiv 12 \equiv 1 \pmod{11} \\
3^6 &\equiv 3 \pmod{11} \\
3^7 &\equiv 9 \pmod{11} \\
3^8 &\equiv 27 \equiv 5 \pmod{11} \\
3^9 &\equiv 3 \cdot 5 \equiv 15 \equiv 4 \pmod{11}.
\end{aligned}$$

The inverse of 3 (mod 11) is 4 (mod 11).

Example 6.45 The last example required quite a bit of effort just to find a single inverse element modulo 11. Let us now demonstrate an easier way of finding all inverse pairings modulo 11. We may ignore 1 (mod 11) and 10 (mod 11) as these are their own inverses. For the rest of the classes between 2 and 9 we are looking for pairs of numbers whose multiplication gives rise to a multiple of 11 plus 1 as follows.

The first multiple of 11 is 11 itself. Here we note that

$$2 \cdot 6 \equiv 12 \equiv 1 \pmod{11} \text{ and } 3 \cdot 4 \equiv 12 \equiv 1 \pmod{11},$$

so 2 (mod 11) and 6 (mod 11) are inverses of one another as well as 3 (mod 11) and 4 (mod 11). To find the inverse of 5 (mod 11) we look for a multiple of 11 closet to a multiple of 5. Here we have that $5 \cdot 9 \equiv 45 \equiv 1 \pmod{11}$ so 5 (mod 11) and 9 (mod 11) are inverses of one another. At this point we are left with 7 (mod 11) and 8 (mod 11) so we know these are inverses of one another. Indeed, $7 \cdot 8 \equiv 56 \equiv 1 \pmod{11}$.

Inverses are sometimes useful in tackling quadratic congruences. Prior to seeing this let us recall that if $a \in \mathbb{R}$, then an expression $x^2 + ax$ can be *completed into a square* if $(a/2)^2$ is added for indeed

$$x^2 + ax + (a/2)^2 = (x + a/2)^2.$$

This completion into a square can be done in the modular world as long as $\overline{2}$ has an inverse. Indeed, let us consider the equation $x^2 + ax$ in the modular setting, specifically modulo m, and assuming that $\overline{2}$ has an inverse modulo m denoted $\tilde{2}$. Then we may write

$$a \equiv 2 \cdot \tilde{2} \cdot a \pmod{m}$$

leading us to the equality

$$x^2 + ax + (\tilde{2} \cdot a)^2 = (x + \tilde{2} \cdot a)^2$$

that we would like to consider in the modular setting. We illustrate this point in the following example.

Example 6.46 Solve the congruence $x^2 + 3x + 9 \equiv 0 \pmod{13}$ for x. Let us first subtract $[9]_{13}$ from both sides as to have $x^2 + 3x \equiv -9 \equiv 4 \pmod{13}$. Next, we complete the square on the left hand side. The inverse of $[2]_{13}$ is $[7]_{13}$ and thus we add $(7 \cdot 3)^2 \equiv 8^2 \equiv 12 \pmod{13}$ to both sides as

to reach

$$\begin{aligned} x^2 + 3x &\equiv 4 \pmod{13} \\ x^2 + 3x + (7 \cdot 3)^2 &\equiv 4 + (7 \cdot 3)^2 \pmod{13} \\ (x + 7 \cdot 3)^2 &\equiv 4 + 12 \pmod{13} \\ (x + 8)^2 &\equiv 3 \pmod{13}. \end{aligned}$$

A rather tedious and annoying inspection of all congruence classes modulo 13 reveals that precisely two of them square to $[3]_{13}$. These are $[4]_{13}$ and $[-4]_{13}$, where the latter is also known as $[9]_{13}$. This yields that either $x + 8 \equiv 4 \pmod{13}$ in which case we can take $x = [9]_{13}$, or $x + 8 \equiv 9 \pmod{13}$ in which case $x = [1]_{13}$ is the answer.

The following theorem frames the entires above discussion.

Theorem 6.47 *Let $n \geq 2$ be an integer. The following are equivalent.*

(i) For every $a \in [n-1]$, the class $[a]_n$ has an inverse.

(ii) If $ab \equiv 0 \pmod{n}$ then either $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$.

(iii) n is prime.

Proof.

$(i) \implies (ii)$: Assuming (i) is true, let $ab \equiv 0 \pmod{n}$. We may assume that $a \not\equiv 0 \pmod{n}$; for otherwise we are done. Then by (i), $[a]_n$ has an inverse, namely $\tilde{a}$. Then

$$\underbrace{\tilde{a} \cdot a}_{\equiv 1 \pmod{n}} \cdot b \equiv \tilde{a} \cdot 0 \equiv 0 \pmod{n}$$

implying that $b \equiv 0 \pmod{n}$ as required.

$(ii) \implies (iii)$: If n is composite then we may write $n = a \cdot b$ where $2 \leq a, b < n$. Then $a \cdot b \equiv n \equiv 0 \pmod{n}$ so that, by (ii), at least one of a and b is congruent to 0 modulo n. This contradicts the assumption that $2 \leq a, b < n$.

$(iii) \implies (i)$: If n is prime then $ax \equiv 1 \pmod{n}$ has a unique solution for any $a \in [n-1]$ by Theorem 6.28.

■

6.2.1.1 Inverses modulo 2^k

Lemma 6.41 left the case $p = 2$ unanswered. In this section we remedy this situation and consider inverses modulo 2^k. Suppose, first, that $k = 1$. As $-1 \equiv 1 \pmod{2}$ every odd $a \in \mathbb{Z}$ is its own inverse modulo 2. Which class then is the inverse of the congruence class $0 \pmod{2}$? There is none. For instance, the inverse of $2k$, $k \in \mathbb{Z}$, modulo 2 would be an x satisfying $(2k)x \equiv 1 \pmod{2}$. As $(2k, 2) = 2 \not| 1$ this equation has no solutions modulo m.

From this discussion we have that the sole solution to $x^2 \equiv 1 \pmod{2}$ is $x \equiv \pm 1 \pmod{2}$ (recall that $-1 \equiv 1 \pmod{2}$ so $\pm 1 \pmod{2}$ is a single class). Let us summarise. The equation $x^2 \equiv 1 \pmod{2}$ has one solution modulo 2. The equation $x^2 \equiv 1 \pmod{p^k}$ with $p \geq 3$ and $k \geq 1$ has two incongruent solutions. We shall now see that the equation $x^2 \equiv 1 \pmod{2^2}$ has two incongruent solutions modulo 4, and that $x^2 \equiv 1 \pmod{2^k}$, $k \geq 3$ has more than two incongruent solutions modulo 2^k.

Lemma 6.48 *The equation $x^2 \equiv 1 \pmod{2^k}$ has*

1. *four incongruent solutions modulo 2^k if $k \geq 3$; namely $\pm 1 \pmod{2^k}$ and $\pm(1+2^{k-1}) \pmod{2^k}$,*
2. *two incongruent solutions if $k = 2$, namely $\pm 1 \pmod 4$,*
3. *and one solution if $k = 1$, namely $\pm 1 \pmod 2$.*

Proof. Let $k \geq 2$. We dealt with the case $k = 1$ prior to the statement of the lemma and thus omitted here. The congruence $x^2 \equiv 1 \pmod{2^k}$, $k \geq 1$, implies that $x^2 - 1 = (x-1)(x+1) \equiv 0 \pmod{2^k}$. As $(x-1)(x+1)$ is equal to a multiple of of 2^k this number is even this together with the fact that $x-1$ and $x+1$ have the same parity it follows that both $x-1$ and $x+1$ must be even. As the difference between $x-1$ and $x+1$ is 2 it must be that at most one of these is divisible by 4; the other can be divided by 2 at most once. That is, one of these numbers is a multiple of 4 and the other is a multiple of 2 but not a multiple of 4. Two cases are then possible:

(i) $2 \mid x+1$ and $2^{k-1} \mid x-1$, or

(ii) $2 \mid x-1$ and $2^{k-1} \mid x+1$

From these two possibilities we infer that

$$x = 2^{k-1}y \pm 1, \ y \in \mathbb{Z}. \tag{6.49}$$

Put another way:

$$x \equiv \pm 1 \pmod{2^{k-1}} \tag{6.50}$$

For each possible value of k we now determine how many incongruent solutions there are modulo 2^k (not modulo 2^{k-1}!!!). For $k = 2$ (6.49) reads as $x = 2y+1, y \in \mathbb{Z}$. So all solutions are odd. Modulo 4 these solutions are partitioned across two congruence classes $1 \pmod 4$ and $3 \pmod 4$. The latter class we note is the same as $-1 \pmod 4$.

For $k \geq 3$ we see four incongruent solutions namely $-1 \pmod{2^k}$,$1 \pmod{2^k}$,$2^{k-1}-1 \pmod{2^k}$, and $2^{k-1}+1 \pmod{2^k}$. These we generate from letting $y \in \{0,1\}$. Any solution coming from a different value of y is congruent to one of the four mentioned. Indeed for a positive y we note that if y is even, i.e., $y = 2z$ for some $z \in \mathbb{Z}$ then $2^{k-1} \cdot 2z \pm 1 \equiv \pm 1 \pmod{2^k}$. If y is odd and ≥ 3, i.e., $y = 2z+1 \geq 3$ for some $z \in \mathbb{Z}$ then

$$2^{k-1}y \pm 1 = (y-1)2^{k-1} + 2^{k-1} \pm 1 = 2^{k-1} \cdot 2z + 2^{k-1} \pm 1 \equiv 2^{k-1} \pm 1 \pmod{2^k}$$

where $k \in \mathbb{Z}$. The treatment of a negative y is similar.

Note that the argument for $k \geq 3$ does not apply when $k = 2$. Indeed, for $k = 2$ the classes $-1 \pmod{2^k}$,$1 \pmod{2^k}$,$2^{k-1}-1 \pmod{2^k}$, and $2^{k-1}+1 \pmod{2^k}$ form precisely the two classes $\pm 1 \pmod 4$. ■

§6.3. Combining moduli: prelude to the Chinese remainder theorem

This section serves as a prelude to § 6.4 in which we introduce the fundamental tool called the *Chinese remainder theorem*. We start off with the following result.

Proposition 6.51 *Let $m_1, \ldots, m_k$ be positive integers. If $a \equiv b \pmod{m_i}$ for every $i \in [k]$ then $a \equiv b \pmod{lcm(m_1, \ldots, m_k)}$.*

Proof. By assumption $m_i \mid a - b$ for every $i \in [k]$. Then $a - b$ is a common multiple of $(m_i)_{i \in [k]}$ and thus $lcm(m_1, \ldots, m_k) \mid a - b$ and the claim follows. ■

If $m_1, \ldots, m_k$ are relatively prime then $lcm(m_1, \ldots, m_k) = m_1 \cdot m_2 \cdot \cdots \cdot m_k$. Indeed, by Theorem 4.71, $lcm(m_1, m_2) = m_1 m_2/(m_1, m_2)$. This extends to $lcm(m_1, \ldots, m_k) = (m_1 \cdot m_2 \cdot \cdots \cdot m_k)/(m_1, \ldots, m_k)$ (by induction). This fact together with Proposition 6.51 yields the following.

Corollary 6.52 *Let $m_1, \ldots, m_k$ be positive integers that are pairwise co-prime. If $a \equiv b \pmod{m_i}$ for every $i \in [k]$ then $a \equiv b \pmod{m_1 \cdot m_2 \cdot \cdots \cdot m_k}$.*

Example 6.53 Suppose we are given two equations $x \equiv 1 \pmod 3$ and $x \equiv 1 \pmod 4$. Any such integer x must then satisfy $x \equiv 1 \pmod{12}$.

For every $i \in [k]$ there exists a $k_i \in \mathbb{Z}$ such that $\text{lcm}(m_1, \ldots, m_k) = k_i m_i$. Having $\text{lcm}(m_1, \ldots, m_k) \mid a - b$ then implies that $k_i m_i \mid a - b$ for every $i \in [k]$. That is for every $i \in [k]$ there exists an integer ℓ_i such that $a - b = \ell_i k_i m_i$. In particular, $m_i \mid a - b$. Then

$$\text{lcm}(m_1, \ldots, m_k) \mid a - b \iff m_i \mid a - b, \forall i \in [k].$$

We may strengthen Proposition 6.51 and Corollary 6.52 to read as follows.

Proposition 6.54 *Let $m_1, \ldots, m_k$ be positive integers.*

1. $$a \equiv b \pmod{m_i}, \ \forall i \in [k] \iff a \equiv b \pmod{lcm(m_1, \ldots, m_k)}.$$

2. *If the integers $m_1, \ldots, m_k$ are pairwise co-prime then*

$$a \equiv b \pmod{m_i}, \ \forall i \in [k] \iff a \equiv b \pmod{m_1 \cdots m_k}).$$

Example 6.55 If $x \equiv 5 \pmod{12}$ then as $\text{lcm}(3, 4) = 12$ then $x \equiv 5 \pmod 3$ and $x \equiv 5 \pmod 4$. The last two congruences can be written $x \equiv 2 \pmod 3$ and $x \equiv 1 \pmod 4$

Let us generalise what we have seen in Example 6.55. Suppose m_1, m_2 are two distinct integers and that $x \equiv r \pmod{\text{lcm}(m_1, m_2)}$. Then $x = \text{lcm}(m_1, m_2) \cdot N + r$. Then

$$x = k_1 m_1 + r \text{ and } x = k_2 m_2 + r$$

as $k_1 m_1 = \text{lcm}(m_1, m_2) = k_2 m_2$ for some two integers k_1 and k_2. We may write $r = \ell_1 m_1 + (r \bmod m_1)$ and $r = \ell_2 m_2 + (r \bmod m_2)$ for some $\ell_1, \ell_2 \in \mathbb{Z}$ to arrive at

$$x = (k_1 + \ell_1) m_1 + (r \bmod m_1) \text{ and } x = (k_2 + \ell_2) m_2 + (r \bmod m_2).$$

We have just established the following.

Lemma 6.56 *Let m_1, m_2 be two distinct integers and let*

$$x \equiv r \pmod{\operatorname{lcm}(m_1, m_2)}.$$

Then

$$x \equiv (r \bmod m_1) \pmod{m_1} \quad \textit{and} \quad x \equiv (r \bmod m_2) \pmod{m_2}$$

Still Example 6.55 raises a subtle point. Given that $x \equiv 2 \pmod 3$ and $x \equiv 1 \pmod 4$ we cannot use Corollary 4.71 to deduce that $x \equiv 5 \pmod{12}$. Put another way, is there a converse to Lemma 6.56? One way to resolve this is to appeal to a stronger tool called the *Chinese remainder theorem* (see Theorem 6.64). To gain appreciation for this stronger tool let us have the following discussion.

Suppose $x \equiv a_1 \pmod{m_1}$ and $x \equiv a_2 \pmod{m_2}$ are given. Then we may write

$$x = k_1 m_1 + a_1 \text{ and } x = k_2 m_2 + a_2.$$

As we seek to "reverse" Lemma 6.56 we take interest in $\operatorname{lcm}(m_1, m_2)$ and write

$$k_1 m_1 = \ell_1 \operatorname{lcm}(m_1, m_2) + b_1 \text{ and } k_2 m_2 = \ell_2 \operatorname{lcm}(m_1, m_2) + b_2$$

as to obtains

$$x = \ell_1 \operatorname{lcm}(m_1, m_2) + b_1 + a_1 \text{ and } x = \ell_2 \operatorname{lcm}(m_1, m_2) + b_2 + a_2.$$

Now we realise the difficulty in attaining a converse for Lemma 6.56; indeed, to attain such a goal we now have to prove that

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{\operatorname{lcm}(m_1, m_2)}.$$

We shall address this point upon proving Theorem 6.64 below for m_1 and m_2 co-prime.

§6.4. The Chinese remainder theorem

For $i \in [r]$ let $a_i, b_i \in \mathbb{Z}$ and let $m_i \in \mathbb{Z}^+$. We consider the problem of finding solutions for a system of linear congruences:

$$a_1 x \equiv b_1 \pmod{m_1}, a_2 x \equiv b_2 \pmod{m_2}, \ldots, a_r x \equiv b_r \pmod{m_r}.$$

The system is not soluble unless $d_i = (a_i, m_i) \mid b_i$ for every $i \in [r]$. Rewriting this system by substituting $a_i = d_i \cdot a_i'$, $m_i = d_i \cdot n_i$, and $b_i = d_i \cdot b_i'$ we get

$$d_1 \cdot a_1' x \equiv d_1 \cdot b_1' \pmod{d_1 \cdot n_1}, \ldots, d_r \cdot a_r' x \equiv d_r \cdot b_r' \pmod{d_r \cdot n_r}.$$

We may then cancel d_i for each $i \in [r]$ in each congruence of the system and obtain the system

$$a_1' x \equiv b_1' \pmod{n_1}, \ldots, a_r' x \equiv b_r' \pmod{n_r}. \tag{6.57}$$

At this point let us note the following.

Lemma 6.58 *Let $a, b, c \in \mathbb{Z}$ and let $m \in \mathbb{Z}^+$. Then $a \equiv b \pmod m$ if and only if $a \cdot c \equiv b \cdot c \pmod{m \cdot c}$.*

Proof. If $mc \mid c(a-b)$ then $m \mid a-b$. Conversely, if $m \mid a-b$ then $a-b = km$ for some $k \in \mathbb{Z}$. Then $c(a-b) = k(mc)$ so that $mc \mid c(a-vb)$. ■

Example 6.59 Consider $4 \equiv 7 \pmod 3$. On the one hand we see that $4 \cdot 2 \equiv 8 \equiv 2 \pmod{3 \cdot 2}$. On the other $7 \cdot 2 \equiv 14 \equiv 2 \pmod{3 \cdot 2}$ so that $4 \cdot 2 \equiv 7 \cdot 2 \pmod{3 \cdot 2}$.

By Lemma 6.58, any solution in $\mathbb{Z}$ that we find for the equation $a_i'x \equiv b_i' \pmod{n_i}$ is also a solution in $\mathbb{Z}$ to the original equation $a_i' \cdot d_i x \equiv b_i' d_i \pmod{n_i d_i}$ and vice versa. That is the set of solutions in $\mathbb{Z}$ of the system (6.57) is exactly the same to that of the original system.

The new system (6.57) is of great appeal to us as in this this system $(a_i', n_i) = 1$ for every $i \in [r]$ implying that for each $i \in [r]$ the ith linear congruence has a unique solution modulo n_i namely $x \equiv c_i \pmod{n_i}$. However, we recall that the original ith equation had d_i incongruent solutions modulo m_i. It seems that something strange is taking place. In $\mathbb{Z}$ we have agreed (due to Lemma 6.58) that no solutions were lost between the systems of equations so how come modulo n_i we have a single solution yet modulo m_i we have d_i solutions?

Example 6.60 Consider the single equation $2x \equiv 2 \pmod 6$. We are suggesting to replace this equation with $x \equiv 1 \pmod 3$. For the latter equation there is a single equation namely $[1]_3$. Note now though that the integers $[1]_3$ are split across two congruences classes modulo 6 and not just one. To see this note that all multiples of 3 (i.e., $[0]_3$) coincide with the disjoint union $[0]_6 \cup [3]_6$. Hence $[1]_3 = [1]_6 \cup [4]_6$.

We have just seen an example to how the representation of the $\mathbb{Z}$-solution modulo m_i can differ from their representation modulo n_i. For instance if the ith equation was our single equation, then modulo n_i we require a single congruence class to represent all solution. These then split into d_i classes modulo m_i.

We may thus reduce our attention to the system

$$x \equiv c_1 \pmod{n_1}, \ldots, x \equiv c_r \pmod{n_r}. \tag{6.61}$$

Every solution of the system (6.61) is a solution of the original system. However, it remains unclear as to how we pass from the system (6.57) to (6.61). In the worst case we would have to solve each equation in (6.57) to get its unique solution and then collect all those solutions in order to form a system of the form (6.61). However, often it will be the case that we will be lucky and simple manipulations can be used to generate (6.61). For instance, given

$$17x \equiv 9 \pmod 3$$

we may replace by $x \equiv 0 \pmod 3$. Indeed, $9 \equiv 0 \pmod 3$ and to have $3 \mid 17x$ it must be that $3 \mid x$ as 3 is prime and $3 \nmid 17$.

In this lecture we shall introduce a theorem called the *Chinese remainder theorem* that will be able to handle systems of the (6.61) providing that the numbers n_i, $i \in [r]$, are pairwise co-prime.

Example 6.62 One way to solve such a system is iteratively as follows. Suppose we are handed the system:

$$\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 2 \pmod 6 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

In this case the first equation is easy as it must be that $x = 5t + 1$, $t \in \mathbb{Z}$. Proceeding to the second we see that we need to require

$$5t + 1 \equiv 2 \pmod 6.$$

This is yet another linear congruence with t as its variable. Solving this we get $t = 6u + 5$, $u \in \mathbb{Z}$

(i.e., $t \equiv 5 \pmod 6$). With this solution to t we get that

$$x = 5(6u + 5) + 1 = 30u + 26, \ u \in \mathbb{Z}.$$

Considering the third equation we see that we must require

$$30u + 26 \equiv 3 \pmod 7$$

which is yet another linear congruence that we need to solve.

We can get the impression that solving such systems can be a fairly tedious job. Fortunately, the Chinese remainder theorem takes some of this "pain" away. We shall require the following in our proof of the Chinese remainder theorem.

Lemma 6.63 *Let $n_1, \ldots, n_r$ be pairwise relatively prime positive integers. Let $M = \prod_i n_i$ and let $M_k = M/n_k$. Then $(M_k, n_k) = 1$.*

Proof. The assumption that $n_1, \ldots, n_r$ are pairwise co-prime implies that M_k shares no common prime factors with n_k for every $k \in [r]$. ■

We arrive at the Chinese remainder theorem.

Theorem 6.64 (The Chinese remainder theorem)
Let $n_1, \ldots, n_r$ be pairwise relatively prime positive integers. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\cdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

has a unique solution modulo $M = \prod_i n_i = \operatorname{lcm}(n_1, \ldots, n_r)$.

Proof. The proof consists of two parts; existence of a solution to the system and uniqueness of this solution.

Existence. For $k \in [r]$ put $M_k = M/n_k$. By Lemma 6.63 $(M_k, n_k) = 1$ so that $M_k \cdot y \equiv 1 \pmod{n_k}$ has a unique solution namely the inverse of M_k modulo n_k denoted y_k. Put

$$x = \sum_{i=1}^{r} a_i \cdot M_i \cdot y_i. \tag{6.65}$$

Then x is a solution to the system. To see this, fix $k \in [r]$; we show that $x \equiv a_k \pmod{n_k}$. Fix $j \in [r] \setminus \{k\}$ and note that $n_k \mid M_j$ it follows that $n_k \mid a_j \cdot M_j \cdot y_j$ as well. This establishes that every summand in (8.4) apart from the kth summand are congruent to $0 \pmod{n_k}$ so that

$$x \equiv a_k \cdot M_k \cdot y_k \pmod{n_k}.$$

As $M_k \cdot y_k \equiv 1 \pmod{n_k}$ we reach $x \equiv a_k \pmod{n_k}$ as required.

Uniqueness. Let x_0 and x_1 be two solutions modulo M for the system. That is $x_0 \equiv x_1 \equiv a_k \pmod{n_k}$ for every $k \in [r]$. Then $n_k \mid x_0 - x_1$ for every $k \in [r]$. Then $M \mid x_0 - x_1$, by Corollary 5.22 so that $x_0 \equiv x_1 \pmod M$. ■

6.4.1 *Applying the Chinese remainder theorem*

Example 6.66 Is there an integer that upon division by 3 leaves a remainder of 1, and upon division by 5 leaves a remainder of 2, and upon division by 7 leaves a remainder of 3? Put another way we seek an $x \in \mathbb{Z}$ satisfying

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 5 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

simultaneously.

We follow the proof of Theorem 6.64. Put $n_1 = 3$, $n_2 = 5$, and $n_3 = 7$. Set $M = 3 \cdot 5 \cdot 7 = 105$ and then let $M_1 = 105/3 = 35$, $M_2 = 105/5 = 21$, and $M_3 = 105/7 = 15$. The next step is to find y_1, y_2, and y_3 where y_i is the inverse of M_i modulo n_i for $i \in [3]$. That is we need to solve each of the linear congruences

$$\begin{aligned} 35 \cdot y_1 &\equiv 1 \pmod 3 \\ 21 \cdot y_2 &\equiv 1 \pmod 5 \\ 15 \cdot y_3 &\equiv 1 \pmod 7. \end{aligned}$$

To find y_1 note that $35 \cdot y_1 = 33 \cdot y_1 + 2y_1$ and that $33 \cdot y_1 \equiv 0 \pmod 3$. Hence we may then replace $35 \cdot y_1 \equiv 1 \pmod 3$ with $2y_1 \equiv 1 \pmod 3$. Then y_1 is the inverse of $2 \pmod 3$ which is $2 \pmod 3$; that is $y_1 \equiv 2 \pmod 3$. For y_2 we note that $21y_2 \equiv 20y_2 + y_2 \equiv y_2 \equiv 1 \pmod 5$; so that $y_2 \equiv 1 \pmod 5$. For y_3 we have $15y_3 \equiv 14y_3 + y_3 \equiv y_3 \equiv 1 \pmod 7$; so $y_3 \equiv 1 \pmod 7$.

By Theorem 6.64

$$x \equiv \sum_i a_i M_i y_i = 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \equiv 157 \equiv 52 \pmod{105}$$

is our solution to the system.

Example 6.67 Find three consecutive numbers each having a square factor. Noting that $2^2, 3^2$, and 5^2 are pairwise co-prime we may try to find an integer a satisfying

$$a \equiv 0 \pmod{2^2},\ a + 1 \equiv 0 \pmod{3^2},\ a + 2 \equiv 0 \pmod{5^2};$$

isolating a in each equation we get the system

$$a \equiv 0 \pmod{2^2}\ a \equiv -1 \pmod{3^2},\ a \equiv -2 \pmod{5^2}.$$

At this point the Chinese remainder theorem asserts that this system has a unique solution modulo $4 \cdot 9 \cdot 25 = 900$. In particular we would get that $a \equiv 548 \pmod{900}$ upon solving this system as shown above. Consequently, we may take $a = 548$ (or any other number in the same congruence class of 548 modulo 900) and let $a + 1 = 549$ and $a + 2 = 550$.

§6.5. Two linear congruences with two variables

Theorem 6.68 *Let a, b, c, d, r and $s \in \mathbb{Z}$. Let $n \in \mathbb{Z}^+$. The system of linear congruences*

$$ax + by \equiv r \pmod{n}$$
$$cx + dy \equiv s \pmod{n}$$

has a unique solution modulo n whenever $gcd(ad - bc, n) = 1$.

Proof. Let us multiply the first congruence of the system by d, the second congruence by b, and subtract the lower result from the upper. These calculations yield

$$(ad - bc)x \equiv dr - bs \pmod{n} \tag{6.69}$$

The assumption $gcd(ad - bc, n) = 1$ ensures that the congruence

$$(ad - bc)z \equiv 1 \pmod{n}$$

has a unique solution; denote this solution by t. When congruence (6.69) is multiplied by t, we obtain

$$x \equiv t(dr - bs) \pmod{n}$$

A value for y is found by a similar elimination process. That is, multiply the first congruence of the system by c, the second one by a, and subtract to end up with

$$(ad - bc)y \equiv as - cr \pmod{n} \tag{6.70}$$

Multiplication of this congruence by t leads to

$$y \equiv t(as - cr) \pmod{n}$$

A solution of the system is now established. ■

§6.6. Divisibility Criteria

Theorem 6.71 *Let*

$$P(x) = \sum_{k=0}^{m} c_k x^k$$

be a polynomial function of x with integral coefficients c_k. If $a \equiv b \pmod{n}$, then $P(a) \equiv P(b) \pmod{n}$.

Proof. Since $a \equiv b \pmod{n}$ then $a^k \equiv b^k \pmod{n}$ for $k = 0, 1, ..., m$. Therefore,

$$c_k a^k \equiv c_k b^k \pmod{n}$$

Adding these $m + 1$ congruences, we obtain

$$\sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k \pmod{n}.$$

Equivalently:

$$P(a) \equiv P(b) \pmod{n}.$$

■

Corollary 6.72 *If a is a solution of $P(x) \equiv 0 \pmod{n}$ and $a \equiv b \pmod{n}$, then b is also a solution.*

Proof. From Theorem 6.71, it is known that $P(a) \equiv P(b) \pmod{n}$. Hence, if a is a solution of $P(x) \equiv 0 \pmod{n}$, then $P(a) \equiv P(b) \equiv 0 \pmod{n}$, making b a solution. ■

Lemma 6.73 (Divisibility by 9 criteria)
Let $N = a_m 10^m + a_{m-1}10^{m-1} + ... + a_1 10 + a_0$ be the decimal expansion of the positive integer N, $0 \leq a_k < 10$, and let $S = a_m + a_{m-1} + ... + a_1 + a_0$. Then $9 \mid N$ if and only if $9 \mid S$.

Proof. Consider the polynomial $P(x) = \sum_{k=0}^{m} a_k x^k$ with integral coefficients. The key observation is that $10 \equiv 1 \pmod{9}$, then by Theorem 6.71, $P(10) \equiv P(1) \pmod{9}$. But $P(10) = N$ and $P(1) = a_m + a_{m-1} + ... + a_1 + a_0 = S$, so that $N \equiv S \pmod{9}$. It follows that $N \equiv 0 \pmod{9}$ if and only if $S \equiv 0 \pmod{9}$. ■

Lemma 6.74 (Divisibility by 11 criteria)
Let $N = a_m 10^m + a_{m-1}10^{m-1} + ... + a_1 10 + a_0$ be the decimal expansion of the positive integer N, $0 \leq a_k < 10$, and let $T = (-1)^m a_m + (-1)^{m-1} a_{m-1} + ... - a_1 + a_0$. Then $11 \mid N$ if and only if $11 \mid T$.

Proof. Consider the polynom $P(x) = \sum_{k=0}^{m} a_k x^k$ with integral coefficients. The key observation is that $10 \equiv -1 \pmod{11}$, then by Theorem 6.71, $P(10) \equiv P(-1) \pmod{11}$. But $P(10) = N$ and $P(-1) = (-1)^m a_m + (-1)^{m-1} a_{m-1} + ... - a_1 + a_0 = T$, so that $N \equiv T \pmod{11}$. It follows that $N \equiv 0 \pmod{11}$ if and only if $T \equiv 0 \pmod{11}$.

■

§6.7. Modular exponentiation

Consider the task of writing a computer program that upon receiving three integers namely a, b, and n as inputs (naturally all are given in their binary representation) outputs the least positive residue of a^b modulo n to which we shall refer here simply as $a^b \pmod{n}$. We immediately encounter a serious problem; what should we do on an input $a = 2$, $b = 644$, and $n = 645$? That is how shall we compute the least positive residue of 2^{644} modulo 645? Any approach involving explicitly writing the value of 2^{644} in memory is doomed as no modern computer can represent this number let alone do calculations with it. In addition, repeatedly raising to power of a means we have to carry out 644 multiplications a number which is exponential in the number of bits required to represent 644. In this section we present an algorithm that is able to calculate the least positive residue of 2^{644} modulo 645 without the need to represent 2^{644} or any number for that matter that the computer cannot represent. All this is possible due to properties of congruences.

Example 6.75 What is the least positive residue of 2^{644} modulo 645? Surely that first calculating 2^{644} would be rather difficult. Here is an approach also called the *modular exponentiation algorithm* to find this residue while avoiding an explicit calculation of 2^{644}.

Step I. Write $644 = 512 + 128 + 4 = (1010000100)_2$.

Step II. Calculate the least residues of $2, 2^2, 2^4, 2^8, \ldots, 2^{512}$ modulo 645 (we stop at 512 as the next power of 2 exceeds our number 2^{644}). Calculating the least residues of these powers of 2 is

done as follows. We start with

$$2 \equiv 2 \pmod{645};$$

from this point we square and reduce modulo 645 after each squaring as follows:

$$\begin{aligned} 2^2 &\equiv 4 \pmod{645} \\ 2^4 &\equiv 4 \cdot 4 \equiv 16 \pmod{645} \\ 2^8 &\equiv 16 \cdot 16 \equiv 256 \pmod{645} \\ 2^{16} &\equiv 391 \pmod{645} \end{aligned}$$

here we have the first step where the reduction modulo 645 is nontrivial. Here we need to calculate $256^2 = 65536$ and then calculate 65536 (mod 645) which is 391. At first glance it seems that we still have to handle fairly large numbers; however these pale by comparison with 2^{644} and so we are willing to press on.

$$\begin{aligned} 2^{32} &\equiv 16 \pmod{645} \\ 2^{64} &\equiv 256 \pmod{645} \\ 2^{128} &\equiv 391 \pmod{645} \\ 2^{256} &\equiv 16 \pmod{645} \\ 2^{512} &\equiv 256 \pmod{645}. \end{aligned}$$

Step III. Recall now that $644 = 512 + 128 + 4$ (which we noted in the first step) so that $2^{644} = 2^{512} \cdot 2^{128} \cdot 2^4$. Consequently, we may write

$$2^{644} = 2^{512} \cdot 2^{128} \cdot 2^4 \equiv 256 \cdot 391 \cdot 16 = 1,601,536 \equiv 1 \pmod{645}.$$

There are a few points to make here. The first being that we replaced nasty calculations of insanely large numbers by square of numbers that are smaller than 645. This we made sure of by insisting on reducing modulo 645 after each time we square. This is what prevent the number to grow too large. The second point to make here is the connection to the binary expansion of 644. Notice that we only multiplied the least residues of powers of 2 whose corresponding bit in the binary expansion of 644 was 1.

The name of the algorithm is *MOD-EXP* (short for modular exponentiation). Let $b_k, \ldots, b_0$ denote the binary representation of b where b_k is the most significant bit and b_0 is the least significant bit. The algorithm reads as follows.

1. $c \leftarrow 0$.
2. $d \leftarrow 1$.
3. for $i \leftarrow k$ down to 0 do:
   (a) $c \leftarrow 2c$.
   (b) $d \leftarrow d \cdot d \bmod n$.
   (c) if $b_i = 1$ then do:
      i. $c \leftarrow c + 1$.
      ii. $d \leftarrow (d \cdot a) \bmod n$.

4. return d.

Prior to proving that this algorithm is correct (i.e., it in fact does return $a^b \pmod{n}$ we quickly make note of its running time.

Lemma 6.76 *Suppose a, b, and n all have k-bit representations. Then the running time of the algorithm is $O(k^3)$.*

Proof. The algorithm iterates $O(k)$ times and in each iteration performs $O(1)$ arithmetic operations most expensive of which require $O(k^2)$ time. The claim follows. ■

Theorem 6.77 *On in put a, b, n the algorithm MOD-EXP returns $a^b \pmod{n}$.*

In order to prove Theorem 6.77 we prove the following stronger result.

Lemma 6.78 *Prior to the ith iteration of the for loop of the algorithm the following two assertions hold:*

1. *c's binary representation is $b_k, \ldots, b_{i+1}$.*
2. *$d = a^c \pmod{n}$.*

Proof. The proof is by induction on the number of iterations performed by the algorithm. Prior to the first iteration we have $i = k$ so that indeed $b_k, \ldots, b_{i+1}$ is empty and indeed $c = 0$ prior to the first iteration. Also, not that prior to the first iteration $1 = d = a^0 \pmod{n}$.

We proceed to the induction step. Let c' and d' denote the values of the variables c and d at the end of an iteration of the for loop and thus constitute the values of c and d prior to the next iteration. Hence prior to the next iteration we have that the induction hypothesis holds for c' and d' (the current values of c and d).

1. Observe the value of c calculated throughout the next iteration. If $b_i = 0$ (where i is the index of the next iteration) then $c = 2c'$ which consists of simply shifting the representation of c' one bit to the left and adding 0 as the least significant bit. If $b_i = 1$ then $c = 2c' + 1$ which consists of making the above shift left of the representation of c' but now placing 1 in the least significant bit. The assertion for the value of c is thus maintained.

2. Consider the value of d calculated throughout the next iteration. If $b_i = 0$ then

$$d = (d')^2 \pmod{n} = (a^{c'})^2 \pmod{n} = a^{2c'} \pmod{n} = a^c \pmod{n}$$

as $c = 2c'$ in the next iteration if $b_i = 0$. If $b_i = 1$ then

$$d = (d')^2 \cdot a \pmod{n} = (a^{c'})^2 \cdot a \pmod{n} = a^{2c'+1} \pmod{n} = a^c \pmod{n}$$

as $c = 2c' + 1$ in the next iteration if $b_i = 1$.

■

We are now in position to prove Theorem 6.77.

Proof of Theorem 6.77. At the end of the for loop of *MOD-EXP* $i = -1$. Thus by Lemma 6.78 $c = b$ and $d = a^c \pmod{n} = a^b \pmod{n}$ holds. ■

§6.8. Exercises

Exercise 1. Solve the linear congruence $17x \equiv 3 \pmod{2 \cdot 3 \cdot 5 \cdot 7}$.

Exercise 2. Let a, b, k, m be integers such that $k, m > 0$. Suppose that

$$a^k \equiv b^k \pmod{m} \text{ and that } a^{k+1} \equiv b^{k+1} \pmod{m}. \tag{6.79}$$

Then these two assumptions are not enough to imply that $a \equiv b \pmod{m}$. Indeed, take $m = a = 4$ and $b = 2$. Then $4^2 \equiv 2^2 \pmod{4}$ and $4^3 \equiv 2^3 \pmod{4}$ but $4 \not\equiv 2 \pmod{4}$.

What condition would you add to (6.79) so that your condition together with (6.79) would imply that $a \equiv b \pmod{m}$? Prove your answer.

Exercise 3. For $n \geq 1$, use congruence theory to establish each of the following divisibility statement without using induction:

1. $7 | 5^{2n} + 3 \cdot 2^{5n-2}$
2. $27 | 2^{5n+1} + 5^{5n+2}$

Exercise 4. Prove or disprove the following claims.

1. If a is an odd integer, then $a^2 \equiv 1 \pmod{8}$
2. For any $a \in \mathbb{Z}$: a^3 is congruent to $0, 1$, or 6 modulo 7.

Exercise 5. Use the theory of congruences to verify that

$$89 | 2^{44} - 1.$$

Exercise 6. Prove that $41 \mid 2^{20} - 1$.

Exercise 7. Let $K = \sum_{i=1}^{100} i!$. By the Division Algorithm we may write K as $K = 12q + r$ uniquely where $0 \leq r < K$. What is r?

Exercise 8. Find all solutions to the equations:

1. $36x \equiv 8 \pmod{102}$.
2. $5x \equiv 2 \pmod{26}$

Exercise 9. Solve the following linear congruence:

$$17x \equiv 9 \pmod{276}$$

Exercise 10. Solve the following system of linear congruences:

$$\begin{aligned} 7x + 3y &\equiv 10 \pmod{16} \\ 2x + 5y &\equiv 9 \pmod{16} \end{aligned}$$

Exercise 11. Find the solution of the system of congruences:

$$3x + 4y \equiv 5 \pmod{13}$$
$$2x + 5y \equiv 7 \pmod{13}$$

Exercise 12. Find the solution of the system of congruences:

$$5x + 8y \equiv 2 \pmod{11}$$
$$3x + 2y \equiv 1 \pmod{11}$$

Exercise 13. Use the Chinese Remainder Theorem to solve the following system.

$$4x \equiv 5 \pmod{3}$$
$$49x \equiv 3 \pmod{4}$$
$$11x \equiv -9 \pmod{5}$$

Exercise 14. Calculate $5^{110} \pmod{131}$.

Exercise 15. Find all the congruence classes that have a modular inverse modulo 9.

Exercise 16. Compute $19^{53} \pmod{503}$.

Exercise 17.

1. Prove that for any integer a, the units digit of a^2 is $0, 1, 4, 5, 6$ or 9.
2. Prove that for any integer a, $a^2 - a + 7$ ends in one of the digits $3, 7$ or 9.

Exercise 18. Find all incongruent solutions to the following equations.

1. $25x \equiv 15 \pmod{29}$.
2. $6x \equiv 15 \pmod{21}$.

Exercise 19. Prove that if $x \equiv a \pmod{n}$ then either $x \equiv a \pmod{2n}$ or $x \equiv a + n \pmod{2n}$.

Exercise 20. Use congruence theory to establish each of the following divisibility statements for $n \geq 1$ without resorting to induction.

1. $13 \mid 3^{n+2} + 4^{2n+1}$; *Hint:* $3 \equiv 16 \pmod{13}$.
2. $43 \mid 6^{n+2} + 7^{2n+1}$.

Exercise 21. Let n be an integer satisfying $n \equiv 1 \pmod{4}$. What are its possible least positive residues modulo 8?

Exercise 22. Let a and n be positive relatively prime integers. Prove that if $b \equiv a \pmod{n}$ then $(b, n) = 1$.

Exercise 23. Let $0 \leq a, b < n$ be integers. Determine the computational complexity of performing the operation $(a + b) \pmod{n}$.

Exercise 24. Given three integers $0 < a, b < n$; how many bit operations are required in order to solve $ax \equiv b \pmod{n}$?

Exercise 25. The following algorithm is proposed for calculating $a^e \pmod{n}$. Prove that this algorithm is correct and analyse its running time. The input are integers a, e, and n where we assume $e \geq 0$, $n \geq 2$ and furthermore that $0 \leq a < n$ (to simplify the running time analysis).

$F(a, e, n)$:

1. If $e = 0$ return 1.
2. Else if $e \bmod 2 = 0$ then:
   (a) $t = F(a, e/2, n)$.
   (b) return $t^2 \bmod n$.
3. Else:
   (a) $t = F(a, e - 1, n)$.
   (b) return $at \bmod n$.

§6.9. Solutions

Some of the solutions have been written by the TAs in the course and thus have a different style of writing to them. Over time we hope to normalise this part of the text as well.

Solution for Exercise 1. The linear congruence $17x \equiv 3 \pmod{2 \cdot 3 \cdot 5 \cdot 7}$ is equivalent to finding a solution for the system of congruences

$$\begin{aligned} 17x &\equiv 3 \pmod{2} \\ 17x &\equiv 3 \pmod{3} \\ 17x &\equiv 3 \pmod{5} \\ 17x &\equiv 3 \pmod{7} \end{aligned}$$

Consider the first equation. To have $17x \equiv 3 \pmod{2}$ we must have $2 \mid 17x - 3$. That is $17x - 3$ must be even. This can only be true if x is odd. The first equation reduces to $x \equiv 1 \pmod{2}$ then. Next consider the second equation $17x \equiv 3 \pmod{3}$; which we may write as $15x + 2x \equiv 0 \pmod{3}$ giving rise to the equation $2x \equiv 0 \pmod{3}$. Now consider the third equation $17x \equiv 3 \pmod{5}$. This we can write as $15x + 2x \equiv 3 \pmod{5}$ which gives rise to the equation $2x \equiv 3 \pmod{5}$. For the fourth and final equation $17x \equiv 3 \pmod{7}$ note that we can write this equation as $14x + 3x \equiv 3 \pmod{7}$ and then write $3x \equiv 3 \pmod{7}$. Overall we are now interested in the following set of equations.

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ 2x &\equiv 0 \pmod{3} \\ 2x &\equiv 3 \pmod{5} \\ 3x &\equiv 3 \pmod{7} \end{aligned}$$

This set of equation is still not in the form over which we can apply the Chinese remainder theorem. The second equation $2x \equiv 0 \pmod 3$ is clearly replaceable by $x \equiv 0 \pmod 3$ (as $3 \mid 2x$ providing that $3 \mid x$). The third equation $2x \equiv 3 \pmod 5$ we may replace by $4x \equiv 6 \equiv 1 \pmod 5$ so that $x \equiv 4 \equiv -6 \pmod 5$ as x is the modular inverse of 4 modulo 5. For the fourth equation $3x \equiv 3 \pmod 7$ we may write $x \equiv 1 \equiv -6 \pmod 7$. Hence we now have the following set of equations.

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 0 \pmod 3 \\ x &\equiv -6 \pmod 5 \\ x &\equiv -6 \pmod 7 \end{aligned}$$

We deliberately took -6 instead of 4 and 1 to show that it does not matter which representative pf 4 and 1 is taken.

From here on end we simply apply the Chinese remainder theorem. We start by forming the product $n = 2 \cdot 3 \cdot 5 \cdot 7 = 210$ and

$$N_1 = \frac{n}{2} = 105, N_2 = \frac{n}{3} = 70, N_3 = \frac{n}{5} = 42, N_4 = \frac{n}{7} = 30$$

Now the linear congruences

$$105x_1 \equiv 1 \pmod 2, 70x_2 \equiv 1 \pmod 3, 42x_3 \equiv 1 \pmod 5, 30x_4 \equiv 1 \pmod 7$$

are satisfied by $x_1 = 1, x_2 = 1, x_3 = -2, x_4 = -3$ respectively. Let see why. For the first question we may write $105x_1 \equiv 104x_1 + x_1 \equiv 1 \pmod 2$ which is the same as $x_1 \equiv 1 \pmod 2$. For the second equation we may write $69x_2 + x_2 \equiv 1 \pmod 3$ which is the same as $x_2 \equiv 1 \pmod 3$. For the third we may write $40x_3 + 2x_3 \equiv 1 \pmod 5$ which is the same as $2x_3 \equiv 1 \pmod 5$. The modular inverse of 2 modulo 5 so that $x_3 \equiv 3 \equiv -2 \pmod 5$. For the fourth equation we may write $28x_4 + 2x_4 \equiv 1 \pmod 7$ which is the same as $2x_4 \equiv 1 \pmod 7$ so that x_4 is the inverse of 2 modulo 7 leading to $x_4 \equiv 4 \equiv -3 \mod 7$. Again we take here -2 and -3 just to show that it does not matter.

Thus, a solution of the system is given by

$$x = 1 \cdot 105 \cdot 1 + 0 \cdot 70 \cdot 1 + (-6) \cdot 42 \cdot (-2) + (-6) \cdot 30 \cdot (-3) = 1149 \pmod{210} = 99 \pmod{210}$$

Solution for Exercise 2. The additional condition is that $(a, m) = 1$. We have that

$$b \cdot a^k \equiv b^{k+1} \pmod m$$

by the assumption that $a^k \equiv b^k \pmod m$. Then

$$b \cdot a^k \equiv a^{k+1} \pmod m,$$

as $a^{k+1} \equiv b^{k+1} \pmod m$, by assumption. Subtracting a^{k+1} from both sides yields

$$b \cdot a^k - a^{k+1} = a^k(b - a) \equiv 0 \pmod m$$

so that $m \mid a^k(b - a)$. The prime factors of a and a^k are the same (only their powers differ). The assumption that $(a, m) = 1$ implies that the prime factorisation of m does not appear in that of a and thus not in that of a^k as well. Hence, $(a^k, m) = 1$. This in turn implies that $m \mid b - a$ so that $a \equiv b \pmod m$.

Solution for Exercise 3.

1. As $5^2 = 25 \equiv 4 \pmod 7$ it follows that $5^{2n} \equiv 4^n \pmod 7$. Next, note that $2^5 \equiv 4 \pmod 7$ it follows $2^{5n} \equiv 4^n \pmod 7$

   For $n \geq 1$, $2^{5n} \cdot 4^{-1} \equiv 4^n \cdot 4^{-1} \pmod 7$ so that $2^{5n-2} \equiv 4^{n-1} \pmod 7$. Then $3 \cdot 2^{5n-2} \equiv 3 \cdot 4^{n-1} \pmod 7$

$$\begin{aligned} 5^{2n} + 3 \cdot 2^{5n-2} &\equiv 4^n + 3 \cdot 4^{n-1} \pmod 7 \\ &\equiv 4 \cdot 4^{n-1} + 3 \cdot 4^{n-1} \pmod 7 \\ &\equiv 7 \cdot 4^{n-1} \pmod 7 \\ &\equiv 0 \pmod 7 \end{aligned}$$

   and the claim follows.

2. As $2^5 \equiv 5 \pmod{27}$ it follows that $2^{5n} \equiv 5^n \pmod{27}$. Then $2^{5n} \cdot 2 \equiv 5^n \cdot 2 \pmod{27}$

$$\begin{aligned} 2^{5n+1} + 5^{n+2} &\equiv 2 \cdot 5^n + 5^{n+2} \pmod{27} \\ &\equiv 5^n \cdot (2 + 25) \pmod{27} \\ &\equiv 5^n \cdot 27 \pmod{27} \\ &\equiv 0 \pmod{27} \end{aligned}$$

   and the claim follows.

Solution for Exercise 4.

1. As a is an odd integer, let $a = 4k + 1$ or $a = 4k + 3$, for some $k \in \mathbb{Z}$.

   $a^2 = 16k^2 + 8k + 1$ or $a^2 = 16k^2 + 24k + 9$

   $a^2 - 1 = 8(2k^2 + k)$ or $a^2 - 1 = 8(2k^2 + 3k + 1)$

   The claim follows $a^2 \equiv 1 \pmod 8$

2. By the Division Algorithm $a = 7q + r$ for some $0 \leq r < 7$. For each of the seven options for r one can show that $(7q + r)^3$ is congruent to 0, 1, or 6 modulo 7. Let us exemplify one case. The treatment of all other cases is similar in spirit (though the details are different).

   Suppose $r = 4$, i.e., a is of the form $7q + 4$. Then

$$\begin{aligned} (7q + 4)^3 &= (7q)^3 + 3 \cdot (7q)^2 \cdot 4 + 3 \cdot (7q) \cdot 4^2 + 4^3 \\ &= (7q)^3 + 3 \cdot (7q)^2 \cdot 4 + 3 \cdot (7q) \cdot 4^2 + 64. \end{aligned}$$

   Note that $64 = 7 \cdot 9 + 1$ so that

$$= (7q)^3 + 3 \cdot (7q)^2 \cdot 4 + 3 \cdot (7q) \cdot 4^2 + 7 \cdot 9 + 1.$$

   Then

$$\begin{aligned} (7q + 4)^3 - 1 &= (7q)^3 + 3 \cdot (7q)^2 \cdot 4 + 3 \cdot (7q) \cdot 4^2 + 7 \cdot 9 \\ &= 7(7^2 q^3 + 3 \cdot 7^2 \cdot q^2 \cdot 4 + 3q \cdot 4^2 + 9) \end{aligned}$$

   implying that in this case $a^3 - 1 \equiv 0 \pmod 7$ so that $a^3 \equiv 1 \pmod 7$.

   Repeating this type of analysis for each of the possible values of r one can prove the statement.

Solution for Exercise 5. Note that $2^{44} = 2^{32} \cdot 2^8 \cdot 2^4$.
Here $2^8 \equiv 78 \pmod{89}$ and $2^4 \equiv 16 \pmod{89}$. Let us calculate $2^{32} \pmod{89}$

$$2^{32} \equiv 2^{16\cdot 2} \equiv (2^{16})^2 \equiv 32^2 \equiv 45 \pmod{89}.$$

Multiplying all results together and reducing modulo 89 we arrive at

$$2^{44} \equiv 2^{32} \cdot 2^8 \cdot 2^4 \equiv 45 \cdot 78 \cdot 16 \equiv 1 \pmod{89}.$$

It follows that $89 | 2^{44} - 1$.

Solution for Exercise 6. We seek to show that $(2^{20} - 1) \equiv 0 \pmod{41}$. Another way of saying this is that we seek to prove that $2^{20} \equiv 1 \pmod{41}$. Note that $20 = 5 \cdot 4$ and that $2^5 = 32$ is a number whose congruence class modulo 41 is easy to sort out indeed $41 = 1 \cdot 32 + 9$ so that $2^5 \equiv 9 \pmod{41}$. Then $(2^5)^4 \equiv 9^4 \pmod{41}$. At this point we note that $9^2 = 81 = 1 \cdot 41 + 40$ so that $81 \equiv 40 \pmod{41}$. As $-1 \equiv 40 \pmod{41}$ we have that $81 \equiv -1 \pmod{41}$. By Lemma 7.37, we have that $81 \pmod{41}$ is its own inverse; that is $81 \cdot 81 \equiv 1 \pmod{41}$. Consequently we may now write that $2^{20} \equiv 1 \pmod{41}$ and be done.

Solution for Exercise 7. Observe that $4! = 24 \equiv 0 \pmod{12}$. Then for every $k \geq 4$ we have that $k! = 4! \cdot 5 \cdots k \equiv 0 \pmod{12}$. Then

$$K \equiv 1! + 2! + 3! + \underbrace{0 \cdots + 0}_{97 \text{ times}} \equiv 9 \pmod{12}.$$

Solution for Exercise 8.

1. Here we have that $(36, 102) = 6$ but $6 \nmid 8$ so there are no solutions to this equation.

2. As $(5, 26) = 1$ there is a unique solution modulo 26. A viable value of x should satisfy $x = x_0 + (26/1) \cdot t$, $t \in \mathbb{Z}$. We set out to find x_0.

   Applying the extended Euclid's algorithm for $(5, 26)$ we first generate the equations:

   $$\begin{aligned} 26 &= 5 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 + 0 \end{aligned}$$

   and arrive at

   $$1 = 26 - 5 \cdot 5 = 1 \cdot 26 - 5 \cdot 5$$

   Then $1 \cdot 2 = (1 \cdot 26 - 5 \cdot 5) \cdot 2$ so that $2 = 2 \cdot 26 + 5 \cdot (-10)$. We may then set $x_0 = -10$ leading to the values of x to be given by

   $$x = -10 + 26t, t \in \mathbb{Z}.$$

   Note now that

   $$x = 16 - 26 + 26t, t \in \mathbb{Z}.$$

   Set $t' = t - 1$ and write

   $$x = 16 + 26t', t' \in \mathbb{Z}.$$

   It follows that $x \equiv 16 \pmod{26}$.

Solution for Exercise 9. First, if $17x \equiv 9 \pmod{276}$, then $17x = 9 + 276n$, for some $n \in \mathbb{Z}$. Therefore $17x = 9 + 3 \cdot 4 \cdot 23 \cdot n$, hence $17x \equiv 9 \pmod 3$, $17x \equiv 9 \pmod 4$ and $17x \equiv 9 \pmod{23}$. From that we get that every solution to the original congruence is also a solution to the above system of congruences. We now prove the opposite i.e. every solution to the system of congruences is also a solution to the original congruence. If

$$\begin{aligned} 17x &= 9 + 3m_1 \\ 17x &= 9 + 4m_2 \\ 17x &= 9 + 23m_3 \end{aligned}$$

for $m_1, m_2, m_3 \in \mathbb{Z}$, then $3m_1 = 4m_2 = 23m_3$. Therefore $4, 23 \mid 3m_1$, and so by Euclid's lemma and since 3 is prime we get that $4, 23 \mid m_1$. Hence $4 \cdot 23 \mid m_1$. Therefore there exists $m \in \mathbb{Z}$ such that $3m_1 = 3 \cdot 4 \cdot 23 \cdot m$, and so $17x = 9 + 3m_1 = 9 + 3 \cdot 4 \cdot 23 \cdot m = 9 + 276 \cdot m$. We can now solve the system of linear congruences:

$$\begin{aligned} 17x &\equiv 9 \pmod 3 \\ 17x &\equiv 9 \pmod 4 \\ 17x &\equiv 9 \pmod{23} \end{aligned}$$

Since $9 \equiv 0 \pmod 3$ and $17 \equiv 2 \pmod 3$, the first congruence is equivalent to $2x \equiv 9 \equiv 0 \pmod 3$. Therefore, there exists $y \in \mathbb{Z}$ such that $2x = 3y$, hence $3 \mid 2x$ and so, by Euclid's lemma $3 \mid 2$ or $3 \mid x$. Since the former is false, the congruence is equivalent to $x \equiv 0 \pmod 3$. Therefore the system of linear congruences is equivalent to

$$\begin{aligned} x &\equiv 0 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ 17x &\equiv 9 \pmod{23} \end{aligned}$$

It must hold that $x \equiv 0 \pmod 3$, then $x = 3k$ for some $k \in \mathbb{Z}$. We substitute into the second congruence of the system and obtain

$$3k \equiv 1 \pmod 4$$

Multiplication of both sides by 3 give us

$$k \equiv 9k \equiv 3 \pmod 4$$

so that $k = 3 + 4j$, where $j \in \mathbb{Z}$. Then

$$x = 3(3 + 4j) = 9 + 12j$$

For x to satisfy the last congruence, we must have

$$17(9 + 12j) \equiv 9 \pmod{23}$$

or $153 + 204j \equiv 9 \pmod{23}$. So it must holds that $204 \equiv -144 \pmod{23}$ which reduces to $3j \equiv 6 \pmod{23}$, so $j \equiv 2 \pmod{23}$. This yields $j = 2 + 23t$ for $t \in \mathbb{Z}$, hence

$$x = 9 + 12j = 9 + 12(2 + 23t) = 33 + 276t$$

Therefore the solution to the system of congruences is $x \equiv 33 \pmod{276}$and, in turn, a solution to $17x \equiv 9 \pmod{276}$.

Solution for Exercise 10. First, $\gcd(7 \cdot 5 - 2 \cdot 3, 16) = \gcd(29, 16) = 1$. Therefore by Theorem 6.68 there exists a solution. The solution is obtained by applying the method developed in the proof of Theorem 6.68. Multiplying the first congruence by 5, the second one by 3 and then subtracting, will result in

$$29x \equiv 5 \cdot 10 - 3 \cdot 9 \equiv 23 \pmod{16}$$

or, what is the same thing, $13x \equiv 7 \pmod{16}$. We multiply both sides by 5, noting that $5 \cdot 13 \equiv 1 \pmod{16}$, and we get $x \equiv 35 \equiv 3 \pmod{16}$. We eliminate the variable x from the system in the manner, and get

$$29y \equiv 7 \cdot 9 - 2 \cdot 10 \equiv 43 \pmod{16}$$

But then $13y \equiv 11 \pmod{16}$, which again we multiply by 5, and result in $y \equiv 55 \equiv 7 \pmod{16}$. The unique solution is

$$x \equiv 3 \pmod{16} \quad y \equiv 7 \pmod{16}$$

Solution for Exercise 11. As $gcd(3 \cdot 5 - 2 \cdot 4, 13) = 1$, a solution exists. First we multiply the first congruence by 5 and get

$$15x + 20y \equiv 25 \pmod{13}. \tag{6.80}$$

Then we multiply the second congruence by 4 and get

$$8x + 20y \equiv 28 \pmod{13}. \tag{6.81}$$

Subtract (6.80)-(6.81):

$$7x \equiv -3 \pmod{13}$$

or by Theorem 7.9

$$14x \equiv -6 \pmod{13}.$$

Therefore $x \equiv 7 \pmod{13}$.
From the first congruence $3x + 4y \equiv 5 \pmod{13}$ follows

$$3x \equiv 5 - 4y \pmod{13} \tag{6.82}$$

If $x \equiv 7 \pmod{13}$ so $3x \equiv 21 \pmod{13}$. Then substitute the result $x \equiv 7 \pmod{13}$ to the (6.82) and get

$$\begin{aligned} 5 - 4y &\equiv 21 \pmod{13} \\ -4y &\equiv 16 \pmod{13} \\ -12y &\equiv 48 \pmod{13} \end{aligned}$$

The solution of the systems of congruences is $y \equiv 9 \pmod{13}$ and $x \equiv 7 \pmod{13}$

Solution for Exercise 12. Noting that $[4]_{11}$ and $[3]_{11}$ are modular inverse, that is $4 \cdot 3 \equiv 1 \pmod{11}$, we multiply the second equation by 4 as to get the equation

$$x + 8y \equiv 4 \pmod{11}.$$

Subtracting this equation from the first one we attain

$$4x \equiv -2 \equiv 9 \pmod{11}.$$

Recalling yet again that $[3]_{11}$ and $[4]_{11}$ are modular inverses we multiply the last equation by 3 yielding

$$x \equiv 3 \cdot 9 \equiv 5 \pmod{11}$$

giving us x. It remains to find y. Isolating for y in the second original equation we may write

$$2y \equiv 1 - 3x \equiv 1 - 3 \cdot 5 \equiv 1 - 4 \equiv -3 \equiv 8 \pmod{11}.$$

AS $[6]_{11}$ and $[2]_{11}$ are modular inverses we may write

$$6 \cdot 2y \equiv 6 \cdot 8 \pmod{11}$$

so that $y \equiv 4 \pmod{11}$.

Solution for Exercise 13. The system is equivalent to:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 1 \pmod 5 \end{aligned}$$

Indeed, $4 \equiv 1 \pmod 3$, $5 \equiv 2 \pmod 3$, $49 \equiv 1 \pmod 4$, $11 \equiv 1 \pmod 5$, $-9 \equiv 5 \pmod 5$.
We put $n_1 = 3, n_2 = 4, n_3 = 5$.
As any two consecutive integers are co-prime and here two of those are prime we have that $3, 4, 5$ are relatively prime to one another. Therefore this system has a unique solution modulo $M = 3 \cdot 4 \cdot 5 = 60$ we can use Chinese Remainder Theorem. Next we set

$$M_1 = \frac{M}{3} = 20, M_2 = \frac{M}{4} = 15, M_3 = \frac{M}{5} = 12$$

The next step is to find y_1, y_2, y_3 where y_i is the inverse of M_i modulo n_i for $i \in [3]$. That is, we need to solve each of the congruences:

$$\begin{aligned} 20y_1 &\equiv 1 \pmod 3, \\ 15y_2 &\equiv 1 \pmod 4, \\ 12y_3 &\equiv 1 \pmod 5 \end{aligned}$$

To find y_1 we note that $20 \equiv -1 \pmod 3$, therefore $y_1 \equiv -1 \pmod 3$ or equivalently $y_1 \equiv 2 \pmod 3$.
For y_2 we note that $15 \equiv -1 \pmod 4$, therefore $y_2 \equiv -1 \pmod 4$ or equivalently $y_2 \equiv 3 \pmod 3$.
For y_3 we note that $12 \equiv 3 \pmod 4$, therefore $y_2 \equiv 3 \pmod 4$.
Thus, a solution of the system is given by

$$x = 2 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 1 \cdot 12 \cdot 3 = 251 \pmod{60} = 11 \pmod{60}$$

Solution for Exercise 14.
Step I. $110 = 64 + 32 + 8 + 4 + 2 = (1101110)_2$

STEP II. We calculate $5^{2^j} \pmod{131}$ for $0 \leq j \leq 6$ as follows:

$$\begin{aligned}
5^2 &\equiv 25 \pmod{131} \\
5^4 &\equiv 25 \cdot 25 \equiv 101 \pmod{131} \\
5^8 &\equiv 101 \cdot 101 \equiv 114 \pmod{131} \\
5^{16} &\equiv 114 \cdot 114 \equiv 27 \pmod{131} \\
5^{32} &\equiv 27 \cdot 27 \equiv 74 \pmod{131} \\
5^{64} &\equiv 74 \cdot 74 \equiv 105 \pmod{131}
\end{aligned}$$

STEP III.

$$\begin{aligned}
5^{110} &\equiv 5^{64+32+8+4+2} \\
&\equiv 5^{64} \cdot 5^{32} \cdot 5^8 \cdot 5^8 \cdot 5^4 \cdot 5^2 \\
&\equiv 105 \cdot 74 \cdot 114 \cdot 101 \cdot 25 \\
&\equiv 60 \pmod{131}
\end{aligned}$$

SOLUTION FOR EXERCISE 15. As $9 = 3^2$, an integer r is relatively prime to 9 if and only if r is not a multiple of 3. Consequently, $[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9$ all have a modular inverse modulo 9. The classes $[1]_9$ and $[8]_9$ are both self-inverse, $[2]_9$ and $[5]_9$ are inverses of one another as well as $[4]_9$ and $[5]_9$.

SOLUTION FOR EXERCISE 16.
STEP I. $53 = 2^5 + 2^4 + 2^2 + 2^0 = (110101)_2$

STEP II. We calculate $19^{2^j} \pmod{503}$ for $0 \leq j \leq 5$ as follows:

$$\begin{aligned}
19^2 &\equiv 361 \pmod{503} \\
19^4 &\equiv 361 \cdot 361 \equiv 44 \pmod{503} \\
19^8 &\equiv 44 \cdot 44 \equiv 427 \pmod{503} \\
19^{16} &\equiv 427 \cdot 427 \equiv 243 \pmod{503} \\
19^{32} &\equiv 243 \cdot 243 \equiv 198 \pmod{503}
\end{aligned}$$

STEP III.

$$\begin{aligned}
19^{503} &\equiv 19^{32+16+4+1} \\
&\equiv 19^{32} \cdot 19^{16} \cdot 19^4 \cdot 19^1 \\
&198 \cdot 243 \cdot 44 \cdot 19 \equiv 406 \\
&\equiv 406 \pmod{503}
\end{aligned}$$

SOLUTION FOR EXERCISE 17.

1. By the Division Algorithm units digit of a^2 is simply $a^2 \pmod{10}$. Let $a = a_n \cdot 10^n + \cdots + a_1 \cdot 10 + a_0$ and note that $a - a_0 \equiv 0 \pmod{10}$ and in particular $a \equiv a_0 \pmod{10}$ implying that $a^2 \equiv a_0^2 \pmod{10}$. The possible values for a_0^2 are given by
$$S = \{b^2 : b \in [0, 9]\} = \{0, 1, 4, 9, 16, 25, 36, 49, 64, 81\}.$$
The possible unit digits of a^2 can be attained by reducing the values of the set S modulo 10. One may check that
$$a^2 \equiv a_0^2 \equiv 0, 1, 4, 5, 6, 9 \pmod{10}.$$

2. As in the previous part of this exercise we are interested in $a^2 - a + 7 \pmod{10}$. Again as in the previous part, if $a = a_n \cdot 10^n + \cdots + a_1 \cdot 10 + a_0$ then $a^2 - a + 7 \equiv a_0^2 - a_0 + 7 \pmod{10}$. Letting a_0 range over $[0, 9]$ we get that the possible values of $a_0^2 - a_0 + 7$ are given by

a_0	$a_0^2 - a_0 + 7$
0	7
1	7
2	9
3	13
4	19
5	27
6	37
7	49
8	63
9	79

Reducing the values we got for $a_0^2 - a_0 + 7$ modulo 10 we get that
$$a^2 - a + 7 \equiv a_0^2 - a_0 + 7 \equiv 3, 7, 9 \pmod{10}.$$

Solution for Exercise 18.

1. As $(25, 29) = 1$ there is a unique solution modulo 29. A viable value of x then satisfy $x = x_0 + (29/1) \cdot t$, $t \in \mathbb{Z}$. We set out to find x_0.

   Applying the extended Euclid's algorithm for $(25, 29)$ we first generate the equations
$$\begin{aligned} 29 &= 25 \cdot 1 + 4 \\ 25 &= 4 \cdot 6 + 1 \\ 4 &= 1 \cdot 4 + 0 \end{aligned}$$
   and arrive at
$$1 = 25 - 4 \cdot 6 = 25 - (29 - 25 \cdot 1) \cdot 6 = 7 \cdot 25 - 6 \cdot 29$$
   Then $1 \cdot 15 = (7 \cdot 25 - 6 \cdot 29) \cdot 15$ so that $15 = 25 \cdot 105 + 29 \cdot (-90)$. We may then set $x_0 = 105$ leading to the values of x to be given by
$$x = 105 + 29t, t \in \mathbb{Z}.$$
   Note now that
$$x = 18 + 29 \cdot 3 + 29t, t \in \mathbb{Z}.$$
   Set $t' = t + 3$ and write
$$x = 18 + 29t', t' \in \mathbb{Z}.$$
   It follows that $x \equiv 18 \pmod{29}$.

2. As $(6, 21) = 3$ and $3|15$ there are three incongruent solutions modulo 21. A viable value of x then satisfy $x = x_0 + (21/3) \cdot t$, where $t \in \mathbb{Z}$. We set out to find x_0.

   Applying the extended Euclid's algorithm for $(6, 21)$ we first generate the equations

$$\begin{aligned} 21 &= 3 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

   and arrive at

$$3 = 21 - 3 \cdot 6$$

   Then $3 \cdot 7 = (21 - 3 \cdot 6) \cdot 7$ so that $21 = -21 \cdot 6 + 7 \cdot 21$. We may then set $x_0 = -21$ leading to the values of x to be given by

$$x = -21 + (21/3)t = -29 + 7t, t \in \mathbb{Z}.$$

   Note now that

$$x = 6 - 5 \cdot 7 + 7t, t \in \mathbb{Z}.$$

   Set $t' = t - 5$ and write

$$x = 6 + 7t', t' \in \mathbb{Z}.$$

   It follows that we have three congruences classes modulo 21. Let t range over a complete set of residues modulo 3. The solutions will be $6 \pmod{21}, 13 \pmod{21}, 20 \pmod{21}$.

Solution for Exercise 19. As $x \equiv a \pmod{n}$ then $x = kn + a$ for some $k \in \mathbb{Z}$. If k is even then $x = 2n \cdot r + a$ implying that $x \equiv a \pmod{2n}$. If k is odd then $x = (2r + 1)n + a = (2n)r + (n + a)$ so that $x \equiv a + n \pmod{2n}$.

Solution for Exercise 20.

1. As $3 \equiv 4^2 \pmod{13}$ it follows that $3^n \equiv 4^{2n} \pmod{13}$. Next, note that $3^{n+2} = 9 \cdot 3^n$ so that $9 \cdot 3^n \equiv 9 \cdot 4^{2n} \pmod{13}$ so that $3^{n+2} \equiv 9 \cdot 4^{2n} \pmod{13}$. Then

$$\begin{aligned} 3^{n+2} + 4^{2n+1} &\equiv 4^{2n} \cdot 9 + 4^{2n+1} \pmod{13} \\ &\equiv 4^{2n}(9 + 4) \pmod{13} \\ &\equiv 4^{2n} \cdot 13 \pmod{13} \\ &\equiv 0 \pmod{13} \end{aligned}$$

   and the claim follows.

2. As $6 \equiv 7^2 \pmod{43}$ then $6^n \equiv 7^{2n} \pmod{43}$ and $6^{n+2} = 6^n \cdot 36 \equiv 7^{2n} \cdot 36 \pmod{43}$. Then

$$\begin{aligned} 6^{n+2} + 7^{2n+1} &\equiv 7^{2n} \cdot 36 + 7^{2n+1} \pmod{43} \\ &\equiv 7^{2n}(36 + 7) \pmod{43} \\ &\equiv 0 \pmod{43}. \end{aligned}$$

Solution for Exercise 21. Numbers like 5 and 9 show that $n \equiv 1, -3 \pmod{8}$ is possible. The integer n being odd implies that $n \not\equiv 0, 2, 4, 6 \pmod{8}$. It remains to determine whether $n \equiv 3, -1 \pmod{8}$ is possible.

1. Having $n \equiv 3 \pmod 8$ would imply that there are integers K and L such that $8L + 3 = 4K + 1$. That is, $L = \frac{K}{2} - \frac{1}{4}$ so that $4L = 2k - 1$ which is impossible as $4L$ is even and $2K - 1$ is odd for any integers K and L. Hence $n \not\equiv 3 \pmod 8$.

2. Having $n \equiv -1 \pmod 8$ implies that $8L - 1 = 4L + 1$ has a solutions in the integers. That is $4L = 2K + 1$ has a solution in the integers which is impossible.

In conclusion if $n \equiv 1 \pmod 4$ then either $n \equiv 1 \pmod 8$ or $n \equiv -3 \pmod 8$.

Solution for Exercise 22. For suppose that $(b, n) > 1$. The there exists a prime p such that $p \mid b$ and $p \mid n$. As by assumption $n \mid b - a$ it follows that $p \mid b - a$ as well. Then $p \mid b - (b - a) = a$ contradicting the assumption that $(a, n) = 1$.

Solution for Exercise 23. Observe that

$$(a + b) \pmod n = \begin{cases} a + b, & \text{if } a + b < n, \\ a + b - n, & \text{if } a + b \geq n. \end{cases}$$

As each of a, b, and n can be represented using $O(\log n)$ bits the number of bit operations required for this calculation is $O(\log n)$.

Solution for Exercise 24. First we must check whether $(a, n) \mid b$. Calculating (a, n) requires $O((\log n)^3)$ bit operations and determining whether $(a, n) \mid b$ requires $O((\log n)^2)$ bit operations.

Solution for Exercise 25. We start by noting that

$$a^e = \begin{cases} a \cdot a^{e-1}, & \text{if } e \text{ is odd}, \\ (a^{e/2})^2, & \text{if } e \text{ is even}. \end{cases}$$

Let $b(e)$ denote the number of ones in the binary expansion of e. We prove the following.

Claim 6.83. *The algorithm computes $a^e \bmod n$ using $\log e - 1$ squaring (modulo n) operations and $b(e)$ multiplications by a (modulo n). Consequently the algorithm requires $O((\log e) \cdot (\log n)^2)$ bit operations.*

Proof. The proof is by induction on e. The claim is true for $e = 0$. Assume it is true for all $f < e$ and consider proving the claim for e.

1. If e is odd write $e = 2k + 1$ then the algorithm first computes a^{2k} (modulo n) using $(\log 2k) - 1$ squaring (modulo n) operations and $b(2k)$ multiplications by a (modulo n) by the induction hypothesis. The algorithm multiplies this result by a. Hence the computation is completed using $(\log 2k) - 1 \leq \log(2k + 1) - 1$ squaring (modulo n) operations and $b(2k) + 1 = b(2k + 1)$ multiplications by a (modulo n). The equality $b(2k) + 1 = b(2k + 1)$ stems from the fact that all even numbers have 0 as their least significant bit.

2. If e is even write $e = 2k$. Then the algorithm first computes a^k using $(\log k) - 1$ squaring operations and $b(k)$ multiplications by a by the induction hypothesis; the result is then squared. Overall the algorithm performed $\log k - 1 + 1 = \log k = \log(2k) - 1$ squaring operations and $b(k) = b(2k)$ multiplications by a. The latter equality stems from the fact that division by two effects the binary expansion by performing a shift right by one bit (i.e., we lose the least significant bit) together with the fact that for an even number the least significant bit is 0 hence the number of ones in the binary expansion of k and $2k$ is the same.

The observant reader may notice that the algorithm considered here is simply the recursive formulation of the algorithm presented in § 6.7. ■

Lecture 7

Theorems of Wilson, Fermat, and Euler

In this lecture we present three results that play a crucial rôle in primality testing. Specifically we present the so called Wilson's theorem, Fermat's little theorem, and its generalisation referred to as Euler's theorem.

§7.1. Wilson's Theorem

Theorem 7.1 (Wilson's theorem)
If p is prime then $(p-1)! \equiv -1 \pmod{p}$.

Why should this be true? Consider $p = 7$ so that

$$(p-1)! = 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6.$$

Note now that

$$\begin{aligned} 2 \cdot 4 &\equiv 1 \pmod{7} \\ 3 \cdot 5 &\equiv 1 \pmod{7} \end{aligned}$$

so that 2 and 4 are inverses of one another modulo 7 and 3 and 5 are inverses of one another modulo 7. Rearranging the expression:

$$6! = 1 \cdot \underbrace{(2 \cdot 4)}_{\equiv 1 \pmod{7}} \cdot \underbrace{(3 \cdot 5)}_{\equiv 1 \pmod{7}} \cdot 6$$

Then $6! \equiv 6 \equiv -1 \pmod{7}$.

With inverses playing a key role here let us be reminded of some facts we have seen regarding this notion.

$$\text{If } p \text{ is a prime then every } a \in [1, p-1] \text{ has an inverse modulo } p. \tag{7.2}$$

Also,

$$\text{if } p \text{ is a prime only 1 and } p-1 \text{ are their own inverses.} \tag{7.3}$$

Proof of Theorem 7.1. For $p = 2$ the claim is trivial: $(2-1)! = 1 \equiv -1 \pmod{2}$. So let us assume $p > 2$ and consequently odd. By (7.2) every term a in the product $(p-1)!$ has an inverse $\tilde{a}$ modulo p. Moreover, only 1 and $p-1$ serve as their own inverse, by (7.3). Hence all terms from 2 up to $p-2$

(of which there is an even number as we do not account for 0, 1, and $p-1$) appearing in the product $(p-1)!$ can be grouped into pairs with both elements in the pairs inverses of one another. That is

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}.$$

Multiplying both sides by $p-1$ (and 1) we reach

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}.$$

■

The converse of Wilson's theorem is true as well.

Theorem 7.4 (Converse of Wilson's theorem)
Let $2 \leq n \in \mathbb{Z}$. If $(n-1)! \equiv -1 \pmod{n}$ then n is prime.

Proof. Assume towards a contradiction that n is composite and satisfies $(n-1)! \equiv -1 \pmod{n}$. Then $n = a \cdot b$ with $2 \leq a, b < n$. As $a < n$ it follows that $a \mid (n-1)!$. As $(n-1)! \equiv -1 \pmod{n}$, by assumption, then $n \mid (n-1)!+1$ and thus $a \mid (n-1)!+1$. It follows that $a \mid ((n-1)!+1)-(n-1)! = 1$ while $a \geq 2$; contradiction. ■

Theorems 7.1 and 7.4 provide a characterisation of the prime numbers.

$$n \text{ is prime} \iff (n-1)! \equiv -1 \pmod{n}. \tag{7.5}$$

We can use this as a test to check primality of integers. Unfortunately (or perhaps we should say fortunately), this characterisation does not yield an efficient algorithm for primality testing.

Example 7.6 Suppose we do not know whether 6 is prime or not. Then we can check that $(6-1)! = 120 \equiv 0 \pmod{6}$ and conclude that 6 is not prime.

Example 7.7 Find the remainder when 15! is divided by 17. By Wilson's theorem as 17 is prime we have that $(17-1)! = 16! \equiv -1 \pmod{17}$. We note in addition that $16 \equiv -1 \pmod{17}$. Then $16! \equiv 16 \pmod{17}$. As $(16, 17) = 1$ we can reduce both sides by 16 to get $15! = 1 \pmod{17}$.

Here is an additional characterisation of the primes arising from Wilson's theorem.

Proposition 7.8 *An integer $n > 1$ is prime if and only if $(n-2)! \equiv 1 \pmod{n}$.*

Proof. By Wilson's theorem

$$n \text{ is prime} \iff (n-1)! \equiv n-1 \pmod{n}.$$

As $(n-1, n) = 1$ we may write

$$\frac{(n-1)!}{n-1} \equiv 1 \pmod{n}$$

It follows that

$$n \text{ is prime} \iff (n-2)! \equiv 1 \pmod{n}.$$

■

Example 7.9 Show that $10! + 1 \equiv 0 \pmod{11}$. We use the approach seen in Wilson's theorem of pairing inverses modulo 11.

$$10! + 1 \equiv 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10 + 1 \equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot (-1) + 1 \equiv 0 \pmod{11}.$$

The inverses modulo 11 we discovered in the lecture about Congruences. Alternatively we can simply just use Wilson's theorem to have $10! \equiv -1 \pmod{11}$ and then obtain the result without resorting to knowing the inverses modulo 11.

§7.2. Fermat's little theorem

Theorem 7.10 (Fermat's little theorem)
Let p be a prime and let $a \in \mathbb{Z}^+$ such that $p \nmid a$. Then

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

Proof. We show that

$$a \cdot (2a) \cdot (3a) \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot (p-1) \pmod{p}. \tag{7.11}$$

For we see that (7.11) can be written as

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

and as $((p-1)!, p) = 1$ (since $(p-1)!$ and p have no common factors) we may reduce $(p-1)!$ on both sides without changing the modulus yielding the assertion of the theorem.

It remains to prove (7.11). Let $S = \{a, 2a, 3a \ldots, (p-1)a\}$. To prove (7.11) it suffices to show that the members of S are:

(a) pairwise incongruent modulo p and

(b) collectively represented by the classes $1, 2, \ldots, p-1$ modulo p.

We start by showing that no member of S resides in the class $0 \pmod{p}$. Indeed, no member of S is divisible by p. For if $p \mid j \cdot a$ for some $j \in [1, p-1]$ then $p \mid j$ by the assumption that $p \nmid a$. This is a contradiction.

Next, we show that the members of S are pairwise incongruent modulo p. For suppose we had $j \cdot a \equiv k \cdot a \pmod{p}$ for some $j, k \in [1, p-1]$ and $j \neq p$. As $(a, p) = 1$ by assumption we arrive at $j \equiv k \pmod{p}$ which is impossible for two distinct numbers below p. ■

Corollary 7.12 *Let p be a prime and let $a \in \mathbb{Z}^+$. Then $a^p \equiv a \pmod{p}$.*

Proof. We consider two complimentary cases; either $p \nmid a$ or $p \mid a$. In the former case, we have that $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem. The claim then follows upon multiplication by a on both sides. In the latter case, $p \mid a$ so that $p \mid a^p$ as well so that $a^p \equiv 0 \equiv a \pmod{p}$. ■

Corollary 7.13 *If p is a prime and $a \in \mathbb{Z}^+$ such that $p \nmid a$. Then a^{p-2} is the inverse of a modulo p.*

Proof. By Fermat's theorem

$$1 \equiv a^{p-1} = a \cdot a^{p-2} \pmod{p}.$$

■

Corollary 7.14 *Let p be a prime and let $a \in \mathbb{Z}^+$ such that $p \not| a$. Then the sole solution of $ax \equiv b \pmod{p}$ is $x \equiv a^{p-2}b \pmod{p}$.*

Proof. By Corollary 7.13, a^{p-2} is the inverse of a modulo p. Hence, given the equation $ax \equiv b \pmod{p}$ we may multiply both sides by a^{p-2} to reach $x \equiv a^{p-2}b \pmod{p}$. ■

Example 7.15 What is the least positive residue of 3^{201} modulo 11? By Fermat's theorem we have

$$\begin{aligned} 3^{10} \equiv 1 \pmod{11} &\implies 3^{200} \equiv (3^{10})^{20} \equiv 1 \pmod{11} \\ &\implies 3 \cdot 3^{200} \equiv 3^{201} \equiv 3 \pmod{11} \end{aligned}$$

and the answer is $3 \pmod{11}$.

Example 7.16 Show that $a^{21} \equiv a \pmod{15}$ for all $a \in \mathbb{Z}^+$. To make use of Fermat's theorem we require that our modulus be prime and 15 is composite. We naturally then turn to the prime factors of 15 which are 3 and 5. The plan now is to show that

$$a^{21} \equiv a \pmod{3} \text{ and } a^{21} \equiv a \pmod{5}. \tag{7.17}$$

For if $3 \mid a^{21} - a$ and $5 \mid a^{21} - a$ then $15 = lcm(3, 5) \mid a^{21} - a$ which is what we seek to prove.

It remains to prove (7.17). We start with division by 5:

$$\begin{aligned} \underbrace{a^5 \equiv a \pmod{5}}_{\text{Fermat's thm.}} &\implies a^{20} = (a^5)^4 \equiv a^4 \pmod{5} \\ &\implies a^{21} \equiv a^5 \equiv a \pmod{5}. \end{aligned}$$

Now we turn to division by 3:

$$\underbrace{a^3 \equiv a \pmod{3}}_{\text{Fermat thm.}} \implies a^{21} = (a^3)^7 \equiv a^7 \pmod{3}.$$

Unlike the case with 5 we are not done yet we now must show that $a^7 \equiv a \pmod{3}$ in order to conclude. This we do as follows.

$$a^6 = (a^3)^2 \equiv a^2 \pmod{3} \implies a^7 \equiv a^3 \equiv a \pmod{3}.$$

Example 7.18 Let $a \in \mathbb{Z}^+$ such that $7 \not| a$. Then $a^3 \equiv 1 \pmod{7}$ or $a^3 \equiv -1 \pmod{7}$. By Fermat's theorem $a^6 \equiv 1 \pmod{7}$ so that $7 \mid a^6 - 1 = (a^3 - 1)(a^3 + 1)$. Then $7 \mid a^3 - 1$ or $7 \mid a^3 + 1$ and the claim follows.

7.2.1 *(Fermat) Pseudoprimes*

Using Wilson's characterisation of the primes will require quite some time for large numbers n as one has to first calculate $(n-1)!$. Fermat's theorem looks more promising in that respect prompting the question: *how can we use Fermat's theorem in order to check primality?*

Fix an integer n.

1. (By Corollary 7.12) if we can find an integer a for which $a^n \not\equiv a \pmod{n}$ holds, then n is not a prime.

2. On the other hand if $a^n \equiv a \pmod{n}$ for some a then n is not necessarily a prime.

Example 7.19 Is 63 prime? As $2^6 = 64$ we gravitate towards choosing $a = 2$ and seek to check whether $2^{63} \not\equiv 2 \pmod{63}$.

$$2^{63} \equiv 2^{60} \cdot 2^3 \equiv (2^6)^{10} \cdot 2^3 \equiv 64^{10} 2^3 \pmod{63}.$$

Note now that $64 \equiv 1 \pmod{63}$. Then

$$2^{63} \equiv 2^3 \equiv 8 \not\equiv 2 \pmod{63}.$$

So we can be sure that 63 is not a prime number.

Now let us see how Fermat's theorem can be fooled as indeed its converse is false. The following example was discovered in 1919 by Sarrus.

Example 7.20 The number 341 is not prime, indeed, $341 = 11 \cdot 31$. Nevertheless, it satisfies the assertion of Fermat's theorem for $a = 2$, i.e., $2^{341} \equiv 2 \pmod{341}$. To prove this congruence we shall use Corollary 6.52. In particular, we shall note that 11 and 31 are co-prime and prove that

$$2^{340} \equiv 1 \pmod{11} \text{ and } 2^{340} \equiv 1 \pmod{31}. \tag{7.21}$$

Given this Corollary 6.52 would yield $2^{340} \equiv 1 \pmod{341}$.

We start with 11:

$$2^{10} \equiv 1 \pmod{11} \implies (2^{10})^{34} \equiv 2^{340} \equiv 1 \pmod{11}.$$

Next we consider 31: As $340 = 5 \cdot 68$ then

$$2^{340} = (2^5)^{68} = 32^{68}.$$

As $32 \equiv 1 \pmod{31}$ we get that

$$2^{340} \equiv 32^{68} \equiv 1 \pmod{31}.$$

Composite numbers that are able to "fool" Fermat's primality test have been endowed with a special name.

Definition 7.22 *Let $b \in \mathbb{Z}^+$. A composite $n \in \mathbb{Z}^+$ satisfying $b^n \equiv b \pmod{n}$ is called a* pseudoprime to the base b.

Example 7.23 341 is pseudoprime to the base 2.

Example 7.24 91 is a pseudoprime to the base 3.

$$2^{90} \equiv (2^{10})^9 \equiv 1024^9 \equiv 1^9 \equiv 1 \pmod{3}.$$

Perhaps we can still salvage our Fermat based primality test. For instance, if the number of pseudoprimes to the base b are finite and if we can get an upper bound n_0 on their largest member we would have a primality test for all integers exceeding n_0. For instance, it is known that the number of primes not exceeding 10^{10} is $455,052,511$ while the number of pseudoprimes to the base 2 not exceeding 10^{10} is only $14,884$. Sadly, while it is known that pseudoprimes to any given base are much more rare than primes these nonetheless form an infinite set.

Theorem 7.25 *Let $b \in \mathbb{Z}^+$. There are infinitely many pseudoprimes to the base b.*

We delegate the proof of Theorem 7.25 to the exercises. Suppose we have that $2^{n-1} \equiv 1 \pmod{n}$. Then n is a pseudoprime to the base 2 but we cannot infer from this congruence whether n is prime. At this point we can try to check various positive integers b with $(n, b) = 1$ whether $b^{n-1} \equiv 1 \pmod{n}$.

Example 7.26 We have learned that 341 is pseudoprime to the base 2. Let us now check whether $7^{340} \not\equiv 1 \pmod{341}$.

$$7^{340} \equiv (7^3)^{113} \cdot 7 \pmod{341}.$$

Observe that

$$7^3 = 343 \equiv 2 \pmod{341}$$

so we get

$$7^{340} \equiv (7^3)^{113} \cdot 7 \equiv 2^{113} \cdot 7 \equiv (2^{10})^{11} \cdot 2^3 \cdot 7 \pmod{341}.$$

Observe that

$$2^{10} \equiv 1024 \equiv 1 \pmod{341}$$

then

$$7^{340} \equiv 2^3 \cdot 7 \equiv 56 \not\equiv 1 \pmod{341},$$

and we discover that 341 is composite through this calculation.

Which is more "abundant" in the integers: the primes or the pseudoprimes (to a base a)? The following result gives an answer; proof of which is beyond the scope of these notes.

Theorem 7.27 Pseudoprimes are rare compared to primes
Let $a \geq 2$ be an integers. Then the number of pseudoprimes to the base a not exceeding x if $o(\pi(x))$ as $x \to \infty$.

7.2.1.1 Infinitely many pseudoprimes to the base 2

A proof of Theorem 7.25 lies beyond the scope of these notes. However, proving that there are infinitely many pseudoprimes to the base 2 is not. We offer this as a substitute to a proof of Theorem 7.25. We require some preparation.

Lemma 7.28 *If d and n are positive integers such that d divides n, then $2^d - 1$ divides $2^n - 1$.*

Proof. Given that $d|n$, there is a positive integer t with $dt = n$. By setting $x = 2^d$ in the identity

$$x^t - 1 = (x - 1)(x^{t-1} + x^{t-2} + \cdots + 1)$$

we find that

$$2^n - 1 = (2^d - 1)(2^{d(t-1)} + 2^{d(t-2)} + \cdots + 2^d + 1).$$

Consequently, we have $2^d - 1$ divides $2^n - 1$. ■

Theorem 7.29 *There are infinitely many pseudoprimes to the base 2.*

Proof. We will show that if n is an odd pseudoprime to the base 2, then $m = 2^n - 1$ is also an odd pseudoprime to the base 2. Because we have at least one odd pseudoprime to the base 2, namely $n_0 = 341$, we will be able to construct infinitely many odd pseudoprimes to the base 2 by taking $n_0 = 341$ and $n_{k+1} = 2^{n_k} - 1$ for $k = 0, 1, 2, 3, \ldots$. These integers are all different, because $n_0 < n_1 < n_2 < \cdots < n_k < n_{k+1} < \cdots$.

To continue the proof, let n be an odd pseudoprime to the base 2, so that n is composite and $2^{n-1} \equiv 1 \pmod{n}$. Because n is composite, we have $n = dt$, with $1 < d < n$ and $1 < t < n$. We will show that $m = 2^n - 1$ is also pseudoprime, by first showing that it is composite, and then by showing that $2^{m-1} \equiv 1 \pmod{m}$.

To see that m is composite, we use Lemma 7.28 to note that $2^d - 1$ divides $(2^n - 1) = m$. To show that $2^{m-1} \equiv 1 \pmod{m}$, note that because $2^n \equiv 2 \pmod{n}$, there is an integer k with $2^n - 2 = kn$. Hence, $2^{m-1} = 2^{2^n-2} = 2^{kn}$. By Lemma 7.28 it follows that $m = 2^n - 1 | (2^{kn} - 1) = 2^{m-1} - 1$. Hence, $2^{m-1} - 1 \equiv 0 \pmod{m}$, so that $2^{m-1} \equiv 1 \pmod{m}$. We conclude that m is also a pseudoprime to the base 2. ■

7.2.2 Carmichael Numbers

Pseudoprimes make the use of Fermat's based primality testing difficult. *Carmichael numbers*[1] make it impossible; luckily these numbers admit a nice characterisation.

Definition 7.30 *An integer n satisfying $b^{n-1} \equiv 1 \pmod{n}$ for all positive integers b satisfying $(b, n) = 1$ is called a* Carmichael number[a].

[a] Another name for these numbers is *absolute pseudoprimes*.

For instance, we have seen in Example 7.24 that 91 is a pseudoprime to the base 3. However, 91 is not a pseudoprime to the base 2 (a fact delegated to the exercises). The existence of Carmichael numbers means that one cannot hope that a number being pseudoprime in one base excludes it from being a pseudoprime in another. Moreover, in 1912, Carmichael conjectured that there are infinitely many such numbers. In 1992 this was proved by Alford, Granville and Pomerance.

Theorem 7.31 *There are infinitely many Carmichael numbers. In particular, for x sufficiently large, $C(x)$ the number of Carmichael numbers not exceeding x satisfies $C(x) > x^{2/7}$.*

Example 7.32 $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number. Let b be an integer such that $(b, n) = 1$. Then $(b, 3) = (b, 11) = (b, 17) = 1$ so that

$$b^2 \equiv 1 \pmod{3},\ b^{10} \equiv 1 \pmod{11},\ b^{16} \equiv 1 \pmod{17},$$

By Fermat's theorem. We seek to employ Corollary 6.52 to show that $b^{560} \equiv 1 \pmod{561}$.

$$\begin{aligned} b^{560} &\equiv (b^2)^{280} \equiv 1 \pmod{3} \\ b^{560} &\equiv (b^{10})^{56} \equiv 1 \pmod{11} \\ b^{560} &\equiv (b^{16})^{35} \equiv 1 \pmod{17}. \end{aligned}$$

[1] Discovered by Carmichael in 1910.

Then $b^{560} \equiv 1 \pmod{561}$, by Corollary 6.52.

Theorem 7.33 *Let $n = q_1 \cdot q_2 \cdots q_k$ be a product of distinct primes (i.e., n is square free). If*

$$(q_j - 1) \mid (n-1) \; \forall j \in [k]$$

then n is a Carmichael number.

Proof. Let b be an integer such that $(b, n) = 1$. Then $(b, q_j) = 1$ for every $j \in [k]$ so that, by Fermat's theorem, $b^{q_j - 1} \equiv 1 \pmod{q_j}$ for every $j \in [k]$. As $(q_j - 1) \mid (n-1)$, by assumption, we may write $n - 1 = t_j(q_j - 1)$ where t_j is some integer for every $j \in [k]$. Then

$$b^{n-1} \equiv (b^{q_j-1})^{t_j} \equiv 1 \pmod{q_j}, \; \forall j \in [k].$$

Then $b^{n-1} \equiv 1 \pmod{n}$ by Corollary 6.52. ■

The converse of Theorem 7.33 is also true and is called the *Korselt criterion*. Proof of the latter requires the notion of *primitive roots* and is postponed until Theorem 10.96.

Example 7.34 The integer 6601 is a Carmichael number; $6601 = 7 \cdot 23 \cdot 41$, and

$$(7-1) \mid 6600, \; (23-1) \mid 6600, \; (41-1) \mid 6600.$$

§7.3. Euler's theorem

Fermat's little theorem aids us in calculating congruences involving exponents where the modulus is prime. We use the so called *Euler's theorem* to conduct similar calculation when the modulus is composite. We thus view Euler's theorem as a generalisation of Fermat's little theorem.

7.3.1 *Euler's totient function*

A function defined over all positive integers is called an *arithmetic function*. Our interest is with a special type of arithmetic functions.

Definition 7.35 *An arithmetic function f is called* multiplicative *if $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$. It is called* completely multiplicative *if $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{Z}^+$.*

Example 7.36 The constant function $n \mapsto 1$ is completely multiplicative.

Example 7.37 The function $n \mapsto n$ is completely multiplicative.

Theorem 7.38 *Let f be a multiplicative function and let $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$ then $f(n) = f(p_1^{a_1}) \cdots f(p_k^{a_k})$.*

Proof. Due to its simplicity we omit the proof of this statement here. The reader in encouraged to prove this theorem using an induction on the number of distinct prime factors of n (i.e., induction on k here). ■

Definition 7.39 *Let $n \in \mathbb{Z}^+$. We write $\varphi(n)$ to denote the number of positive integers not exceeding n that are co-prime with n; that is*

$$\varphi(n) = |\{k \in [n] : (k, n) = 1\}|.$$

The function $\varphi(\cdot)$ is called *Euler's totient function*. The origin of the word *Totient* is from the Latin word *tot* which means *many*.

Example 7.40 The set

$$1, 7, 11, 13, 17, 19, 23, 29$$

consists of all positive integers not exceeding 30 that are co-prime with 30. Hence, $\varphi(30) = 8$.

Example 7.41

$$\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(5) = 4, \varphi(6) = 2, \varphi(7) = 6.$$

Note that $\varphi(1) = 1$ as $(1, 1,) = 1$, trivially. For every $n > 1$ we have $(n, n) = n > 1$ so that $\varphi(n) \leq n - 1$, whenever $n > 1$.

$$\text{if } n \text{ is prime then } \varphi(n) = n - 1. \tag{7.42}$$

If n is composite then n has at least one non-trivial divisor $2 \leq d < n$ so that

$$\text{if } n \text{ is composite then } \varphi(n) \leq n - 2. \tag{7.43}$$

We have just proved the following.

Proposition 7.44 *$\varphi(n) = n - 1$ if and only if n is prime.*

Lemma 7.45 *Let p be prime and let $k > 0$. Then*

$$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$$

Proof. As $(n, p^k) = 1$ if and only if $p \not| n$ it is easier to determine $\varphi(n)$ by subtracting from p^k (the size of the set $\{1, \ldots, p^k\}$) those numbers divisible by p that do not exceed p^k. These numbers are simply the multiples of p: $p, 2p, 3p, \ldots, (p^{k-1})p$. That is, there are p^{k-1} multiples of p in the set $\{1, \ldots, p^k\}$. Discarding these integers implies the lemma. ■

Example 7.46 $\varphi(25) = \varphi(5^2) = 5^2 - 5 = 20$

At this stage we are capable to evaluate φ at prime powers. To be able to evaluate this function at every positive integer it suffices to prove that this function is multiplicative. Indeed, if prove that φ is multiplicative then given $n = p_1^{a_1} \ldots p_k^{a_k}$ then

$$\varphi(n) = \varphi(p_1^{a_1}) \ldots \varphi(p_k^{a_k})$$

by Theorem 7.38. We set out to prove that φ is multiplicative, that is, we seek to prove the following result.

Theorem 7.47 *$\varphi(mn) = \varphi(m)\varphi(n)$ whenever $(m, n) = 1$.*

The following two lemmas will facilitate our claims.

Lemma 7.48 *$(a, bc) = 1 \iff (a, b) = 1$ and $(a, c) = 1$.*

Proof. One proof for this lemma employs the fundamental theorem of arithmetics. Here we note that if a and bc share no prime factors then surely a shares no common prime factors with b or c and vice versa.

Here is another proof from first principles. Suppose $(a, bc) = 1$ and let $d = (a, b)$. Then $d \mid a$ and $d \mid bc$ so that $1 = (a, bc) \geq d$ implying that $(a, b) = 1$. A similar argument shows that $(a, c) = 1$.

Conversely, suppose that $(a, b) = 1 = (a, c)$ and let $d' = (a, bc)$. Assume towards contradiction that $d' > 1$ and thus admits a prime divisor p. As $d \mid a$ then $p \mid a$. As $d \mid bc$ then $p \mid bc$ so that $p \mid b$ or $p \mid c$. In the former case $(a, b) \geq p > 1$ which is a contradiction, and in the latter case $(a, c) \geq p > 1$ which is a contradiction. ■

Lemma 7.49 *$(qm + r, m) = (r, m)$.*

Proof. Show that every common divisor of r and m is a common divisor of $qm + r$ and m and vice versa. We leave the details to the reader. ■

We seek to count the members of $[1, mn]$ that are relatively prime to mn. As $(\ell, mn) = 1$ if and only if $(\ell, m) = 1$ and $(\ell, n) = 1$, by Lemma 7.48, we may reduce the task of counting numbers in $[1, mn]$ relatively prime to mn to first round up all numbers that are relatively prime to m and of those count all those relatively prime to n. This two step procedure is easier to see through the following matrix M:

$$\begin{array}{cccccc}
1 & 2 & \dots & r & \dots & m \\
m+1 & m+2 & \dots & m+r & \dots & 2m \\
2m+1 & 2m+2 & \dots & 2m+r & \dots & 3m \\
\vdots & \vdots & & \vdots & & \vdots \\
(n-1)m+1 & (n-1)m+2 & \dots & (n-1)m+r & \dots & nm
\end{array}$$

Consider the rth column of M. This column consists of the numbers

$$\{qm + r : q \in [0, n-1]\};$$

each member of this column is relatively prime to m if and only if $(r, m) = 1$, by Lemma 7.49. Of these m possible columns of M precisely $\varphi(m)$ of those have all their entries relatively prime to m.

Claim 7.50. *Each column M contains precisely $\varphi(n)$ members that are relatively prime to n.*

Proof. Fix a column $C = \{qm + r : q \in [0, n-1]\}$ of M. The members of C are all incongruent modulo n. For if

$$jm + r \equiv km + r \pmod{n}$$

for some two distinct $j, k \in [n]$ then $j \equiv k \pmod{n}$ (recall that $(m, n) = 1$) which is impossible. Hence, the members of C are represented by the canonical complete systems of residues $\{0, 1, \dots, n-1\}$. The latter contains $\varphi(n)$ members that are relatively prime to n and consequently so does C (see Exercise 22 for details). ■

It now follows that each of the $\varphi(m)$ columns of M with all their members relatively prime to m contains $\varphi(n)$ members that are relatively prime to n. We have just proved Theorem 7.47.

The fact that φ is multiplicative coupled with Theorem 7.38 yield the following.

Theorem 7.51 *Let $1 < n = p_1^{a_1} \dots p_k^{a_k}$ then*

$$\begin{aligned}\varphi(n) &= \left(p_k^{a_k} - p_k^{a_k-1}\right) \dots \left(p_1^{a_1} - p_1^{a_1-1}\right) \\ &= n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right).\end{aligned}$$

Example 7.52

$$\varphi(900) = \varphi(2^2 \cdot 3^2 \cdot 5^2) = 900\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 900 \cdot \frac{8}{30} = 240$$

Example 7.53 The function φ is not complete multiplicative. Consider 2 and 4 then $\varphi(2 \cdot 4) = \varphi(8) = 4$ while $\varphi(2) \cdot \varphi(4) = 1 \cdot 2 = 2$.

We conclude this section with a certainly respectable utilisation of Euler's totient function as this is used to prove the infinitude of primes.

Proof of Theorem 5.23. For suppose $p_1, \dots, p_n$ are the only primes. Set $N := \prod_{i=1}^n p_i$. Any $1 < n < N$ must admit a common factor with N so that $(N, n) \neq 1$ whenever $1 < n < N$. Consequently, $\varphi(N) = 1$, by definition. On the other hand,

$$\varphi(N) = \varphi(p_1 \cdots p_n) = \prod_{i=1}^n \varphi(p_i) = \prod_{i=1}^n (p_i - 1) > 1;$$

a contradiction. ■

7.3.1.1 Additional properties of Euler's Totient function

Proposition 7.54 *For $n > 2$, $\varphi(n)$ is even.*

Proof. Let $a \in [1, n]$ such that $a < n/2$ (observe that $n/2$ need not be an integer. Then $(a, n) = (n - a, n)$ and as $n > 2$ and $1 < a < n/2$ we have that a and $n - a$ are distinct numbers. Then the set of ordered pairs $\{(a, n - a) : a \in [1, n], a < n/2, (a, n) = 1\}$ consists of pairs whose members are distinct and both relatively prime to n. In particular, the pair $(n/2, n/2)$ does not appear in this set. This is clear of n is odd. If n is even then $(n/2, n) = n/2 > 1$ as $n > 2$. It now follows that as all numbers relatively prime to n can be arranged in pairs (as above) that there is an even number of them. ■

Here is an alternative proof of Proposition 7.54 using the properties of φ.

Proof of Proposition 7.54 - alternative proof. We consider two complimentary cases. Either n has an odd prime factor or it does not (in which case it is a power of 2). In the latter case let p be some odd prime factor of n so that $n = p^k m$ for some $k \in \mathbb{Z}^+$ and such that $(p^k, m) = 1$. Then

$$\varphi(n) = \varphi(p^k)\varphi(m) = p^{k-1}(p - 1)\varphi(m)$$

which is even as $p - 1$ is even. (Note that the case $k = 1$ is covered here as well).

In the former case, $n = 2^k$ for some $k \in \mathbb{Z}^+$. By assumption that $n > 2$ we have that $k > 1$ and then

$$\varphi(2^k) = 2^{k-1}(2 - 1) = 2^{k-1}$$

so that the claim follows. ■

Proposition 7.55 *If n has r distinct odd prime factors then $2^r \mid \varphi(n)$.*

Proof. Let $p_1, \ldots, p_r$ be r distinct odd prime factors of n. Then $n = p_1^{k_1} \ldots p_r^{k_r} \cdot m$ such that $(p_1^{k_1} \ldots p_r^{k_r}, m) = 1$. Then

$$\varphi(n) = \varphi(p_1^{k_1} \ldots p_r^{k_r})\varphi(m) = p_1^{k_1-1}(p_1 - 1) \ldots p_r^{k_r-1}(p_r - 1) \cdot \varphi(m).$$

As $p_i - 1$ is even for every $i \in [r]$ the claim follows. ■

Proposition 7.56 *There are infinitely many n for which $\varphi(n)$ is a perfect square.*

Proof. For every odd integer $k = 2m + 1 > 1$ we have that $\varphi(2^k) = 2^{k-1} = 2^{2m} = (2^m)^2$. ■

Definition 7.57 *Let f be an arithmetic function. The* summation function of f *is given by*

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

We write $\Phi(n)$ to denote the summation function of φ. The following asserts that Φ is the identity function.

Theorem 7.58 *For every $n \geq 1$: $\Phi(n) = n$.*

Proof. For each divisor d of n define

$$C_d = \{m \in [1, n] : (m, n) = d\}.$$

Then the sets $(C_d)_{d|n}$ form a partition of the set $[1, n]$, that is, $[1, n] = \bigsqcup_{d|n} C_d$. Indeed, every $m \in [1, n]$ is either relatively prime to n in which case $m \in C_1$ or is not relatively prime to n and in which case there is a common divisor d of n and m such that $(m, n) = d$. Then

$$n = \sum_{d|n} |C_d|.$$

For an integer $m \in [1, n]$ we have that $(m, n) = d$ if and only if $(m/d, n/d) = 1$; that is, $m \in C_d$ if and only if $(m/d, n/d) = 1$. Hence, $|C_d| = \varphi(n/d)$ implying that

$$n = \sum_{d|n} \varphi(n/d).$$

Observe that for every divisor d of n we have that n/d is a divisor of n. This means that d and n/d while not equal still range over the same set of integers, namely the divisors of n. Hence

$$n = \sum_{d|n} \varphi(n/d) = \sum_{d|n} \varphi(d).$$

■

Example 7.59 For which integers n does $\varphi(3n) = 3\varphi(n)$ hold? We start by observing that if $(3, n) = 1$ then $\varphi(3n) = \varphi(3)\varphi(n) = 2\varphi(n)$; which is not exactly what we want. Now we note that

$$\varphi(3^2 n) = \varphi(3^2)\varphi(n) = (3^2 - 3)\varphi(n) = 3\underbrace{(3-1)}_{\varphi(3)}\varphi(n) = 3\varphi(3n).$$

This experiment shows that if instead of n we would have started with $3n$ we would have succeeded. So let us assume now that $n = 3^k m$, $k \geq 1$, where $(3, m) = 1$ and observe that we may write $n = 3m'$ so that

$$\varphi(3 \cdot 3m') = \varphi(3^2 m') = \varphi(3^2)\varphi(m') = 3(3-1)\varphi(m') = 3\varphi(3m').$$

In particular this shows that $\varphi(3n) = 3\varphi(n)$ holds if and only if $n = 3^k \cdot m$, $k \geq 1$ and $(3, m) = 1$. So this identity would holds for multiples of 3. Note that both direction of the if and only if are proved in one stroke through the equalities.

In fact a stronger property holds here. Let us show that 3 is not special and that $p\varphi(n) = \varphi(pn)$ holds if and only if n is a multiple of p. Both directions of the proof are included in the following equalities. Any multiple of p has the form $p^k m$, $k \geq 1$, where $(p, m) = 1$. Then

$$\varphi(p \cdot pm) = \varphi(p^2)\varphi(m) = p(p-1)\varphi(m) = p\varphi(p)\varphi(m) = p\varphi(pm).$$

7.3.2 *Euler's theorem*

The aim of this section is to prove the following generalisation of Fermat's little theorem.

Theorem 7.60 (Euler's theorem)
Let $1 < n \in \mathbb{Z}^+$ and let $a \in \mathbb{Z}$ satisfy $(a, n) = 1$. Then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Definition 7.61 *Let $n \geq 1$. A set of $\varphi(n)$ integers such that*
(i) each is relatively prime to n, and
(ii) any two distinct members are incongruent modulo n
is called a reduced system of residues modulo n.

Example 7.62 The canonical way to think of a reduced system of residues modulo an integer $n \geq 1$ is by taking representatives from each of the $\varphi(n)$ congruences classes identified by integers in $[1, n-1]$. For instance, the set $\{1, 3, 5, 7\}$ is the canonical reduced system of residues modulo 8. The set $\{3, 9, 15, 21\}$ is another example for such a system. Note that $9 \equiv 1 \pmod 8$, $15 \equiv 7 \pmod 8$, and that $21 \equiv 5 \pmod 8$. So the new set simply employs "new" class names for the classes seen in $\{1, 3, 5, 7\}$. Like the original set the new set also has the property that each of its members is relatively prime to 8.

The observant reader may notice that the new set was obtained from the old set by scaling it by 3 (i.e., multiplying each element by 3). The reason we were able to have the new set keep all properties of a reduced system of residues is that $(3, 8) = 1$.

This next lemma explains the phenomenon seen in the last example.

Lemma 7.63 *Let $n \geq 1$ and let $a \geq 1$ such that $(a, n) = 1$. If $r_1, \ldots, r_{\varphi(n)}$ is a reduced system of residues modulo n then so is $a \cdot r_1, \ldots, a \cdot r_{\varphi(n)}$.*

Proof. We verify the terms appearing in Definition 7.61. To verify term (i) assume towards a contradiction that $(ar_j, n) > 1$ for some $j \in [1, \varphi(n)]$ and let p be a prime divisor of (ar_j, n). Then either

$$p \mid a \text{ and } p \mid n$$

or

$$p \mid r_j \text{ and } p \mid n.$$

As $(a, n) = 1$, by assumption, the first alternative is impossible. Similarly, as $(r_j, n) = 1$, by assumption, the second alternative is also impossible. We reach a contradiction and thus verify (i) for every $j \in [1, \varphi(n)]$.

We proceed to term (ii) in Definition 7.61. Suppose that $ar_j \equiv ar_k \pmod{n}$ for some two distinct $j, k \in [1, \varphi(n)]$. Then as $(a, n) = 1$, by assumption, it follows that $r_j \equiv r_k \pmod{n}$ which is a contradiction to those being incongruent. ■

Prior to proving Euler's theorem let us be reminded of the proof we provided for Fermat's little theorem. To Prove Fermat's result we showed that

$$a \cdot (2a) \cdot (3a) \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot (p-1) \pmod{p}.$$

This congruence asserts that the set $\{a, 2a, 3a, \ldots, (p-1)a\}$ is represented modulo p by the *reduced system of residues modulo p* given by $[1, p-1]$. In Euler's theorem we substitute the prime p with a composite number n. However, the proof of Euler's theorem is essentially the same as that of Fermat's little theorem as seen next.

Proof of Theorem 8.15. Let n and a be given as specified by Euler's theorem. For any reduced system of residues modulo n namely $\{r_1, \ldots, r_{\varphi(n)}\}$ the set $\{ar_1, \ldots, ar_{\varphi(n)}\}$ is a reduced system of residues modulo n by Lemma 7.63. That is

$$(ar_1) \cdot (ar_2) \cdot (ar_3) \cdots (ar_{\varphi(n)}) \equiv r_1 \cdot r_2 \cdots r_{\varphi(n)} \pmod{n},$$

holds. We may then write write

$$a^{\varphi(n)} r_1 \cdot r_2 \cdots r_{\varphi(n)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(n)} \pmod{n};$$

and then reduce all r_i's without changing the modulo as all these are relatively prime to n yielding Euler's result. ■

We have seen how to use Fermat's little theorem to deduce inverses modulo a prime. Euler's theorem grants us a similar ability modulo composite numbers.

Corollary 7.64 *Let $n > 1$ be a positive integer and let a be an integer such that $(a, n) = 1$. Then the inverse of a modulo n is $a^{\varphi(n)-1}$.*

Proof. By Euler's theorem

$$1 \equiv a \cdot a^{\varphi(n)-1} \pmod{n}.$$

■

7.3.2.1 The Chinese remainder theorem: revisited

We use Euler's theorem to provide an alternative proof of the Chinese remainder theorem.

PROOF OF THEOREM 6.64. For $k \in [r]$ set $M_k = M/n_k$. Then

$$x = a_1 M_1^{\varphi(n_1)} + a_2 M_2^{\varphi(n_2)} + \cdots + a_r M_r^{\varphi(n_r)}.$$

As $M_j \equiv 0 \pmod{n_i}$ whenever $i \neq j$ we have that

$$x \equiv a_i M_i^{\varphi(n_i)} \pmod{n_i},$$

for every $i \in [r]$. Next, as $(M_i, n_i) = 1$ we have that

$$M_i^{\varphi(n_i)} \equiv 1 \pmod{n_i},$$

by Euler's theorem, for every $i \in [r]$. Then

$$x \equiv a_i \pmod{n_i},$$

for every $i \in [r]$.

The uniqueness part remains as in the original proof. ■

§7.4. THE RSA CRYPTO-SYSTEM

In this section we consider two cryptographic applications.

- *Encryption.* In this application we seek to send messages between two parties, namely Alice and Bob, and we seek that no third party, namely Eve, who might be eavesdropping to the communication channel would be able to obtain the content of the messages that Alice and Bob transmit between one another. To that end we seek to *jumble* the messages of Alice and Bob into some *ciphertext* that Eve would have a spend considerable computational resources in order to un-jumble, sort of speak, as to attain its content rendering the content obsolete by the time Eve is able to obtain it.

- *Digital signatures.* In this application we are not worried with eavesdropping and consequently will not be attempting to protect our messages from being read. We are however interested in being able to certify for one who is reading actual original messages put out by us that it were indeed us who sent the message. We are then interested in a form of *digital signature* for our messages that would be exceptionally hard to forge.

Both of these applications can be realised (with varying degrees of success) through two quite separate cryptographic schemes whose common theme is that a certain secrete piece of information, often referred to as the *key*, is used in order to encrypt and/or sign messages.

The first more naïve discipline is that of *private key encryption.* Under this scheme, encryption of messages, for instance, is attained by having both Alice and Bob be familiar with a certain secret key that can be used to both encrypt and decrypt messages. The canonical example for this scheme is the traditional *Caesar code* in which both Alice and Bob agree on a permutation φ of the alphabet used to convey messages; then to encrypt a message Alice applies φ to the message creating a ciphertext to transmit to Bob; upon receiving the ciphertext, Bob applies φ^- to it in order to retrieve the original message. The major flaw of this scheme is that both Alice and Bob have to somehow agree on φ; this can surely not entail transmitting φ itself which renders the whole approach quite limited.

Much more can be said about private key encryption systems that we omit here, for indeed our aim here is to introduce the RSA cryptosystem which is an instance of what is known as a *public key encryption system* which is certainly more advanced than the private key scheme. In the former, we equip each of Alice and Bob with two functions called *keys*. Alice has in her possession the keys P_A and S_A and Bob has the keys P_B and S_B. The keys P_A and P_B are the *public* keys of Alice and Bob, respectively, and these are public in the sense that both Alice and Bob publish these keys in plain sight for all to see including Eve. On the other hand, S_A and S_B are the *secret* keys of Alice and Bob, respectively, that they keep in secrete from the whole world include parties they communicate with directly.

All four functions are of the form $\mathcal{M} \to \mathcal{M}$ where $\mathcal{M}$ is the set of all acceptable messages. In particular, all these functions are permutations in the sense that for every $m \in \mathcal{M}$ the images $P_A(m), S_A(m), P_B(m)$, and $S_B(m)$ are all permutations of m. The functions P_A and S_A are inverses of one another so that for every $m \in \mathcal{M}$

$$S_A(P_A(m)) = m = P_A(S_A(m)).$$

The same is true for P_B and S_B.

Given such four functions we implement message encryption and digital signing as follows.

- *Encryption.* Suppose that Bob is interested in sending Alice a message that only she could read based on the assumption that S_A is not compromised in the sense that only Alice knows it. This process is as follows.

  1. Let m be Bob's message to Alice.
  2. Owing to P_A being publicly known, Bob is able to send $P_A(m)$ to Alice.
  3. Upon receiving $P_A(m)$, Alice computes $S_A(P_A(m))$ using S_A known only to her, by assumption, and retrieves m.

- *Digital signature.* In this application Alice has a message m that she seeks to sign so that anyone who reads m would be able to verify that m indeed originated from Alice and moreover that this signature could not be forged and this way convince parties that fake messages not originating from Alice actually did. Note that in this application Alice has no desire to hide m from the public and consequently she is not interested in encrypting it. We implement this application as follows.

  1. Let m be the message that Alice seeks to sign.
  2. Alice computes $\sigma := S_A(m)$.
  3. Alice publishes the pair (m, σ).
  4. If say Bob, or anyone else for that matter, seeks to authenticate that m was indeed written by Alice, he computes $P_A(\sigma)$ (using the publicly available key of Alice, namely P_A) and compares $P_A(\sigma)$ with m. If equality holds, Bob can be assured that m originated from Alice; otherwise he knows that m is a fake message.

The above implementation are certainly simple; assuming of course that such four function can actually be defined. We now tend to this matter.

RSA KEY GENERATION ALGORITHM:

1. Let q and q be two 'large' primes.
2. Set $n := pq$.
3. Let e be an odd number s.t. $(e, \varphi(n)) = 1$ (lets assume there is one for now).

4. Set d to be the modular inverse of e modulo $\varphi(n)$.
5. Set public key to be the pair (e, n) and the secret key to be (d, n).

This algorithm ended by producing pairs of numbers for the keys instead of functions. This is because here the agreement is that if, say Alice, was to use this algorithm to generate P_A and S_A then these are given by

$$P_A(m) := m^e \pmod{n} \text{ and } S_A(m) := m^d \pmod{n} \tag{7.65}$$

whenever $m \in \{[0]_n, \ldots, [n-1]_n\}$. The modular exponentiation involved in these two functions can of course be carried out using the algorithm presented in § 6.7 handling this issue.

Theorem 7.66 *Let P_A and S_A be as defined in (7.65). Then*

$$P_A(S_A(m)) = m = S_A(P_A(m))$$

for every $m \in \{[0]_n, \ldots, [n-1]_n\}$.

Proof. By definition, $P_A(S_A(m)) = m^{ed} \pmod{n} = S_A(P_A(m)$; this establishes that P_A and S_A are inverses of one another (as functions) and are thus both bijections. It remains to prove that $P_A(S_A(m)) = m$ whenever $m \in \{[0]_n, \ldots, [n-1]_n\}$. That is, we seek to prove that

$$m^{ed} \equiv m \pmod{n}$$

whenever $m \in \{[0]_n, \ldots, [n-1]_n\}$. Suffice to prove then that

$$m^{ed} \equiv m \pmod{p} \text{ and } m^{ed} \equiv m \pmod{q}.$$

We present the argument asserting the former. If $m \equiv 0 \pmod{p}$ the claim holds trivially, so we may assume that $m \not\equiv 0 \pmod{p}$. By definition, $ed \equiv 1 \pmod{\varphi(n)}$ and $\varphi(n) = (p-1)(q-1)$, by Theorem 7.51. Then

$$\begin{aligned}(p-1)(q-1) \mid ed - 1 &\implies ed - 1 = k(p-1)(q-1)\\ &\implies ed = 1 + k(p-1)(q-1),\end{aligned}$$

for some integer k. We may now write that

$$m^{ed} \equiv m^{1+k(p-1)(q-1)} \equiv m \cdot (m^{p-1})^{k(q-1)} \pmod{p}.$$

The assumption that $m \not\equiv 0 \pmod{p}$ implies that $(m, p) = 1$. (indeed, let $h \equiv m \pmod{p}$, then $h \in [1, p-1]$ owing to $p \not| m$). Fermat's little theorem, namely Theorem 7.10, now implies that $m^{ed} \equiv m \pmod{p}$ as required. ■

§7.5. Exercises

Exercise 1. Prove Fermat's little theorem (i.e., Corollary 7.12) that $a^p \equiv a \pmod{p}$ whenever p is a prime and $a \in \mathbb{Z}^+$ by induction on a.

Exercise 2. Let $p > 2$ be a prime and let $a_1, \ldots, a_p$ and $b_1, \ldots, b_p$ be two complete systems of residues modulo p where $a_p \equiv b_p \equiv 0 \pmod{p}$. Prove that $a_1b_1, a_2b_2, \ldots, a_pb_p$ is not a complete system of residues modulo p.

Hint: Wilson's theorem.

Exercise 3.

(a) Let n and m be two positive integers such that every prime divisor of m divides n. Prove that $\varphi(m \cdot n) = m\varphi(n)$.

(b) Conclude that if p is prime and $k \geq 2$, then $\varphi(\varphi(p^k)) = p^{k-2}\varphi((p-1)^2)$.

Exercise 4. Use Fermat's little theorem, Euler's theorem, and the Chinese remainder theorem to solve the following system of congruences.

$$\begin{aligned} 7x &\equiv 11 \pmod{51} \\ 8x &\equiv 21 \pmod{61} \\ 9x &\equiv 31 \pmod{71}. \end{aligned}$$

Exercise 5.

1. Show that
$$\sum_{i=1}^{p-1} i^{p-1} \equiv -1 \pmod{p}$$
for **every** prime p.

   Hint: Fermat's little theorem.

2. Show that
$$\sum_{i=1}^{p-1} i^{p} \equiv 0 \pmod{p}$$
whenever p is an **odd** prime.

   Hint: Fermat's little theorem.

Exercise 6. Show that 45 is pseudoprime to the bases 17 and 19.

Exercise 7. Let a and b be positive relatively prime integers. Show that

$$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{a \cdot b}.$$

Hint:

1. Euler's theorem (i.e., his generalisation to Fermat's little theorem).
2. Recall that if $s \equiv t \pmod{n_1}$ and $s \equiv t \pmod{n_2}$ and $(n_1, n_2) = 1$ then $s \equiv t \pmod{n_1 \cdot n_2}$.

Exercise 8. Given a prime number p, establish the congruence

$$(p-1)! \equiv p - 1 \pmod{1 + 2 + 3 + \cdots (p-1)}$$

Exercise 9. If p is a prime, prove that for any integer a,

$$p | a^p + (p-1)!a$$

and

$$p|(p-1)!a^p + a.$$

Exercise 10. For a prime p and $0 \leq k \leq p-1$, show that $k!(p-k-1)! \equiv (-1)^{k+1} \pmod{p}$.

Exercise 11. If p and q are distinct primes, prove that for any integer a,

$$pq|a^{pq} - a^p - a^q + a$$

Exercise 12. Use Fermat's little theorem to verify that 17 divides $11^{104} + 1$.

Exercise 13.

1. If $gcd(a, 35) = 1$, show that $a^{12} \equiv 1 \pmod{35}$.
2. If $gcd(a, 133) = gcd(b, 133) = 1$, show that $133|a^{18} - b^{18}$.

Exercise 14. Assume that p and q are distinct odd primes such that $p-1|q-1$. If $gcd(a, pq) = 1$, show that $a^{q-1} \equiv 1 \pmod{pq}$.

Exercise 15. Let n be a positive integer. For an integer a relatively prime to n write $\overline{a}$ to denote its inverse modulo n. Prove that if n is a pseudoprime to the base a then it is also a pseudoprime to the base $\overline{a}$.

Exercise 16. Prove that for any integer a relatively prime to 2730 it holds that $a^{13} \equiv a \pmod{2730}$.

Exercise 17. Show that if $(a, n) = (a-1, n) = 1$ then $\sum_{i=1}^{\varphi(n)} a^{i-1} \equiv 0 \pmod{n}$.

Exercise 18. For a positive integer n let $R_n := \{\ell \in [n] : (\ell, n) = 1\}$ (i.e., R_n is the canonical reduced system of residues modulo n). Prove that for $n > 2$

$$\sum_{r \in R_n} r = \frac{n\varphi(n)}{2}. \tag{7.67}$$

(note that $\varphi(n)$ is even for $n > 2$ so the right hand side here is an integer).

Exercise 19. Let A be a reduced system of residues modulo $n > 2$. Show that

$$\sum_{a \in A} a \equiv 0 \pmod{n}.$$

Exercise 20.

(a) Prove that $5 \mid a^{12} - 1$ whenever $(a, 5) = 1$.

(b) Prove that $7 \mid a^{12} - 1$ whenever $(a, 7) = 1$.

(c) Prove that $35 \mid a^{12} - 1$ whenever $(a, 35) = 1$.

Exercise 21. Prove theorem 7.25.

Exercise 22. Prove that 91 is not a pseudoprime to the base 2.

Exercise 23. Let p be an odd prime and let $p - 1 = 2^s t$ for some $1 \leq s \in \mathbb{Z}$ and odd $t \in \mathbb{Z}$. Prove that if $(a, p) = 1$ then either

$$a^t \equiv 1 \pmod{p}$$

or

$$a^{2^i t} \equiv -1 \pmod{p}$$

for some integer i satisfying $0 \leq i \leq s-1$.

Exercise 24. Determine whether the following system is soluble. If it is find the solutions.

$$\begin{aligned} 3^9 x &\equiv 15 \pmod{48} \\ 47x &\equiv 20 \pmod{3} \\ 24 \cdot 2 \cdot 21x &\equiv 14 \pmod{22}. \end{aligned}$$

Exercise 25. Let $p \equiv 3 \pmod{4}$ be prime. Prove that

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

§7.6. Solutions

Some of the solutions have been written by the TAs in the course and thus have a different style of writing to them. Over time we hope to normalise this part of the text as well.

Solution for Exercise 1. The proof is by induction on a. For $a = 1$ the claim is trivial. Assume then that the claim holds for $a = b$ and consider $a = b + 1$. Then, by the binomial theorem,

$$(b+1)^p \equiv \sum_{j=0}^{p} \binom{p}{j} b^j = b^p + pb^{p-1} + \cdots + pb + 1 \pmod{p}.$$

For $0 < j < p$ the coefficient $\binom{p}{j}$ is divisible by p so that $\binom{p}{j} b^j \equiv 0 \pmod{p}$ for all such j. It follows that

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

By the induction hypothesis $b^p \equiv b \pmod{p}$ so that

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

and the claim follows.

Solution for Exercise 2. For $a_1b_1, a_2b_2, \ldots, a_pb_p$ to be a complete system of residues modulo p under the assumption that $a_p \equiv b_p \equiv 0 \pmod{p}$ it must be that

$$(a_1b_1) \cdot (a_2b_2) \cdots (a_{p-1}b_{p-1}) \equiv (p-1)! \equiv -1 \pmod{p}, \tag{7.68}$$

by Wilson's theorem. To show that $a_1b_1, a_2b_2, \ldots, a_pb_p$ does not form a complete system of residues we show that (7.68) does not hold. Indeed, by Wilson's theorem we have that

$$a_1 \cdot a_2 \cdots a_{p-1} \equiv b_1 \cdot b_2 \cdots b_{p-1} \equiv -1 \pmod{p}.$$

Hence,

$$(a_1b_1) \cdot (a_2b_2) \cdots (a_{p-1}b_{p-1}) \equiv (-1)^2 \equiv 1 \pmod{p}.$$

As $p > 2$ we have that $-1 \not\equiv 1 \pmod{p}$. The claim follows.

Solution for Exercise 3.

(a) Let $m = p_1^{a_1} \cdots p_k^{a_k}$ and let $n = p_1^{b_1} \cdots p_k^{b_k} q_1^{\ell_1} \cdots q_r^{\ell_r}$ where $p_i \neq q_j$ for every $i \in [k]$ and $j \in [r]$. Then

$$\begin{aligned}
\varphi(mn) &= \varphi(p_1^{a_1+b_1} \cdots p_k^{a_k+b_k} q_1^{\ell_1} \cdots q_r^{\ell_r}) \\
&= p_1^{a_1+b_1} \cdots p_k^{a_k+b_k} q_1^{\ell_1} \cdots q_r^{\ell_r} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_k}\right) \\
&\left(p_1^{a_1} \cdots p_k^{a_k}\right) \left(p_1^{b_1} \cdots p_k^{b_k} q_1^{\ell_1} \cdots q_r^{\ell_r} \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_k}\right)\right) \\
&= m\varphi(n)
\end{aligned}$$

(b) We start by noting that $\varphi(p^k) = p^{k-1}(p-1)$. As $(p, p-1) = 1$ then $(p^{k-1}, p-1) = 1$. Consequently,

$$\begin{aligned}
\varphi(\varphi(p^k)) &= \varphi(p^{k-1}(p-1)) \\
&= \varphi(p^{k-1})\varphi(p-1) \\
&= p^{k-2}(p-1)\varphi(p-1).
\end{aligned}$$

By the first part of the question we have that $n\varphi(n) = \varphi(n^2)$ and apply this identity with $n = p-1$. We arrive at

$$= p^{k-2}\varphi((p-1)^2).$$

Solution for Exercise 4. Let us first note that $51 = 3 \cdot 17$, that 61 is prime (because no integer number between 2 and $\sqrt{61} \approx 7.8$ divides 61), and that 71 is prime (because no integer number between 2 and $\sqrt{71} \approx 8.4$ divides 71). Consequently each equation in our system has a unique solution as $(7, 51) = 1 \mid 11$, $(8, 61) = 1 \mid 21$, and $(9, 71) = 1 \mid 31$.

As 7 and 51 are co-prime we have, by Euler's theorem, that $7^{\varphi(51)} \equiv 1 \pmod{51}$. We may thus replace the equation $7x \equiv 11 \pmod{51}$ in our system with the equation $x \equiv 7^{\varphi 51-1} \cdot 11 \pmod{51}$ by multiplying the original equation by $7^{\varphi(51)-1}$ on both its sides. We note further that $\varphi(51) = \varphi(3)\varphi(17) = 2 \cdot 16 = 32$ so that the equation we arrive at here is $x \equiv 7^{31} \cdot 11 \pmod{51}$.

We proceed in a similar with the other two equations. However, as the moduli of these two equations are primes we use Fermat's little theorem instead of Euler's theorem. That is, we have that $8^{60} \equiv 1 \pmod{61}$ and that $9^{70} \equiv 1 \pmod{71}$. Multiplying the second equation on both sides by 8^{59} and the third equation on both its sides by 9^{69} we arrive at the system

$$\begin{aligned}
x &\equiv 7^{31} \cdot 11 \pmod{51} \\
x &\equiv 8^{59} \cdot 21 \pmod{61} \\
x &\equiv 9^{69} \cdot 31 \pmod{71}.
\end{aligned}$$

Next we simplify each equation further. For the first equation we note that $7^5 \equiv 28 \pmod{51}$, that $28^6 \equiv 25 \pmod{51}$, and that $25 \cdot 77 \equiv 1925 \equiv 38 \pmod{51}$. Hence for the first equation we have

$$x \equiv 7^{31} \cdot 11 \equiv (7^5)^6 \cdot 77 \equiv 38 \pmod{51}.$$

We turn to the second equation. Here we have that $8^2 \equiv 64 \equiv 3 \pmod{61}$ and that $3^5 \equiv -1 \pmod{61}$ so that

$$x \equiv (8^2)^{29} \cdot 8 \cdot 21 \equiv (3^5)^5 \cdot 3^4 \cdot 8 \cdot 21 \equiv -1 \cdot 3^4 \cdot 8 \cdot 3 \cdot 7 \equiv 8 \cdot 7 \equiv 56 \pmod{61}$$

Finally we consider the third equation as simplify as follows.

$$x \equiv (9^2)^{34} \cdot 9 \cdot 31 \equiv (10^7)^4 \cdot 10^6 \cdot 9 \cdot 31 \equiv 57 \cdot 36 \cdot 9 \cdot 31 \equiv 35 \pmod{71}.$$

We arrive at the system

$$\begin{aligned} x &\equiv 38 \pmod{51} \\ x &\equiv 56 \pmod{61} \\ x &\equiv 35 \pmod{71}. \end{aligned}$$

to which we apply the Chinese remainder theorem as 51, 61, and 71 are pairwise co-prime. We arrive at

$$x \equiv 185984 \pmod{51 \cdot 61 \cdot 71}$$

where $51 \cdot 61 \cdot 71 = 220881$.

Solution for Exercise 5.

1. For every $i \in [1, p-1]$ we have that $i^{p-1} \equiv 1 \pmod{p}$, by Fermat's little theorem. Hence

$$\sum_{i=1}^{p-1} i^{p-1} \equiv \sum_{i=1}^{p-1} 1 \equiv p-1 \equiv -1 \pmod{p}.$$

2. For every $i \in [1, p-1]$ we have that $i^p \equiv i \pmod{p}$, by Fermat's little theorem. Hence

$$\sum_{i=1}^{p-1} i^p \equiv \sum_{i=1}^{p-1} i \pmod{p}.$$

Recall that $\sum_{i=1}^{p-1} i = \frac{p(p-1)}{2}$. For $p = 2$ note that $\frac{p(p-1)}{2} = \frac{2(2-1)}{2} = 1 \not\equiv 0 \pmod{2}$. This is the reason the statement is restricted only for odd primes. Indeed when p is odd then $\frac{p(p-1)}{2} \equiv 0 \pmod{p}$. The claim follows.

Solution for Exercise 6. We start with 17 and show that $17^{45} \equiv 17 \pmod{45}$. We start by considering powers of 17 that are close to a multiple of 45. Surely 17 is not close. After trying 17^2, 17^3, we stumble upon $17^4 \equiv 1 \pmod{45}$. Sadly 45 is not a multiple of 4. But 44 is. So we write

$$17^{45} \equiv (17^4)^{11} \cdot 17 \equiv 1^{11} \cdot 17 \equiv 17 \pmod{45}.$$

Next we consider 19 and show that $19^{45} \equiv 19 \pmod{45}$. As before we start by looking at powers of 19 that are close to multiples of 45. Here the search ends fairly fast as $19^2 \equiv 1 \pmod{45}$. Again 45 is not even but 44 is forcing us into

$$19^{45} \equiv (19^2)^{22} \cdot 19 \equiv 19 \pmod{45}.$$

Solution for Exercise 7. By Euler's theorem

$$a^{\varphi(b)} \equiv 1 \pmod{b} \quad \text{and} \quad b^{\varphi(a)} \equiv 1 \pmod{a}.$$

Surely $a^{\varphi(b)} \equiv 0 \pmod{a}$. Then

$$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{a}.$$

In a similar manner as $b^{\varphi(a)} \equiv 0 \pmod{b}$. Then

$$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{b}.$$

Then as $(a, b) = 1$ we get

$$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{a \cdot b}.$$

Solution for Exercise 8. From Wilson's Theorem

$$(p-1)! \equiv -1 \equiv p-1 \pmod{p}.$$

Then $p|(p-1)! - (p-1)$. Now for all $n \in \mathbb{N}$

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Then if $n = p - 1$

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

Since $p - 1$ is even, $\frac{p-1}{2}$ is an integer, and clearly, $\frac{p-1}{2} < (p-1)$.

Let us note that, $(p-1)$ divides $[(p-1)! - (p-1)]$ and $\frac{(p-1)}{2}$ divides $[(p-1)! - (p-1)]$.
Also, $gcd(\frac{(p-1)}{2}, p) = 1$, since p is prime.
We have that p and $\frac{p-1}{2}$ divide $(p-1)! - (p-1)$, so $\frac{(p-1)p}{2} = 1+2+\cdots+(p-1)$ divides $(p-1)! - (p-1)$ or

$$(p-1)! \equiv p-1 \pmod{1 + 2 + 3 + \cdots (p-1)}.$$

Solution for Exercise 9. Let us prove the first statement. By Fermat's little Theorem for any $a \in \mathbb{Z}^+$

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

By Wilson's Theorem we have

$$-1 \equiv (p-1)! \pmod{p}.$$

Multiplying we get

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

or

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

and

$$p|a^p + (p-1)!a.$$

Now we prove the second statement. As in the first we use Wilson's Theorem and Fermat's little Theorem

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

Multiplying together we get,

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

or

$$p|(p-1)!a^p + a$$

Solution for Exercise 10. First, let us note that

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdot 3 \cdots (p-k-1)(p-k) \cdots (p-2)(p-1) \\ &= (p-k-1)!(p-k) \cdots (p-2)(p-1)\end{aligned}$$

But

$$\begin{aligned}p-1 &\equiv -1 \pmod p \\ p-2 &\equiv -2 \pmod p \\ &\cdots \\ p-k &\equiv -k \pmod p\end{aligned}$$

By multiplying we have

$$(p-k) \cdots (p-2)(p-1) \equiv (-k) \cdots (-2)(-1) \pmod p.$$

But $(-k) \cdots (-2)(-1) = (-1)^k k!$ so

$$\begin{aligned}(p-k) \cdots (p-2)(p-1) &\equiv (-1)^k k! \pmod p \\ (p-k-1)!(p-k) \cdots (p-2)(p-1) &\equiv (-1)^k k!(p-k-1)! \pmod p \\ (p-1)! &\equiv (-1)^k k!(p-k-1)! \pmod p\end{aligned}$$

By Wilson's Theorem $(p-1)! \equiv -1 \pmod p$. Therefore

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

Since $(-1)^k \cdot (-1)^k = 1$ and $(-1) \cdot (-1)^k = (-1)^{k+1}$ after multiplying both sides by $(-1)^k$ we get

$$(-1)^{k+1} \equiv k!(p-k-1)! \pmod p$$

Solution for Exercise 11. Suffice to prove that $p \mid a^{pq} - a^p - a^q + a$ and that $q \mid a^{pq} - a^p - a^q + a$ as that implies that both p and q are factors of $a^{pq} - a^p - a^q + a$ implying the claim. We set out to prove that $q \mid a^{pq} - a^p - a^q + a$; the argument proving $p \mid a^{pq} - a^p - a^q + a$ is symmetrical and thus omitted. By Corollary 7.12 $(a^p)^q \equiv a^p \pmod q$ and $a^q \equiv a \pmod q$. Hence $q \mid (a^p)^q - a^p$ and $q \mid a^q - a$. Then

$$q \mid \big((a^p)^q - a^p\big) - \big(a^q - a\big) = a^{pq} - a^p - a^q + a.$$

Solution for Exercise 12. Since $17 \nmid 11$, by Fermat's Theorem $11^{16} \equiv 1 \pmod{17}$.

$$(11^{16})^6 = 11^{96} \equiv 1 \pmod{17}$$

But $121 = 11^2$ and $7 \cdot 17 = 119 = 121 - 2$ then

$$\begin{aligned}11^2 &\equiv 2 \pmod{17} \\ 11^8 &\equiv 2^4 \equiv 16 \pmod{17}.\end{aligned}$$

By multiplying

$$\begin{aligned} 11^{96} \cdot 11^{8} &\equiv 16 \pmod{17} \\ 11^{104} &\equiv 16 \pmod{17}. \end{aligned}$$

But $16 \equiv -1 \pmod{17}$ so $11^{104} \equiv -1 \pmod{17}$. Therefore 17 divides $11^{104} + 1$.

Solution for Exercise 13.

1. Since $35 = 7 \cdot 5$, then $gcd(a, 7) = 1$ and $gcd(a, 5) = 1$.
   By Fermat's Theorem $a^6 \equiv 1 \pmod 7$ and $a^4 \equiv 1 \pmod 5$. So

   $$\begin{aligned} a^{12} = a^6 \cdot a^6 &\equiv 1 \pmod 7 \\ (a^4)^3 = a^{12} &\equiv 1^3 \pmod 5 \end{aligned}$$

   Since $gcd(5, 7) = 1$ by multiplying we get

   $$35 | a^{12} - 1$$

   The claim follows.

2. We have $133 = 7 \cdot 19$ and

   $$gcd(a, 19) = gcd(b, 19) = 1.$$

   By Fermat's Theorem

   $$a^{18} \equiv 1 \pmod{19}, \quad b^{18} \equiv 1 \pmod{19}$$

   Subtracting these two equations we arrive at

   $$a^{18} - b^{18} \equiv 1 - 1 \equiv 0 \pmod{19}.$$

   Therefore $19 | a^{18} - b^{18}$. Since

   $$gcd(a, 7) = gcd(b, 7) = 1$$

   then by Fermat's Theorem

   $$\begin{aligned} a^6 &\equiv 1 \pmod 7 \\ b^6 &\equiv 1 \pmod 7 \\ a^6 - b^6 &\equiv 0 \pmod 7. \end{aligned}$$

   Therefore $7 | a^6 - b^6$. Since $a^{18} - b^{18} = (a^6)^3 - (b^6)^3 = (a^6 - b^6)((a^6)^2 + a^6 b^b + (b^6)^2)$ then

   $$7 | a^{18} - b^{18}$$

   and

   $$7 \cdot 19 = 133 | a^{18} - b^{18}.$$

Solution for Exercise 14. We have $gcd(a, pq) = 1$ so $gcd(a, p) = gcd(a, q) = 1$ where p, q are

distinct primes. By Fermat's Theorem $a^{p-1} \equiv 1 \pmod{p}$ and $a^{q-1} \equiv 1 \pmod{q}$.
Since $p-1|q-1$, then $q-1 = k(p-1)$ for some $k \in \mathbb{Z}$.

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod{p} \\ a^{k(p-1)} &\equiv 1 \pmod{p} \\ a^{q-1} &\equiv 1 \pmod{p} \end{aligned}$$

Therefore $p|a^{q-1}-1$ and $q|a^{q-1}-1$. So

$$pq|a^{q-1}-1$$

and

$$a^{q-1} \equiv 1 \pmod{pq}$$

Solution for Exercise 15. By assumption, $a^n \equiv a \pmod{n}$. Multiplying by $\overline{a}^n$ on both sides we get

$$\overline{a}^n a^n \equiv \overline{a}^n a \pmod{n}.$$

As $\overline{a}^n a^n \equiv 1 \pmod{n}$ (indeed, $\overline{a}^n a^n \equiv \underbrace{(\overline{a}a)\cdot(\overline{a}a)\cdots(\overline{a}a)}_{n \text{ times}} \pmod{n}$) , then

$$1 \equiv \overline{a}^n a \pmod{n}.$$

Multiplying by $\overline{a}$ on both sides we get

$$\overline{a}^n \equiv \overline{a} \pmod{n}.$$

Solution for Exercise 16. We start with the prime factorisation of 2730 which is $2730 = 2{\cdot}3{\cdot}5{\cdot}7{\cdot}13$. We seek to apply Euler's theorem. For this we need the values of φ at the factors of 2730 which is a triviality:

$$\varphi(2) = 1, \varphi(3) = 2, \varphi(5) = 4, \varphi(7) = 6, \varphi(13) = 12.$$

As a is relatively prime to 2730, by assumption we may use Euler's theorem to generate the following:

$$\begin{aligned} \underbrace{a^1 \equiv 1 \pmod{2}}_{\text{Euler}} &\implies a^{12} \equiv 1 \pmod{2} \\ a^2 \equiv 1 \pmod{3} &\implies a^{12} \equiv 1 \pmod{3} \\ a^4 \equiv 1 \pmod{5} &\implies a^{12} \equiv 1 \pmod{5} \\ a^6 \equiv 1 \pmod{7} &\implies a^{12} \equiv 1 \pmod{7} \\ & \qquad\quad a^{12} \equiv 1 \pmod{13}. \end{aligned}$$

These congruences then imply that $a^{12} \equiv 1 \pmod{2 \cdot 3 \cdot 5 \cdot 7 \cdot 13}$; multiplying by a on both sides gives us that

$$a^{13} \equiv a \pmod{2730}$$

as required.

Solution for Exercise 17. From the theory of polynomial factorisation (i.e., from high school) we have the identity

$$a^{\varphi(n)} - 1 = (a-1)\left(a^{\varphi(n)-1} + \cdots + a^2 + a + 1\right).$$

As $(a, n) = 1$ we also have that $a^{\varphi(n)} \equiv 1 \pmod{n}$ so that $a^{\varphi(n)} - 1 \equiv 0 \pmod{n}$. Then

$$(a-1)\left(a^{\varphi(n)-1} + \cdots + a^2 + a + 1\right) \equiv 0 \pmod{n}.$$

As $(a-1, n) = 1$ we reduce by $a - 1$ and get

$$a^{\varphi(n)-1} + \cdots + a^2 + a + 1 \equiv 0 \pmod{n}.$$

Solution for Exercise 18. We first note that whenever $n \geq 2$, for every $a \in \mathbb{Z}$ it holds that $(a, n) = 1$ if and only if $(n - a, n) = 1$. Therefore $R_n = \{\ell \in [n] : (n - \ell, n) = 1\}$. Thus,

$$\sum_{r \in R_n} r = \sum_{r \in R_n} n - r = \varphi(n)n - \sum_{r \in R_n} r$$

Hence, $2\sum_{r \in R_n} r = \varphi(n)n$. The claim follows.

Solution for Exercise 19. Let R_n be the canonical reduced system of residues modulo n. Then, as $n > 2$, we have

$$\sum_{r \in R_n} r = \frac{n\varphi(n)}{2} \equiv 0 \pmod{n},$$

where the first equality is due to (7.67). As the sets A and R_n both serve as reduced systems of residues modulo n, the members of A are congruent to the members of R_n in some order modulo n rendering

$$\sum_{a \in A} a \equiv \sum_{r \in R_n} r \equiv 0 \pmod{n}$$

as required.

Solution for Exercise 20.

(a) By Fermat's theorem $a^4 \equiv 1 \pmod{5}$. Then $a^{12} \equiv (a^4)^3 \equiv 1 \pmod{5}$ so that $a^{12} - 1 \equiv 0 \pmod{5}$.

(b) By Fermat's theorem $a^6 \equiv 1 \pmod{7}$. Then $a^{12} \equiv (a^6)^2 \equiv 1 \pmod{7}$ so that $a^{12} - 1 \equiv 0 \pmod{7}$.

(b) As $35 = 5 \cdot 7$ and $(5, 7) = 1$ then $a^{12} - 1 \equiv 0 \pmod{35}$ by the previous two section of the problem.

Solution for Exercise 21. TODO

Solution for Exercise 22.

$$2^{90} \equiv (2^{10})^9 \equiv 1024^9 \equiv 0 \pmod{2}.$$

Solution for Exercise 23. As p is prime only $[1]_p$ and $[-1]_p$ are their own inverses. That is the only solutions for $x^2 \equiv 1 \pmod{p}$ are $\pm 1 \pmod{p}$. We use this fact as follows. Assume towards a contradiction that the claim is false and that $a^t \not\equiv 1 \pmod{p}$ and that for every $i \in [0, s-1]$: $a^{2^i t} \not\equiv -1 \pmod{p}$. By Fermat's little theorem $a^{p-1} \equiv a^{2^s t} \equiv 1 \pmod{p}$. Then $(a^{2^{s-1}t})^2 \equiv 1 \pmod{p}$ implying that $a^{2^{s-1}t}$ is its own inverse modulo p; hence $a^{2^{s-1}t} \equiv \pm 1 \pmod{p}$. By assumption, $a^{2^{s-1}t} \not\equiv -1 \pmod{p}$ so we conclude

that $a^{2^{s-1}t} \equiv 1 \pmod{p}$ must hold. Repeating this argument until the exponent of 2 is exhausted leads to the congruence $a^t \equiv 1 \pmod{p}$. This contradicts our initial assumption.

Solution for Exercise 24. We commence by migrating to a more pleasant system. We start with the first equation namely $3^9 x \equiv 15 \pmod{48}$. Noting that $3 \mid 3^9$, $3 \mid 15$, and $3 \mid 48$ we see that this equation is equivalent to $3^8 \equiv 5 \pmod{16}$. Noting that $\varphi(16) = 8$ and that $(3, 16) = 1$ we have $3^8 \equiv 1 \pmod{16}$. Hence we may replace the first equation with $x \equiv 5 \pmod{16}$. This equation we note is soluble.

We proceed to the second equation. This we rewrite as $45x + 2x \equiv 20 \pmod{3}$ which is equivalent to $2x \equiv 20 \pmod{3}$ as $45 \equiv 0 \pmod{3}$. As $(2, 3) = 1$ we may then reduce by 2 and arrive at $x \equiv 10 \pmod{3}$. This equation we note is soluble.

For the final equation we note that $7 \mid 21$, $7 \mid 14$ and that $7 \mid 77$. Hence we may write $24 \cdot 2 \cdot 3x \equiv 2 \pmod{11}$. This we rewrite as $6 \cdot 2 \cdot 4 \cdot 3x \equiv 2 \pmod{11}$. Recalling that 6 and 2 and 4 and 3 are modular inverses of one another respectively modulo 11 we have that $6 \cdot 2 \cdot 4 \cdot 3 \equiv 1 \pmod{11}$. Hence for the third equation we have $x \equiv 2 \pmod{11}$. This equation is soluble as well.

The new system is then

$$\begin{aligned} x &\equiv 5 \pmod{16} \\ x &\equiv 10 \pmod{3} \\ x &\equiv 2 \pmod{11}. \end{aligned}$$

As $16, 3$, and 11 are pairwise co-prime this system has a solution by the Chinese reminder theorem. We leave this calculation to the reader.

Solution for Exercise 25. Owing to the congruence $p - i \equiv -i \pmod{p}$ for every $i \in \{-1, -2, \ldots, -(p-1)/2\}$ we can write

$$\begin{aligned} (p-1)! &\equiv 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \cdot (-2) \cdot (-1) \\ &\equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \frac{p+1}{2} \cdot \left(-\frac{p-1}{2}\right) \\ &\equiv (-1)^{(p-1)/2} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}. \end{aligned}$$

Then

$$-1 \equiv (-1)^{(p-1)/2} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$$

by Wilson's theorem. Multiplying both sides by $(-1)^{(p-1)/2}$ we arrive at

$$(-1)^{(p+1)/2} \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}.$$

Recalling that p is of the form $4k + 3$ leads us to note that $(p+1)/2$ is of the form $(4k+4)/2 = 2k + 2$ which is clearly even. The claim follows.

Lecture 8

Quadratic residues

Let p be an odd prime and let a be an integer such that $p \not| a$.

Is a a perfect square modulo p?

Put another way, is there an integer x such that

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

Why should this question be of any interest to us? We did take interest in solving equations of the form $ax \equiv b \pmod{m}$. Hence it is only natural that the next step would be to ask about equations of the form $ax^2 + bx + c \equiv 0 \pmod{m}$, say.

When $m = p$ is an odd prime and $(a, p) = 1$ the following can be said. The assumptions that p is odd and $(a, p) = 1$ imply that $(4a, p) = 1$. Then the equation

$$ax^2 + bx + c \equiv 0 \pmod{p} \tag{8.1}$$

is equivalent to

$$4a(ax^2 + bx + c) \equiv 0 \pmod{p}.$$

The identity

$$4a(ax^2 + bx + c) = (2ax + b)^2 - (b^2 - 4ac),$$

allows us to focus on the equation

$$(2ax + b)^2 \equiv (b^2 - 4ac) \pmod{p}.$$

Setting $y = 2ax + b$ and $d = b^2 - 4ac$ yields the more pleasant quadratic equation

$$y^2 \equiv d \pmod{p} \tag{8.2}$$

Now, if $x \equiv x_0 \pmod{p}$ is a solution of (8.1) then $y = 2ax_0 + b$ is a solution to (8.2). Conversely, if $y \equiv y_0 \pmod{p}$ is a solution to (8.2) then the equation $2ax \equiv y_0 - b \pmod{p}$ has a unique solution (as $(2a, p) = 1$) for x modulo p; this solution solves (8.1).

We then see that in order to solve (8.1) we would first like to solve the quadratic equation $y^2 \equiv d \pmod{p}$ and then given a solution y_0 to such an equation solve the linear equation $y_0 \equiv 2ax - b \pmod{p}$. As we already know how to solve linear congruences we focus in this lecture on the quadratic equation.

The general form of the quadratic equation that we seek to solve is as follows. Given an odd prime p and an a such that $(a, p) = 1$ are there any values of x for which

$$x^2 \equiv a \pmod{p}? \tag{8.3}$$

Let us note that if $x_0 \pmod p$ is a solution to this quadratic equation then so is $(p - x_0) \pmod p$ as indeed

$$(p - x_0)^2 \equiv p^2 - 2px_0 + x_0^2 \equiv x_0^2 \pmod p.$$

Now, $p - x_0 \equiv -x_0 \pmod p$ leading us to the statement

$$\text{if } x_0 \pmod p \text{ is a solution to } x^2 \equiv a \pmod p \text{ so is } -x_0 \pmod p. \tag{8.4}$$

As the degree of the polynomial here is 2 we know that there are no additional incongruent solutions modulo p by the following result of Lagrange.

Theorem 8.5 (Lagrange's theorem)
If p is a prime and

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

is a polynomial of degree $n \geq 1$ with integral coefficients such that $p \not| a_n$ then the equation

$$f(x) \equiv 0 \pmod p$$

has at most n incongruent solutions modulo p.

Proof. The proof is by induction on n. For $n = 1$, we have $f(x) = a_1 x + a_0$ with $p \nmid a_1$. A root of $f(x)$ modulo pp is a solution to the linear congruence $a_1 x \equiv -a_0 \pmod p$. Owing to $(a_1, p) = 1$, this congruence has a unique solution modulo m, by Corollary 6.33, and thus the claim holds for $n = 1$.

Suppose the theorem is true for polynomials of degree $n - 1$ and let $f(x)$ be a degree n polynomial with leading coefficient not divisible by p. Assume that $f(x)$ admits $n + 1$ incongruent roots modulo p, namely, $c_0, c_1, \ldots, c_n$. Then

$$\begin{aligned} f(x) - f(c_0) &= a_n(x^n - c_0^n) + \cdots + a_1(x - c_0) \\ &= a_n(x - c_0)(x^{n-1} + x^{n-2}c_0 + \cdots + xc_0^{n-2} + c_0^{n-1}) \\ &\quad + a_{n-1}(x - c_0)(x^{n-2} + x^{n-3}c_0 + \cdots + xc_0^{n-3} + c_0^{n-2}) \\ &\quad + \cdots + a_1(x - c_0) \\ &= (x - c_0)g(x) \end{aligned}$$

where $g(x)$ is a degree $n - 1$ polynomial with $_n$ as a leading coefficient.

Let us now note that $c_1, \ldots, c_n$ are all roots of $g(x)$ modulo p. To see this, fix $k \in [1, n]$. Owing to $f(c_0) \equiv f(c_k) \pmod p$, it follows that

$$f(c_k) - f(c_0) = (c_k - c_0)g(c_k) \equiv 0 \pmod p.$$

As $c_k \not\equiv c_0 \pmod p$, by assumption, it follows that $g(c_k) \equiv 0 \pmod p$ and that c_k is a root of $g(x)$ modulo p.

We have just established that the polynomial $g(x)$ which satisfies the induction hypothesis admits n roots; a contradiction. ■

That is,

$$\text{Congruence (8.3) either has no solution or precisely two incongruent solutions modulo } p. \tag{8.6}$$

Through (8.4) we noted that if $x_0 \pmod p$ is a solution then so is $-x_0 \pmod p$. Here in (8.6) we are essentially claiming that it also must hold that $x_0 \not\equiv -x_0 \pmod p$. The following lemma summarises the above discussion without resorting to Lagrange's theorem.

Lemma 8.7 *Let p be an odd prime and let $a \in \mathbb{Z}$ such that $(a, p) = 1$. Then*

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

either has no solutions or exactly two incongruent solutions modulo p.

Proof. We have seen that if $x_0 \pmod{p}$ is a solution for $x^2 \equiv a \pmod{p}$ then so is $-x_0 \pmod{p}$ forms a solution. We note that $x_0 \not\equiv -x_0 \pmod{p}$ for otherwise, if $x_0 \equiv -x_0 \pmod{p}$ then $2x_0 \equiv 0 \pmod{p}$. Then $p \mid 2$ or $p \mid x_0$. Surely $p \mid 2$ is impossible. As $x_0^2 \equiv a \pmod{p}$ having $p \mid x_0$ implies that $p \mid a$ which contradicts the assumption.

It remains to show that there are no more than two incongruent solutions modulo p. To see this let x_0 and x_1 be solutions to $x^2 \equiv a \pmod{p}$. Then $x_0^2 \equiv x_1^2 \equiv a \pmod{p}$ so that $x_0^2 - x_1^2 \equiv (x_0 - x_1)(x_0 + x_1) \equiv 0 \pmod{p}$. Then $p \mid x_0 - x_1$ or $p \mid x_0 + x_1$. In the former case $x_1 \equiv x_0 \pmod{p}$ and in the latter case $x_1 \equiv -x_0 \pmod{p}$. ■

To understand the appeal that Lemma 8.7 has for us one ought to consider quadratic equations over $\mathbb{R}$. The equation $ax^2 + bx + c = 0$ either has no solutions over $\mathbb{R}$, one solution, or two solutions. For quadratic equations modulo an odd prime Lemma 8.7 asserts that the situation is simpler: either there are no solution or precisely two. Lemma 8.7 only handles quadratic equations modulo an odd prime. For $p = 2$ the lemma is false; indeed for $p = 2$ a quadratic equation can have a single solution.

Example 8.8 The equation $x^2 \equiv 1 \pmod{2}$ has one solution. Indeed any $x \equiv 1 \pmod{2}$ is a solution and any $x \equiv -1 \pmod{2}$ is a solution. However $-1 \equiv 1 \pmod{2}$. Moreover, in Lemma 6.48 we have seen that for $k \geq 3$ the equation $x^2 \equiv 1 \pmod{2^k}$ has *four* incongruent solutions.

Definition 8.9 *Let $m > 1$ be an integer. We say that $a \in \mathbb{Z}$ is a* quadratic residue modulo m *if $(a, m) = 1$ and $x^2 \equiv a \pmod{m}$ has a solution.*

If $x^2 \equiv a \pmod{m}$ has no solution then a is called a *quadratic non-residue modulo m*. For a prime p we can express this definition more clearly. The integers captured by any of the congruence classes found in the multiset[1] $\{[1^2]_p, [2^2]_p, \ldots, [(p-1)^2]_p\}$. Indeed, the squares of the canonical set of representatives modulo p includes all congruence classes that contain quadratic residues. Which congruence classes are captured through the multiset $\{[1^2]_p, [2^2]_p, \ldots, [(p-1)^2]_p\}$? The following example provides an answer for $p = 11$.

Example 8.10 What are the quadratic residues modulo 11?

$$\begin{aligned}
1^2 &\equiv 10^2 \equiv 1 \pmod{11} \\
2^2 &\equiv 9^2 \equiv 4 \pmod{11} \\
3^2 &\equiv 8^2 \equiv 9 \pmod{11} \\
4^2 &\equiv 7^2 \equiv 5 \pmod{11} \\
5^2 &\equiv 6^2 \equiv 3 \pmod{11},
\end{aligned}$$

so that $\{1, 3, 4, 5, 9\}$ are quadratic residues modulo 11 while $2, 6, 7, 8, 10$ are the quadratic non-residues modulo 11. Note that each quadratic residue has two solutions whose square yields that residue. More importantly, we got an answer to the question that prompted this example. The distinct congruence classes captured through $\{1^2, 2^2, \ldots, 10^2\}$ are precisely $\{1^2, 2^2, 3^2, 4^2, 5^2\} =$

[1] By *multiset* we mean a set with repetitions allowed which makes it a collection and not a set; another name for collection is *multiset*.

$\{1, 3, 4, 5, 9\}$. That is the set $\{1^2, 2^2, \ldots, 10^2\}$ is represented by $\frac{11-1}{2}$ distinct congruence classes.

For an odd prime p the number of quadratic residues and the the number of quadratic non-residues modulo p are equal.

Theorem 8.11 *If p is an odd prime then there are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues modulo p amongst $\{1, 2, \ldots, p-1\}$. In particular, every quadratic residue modulo p is congruent to one of the members of $\{1^2, 2^2, \ldots, ((p-1)/2)^2\}$ which are all pairwise incongruent modulo p.*

Proof. As mentioned above, the congruence classes modulo p capturing all quadratic residues modulo p are the classes capturing the squares $1^2, 2^2, \ldots, (p-1)^2$ modulo p. As for each $x \in [1, p-1]$ we have that $x^2 \equiv (p-x)^2 \equiv (-x)^2 \pmod{p}$ it follows that

$$\begin{aligned} 1^2 &\equiv (p-1)^2 \pmod{p} \\ 2^2 &\equiv (p-2)^2 \pmod{p} \\ \vdots \quad & \quad \vdots \qquad\qquad \text{(recall here that } p \text{ is odd)} \\ \left(\tfrac{p-1}{2}\right)^2 &\equiv \left(\tfrac{p+1}{2}\right)^2 \pmod{p}; \end{aligned}$$

demonstrating that the congruence classes of the members of $\{1^2, 2^2, \ldots, ((p-1)/2)^2\}$ capture all squares $\{1^2, 2^2, \ldots, (p-1)^2\}$. This gives us an upper bound on the number of quadratic residues modulo p.

It is still possible that fewer congruence classes can be used to capture all quadratic residues. We show now that this is impossible. To that end we show that the members of $\{1^2, 2^2, \ldots, ((p-1)/2)^2\}$ are all incongruent modulo p. For suppose that there would have been $r^2 \equiv s^2 \pmod{p}$ for some $1 \leq s < r \leq (p-1)/2$. Then $p \mid r^2 - s^2 = (r+s)(r-s)$ so that $p \mid r+s$ or $p \mid r-s$. Note that $2 \leq r+s \leq p-2$ and that $1 \leq r-s \leq (p-1)/2$ hence both options are impossible. ■

Example 8.12 Here are the quadratic residues modulo 19:

$$\begin{aligned} 1^2 &\equiv 18^2 \equiv 1 \pmod{19} \\ 2^2 &\equiv 17^2 \equiv 4 \pmod{19} \\ 3^2 &\equiv 16^2 \equiv 9 \pmod{19} \\ 4^2 &\equiv 15^2 \equiv 16 \pmod{19} \\ 5^2 &\equiv 14^2 \equiv 6 \pmod{19} \\ 6^2 &\equiv 13^2 \equiv 17 \pmod{19} \\ 7^2 &\equiv 12^2 \equiv 11 \pmod{19} \\ 8^2 &\equiv 11^2 \equiv 7 \pmod{19} \\ 9^2 &\equiv 10^2 \equiv 5 \pmod{19}. \end{aligned}$$

§8.1. Euler's criterion

The following result of Euler aids us in identifying quadratic residues and quadratic non-residues modulo a prime.

Theorem 8.13 (Euler's criterion)
Let p be an odd prime and let a be an integer such that $(a,p)=1$. Then a is a quadratic residue modulo p if and only if

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

We shall prefer an alternative more illuminating formulation of Euler's criterion employing the following notation put forth by Legendre.

Definition 8.14 *Let p be an odd prime and let a be an integer relatively prime to p. Then the* Legendre symbol *is given by*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ is a quadratic residue modulo } p \\ -1, & a \text{ is a quadratic non-residue modulo } p \end{cases}$$

Another definition of the Legendre symbol is to set it to zero if $p \mid a$:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & p \mid a, \\ 1, & p \nmid a \text{ and } x^2 \equiv a \pmod{p} \text{ is soluble}, \\ -1, & \text{otherwise.} \end{cases}$$

Theorem 8.15 (Euler's criterion - alternative formulation)
Let p be an odd prime and let a be relatively prime to p. Then

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

Proof. We present an argument due to Dirichlet. Suppose, first, that $\left(\frac{a}{p}\right) = 1$. Then $x^2 \equiv a \pmod{p}$ has a solution, namely $x_0^2 \equiv a \pmod{p}$. Then

$$a^{(p-1)/2} = (x_0^2)^{(p-1)/2} \equiv x_0^{p-1} \pmod{p}.$$

As $(x_0, p) = 1$ we have by Fermat's little theorem that

$$x_0^{p-1} \equiv 1 \pmod{p}$$

concluding the argument in this case.

Suppose, second, that $\left(\frac{a}{p}\right) = -1$ so that $x^2 \equiv a \pmod{p}$ has no solutions. For each integer b with $(b,p)=1$ the linear congruence $by \equiv a \pmod{p}$ has a unique solution modulo p. Let $y_{a,b}$ denote the canonical representative modulo p of this unique solution so that $y_{a,b} \in [1, p-1]$ (zero is excluded here as $a \neq 0$). Now, as $x^2 \equiv a \pmod{p}$ has no solution it follows that $y_{a,b} \neq b$. In fact, for any pair of $b, b' \in [1, p-1]$ with $b \neq b'$ it must hold that $y_{a,b} \neq y_{a,b'}$. For otherwise

$$by_{a,b} \equiv b'y_{a,b'} \equiv b'y_{a,b} \pmod{p}$$

holds. As $1 \leq y_{a,b} \leq p-1$ then $(y_{a,b}, p) = 1$ allowing us to reduce it in the last congruence as to arrive at $b \equiv b' \pmod{p}$ which is a contradiction.

Then the set of pairs $\{\{b, y_{a,b}\} : b \in [1, p-1]\}$ forms a partition of the set $[1, p-1]$ into $(p-1)/2$ pairs; each pair with the product of its members congruent to a modulo p. Consequently we may write

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

By Wilson's theorem $(p-1)! \equiv -1 \pmod{p}$. This concludes the proof in this case. ■

Important comment: As $\left(\frac{a}{p}\right) = \pm 1$ it follows that when we say that $\left(\frac{a}{p}\right) \equiv 1 \pmod{p}$ then $\left(\frac{a}{p}\right) = 1$. When we say that $\left(\frac{a}{p}\right) \equiv -1 \pmod{p}$ then $\left(\frac{a}{p}\right) = -1$.

8.1.1 *Properties of the Legendre symbol*

A corollary of Theorem 8.11 is the following.

Corollary 8.16 *Let p be an odd prime. Then*

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

Proposition 8.17 (Properties of the Legendre symbol)
Let p be an odd prime and let a, b be integers co-prime with p. Then

1. *if $a \equiv b \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;*
2. *$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$; i.e., the function $\left(\frac{\cdot}{p}\right) : \mathbb{Z} \to \mathbb{Z}$ is multiplicative.*
3. *$\left(\frac{a^2}{p}\right) = 1$;*
4. *$\left(\frac{1}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.*
5. *$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{a}{p}\right)$.*

Proof.

1. If $a \equiv b \pmod{p}$ then the equation $x^2 \equiv a \pmod{p}$ is soluble if and only if $x^2 \equiv b \pmod{p}$ is soluble.
2. Using Euler's criterion :

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

We reached $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right) \pmod{p}$. To reach $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ suppose that $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \neq \left(\frac{ab}{p}\right)$. As $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \in \{-1, +1\}$ our assumption for inequality would imply that $-1 \equiv 1 \pmod{p}$. This is impossible as $p > 2$.

3. Just note that $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right)$, by the previous part of this proposition. Then note that $\left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = 1$ always as $\left(\frac{a}{p}\right) = \pm 1$.

4. Applying Euler's criterion will grant us $\left(\frac{1}{p}\right) \equiv 1 \pmod{p}$ and $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod{p}$; we reach the desired equalities by a similar argument to the one shown in the previous part of the proposition.

■

In the last proposition we considered $\left(\frac{-1}{p}\right)$ and showed that it is equal to $(-1)^{(p-1)/2}$. This however leaves matters rather obscure regarding the question when is -1 a quadratic residue modulo p; indeed, we see that the answer depends on whether $(p-1)/2$ is even or odd. We would like to have a better understanding of this problem.

Proposition 8.18 *If p is an odd prime then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod{4}, \\ -1, & p \equiv -1 \pmod{4}. \end{cases}$$

Proof. As p is odd we either have $p \equiv 1 \pmod{p}$ or $p \equiv 3 \pmod{4}$. Hence, by the properties of the Legendre symbol we have that in the former case $p = 4k+1$ so that $\left(\frac{-1}{p}\right) = (-1)^{2k} = 1$. In the latter case $p = 4k+3$ so that $\left(\frac{-1}{p}\right) = (-1)^{2k+1} = -1$. ■

Example 8.19 Find solutions if any to $x^2 \equiv -46 \pmod{17}$. We evaluate $\left(\frac{-46}{17}\right)$.

$$\left(\frac{-46}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{46}{17}\right) = (-1)^{\frac{17-1}{2}}\left(\frac{46}{17}\right) = \left(\frac{46}{17}\right) = \left(\frac{12}{17}\right)$$

where the last equality is since $46 \equiv 12 \pmod{17}$. Now

$$\left(\frac{12}{17}\right) = \left(\frac{3 \cdot 2^2}{17}\right) = \left(\frac{3}{17}\right).$$

Next, using Euler's criterion we may write

$$\left(\frac{3}{17}\right) \equiv 3^{(17-1)/2} \equiv 3^8 \equiv 81^2 \pmod{17}.$$

As $81 \equiv -4 \pmod{17}$ we get

$$\left(\frac{3}{17}\right) \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17}.$$

We discovered that the equation has no solutions.

8.1.2 *Infinitely many primes of the form* $4n+1$

We proved that there are infinitely many primes of the form $4n+3$ which is equivalent to the form $4n-1$. Here we consider primes of the form $4n+1$.

Theorem 8.20 *There are infinitely many primes of the form $4n+1$.*

Proof. Suppose that there are only finitely many such primes $S = \{p_1, \dots, p_n\}$ and set

$$N = (2 \cdot p_1 \cdots p_n)^2 + 1.$$

As N is of the of the form $4k+1$ it is odd and thus admits an odd prime divisor namely p. That is

$$(2 \cdot p_1 \cdots p_n)^2 \equiv -1 \pmod{p},$$

which in turn implies that $\left(\frac{-1}{p}\right) = 1$. The latter occurs if and only if $p \equiv 1 \pmod 4$ and thus $p \in S$, by assumption. It follows that $p \mid (2 \cdot p_1 \cdots p_n)^2$ and consequently $p \mid N - (2 \cdot p_1 \cdots p_n)^2 = 1$; contradiction as $p > 2$. ■

§8.2. Gauss' lemma

Another criterion for identifying quadratic residues modulo an odd prime is the following result by Gauss.

Lemma 8.21 (Gauss' lemma)
Let p be an odd prime and let a be an integer such that $(a,p) = 1$. Let $X = \{a, 2a, 3a, \dots, \frac{p-1}{2}a\}$, and let s denote the number of members of X whose least positive residues is $> p/2$. Then

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

Proof. Let $u_1, \dots, u_s$ be the least positive residues of members of X such that $p/2 < u_i < p$ for every $i \in [s]$, and let $v_1, \dots, v_t$ be the least positive residues of the members of X such that $0 < v_i < p/2$ for every $i \in [t]$. Note that as $(a,p) = 1$ no member of X is divisible by p as none of its members is congruent to 0. Moreover, as p is odd there is no congruence class containing $p/2$. That is $s + t = \frac{p-1}{2}$ and moreover

$$u_1 \cdots u_s \cdot v_1 \cdots v_t \equiv a(2a) \cdots \left(\frac{p-1}{2}a\right) \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}. \tag{8.22}$$

It follows that $Y = \{p - u_1, \dots, p - u_s, v_1, \dots, v_t\} \subseteq [1, \frac{p-1}{2}]$ and we show that

$$\text{the members of } Y \text{ are congruent to the members of } \left[1, \frac{p-1}{2}\right] \text{ modulo } p. \tag{8.23}$$

so that $Y = [1, (p-1)/2]$ in fact holds. Assuming (8.23) we conclude the proof as follows.

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv \underbrace{(p-u_1)(p-u_2)\cdots(p-u_s)v_1v_2\cdots v_t}_{Y} \\ &\equiv (-u_1)(-u_2)\cdots(-u_s)v_1\cdots v_t \pmod{p}\end{aligned}$$

so that

$$\left(\frac{p-1}{2}\right)! \equiv (-1)^s u_1 u_2 \cdots u_s v_1 \cdots v_t \pmod{p}.$$

Then, by (8.22)

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

and as $\left(\left(\frac{p-1}{2}\right)!, p\right) = 1$ we get

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

Multiplying both sides by $(-1)^s$ we get

$$(-1)^{2s} a^{\frac{p-1}{2}} \equiv (-1)^s \pmod{p}$$

so that

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

By Euler's criterion we have $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)$ then

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

We get that $\left(\frac{a}{p}\right) = (-1)^s$ as $\left(\frac{a}{p}\right) = \pm 1$.

It remains to prove (8.23). Above we have excluded the possibility of any member of Y being equal to 0. It suffices then to show that the members of Y are pairwise incongruent modulo p. By definition, $v_i \not\equiv v_j \pmod{p}$ whenever $i \neq j$. As $u_i \not\equiv u_j \pmod{p}$ whenever $i \neq j$ it follows that $p - u_i \not\equiv p - u_j \pmod{p}$ whenever $i \neq j$. It remains to show that there exist no i and j such that $p - u_i \equiv v_j \pmod{p}$. Indeed, for if such a congruence does hold then let $ra \in X$ be the member of X congruent to u_i and let $ka \in X$ be the member of X congruent to v_j so that $p - ra \equiv ka \pmod{p}$. Then $-ra \equiv ka \pmod{p}$ and as $(a, p) = 1$ then $-r \equiv k \pmod{p}$. By the definition of the set X we have that $r, k \in [1, \frac{p-1}{2}]$ so that $-r \equiv p - r \pmod{p}$ and $p - r > \frac{p-1}{2}$. So the congruence $-r \equiv k \pmod{p}$ is impossible. ■

8.2.1 *Determining* $\left(\frac{2}{p}\right)$

When is 2 a quadratic residue modulo a prime p?

Proposition 8.24 *If p is an odd prime then*

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

An equivalent formulation of Proposition 8.24 is then the following.

Proposition 8.25 *If p is an odd prime then*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod{8}, \\ -1, & p \equiv \pm 3 \pmod{8}. \end{cases}$$

This formulation arises easily once we note the division by 8 in the exponent and choose to apply the division algorithm to p. In particular, p being odd suggests that we need only consider the forms $8k+1$, $8k+3$, $8k+5$, and $8k+7$ for p.

The following lemma will facilitate our proof of Proposition 8.24.

Lemma 8.26 *Let ℓ be a positive odd number. Then*

$$\frac{p-1}{2} - \lfloor p/4 \rfloor \equiv \frac{p^2-1}{8} \pmod 2. \tag{8.27}$$

Proof. The claim holds for an integer ℓ if and only if it holds for $\ell+8$. To see this note that on the one hand

$$\frac{(\ell+8)-1}{2} - \lfloor (\ell+8)/4 \rfloor = \left(\frac{\ell-1}{2}+4\right) - (\lfloor \ell/4 \rfloor + 2) \equiv \frac{\ell-1}{2} - \lfloor \ell/4 \rfloor \pmod 2;$$

and on the other hand

$$\frac{(\ell+8)^2-1}{8} = \frac{\ell^2-1}{8} + 2\ell + 8 \equiv \frac{\ell^2-1}{8} \pmod 2.$$

This if and only if interests us only when ℓ is odd. Hence we are only interested in integers of the form $8k \pm 1$ and $8k \pm 3$. We leave the details of verifying (8.27) for each of these forms to the reader. ■

We now prove Proposition 8.24.

Proof of Proposition 8.24. Set $X = \{1 \cdot 2, 2 \cdot 2, \ldots, 2 \cdot \frac{p-1}{2}\}$ and let s denote the number of members of X whose least positive residue modulo p is $> p/2$. Then $\left(\frac{2}{p}\right) = (-1)^s$ by Gauss' lemma. As $X \subseteq [1, p-1]$ we need only count how many members of X are $> p/2$. Note that $2j < p/2$ as long as $j \leq \lfloor p/4 \rfloor$. As j ranges over $[1, (p-1)/2]$ it follows that $s = |X| - \lfloor p/4 \rfloor = (p-1)/2 - \lfloor p/4 \rfloor$. Hence, by Gauss' lemma we have that

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - \lfloor p/4 \rfloor}.$$

For our purposes the parity of s suffices. To this end we seek to determine the congruence class of $\frac{p-1}{2} - \lfloor p/4 \rfloor$ modulo 2 in order to determine the value of $\left(\frac{2}{p}\right)$. Lemma 8.26 asserts that $\frac{p-1}{2} - \lfloor p/4 \rfloor \equiv \frac{p^2-1}{8} \pmod 2$ and thus the claim follows. ■

8.2.2 *Infinitely many primes of the form $8k-1$*

Theorem 8.28 *There are infinitely many primes of the form $8k-1$.*

Proof. Assume towards a contradiction that there are only finitely many such primes and let $S = \{p_1, \ldots, p_n\}$ denote the set of all such primes. Set

$$N = (4p_1 \cdots p_n)^2 - 2.$$

As $N = 2^4(p_1 \cdots p_n)^2 - 2$ we have that $N/2 = 2^3(p_1 \cdots p_n)^2 - 1$ is of the form $8k-1$ and thus clearly odd. Hence, $N/2$ has at least one odd prime divisor p. This p is also a prime factor of N, and thus

$$(4p_1 \cdots p_n)^2 \equiv 2 \pmod p$$

i.e., $\left(\frac{2}{p}\right) = 1$ so that $p \equiv \pm 1 \pmod 8$, by Proposition 8.25. We may in fact assume that $p \equiv -1 \pmod 8$ as if all odd prime divisors of $N/2$ (recall that $N/2$ does not have 2 as a factor)) are of the form $8k+1$ then $N/2$ would also be of that form and $N/2$ is of the form $8k-1$. If $p \in S$ then $p \mid (4p_1 \cdots p_n)^2$. This coupled with the fact that $p \mid N$ implies that $p \mid N - (4p_1 \cdots p_n)^2 = 2$; which is a contradiction as $p > 2$. ■

8.2.3 A more practical version of Gauss' lemma

Revisiting Gauss' lemma (see Lemma 8.21) it is clear that the parameter s defined in that lemma is not a convenient quantity for us; its definition its quite abstract and there is no clear methodology for calculating it. We are then interested in a more practical version of this lemma through which calculations of Legendre symbols will be easier. This is the subject of this section.

The quantity $(-1)^s$ (seen in Gauss' lemma) suggests that the exact value of s is not of primary interest to us as far as calculation of Legendre symbols is concerned. More important is the parity of s. That is, what is its least positive residue modulo 2. In this section we shall replace the parameter s with a different quantity to which we shall refer as $T(a,p)$ (its definition follows below), where a and p are as defined in Lemma 8.21. Below we prove that

$$T(a,p) \equiv s \pmod 2 \tag{8.29}$$

and more importantly we shall see that the exact value of $T(a,p)$ can easily be calculated by hand.

In the proof of Gauss' lemma property (8.23) played a key rôle. Let us be reminded of it. In the course of the proof of Gauss' lemma we defined $u_1, \ldots, u_s$ to be the least non-negative residues of members of $X := \{a, 2a, 3a, \ldots, a(p-1)/2\}$ satisfying $p/2 < u_i \le p-1$ and have defined $v_1, \ldots, v_t$ to be the least positive residues of members of X satisfying $0 < v_i < p/2$. We have established in that proof that

$$\{p-u_1, \ldots, p-u_s, v_1, \ldots, v_t\} = [1, (p-1)/2].$$

This gives rise to the following pleasant identity

$$\sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{s}(p-u_i) + \sum_{i=1}^{t} v_i = ps - \sum_{i=1}^{s} u_i + \sum_{i=1}^{t} v_i. \tag{8.30}$$

Lemma 8.31 (Practical alternative of Gauss' lemma)
Let p be an odd prime and let a be an odd integer such that $p \nmid a$. Then

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

where

$$T(a,p) := \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor.$$

Prior to a proof of this result let us consider some motivating examples for it that demonstrate the ease in which one can calculate $T(a,p)$.

Example 8.32 Calculate $\left(\frac{7}{11}\right)$.

$$T(7,11) = \sum_{j=1}^{(11-1)/2} \left\lfloor \frac{j \cdot 7}{11} \right\rfloor = \lfloor 11/7 \rfloor + \lfloor 14/11 \rfloor + \lfloor 21/11 \rfloor + \lfloor 28/11 \rfloor + \lfloor 35/11 \rfloor = 7.$$

Then

$$\left(\frac{7}{11}\right) = (-1)^7 = -1.$$

Example 8.33 Calculate $\left(\frac{11}{7}\right)$

$$T(11,7) = \sum_{j=1}^{(7-1)/2} \left\lfloor \frac{j \cdot 11}{7} \right\rfloor = \lfloor 11/7 \rfloor + \lfloor 22/7 \rfloor + \lfloor 33/7 \rfloor + \lfloor 33/7 \rfloor = 8.$$

Then

$$\left(\frac{11}{7}\right) = (-1)^8 = 1.$$

These last two examples vividly show that if p and q are two distinct primes then

$$T(p,q) \neq T(q,p)$$

is possible.

We now prove Lemma 8.31.

Proof of Lemma 8.31. Let X, s, $u_1, \ldots, u_s$, and $v_1, \ldots, v_t$ be as above (or as defined in the Gauss' lemma). As explained above, it suffices to prove that $T(a,p) \equiv s \pmod 2$. By the division theorem

$$ja = p \left\lfloor \frac{ja}{p} \right\rfloor + r_{ja}$$

for every $j \in [1, (p-1)/2]$ and where r_{ja} is the least positive remainder of ja modulo p. Summing up these $(p-1)/2$ equations we arrive at

$$\begin{aligned} \sum_{j=1}^{(p-1)/2} ja &= \sum_{j=1}^{(p-1)/2} p \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{i=1}^{s} u_i + \sum_{i=1}^{t} v_i \\ &= pT(a,p) + \sum_{i=1}^{s} u_i + \sum_{i=1}^{t} v_i. \end{aligned}$$

By (8.30)

$$\begin{aligned} \sum_{j=1}^{(p-1)/2} ja - \sum_{j=1}^{(p-1)/2} j &= pT(a,p) + \sum_{i=1}^{s} u_i + \sum_{i=1}^{t} v_i - ps + \sum_{i=1}^{s} u_i - \sum_{i=1}^{t} v_i \\ &= pT(a,p) - ps + 2\sum_{i=1}^{s} u_i. \end{aligned}$$

Simplifying the left hand side of this last equality we arrive at

$$\underbrace{(a-1)\sum_{j=1}^{(p-1)/2} j}_{\text{even}} = pT(a,p) - ps + \underbrace{2\sum_{i=1}^{s} u_i}_{\text{even}}.$$

Reducing this last equality modulo 2 we arrive at

$$ps \equiv pT(a,p) \pmod 2$$

here we can reduce p as $(2,p)=1$ and obtain $T(a,p) \equiv s \pmod 2$ completing the proof. ■

8.2.4 A combinatorial interpretation of $T(a,p)$

The term $T(a,p)$ has a combinatorial meaning in the sense that it is the number of certain pairs of integers satisfying a certain property. In Example 8.33 we have determined that $\left(\frac{11}{7}\right) = 1$. We did so by evaluating the parity of

$$T(11,7) = \sum_{j=1}^{(7-1)/2} \left\lfloor \frac{11\cdot j}{7} \right\rfloor = \sum_{j=1}^{3} \left\lfloor \frac{11\cdot j}{7} \right\rfloor.$$

What did we actually sum here? We ranged over pairs of the form $\left(j, \left\lfloor \frac{11\cdot j}{7} \right\rfloor\right)$ allowing j to determine the number of pairs considered. One easily notices that this sum involves pairs taken from the *rectangle*

$$R := \{(x,y) \in \mathbb{R}^2 : 0 \le x \le 7/2 \text{ and } 0 \le y \le q/2\}.$$

In fact we can further restrict and say that all pairs considered are restricted to the *lattice* arising from R namely

$$\mathcal{L}(R) := \{(x,y) \in \mathbb{Z}^2 : 0 \le x \le 7/2 \text{ and } 0 \le y \le 11/2\}.$$

As 7 and 11 are both odd, we may replace $7/2$ and $11/2$ by $(7-1)/2$ and $(11-1)/2$ and write

$$\mathcal{L}(R) = \{(x,y) \in \mathbb{Z}^2 : 0 \le x \le (7-1)/2 \text{ and } 0 \le y \le (11-1)/2\}.$$

One benefit to considering $\mathcal{L}(R)$ is that $|\mathcal{L}(R)| = \frac{7-1}{2}\cdot\frac{11-1}{2}$ (which will come in handy later on). A second benefit being that in $\mathcal{L}(R)$ we can see more clearly what pairs do we sum over while trying to evaluate $T(11,7)$.

In R consider the line passing through the points $(0,0)$ and $(7/2, 11/2)$. This line defines a linear function given by $y = \frac{11}{7}x$ (which reminds us of the summand $\left\lfloor \frac{11j}{7} \right\rfloor$ considered while evaluating $T(11,7)$) which we can also write as $7y = 11x$. The latter form together with the fact that $(7,11)=1$ implies that no point (i.e., pair) in $\mathcal{L}(R)$ satisfies the equation $7y = 11x$. For if there would be such a point $(x_0, y_0) \in \mathcal{L}(R)$ satisfying $7y_0 = 11x_0$ then that would imply $11 \mid 7y_0$ so that $11 \mid 7$ or $11 \mid y_0$. Both are impossible; the first is clear, the second stems from the fact that $y_0 \le (11-1)/2$.

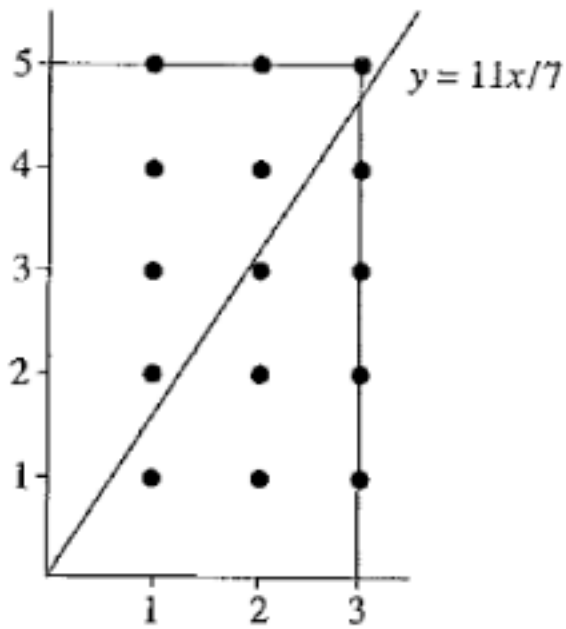


Figure 8.1: R, $\mathcal{L}(R)$, and $11x/7$.

Consider now a lattice point $(j, y) \in \mathcal{L}(R)$ that lies beneath the line $11x/7$. The value for j is clearly in $\{0, 1, 2, 3\}$. For y we surely have $y \leq 11j/7$. As y is an integer we can in fact have $y \leq \lfloor 11j/7 \rfloor$. Letting $\mathcal{T} \subseteq \mathcal{L}(R)$ denote the set of lattice point found strictly bellow the line $7y = 11x$ (so that $(0, 0) \notin \mathcal{T}$). We have just argued that for each $j \in 1, 2, 3$ there are precisely $\lfloor 11j/7 \rfloor$ points y such that $(j, y) \in \mathcal{T}$; that is

$$|\mathcal{T}| = \sum_{j=1}^{(7-1)/2} \left\lfloor \frac{11j}{7} \right\rfloor = T(11, 7).$$

Let $\mathcal{U} \subseteq \mathcal{L}(R)$ denote the lattice points found strictly above the line $7y = 11x$ (so $(0, 0) \notin \mathcal{U}$). Any such point (j, y) satisfies $j \in \{1, 2, 3\}$. For y we have $\lceil 11j/7 \rceil \leq y \leq (11 - 1)/2$. Note that if $y > 11x/7$ then $x < 7y/11$. This suggests that we can count $|\mathcal{U}|$ in the same way we did $\mathcal{T}$. That is we simply rotate Figure 8.1 along the line $7y = 11x$ and then have in the argument above we had for $\mathcal{T}$ the rôles of 7 and 11 replace one another and the rôles of x and y replace one another. Doing so leads to

$$|\mathcal{U}| = \sum_{j=1}^{(11-1)/2} \left\lfloor \frac{7j}{11} \right\rfloor = T(7, 11).$$

Recall now that no lattice point lies on the line $7y = 11x$. Hence

$$|\mathcal{U}| + |\mathcal{T}| = |\mathcal{L}(R)| = T(7, 11) + T(11, 7).$$

Recall also that $|\mathcal{L}(R)| = \frac{11-1}{2} \cdot \frac{7-1}{2}$ so that

$$\frac{11 - 1}{2} \cdot \frac{7 - 1}{2} = T(7, 11) + T(11, 7).$$

We have just proved the following.

Proposition 8.34 *Let p and q be distinct odd primes. Then*

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

Proof of this is left to the exercises.

§8.3. The law of quadratic reciprocity

Above we have determined $\left(\frac{1}{p}\right)$, $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ for an odd prime p and have seen applications using these results. In this section we continue by considering $\left(\frac{p}{q}\right)$ for two distinct odd primes p and q. The main result of this section called the *law of quadratic reciprocity* asserts that knowledge about $\left(\frac{p}{q}\right)$ can be used to deduce the value $\left(\frac{q}{p}\right)$ (hence the use of the word 'reciprocity'). This result was conjectured by Euler and proved initially by Gauss (at the age of 18).

Theorem 8.35 (The law of quadratic reciprocity)
Let p and q be distinct odd primes. Then

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \tag{8.36}$$

Since Gauss' proof of this result additional 153 new proofs for this result have been published. Amongst the authors providing a proof for this result we have people such as Cauchy, Dirichlet, Kronecker, and Einstein.

8.3.1 *Implications*

Prior to a proof of Theorem 8.35 we consider several implications of it. Consider the term $\frac{p-1}{2} \cdot \frac{q-1}{2}$ appearing on the left hand side of (8.36). Owing to p and q being odd these are either $\equiv 1 \pmod 4$ or $\equiv 3 \pmod 4$.

Observation 8.37. *$\frac{p-1}{2} \cdot \frac{q-1}{2}$ is even if and only if at least one of p and q is congruent to 1 modulo 4.*

Observation 8.38. *If $p \equiv q \equiv 3 \pmod 4$ then $\frac{p-1}{2} \cdot \frac{q-1}{2}$ is odd.*

These observations together with the law of quadratic reciprocity yield the following.

Corollary 8.39 *Let p and q be distinct odd primes.*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4, \\ -1, & p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Multiplying (8.36) by $\left(\frac{q}{p}\right)$ on both sides and owing to $\left(\frac{q}{p}\right)^2 = 1$ we arrive at the following.

Corollary 8.40 *Let p and q be distinct odd primes.*

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4, \\ -\left(\frac{q}{p}\right), & p \equiv q \equiv 3 \pmod 4. \end{cases} \tag{8.41}$$

Example 8.42 Let $a = \pm 2^{k_0} q_1^{k_1} q_2^{k_2} \cdots q_r^{k_r}$ such that $a \neq \pm 1$ and each q_i is an odd prime. Let p be an odd prime $p \nmid a$. Then the fact that the Legendre symbol is multiplicative (see Proposition 8.17 second property) yields

$$\begin{aligned} \left(\frac{a}{p}\right) &= \left(\frac{\pm 1 \cdot 2^{k_0} q_1^{k_1} q_2^{k_2} \cdots q_r^{k_r}}{p}\right) \\ &= \left(\frac{\pm 1}{p}\right)\left(\frac{2}{p}\right)^{k_0}\left(\frac{q_1}{p}\right)^{k_1} \cdots \left(\frac{q_r}{p}\right)^{k_r}. \end{aligned}$$

For $\left(\frac{\pm 1}{p}\right)$ and $\left(\frac{2}{p}\right)$ we have an answer by prior results. Using (8.41) we can replace $\left(\frac{q_i}{p}\right)$ with $\pm\left(\frac{p}{q_i}\right)$. The gain of this being that $q_i < p$ as $p \nmid a$. The goal now is to enter a chain of replacements of each Legendre symbol until we reach $\left(\frac{\pm 1}{q}\right)$ or $\left(\frac{2}{q}\right)$ for some odd prime q. The next example makes this process precise.

Example 8.43 Calculate $\left(\frac{29}{53}\right)$. Noting that $29 \equiv 53 \equiv 1 \pmod 4$ allows us to write

$$\left(\frac{29}{53}\right) = \left(\frac{53}{29}\right)$$

by (8.41). Owing to $53 \equiv 24 \pmod{29}$ we can write

$$\left(\frac{29}{53}\right) = \left(\frac{53}{29}\right) = \left(\frac{24}{29}\right).$$

by the first property listed in Proposition 8.17. As $24 = 2 \cdot 3 \cdot 4$ we arrive at

$$\left(\frac{29}{53}\right) = \left(\frac{2}{29}\right)\left(\frac{3}{29}\right)\underbrace{\left(\frac{2^2}{29}\right)}_{=1} = \left(\frac{2}{29}\right)\left(\frac{3}{29}\right).$$

Owing to $29 \equiv 5 \equiv -3 \pmod 8$,

$$\left(\frac{2}{29}\right) = -1$$

by Proposition 8.25. More interesting is the treatment of $\left(\frac{3}{29}\right)$. Surely $3 \equiv 3 \pmod 4$ and $29 \equiv 1 \pmod 4$, then $\left(\frac{3}{29}\right) = \left(\frac{29}{3}\right)$ by (8.41). Then $29 \equiv 2 \pmod 3$ and the first property listed

in Proposition 8.17 yield

$$\left(\frac{29}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

where the last equality is due to by Proposition 8.25. We thus conclude that

$$\left(\frac{29}{53}\right) = \left(\frac{2}{29}\right)\left(\frac{2}{3}\right) = (-1)(-1) = 1.$$

8.3.1.1 Determining $\left(\frac{3}{p}\right)$

As $3 \equiv 3 \pmod 4$, equation (8.41) assumes the following simpler form.

$$\left(\frac{3}{p}\right) = \begin{cases} \left(\frac{p}{3}\right), & p \equiv 1 \pmod 4, \\ -\left(\frac{p}{3}\right), & p \equiv 3 \pmod 4. \end{cases}$$

Using the first property of Proposition 8.17 we may write

$$\left(\frac{p}{3}\right) = \begin{cases} 1, & p \equiv 1 \pmod 3, \\ -1 & p \equiv 2 \pmod 3. \end{cases}$$

Then $\left(\frac{3}{p}\right) = 1$ if and only if $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = 1$ or if $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ and $\left(\frac{p}{3}\right) = -1$. More succinctly we can write the following.

Observation 8.44. *Let p be an odd prime, $p \neq 3$. Then $\left(\frac{3}{p}\right) = 1$ if and only if*

(i) $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$

or

(ii) $p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$.

For (i) we can use Proposition 6.51 to learn that $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod 3$ implies $p \equiv 1 \pmod{12}$ (see Example 6.53 as well). For (ii) we can use Theorem 6.64 to learn that $p \equiv 3 \pmod 4$ and $p \equiv 2 \pmod 3$ implies $p \equiv 11 \equiv -1 \pmod{12}$. It follows that $\left(\frac{3}{p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{12}$.

In a similar manner we note that $\left(\frac{3}{p}\right) = -1$ if and only if $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = -1$ or $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ and $\left(\frac{p}{3}\right) = -1$. More concisely we write as follows.

Observation 8.45. *Let $p \neq 3$ be an odd prime. Then $\left(\frac{3}{p}\right) = -1$ if and only if*

(i') $p \equiv 1 \pmod 4$ and $p \equiv 2 \pmod 3$,

or

(ii') $p \equiv 3 \pmod 4$ and $p \equiv 1 \pmod 3$.

Using Theorem 6.64 we may write the condition in (i') more concisely as $p \equiv 5 \pmod{12}$ and the condition (ii') as $p \equiv -5 \pmod{12}$ leading us to the following formulation.

Proposition 8.46 *If $p \neq 3$ is an odd prime then*

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod{12}, \\ -1, & p \equiv \pm 5 \pmod{12}. \end{cases}$$

8.3.2 Proof of the law of quadratic reciprocity

By Gauss' lemma (i.e., Lemma 8.21) one may write

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

where s_q is defined to be the number of members x in the set

$$X_q := \left\{p, 2p, 3p, \ldots, \frac{q-1}{2} \cdot p\right\}$$

satisfying

$$x = kq + r$$

with $r > q/2$. That is, all members of X_q that can be found in one of the classes $[(q+1)/2]_q, \ldots, [q-1]_q$. In a similar manner

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

where s_p is the number of members of

$$X_p := \left\{q, 2q, 3q, \ldots, \frac{p-1}{2} \cdot q\right\}$$

whose least positive residue is $> p/2$. Then

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

Hence, in order to establish the law of quadratic reciprocity it suffices to prove

$$s_p + s_q \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod{2}.$$

As $s_p \equiv T(p,q) \pmod 2$ and $s_q \equiv T(q,p) \pmod 2$, by (8.29); suffices then to prove

$$T(q,p) + T(p,q) = \frac{p-1}{2} \cdot \frac{q-1}{2};$$

a fact already established in Proposition 8.34. This concludes the proof of the law of quadratic reciprocity.

§8.4. Quadratic residues for composite moduli

So far we have only considered results for quadratic residues modulo a prime number; yet Definition 8.9 allows for quadratic residues modulo any integer. Our focus on prime numbers was for a good reason; indeed, quadratic residues modulo a prime behave much more "regularly" than those modulo a composite number.

Example 8.47 What are the quadratic residues modulo 8? By Definition 8.9 we need only consider integers relatively prime to 8. All such integers are captured through the reduced system of residues modulo 8 namely $\{1, 3, 5, 7\}$. However, note that $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \pmod 8$ so all the integers congruent to 1 modulo 8 form quadratic residues modulo 8. Unlike the case for primes, here only a single congruence class captures all quadratic residues.

Example 8.48 What are the quadratic residues modulo 18? A reduced system of residues modulo 18 is given by the set $\{1, 5, 7, 11, 13, 17\}$. Here we note that

$$\begin{aligned} 1^2 &\equiv 17^2 \equiv 1 \pmod{18} \\ 5^2 &\equiv 13^2 \equiv 7 \pmod{18} \\ 7^2 &\equiv 11^2 \equiv 13 \pmod{18}; \end{aligned}$$

then $1, 7, 13 \pmod{18}$ are the sole congruence classes that capture quadratic residues modulo 18.

A systematic approach for solving congruences modulo composite numbers begins with the following generalisation of Lemma 8.7.

Lemma 8.49 *Let p be an odd prime, let $k \geq 1$ and let $a \in \mathbb{Z}$ such that $(a, p) = 1$. Then*

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

either has no solutions or exactly two incongruent solutions modulo p.

Proof. Adapt the proof presented for Lemma 8.7; we leave this to the exercises. ■

Lemma 8.50 *Let $p > 2$ be a prime, let $k \geq 1$ be an integer, and let a be an integer relatively prime to p. Then the congruence $x^2 \equiv a \pmod{p^{k+1}}$ has a solution if and only if the congruence $x^2 \equiv a \pmod{p^k}$ has a solution.*

Proof. As $p^k \mid p^{k+1}$, we have that if $x_0^2 \equiv a \pmod{p^{k+1}}$ then $x_0^2 \equiv a \pmod{p^k}$. The converse we prove by induction on k. For the induction basis we consider $k = 1$ and seek to show that if $x_0^2 \equiv a \pmod p$ then there exists an x_1 such that $x_1^2 \equiv a \pmod{p^2}$. From the assumption that $x_0^2 \equiv a \pmod p$, we have that $x_0^2 = jp + a$ for some $j \in \mathbb{Z}$ which in turn implies

$$(2x_0, p^2) = 1. \tag{8.51}$$

To see this, assume towards contradiction that $(2x_0, p^2) > 1$; then $(2x_0, p^2) = p$ so that $p \mid 2x_0$ and thus $p \mid x_0$. Consequently, $p \mid x_0^2$ contradicting the assumption $x_0^2 \equiv a \pmod p$.

Owing to (8.51), the congruence $(2x_0)y \equiv -j \pmod{p^2}$ (i.e., y is the variable here) has a (unique) solution namely $y = y_0$. Then $x_1 := x_0 + 2x_0y_0$ is a solution to $x^2 \equiv a \pmod{p^2}$. To see this note that

$$\begin{aligned} x_1^2 &\equiv (x_0 + y_0p)^2 \\ &\equiv x_0^2 + 2x_0y_0p + y_0^2p^2 \\ &\equiv x_0^2 + 2x_0y_0p \\ &\equiv a + jp + 2x_0y_0p \\ &\equiv a + p(j + 2x_0y_0) \\ &\equiv a + p(j - j) \\ &\equiv a \pmod{p^2}. \end{aligned}$$

The induction step is similar to the induction basis and is left to the reader. ■

The proof of Lemma 8.50 provides an algorithm for solving a congruence of the form $x^2 \equiv a \pmod{p^2}$ where p is an odd prime. Here are the steps of this algorithm.

1. Solve $x^2 \equiv a \pmod{p}$. This essentially amounts to determining whether any of the numbers
$$\left\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}$$
is congruent to a modulo p. If we find an $x_0 \in \{1, 2, \ldots, (p-1)/2\}$ such that $x_0^2 \equiv a \pmod{p}$ we know that $p - x_0$ also satisfies this. Sometimes it would be more economic to first evaluate $\left(\frac{a}{p}\right)$ to avoid a situation of the given congruence having no solutions and we conduct a search regardless. Indeed, the properties of Legendre symbols can make the determination of whether a solution exist faster.

2. Suppose then that $\left(\frac{a}{p}\right) = 1$ and that $\{x_0, p - x_0\}$ are solutions for some $x_0 \in \{1, 2, \ldots, (p-1)/2\}$. For each $\tilde{x} \in \{x_0, p - x_0\}$ we generate a solution for the original congruence as follows.
   (a) Write $(\tilde{x})^2 = jp + a$.
   (b) Solve the *linear* congruence
   $$(2\tilde{x})y \equiv -j \pmod{p^2}$$
   which now has a unique solution modulo p^2 namely some $[y_0]_{p^2}$.
   (c) Define $z := \tilde{x} + 2\tilde{x}y_0$.
   (d) $[z]_{p^2}$ is a solution for the original congruence.

If one then seeks to solve $x^2 \equiv a \pmod{p^3}$ the inductive argument seen in the proof of Lemma 8.50 suggests that we can repeat the algorithm above by first solving $x^2 \equiv a \pmod{p^2}$ determining whether this is soluble or not. If it is soluble we get two solutions modulo p^2. Each of those gives rise to a solution modulo p^3 for the original congruence. More generally we have the following.

Corollary 8.52 *Let $p > 2$ be a prime, let $a \in \mathbb{Z}$ be co-prime to p, and let $k \geq 1$ be an integer. Then the congruence $x^2 \equiv a \pmod{p^k}$ has no solutions if a is a quadratic non-residue modulo p and has precisely two incongruent solutions if a is a quadratic residue modulo p.*

Proposition 8.53 *Let $n = p_1^{a_1} \cdots p_k^{a_k}$ be an odd integer. If $\left(\frac{a}{p_i}\right) = -1$ for some $i \in [k]$ then there are no solutions to the congruence $x^2 \equiv a \pmod{n}$. Otherwise this congruence has 2^k incongruent solution.*

Proof. It suffices that we count the number of solutions for the following system of quadratic congruences.
$$\begin{aligned} x^2 &\equiv a \pmod{p_1^{a_1}} \\ x^2 &\equiv a \pmod{p_2^{a_2}} \\ &\vdots \\ x^2 &\equiv a \pmod{p_k^{a_k}}. \end{aligned}$$

By Corollary 8.52, $\left(\frac{a}{p_i}\right) = -1$ for some $i \in [k]$ then the congruence $x^2 \equiv a \pmod{p_i^{a_i}}$ is not soluble rendering that the entire system has no solutions.

If, however, $\left(\frac{a}{p_i}\right) = 1$ for every $i \in [k]$ then each equation in the system has precisely two incongruent solutions, by Corollary 8.52, namely $x \equiv c_{i,1} \pmod{p_i^{a_i}}$ and namely $x \equiv c_{i,2} \pmod{p_i^{a_i}}$. Let $\mathcal{E}_i$ denote these two congruences for $i \in [k]$. By selecting one congruence from $\mathcal{E}_i$ for each i we may generate a system of linear congruences each with a unique solution modulo n. The number of such systems one can generate is 2^k. ■

§8.5. Exercises

Exercise 1.

(a) Let $p > 2$ be a prime. Prove that

$$\left(\frac{-4}{p}\right) = \begin{cases} 1, & p \equiv 1, -3 \pmod 8, \\ -1, & p \equiv -1, 3 \pmod 8. \end{cases} \tag{8.54}$$

(b) Let $a_1, \ldots, a_k$ be k integers all of the form $8k+5$. Prove that $(a_1 \cdot a_2 \cdots a_k)^2 + 4$ is of the form $8k+5$ as well.

(c) Prove that there are infinitely many primes of the form $8k+5$.

Exercise 2. Prove Proposition 8.34.

Exercise 3. Prove Lemma 8.49.

Exercise 4. Find all solutions for the congruence $x^2 \equiv 1 \pmod{15}$.

Exercise 5. Consider

$$x^2 \equiv 196 \pmod{1357}.$$

(a) Show that this congruence is soluble without finding an actual solution.

(b) Find all solutions.

Exercise 6. How many incongruent solutions are there for the congruence $x^2 \equiv 31 \pmod{75}$?

Exercise 7. Find all solutions of the equation

$$x^2 + x + 1 \equiv 0 \pmod 7.$$

Exercise 8. Let $p > 2$ be a prime and let $b \in \mathbb{Z}^+$ satisfy $(p, b) = 1$. Prove that

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

Exercise 9. Let $p > 2$ be a prime. Prove that

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & p \equiv 1, 3 \pmod 8, \\ -1, & p \equiv -1, -3 \pmod 8. \end{cases}$$

Exercise 10. Evaluate the following Legendre symbols.

1. $\left(\frac{5}{13}\right)$.
2. $\left(\frac{19}{23}\right)$.
3. $\left(\frac{-23}{59}\right)$.
4. $\left(\frac{20}{31}\right)$.
5. $\left(\frac{18}{43}\right)$.
6. $\left(\frac{-72}{131}\right)$.
7. $\left(\frac{71}{73}\right)$.
8. $\left(\frac{-219}{383}\right)$.
9. $\left(\frac{461}{773}\right)$.
10. $\left(\frac{501}{773}\right)$.

Exercise 11. Use Lemma 8.21 to evaluate the following Legendre symbols. In each case specify the integer s (per Lemma 8.21) explicitly.

1. $\left(\frac{5}{19}\right)$.
2. $\left(\frac{11}{23}\right)$.

Exercise 12. Prove that -4 and $(p-1)/4$ are both quadratic residues modulo p whenever $p \equiv 1 \pmod{p}$.

Exercise 13. Determine whether the equation $3x^2 + 6x + 5 \equiv 0 \pmod{89}$ is soluble.

Exercise 14. Let p be an odd prime not equal to 5. Prove that

$$\left(\frac{5}{p}\right) = \begin{cases} 1, & p \equiv 1, 9, 11, 19 \pmod{20}, \\ -1, & \textit{otherwise}. \end{cases}$$

Exercise 15. Prove that there are infinitely many primes of the form $5n - 1$.

Exercise 16. Determine $\left(\frac{-3}{p}\right)$.

Exercise 17. Prove that every prime factor p of integers of the form $n^2 - n + 1$ is either 3 or of the form $6k + 1$.

§8.6. Solutions

Some of the solutions have been written by the TAs in the course and thus have a different style of writing to them. Over time we hope to normalise this part of the text as well.

Solution for Exercise 1.

(a) By the properties of the Legendre symbol $\left(\frac{-4}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-2}{p}\right)$. We also know

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod 8, \\ -1, & p \equiv \pm 3 \pmod 8. \end{cases}$$

We also have

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & p \equiv 1, 3 \pmod 8, \\ -1, & p \equiv -1, -3 \pmod 8. \end{cases}$$

Then

$$\left(\frac{-4}{p}\right) = \begin{cases} 1, & p \equiv 1, -3 \pmod 8, \\ -1, & p \equiv -1, 3 \pmod 8. \end{cases}$$

(b) First show that if we square a number of the form $8k+5$ we get a number of the form $8k+1$. The product of numbers of the form $8k+1$ is again of the form $8k+1$. Then $(a_1 \cdot a_2 \cdots a_k)^2$ has the form of $8k+1$. Adding 4 we reach $8k+5$.

(c) Assume towards a contradiction that there are only finitely many such primes and let $S = \{p_1, \ldots, p_n\}$ denote the finite set of all such primes. Set

$$N = \left(\prod_{s \in S} s\right)^2 + 4.$$

Then N has the form $8k+5$, by part (b) of this question. As N is odd and of the form $8k+5$ it follows that it has an odd prime divisor q that is not of the form $8k+1$. Indeed, if all factors of N would have been of the form $8k+1$ then N would have been of that form. It follows then that

$$\left(\prod_{s \in S} s\right)^2 = -4 \pmod q$$

so that $\left(\frac{-4}{q}\right) = 1$. By part (a) of this problem q must be of the form $8k+5$. If $q \in S$ then $q \mid \left(\prod_{s \in S} s\right)^2$ and consequently $q \mid N - \left(\prod_{s \in S} s\right)^2 = 4$ yet $q \geq 5$ as it is of the form $8k+5$.

Solution for Exercise 2. Read § 8.2.4.

Solution for Exercise 3. If x_0 is a solution so is $p^k - x_0 \equiv -x_0 \pmod{p^k}$ is a solution. These two solutions are incongruent modulo p^k for otherwise $x_0 \equiv -x_0 \pmod{p^k}$ implying that $p^k \mid 2x_0$. As $x_0^2 \equiv a \pmod{p^k}$ and $(p, a) = 1$ then $(x_0, p) = 1$. Furthermore, $(2, p) = 1$. It follows that $2x_0$ and have no common factors with p^k yielding a contradiction.

It remains to show that no additional incongruent solutions are possible. Let x_0 and x_1 be two solutions to the congruence. Then $x_1^2 \equiv x_0^2 \pmod{p^k}$ so that $p^k \mid (x_1 + x_0)(x_1 - x_0)$. As $p \mid p^k$ then $p \mid (x_1 + x_0)(x_1 - x_0)$ implying that $p \mid x_1 + x_0$ or $p \mid x_1 - x_0$ implying the claim.

Solution for Exercise 4. Note that $x^2 \equiv 1 \pmod{15}$ if and only if $x^2 \equiv 1 \pmod 3$ and $x^2 \equiv 1 \pmod 5$. From the equation $x^2 \equiv 1 \pmod 3$ we get that $x \equiv 1 \pmod 3$ or $x \equiv 2 \pmod 3$. Next, from the equation $x^2 \equiv 1 \pmod 5$ we get that $x \equiv 1 \pmod 5$ or $x \equiv 4 \pmod 5$. We have thus generated four systems of equations each consisting of two equations. Applying the Chinese remainder to each of these systems yields four incongruent solutions $x \equiv 1, 4, 11, 14 \pmod{15}$.

Solution for Exercise 5.

(a) As $1357 = 23 \cdot 59$ the given congruence is soluble if and only if the system

$$x^2 \equiv 196 \pmod{23}$$
$$x^2 \equiv 196 \pmod{59}$$

is soluble. To determine whether this system is soluble we need to determine the value of $\left(\frac{196}{23}\right) \cdot \left(\frac{196}{59}\right)$. The system is soluble if and only if this product evaluates to 1.

As $196 \equiv 12 \pmod{23}$ we have

$$\left(\frac{196}{23}\right) = \left(\frac{12}{23}\right) = \left(\frac{3}{23}\right) \cdot \left(\frac{2^2}{23}\right) = \left(\frac{3}{23}\right) = 1,$$

where the last equality is due to Proposition 8.46. For the evaluation of $\left(\frac{196}{59}\right)$ we shall employ the law of quadratic reciprocity as follows.

$$\left(\frac{196}{59}\right) = \left(\frac{19}{59}\right) = -\left(\frac{59}{19}\right) = -\left(\frac{2}{19}\right) = -(-1) = 1,$$

where for the second equality we used the law of quadratic reciprocity, and for the second to last we used Proposition 8.24.

(b) So far we have determined that the given congruence is soluble. We now address the issue of finding the solution. We are confronted with solving each of the congruences

$$x^2 \equiv 196 \pmod{23}$$
$$x^2 \equiv 196 \pmod{59}$$

separately finding the two solutions for each and then apply the Chinese remainder theorem. We do this next.

For the congruence $x^2 \equiv 196 \pmod{23}$ we calculated that $x \equiv 9, 14 \pmod{23}$ are its two solutions. For the congruence $x^2 \equiv 196 \pmod{59}$ we calculated that $x \equiv 14, 45 \pmod{59}$ are its solutions. This we do by hand as follows (with the aid of a calculator). Consider $x^2 \equiv 196 \pmod{23}$ which we replace by $x^2 \equiv 12 \pmod{23}$ as $196 \equiv 12 \pmod{23}$. As we already know that there is a solution to this we look for $x \in \{1, 2, \ldots, 11\}$ satisfying $x^2 \equiv 12 \pmod{23}$. By trial and error and eliminating obvious candidates that cannot lead to a solution we arrive at $x = 9$ and then its partner is $23 - 9 = 14$. We do the same for $x^2 \equiv 196 \equiv 19 \pmod{59}$.

We arrive to the application of the Chinese remainder theorem which we apply four times. Once for each of the systems listed here:

$$x \equiv 14 \pmod{23} \text{ and } x \equiv 14 \pmod{59}$$
$$x \equiv 14 \pmod{23} \text{ and } x \equiv 45 \pmod{59}$$
$$x \equiv 9 \pmod{23} \text{ and } x \equiv 14 \pmod{59}$$
$$x \equiv 9 \pmod{23} \text{ and } x \equiv 45 \pmod{59}.$$

Each application of the Chinese remainder theorem would produce a solution for the congruence $x^2 \equiv 196 \pmod{1357}$. For the first congruence in the system we actually see that there is no need to use the Chinese remainder theorem on it as there the solutions is clear and it is $[14]_{1357}$. For the other three we do use the Chinese remainder theorem in order to get the three other solutions namely $[635]_{1357}, [722]_{1357}$, and $[1343]_{1357}$.

Solution for Exercise 6. As $75 = 3 \cdot 5^2$, Proposition 8.53 asserts that need to evaluate the Legendre symbols $\left(\frac{31}{3}\right)$ and $\left(\frac{31}{5}\right)$. Noting that $31 \equiv 1 \pmod 3$ and $31 \equiv 1 \pmod 5$ we have that $\left(\frac{31}{3}\right) = \left(\frac{1}{3}\right) = 1$ and that $\left(\frac{31}{5}\right) = \left(\frac{1}{5}\right) = 1$. Hence, by Proposition 8.53 the congruence has 4 incongruent solutions modulo 75.

Solution for Exercise 7. The idea is to manipulate the given equation until one reaches an equation of the form $y^2 \equiv a \pmod 7$ which we know how to solve.

For instance, here we add $-7x + 8$ to both sides in order to complete the square and get the form $(a + b)^2$ on the left hand side.

$$x^2 + x + 1 - 7x + 8 \equiv (x - 3)^2 \equiv -7x + 8 \pmod 7.$$

Surely $-7x + 8 \equiv 1 \pmod 7$ so we arrive at

$$(x - 3)^2 \equiv 1 \pmod 7.$$

We have reached an equation of the form $y^2 \equiv 1 \pmod 7$. Hence $y \equiv= 1, 6 \pmod 7$. Hence, $x \equiv 4, 9 \pmod 7$.

Solution for Exercise 8. Using the fundamental properties of the Legendre symbol we get

$$\begin{aligned}\sum_{i=1}^{p-1} \left(\frac{i \cdot b}{p}\right) &= \left(\frac{b}{p}\right)\left(\frac{1}{p}\right) + \left(\frac{b}{p}\right)\left(\frac{2}{p}\right) + \cdots + \left(\frac{b}{p}\right)\left(\frac{p-1}{p}\right) \\ &= \left(\frac{b}{p}\right) \sum_{i=1}^{p-1} \left(\frac{i}{p}\right).\end{aligned}$$

In the lecture on Euler's criterion we proved that $\sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = 0$ when $p > 2$.

Solution for Exercise 9. By the properties of the Legendre symbol $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{2}{p}\right)$. In the corresponding lecture we have seen that

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \pmod 8, \\ -1, & p \equiv \pm 3 \pmod 8. \end{cases}$$

If $p \equiv 1 \pmod 8$ then $(p - 1)/2 \equiv 0 \pmod 2$ and then $(-1)^{\frac{p-1}{2}} = 1$ so that $\left(\frac{-2}{p}\right) = 1$ in this case. We leave the resolution of the remaining cases to the reader.

Solution for Exercise 10.

1. We first evaluate

$$\begin{aligned} T(5,13) &= \sum_{j=1}^{6} \left\lfloor \frac{j\cdot 5}{13} \right\rfloor \\ &= \lfloor 5/13 \rfloor + \lfloor 10/13 \rfloor + \lfloor 15/13 \rfloor + \lfloor 20/13 \rfloor + \lfloor 25/13 \rfloor + \lfloor 30/13 \rfloor \\ &= 0+0+1+1+1+2 = 5. \end{aligned}$$

Then $\left(\frac{5}{13}\right) = (-1)^5 = -1$ by Lemma 8.31.

2. Calculating $T(19,23)$ is a bit tedious. A shorter evaluation is possible by exploiting the properties of the Legendre symbol. Easy to observe that $19 \equiv -4 \pmod{23}$. Then

$$\left(\frac{19}{24}\right) = \left(\frac{-4}{23}\right) = \left(\frac{-1\cdot 2^2}{23}\right) = \left(\frac{-1}{23}\right)\cdot\left(\frac{2^2}{23}\right) = \left(\frac{-1}{23}\right) = (-1)^{(23-1)/2} = -1.$$

3. Let us note that $59 - 23 = 36 = 6^2$. We can use this neat observation as follows.

$$-23 \equiv -23 + 59 \equiv 36 \equiv 6^2 \pmod{59}.$$

Then

$$\left(\frac{-23}{59}\right) = \left(\frac{6^2}{59}\right) = 1.$$

4. We start with

$$\left(\frac{20}{31}\right) = \left(\frac{2^2\cdot 5}{31}\right) = \left(\frac{2^2}{31}\right)\cdot\left(\frac{5}{31}\right) = \left(\frac{5}{31}\right).$$

Luckily, $5 \equiv 36 \equiv 6^2 \pmod{31}$ so that $\left(\frac{20}{31}\right) = \left(\frac{5}{31}\right) = \left(\frac{6^2}{31}\right) = 1$.

5. Write $\left(\frac{18}{43}\right) = \left(\frac{2\cdot 3^2}{43}\right) = \left(\frac{2}{43}\right) = -1$, by Proposition 8.25 (observe that $43 \equiv 3 \pmod 8$).

6. Write

$$\left(\frac{-72}{131}\right) = \left(\frac{-3^2\cdot 2^2\cdot 2}{131}\right) = \left(\frac{-1}{131}\right)\cdot\left(\frac{2}{131}\right).$$

As $\left(\frac{-1}{131}\right) = (-1)^{(131-1)/2} = -1$ and as $131 \equiv 3 \pmod 8$ we have $\left(\frac{2}{131}\right) = -1$ by Proposition 8.25. We then have $\left(\frac{-72}{131}\right) = 1$.

7. Both 71 and 73 are primes. We appeal to Corollary 8.40; and observe that $73 \equiv 1 \pmod 4$ so that $\left(\frac{71}{73}\right) = \left(\frac{73}{71}\right)$.

$$\left(\frac{73}{71}\right) = \left(\frac{71+2}{71}\right) = \left(\frac{2}{71}\right).$$

For the last equality we used the triviality that $\left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right)$; indeed, $a \equiv a+p \pmod p$ so that the equation $x^2 \equiv a+p \pmod p$ has a solution if and only if $x^2 \equiv a \pmod p$. To determine $\left(\frac{2}{71}\right)$

we turn to Proposition 8.25. Observe that $71 \equiv -1 \pmod 8$ so that $\left(\frac{2}{71}\right) = 1$. It now follows that $\left(\frac{71}{73}\right) = 1$.

8. Observe that 219 is composite (indeed, $219 = 3 \cdot 73$) and that 383 is prime.

$$\left(\frac{-219}{383}\right) = \left(\frac{-1}{383}\right) \cdot \left(\frac{3}{383}\right) \cdot \left(\frac{73}{383}\right).$$

Then $\left(\frac{-1}{383}\right) = (-1)^{(383-1)/2} = -1$, $\left(\frac{3}{383}\right) = 1$ by Proposition 8.46 as $383 \equiv -1 \pmod{12}$. It remains to evaluate $\left(\frac{73}{383}\right)$. As $383 \equiv 3 \pmod 4$ we have $\left(\frac{73}{383}\right) = \left(\frac{383}{73}\right)$ by Corollary 8.40. Then as $383 \equiv 18 \pmod{73}$ we arrive at

$$\left(\frac{383}{73}\right) = \left(\frac{18}{73}\right) = \left(\frac{2 \cdot 3^2}{73}\right) = \left(\frac{2}{73}\right) = 1,$$

where the last equality is owing to Proposition 8.25 and the fact that $73 \equiv 1 \pmod 8$. We conclude that $\left(\frac{-219}{383}\right) = -1$.

9. With some effort we discover that 461 and 773 are both primes. Owing to Corollary 8.40 and owing to $461 \equiv 1 \pmod 4$ we have $\left(\frac{461}{773}\right)$. Noting that $773 \equiv 312 \pmod{461}$ we have the following evaluation.

$$\begin{aligned}\left(\frac{773}{461}\right) &= \left(\frac{312}{461}\right) = \left(\frac{2^3 \cdot 3 \cdot 13}{461}\right) \\ &= \left(\frac{2 \cdot 3 \cdot 13}{461}\right) = \left(\frac{2}{461}\right) \cdot \left(\frac{3}{461}\right) \cdot \left(\frac{13}{461}\right).\end{aligned}$$

By Proposition 8.25 and the fact that $461 \equiv -3 \pmod 8$ we have $\left(\frac{2}{461}\right) = -1$. Next, by Proposition 8.46 and the fact that $461 \equiv 5 \pmod{12}$ we arrive at $\left(\frac{3}{461}\right) = -1$. Finally, for $\left(\frac{13}{461}\right)$ we again appeal to Corollary 8.40 to get $\left(\frac{13}{461}\right) = \left(\frac{461}{13}\right)$. As $461 \equiv 6 \pmod{13}$ we have

$$\left(\frac{13}{461}\right) = \left(\frac{461}{13}\right) = \left(\frac{6}{13}\right) = \left(\frac{2}{13}\right) \cdot \left(\frac{3}{13}\right).$$

As $13 \equiv 1 \pmod{12}$, Proposition 8.46 yields $\left(\frac{3}{13}\right) = 1$. As $13 \equiv -3 \pmod 8$, Proposition 8.25 yields $\left(\frac{2}{13}\right) = -1$. All together we arrive at $\left(\frac{461}{773}\right) = -1$.

10. 501 is divisible by 3; indeed $501 = 3 \cdot 167$. Yet 167 is a prime number. Then

$$\left(\frac{501}{773}\right) = \left(\frac{167}{773}\right)\left(\frac{3}{773}\right).$$

As $773 \equiv 1 \pmod 4$ then by the law of quadratic reciprocity we have

$$\left(\frac{501}{773}\right) = \left(\frac{773}{167}\right)\left(\frac{773}{3}\right).$$

Now, as $773 \equiv 105 \pmod{167}$ and $773 \equiv 2 \pmod 3$ we may write

$$\left(\frac{501}{773}\right) = \left(\frac{105}{167}\right)\left(\frac{2}{3}\right).$$

As $3 \equiv 3 \pmod 8$ then $\left(\frac{2}{3}\right) = -1$ by Proposition 8.25. It remains to evaluate $\left(\frac{105}{167}\right)$. Noting that $105 = 3 \cdot 5 \cdot 7$ we arrive at

$$\left(\frac{105}{167}\right) = \left(\frac{3}{167}\right)\left(\frac{5}{167}\right)\left(\frac{7}{167}\right).$$

As $167 \equiv 3 \pmod 4$ then by the law of quadratic reciprocity we have

$$\left(\frac{105}{167}\right) = \left(-\left(\frac{167}{3}\right)\right)\left(\frac{167}{5}\right)\left(-\left(\frac{167}{7}\right)\right).$$

Then

$$\left(\frac{105}{167}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right)\left(\frac{6}{7}\right)$$

By Proposition 8.25 $\left(\frac{2}{3}\right) = \left(\frac{2}{5}\right) = -1$ hence

$$\left(\frac{105}{167}\right) = \left(\frac{6}{7}\right) = \left(\frac{2}{7}\right)\left(\frac{3}{7}\right).$$

By Proposition 8.25 $\left(\frac{2}{7}\right) = 1$ and by Proposition 8.46 $\left(\frac{3}{7}\right) = -1$. Hence,

$$\left(\frac{105}{167}\right) = -1.$$

We may now write that

$$\left(\frac{501}{773}\right) = 1.$$

Solution for Exercise 11.

1. For $p = 19$ we have $(p-1)/2 = 9$. Form the set

$$X := \{5, 10, 15, 20, 25, , 30, 35, 40, 45\}.$$

The integer s (per Lemma 8.21) is the number of members of X whose least positive residue modulo 19 is $> 19/2 = 9.5$. Reducing all members of X modulo 19 we arrive at

$$\{5, 10, 15, 20, 25, , 30, 35, 40, 45\} \equiv \{5, 10, 15, 1, 6, 11, 16, 2, 7\} \pmod{19}.$$

Then $s = 4$ and $\left(\frac{5}{19}\right) = (-1)^4 = 1$.

2. Here $p = 23$ so that $(p-1)/2 = 11$

$$\begin{aligned} X &:= \{11, 22, 33, 44, 55, 66, 77, 88, 99, 110, 121\} \\ &\equiv \{11, 22, 10, , 21, 9, 20, 8, 19, 7, 18, 6\} \pmod{23} \end{aligned}$$

As $p/2 = 23/2 = 11.5$ we have that $s = 5$ so that $\left(\frac{11}{23}\right) = (-1)^5 = -1$.

Solution for Exercise 12. By assumption $p \equiv 1 \pmod 4$ so that $p \equiv 1, -3 \pmod 8$ (see Exercise 21 In Lecture 6). It being prime implies $p > 2$. Then $\left(\frac{-4}{p}\right) = 1$ by (8.54). Next we consider whether

$$x^2 \equiv \frac{p-1}{4} \pmod p$$

has a solution modulo p. Rearranging

$$\begin{aligned} x^2 \equiv \frac{p-1}{4} \pmod p &\iff 4x^2 \equiv p - 1 \pmod p \\ &\iff (2x)^2 \equiv -1 \pmod p. \end{aligned}$$

Writing $y = 2x$ we arrive at $y^2 \equiv -1 \pmod p$. As $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ then $p = 4k + 1$ for some $k \in \mathbb{Z}$ leads to $\left(\frac{-1}{p}\right) = 1$ so that the equation $y^2 \equiv -1 \pmod p$ has a solution. Let $y_0 \in \mathbb{Z}$ be a solution to the latter quadratic equation. The equation $2x \equiv y_0 \pmod p$ has a (unique) solution as $(2, p) = 1$ and the claim follows.

Solution for Exercise 13. We appeal to the discussion surrounding (8.1) and (8.2). Observe that 89 is prime so that $(3, 89) = 1$. The equation here set $a = 3$, $b = 6$, and $c = 5$. Define $y = (2a)x + b = 6x + 6$ and $d = b^2 - 4ac = 36 - 4 \cdot 3 \cdot 5 = -24$. The original equation is soluble if and only if the equation $6x + 6 \equiv -24 \pmod{89}$ is soluble. We seek to determine whether $6x \equiv -30 \pmod{89}$ is soluble then. This we see to be true as $(6, 89) = 1$. In fact $x \equiv -5 \pmod{89}$ is the solution.

Solution for Exercise 14. Suffice to prove that $\left(\frac{5}{p}\right) = 1$ if and only if $p \equiv 1, 9, 11$ or $19 \pmod{20}$. Assume first then that $p \equiv 1, 9, 11$ or $19 \pmod{20}$. Then $p \equiv 1, 9, 11$ or $19 \pmod{\operatorname{lcm}(4, 5)}$ which in particular implies that $p \equiv 1, 9, 11$ or $19 \pmod 5$. This in turn means that

$$p \equiv 1 \text{ or } 4 \pmod 5. \tag{8.55}$$

Now, as $5 \equiv 1 \pmod 4$ then $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ by the law of quadratic reciprocity. Then, by (8.55), $\left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1$ or $\left(\frac{p}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1$.

Assume second that $\left(\frac{5}{p}\right) = 1$. As $5 \equiv 1 \pmod 4$ then $1 = \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. Thus by Euler's criterion we may write

$$1 \equiv p^{(5-1)/2} \equiv p^2 \pmod 5$$

implying that p is its own inverse modulo 5; hence $p \equiv 1$ or $4 \pmod 5$. Moreover, as p is odd we know that $p \equiv 1$ or $3 \pmod 4$ as well. That is

$$p \equiv 1 \text{ or } 4 \pmod 5 \text{ and } p \equiv 1 \text{ or } 3 \pmod 4.$$

Hence there are four cases to consider for p.

1. If $p \equiv 1 \pmod 5$ and $p \equiv 1 \pmod 4$ then $p \equiv 1 \pmod{20}$.
2. If $p \equiv 1 \pmod 5$ and $p \equiv 3 \pmod 4$ then by the Chinese theorem we get that $p \equiv 11 \pmod{20}$.
3. If $p \equiv 4 \pmod 5$ and $p \equiv 1 \pmod 4$ then $p \equiv 9 \pmod{20}$.
4. If $p \equiv 4 \pmod 5$ and $p \equiv 3 \pmod 4$ then by the Chinese theorem we get that $p \equiv 19 \pmod{20}$.

We omit the tedious though short calculations incurred by applying the Chinese remainder theorem in each case.

Solution for Exercise 15. Assume that there are finitely many primes of the form $5n-1$. Let $S = \{p_1, \ldots, p_n\}$ denote this finite set of primes. Observe that surely $p_n > 5$ and choose $n > p_n$ to an arbitrary integer. Put $N := 5(n!)^2 - 1$. Then N is odd as $(n!)^2$ is even (2 is surely a factor of $n!$ and thus also of $(n!)^2$) so that $5(n!)^2$ is even implying that n is odd. All factors of N are then odd. Let p be an arbitrary prime factor of N. For any such p we have

$$5(n!)^2 \equiv 1 \pmod p.$$

This congruence together with the fact that $\left(\frac{1}{p}\right) = 1$ (always) leads to

$$1 = \left(\frac{1}{p}\right) = \left(\frac{5(n!)^2}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{(n!)^2}{p}\right) = \left(\frac{5}{p}\right).$$

By the result of Exercise 14 we have that $\left(\frac{5}{p}\right) = 1$ if and only if $p \equiv 1$ or $4 \pmod 5$ assuming $p \neq 5$.

To show that $p \neq 5$ we prove a stronger assertion that in fact $p > n$. For if $p \leq n$ then $p \mid n!$ so that $p \mid (n!)^2$ and then $p \mid N - 5(n!)^2 = 1$ while $p > 2$. This then establishes that all prime factors of N are > 5.

It now holds that all prime factors are > 5 and reside in either $[1]_5$ or $[4]_5$. If $p \equiv 4 \pmod 5$ then we have a contradiction as $p > n > p_n$ implying that $p \notin S$ and of the form $5n+4$. Assume then that factors of N reside in $[1]_5$. Here we observe that the product of any two number of the form $5n+1$ is again of the same form. Indeed,

$$(5n+1)(5k+1) = 5 \cdot 5 \cdot n \cdot k + 5k + 5n + 1 = 5(5nk + k + n) + 1.$$

That is, if all factors of N are in $[1]_5$ then N is of that form as well. This we see is not possible as N is clearly of the form $5n+4$. We arrive at a contradiction to the assumptions hat all factors of N are in $[1]_5$. The proof is now complete.

Solution for Exercise 16. Following Propositions 8.18 and 8.46 and the fact that $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$ we arrive at:

1. $\left(\frac{-3}{p}\right) = 1$ if

$$p \equiv 1 \pmod 4 \text{ and } p \equiv 1 \pmod{12}$$

or

$$p \equiv 1 \pmod 4 \text{ and } p \equiv -1 \pmod{12}$$

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

$$p \equiv -1 \pmod 4 \text{ and } p \equiv 5 \pmod{12}$$

or

$$p \equiv -1 \pmod 4 \text{ and } p \equiv -5 \pmod{12}$$

We now simplify these conditions. Consider the condition

$$p \equiv 1 \pmod 4 \text{ and } p \equiv 1 \pmod{12}.$$

Writing $p = 4k + 1$ and considering $4k + 1 \equiv 1 \pmod{12}$ we arrive at $4k \equiv 0 \pmod{12}$. A multiple of 4 namely $4k$ coincides with a multiple of 12 providing that $k \equiv 0 \pmod 3$. This in turn means that p is of the form $4 \cdot 3 \cdot \ell + 1 = 6 \cdot (2\ell) + 1$ so that $p \equiv 1 \pmod 6$.

For the condition

$$p \equiv 1 \pmod 4 \text{ and } p \equiv -1 \pmod{12}$$

we proceed in a similar manner and write again $p = 4k + 1$ and require that $4k + 1 \equiv -1 \pmod{12}$ implying $4k \equiv -2 \pmod{12}$ which in turn gives $2k \equiv -1 \pmod 6$. Rewriting this as $(-2)k \equiv 1 \pmod 6$ and then as $4k \equiv 1 \pmod 6$. Here we have a linear congruence where $(4, 6) = 2 \not| 1$ and so this equation has no solution meaning that this condition is void and p never satisfies this condition.

Next, we observe the condition

$$p \equiv -1 \pmod 4 \text{ and } p \equiv 5 \pmod{12}.$$

As before, we write $p = 4k - 1$ and consider the equation $4k - 1 \equiv 5 \pmod{12}$ which is the same as $4k \equiv 6 \pmod{12}$ which we may rewrite as $2k \equiv 3 \pmod 6$. For the latter linear congruence we have $(2, 6) = 2 \not| 3$ and so this equation has no solution and p never satisfies this condition.

Finally, we have the condition

$$p \equiv -1 \pmod 4 \text{ and } p \equiv -5 \pmod{12}.$$

Write $p = 4k - 1$ and we attempt to solve $4k - 1 \equiv -5 \pmod{12}$ for k. Write $4k \equiv -4 \equiv 8 \pmod{12}$ leading to $k \equiv 3 \equiv 0 \pmod 3$. Then p is of the form $4(3\ell) - 1 = 6(2\ell) - 1$ so that $p \equiv -1 \pmod 6$.

We have just proved that

$$\left(\frac{-3}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod 6 \\ -1, & p \equiv -1 \pmod 6. \end{cases} \tag{8.56}$$

Solution for Exercise 17. Surely $n^2 - n + 1$ for every $n \in \mathbb{Z}$. Indeed, if n is odd then n^2 is odd (as 2 is not a factor of n^2 trivially). Then $n^2 - n$ is even and then $n^2 - n + 1$ is odd. Alternatively, if n is even so is n^2 and $n^2 - n$ as well so that $n^2 - n + 1$ is odd.

Fix n and consider $n^2 - n + 1$ and let p be some factor of the latter. We assume that $p \neq 3$ and show that $p \equiv 1 \pmod 6$. The assumption that $p \neq 3$ and the fact that $n^2 - n + 1$ is odd implies that $p > 3$. Having $p \mid n^2 - n + 1$ implies that $p \mid 4n^2 - 4n + 4 = (2n - 1)^2 + 3$ so that $p \mid (2n - 1)^2 + 3$; or put another way $(2n - 1)^2 \equiv -3 \pmod p$ which means $\left(\frac{-3}{p}\right) = 1$ so that $p \equiv 1 \pmod 6$ by (8.56).

Part III

Algebraic structures

Lecture 9

Permutations

If X is a non-empty set, a bijection $X \to X$ is called a *permutation*. We write S_X to denote the set of all permutations of X. If $X = [n]$ then we write S_n instead of S_X. Trivially, $|S_n| = n!$.

Example 9.1 A permutation of the numbers $1, 2$, and 3 is a *rearrangement* of these numbers in a definite order. The six possibilities are

$$1\,2\,3 \quad 1\,3\,2 \quad 2\,1\,3 \quad 2\,3\,1 \quad 3\,1\,2 \quad 3\,2\,1$$

These can also be viewed as mappings, for instance the permutation 3 1 2 is given by the bijection

$$\begin{aligned} 1 &\to 3 \\ 2 &\to 1 \\ 3 &\to 2. \end{aligned}$$

More explicitly, this means that we have defined a mapping $\alpha : [3] \to [3]$ satisfying

$$\alpha(1) = 3 \quad \alpha(2) = 1 \quad \alpha(3) = 2.$$

This we prefer to write in the more economical fashion

$$\alpha := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

where the top row denotes the domain of α and the bottom one denotes its range.

Two permutations of a set X are *equal* if these are equal as functions (see Lemma 1.31). Given two permutations σ and τ of X we write $\sigma\tau$ to denote the composition $\sigma \circ \tau$ and called this composition the *product*[1] of σ and τ. One notices that S_X is *closed* under the product operation of its members. That is

$$\text{if } \tau, \sigma \in S_X \text{ then } \tau\sigma \in S_X.$$

Definition 9.2 *Let $\sigma, \tau \in S_X$ (for some X). If $\tau\sigma = \sigma\tau$ then we say that these two permutations* commute.

[1] Some call this the *composite* of the two permutations.

Example 9.3 Consider

$$\sigma := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ and } \tau := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Then

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ and } \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

so that $\sigma\tau \neq \tau\sigma$.

While commutativity of permutations is not always guaranteed, one can easily check that associativity always is; that is

$$(\sigma\tau)\mu = \sigma(\tau\mu)$$

holds whenever $\sigma, \tau, \mu \in S_X$.

The identity function $\mathbf{1}_X$ over X given by $x \mapsto x$ for every $x \in X$ is clearly a permutation. Moreover, $\mathbf{1}_X$ commutes with every member of S_X. Permutations σ being bijections admit inverses σ^{-1} which are bijections themselves and thus permutations. Observe that

$$\sigma\sigma^{-1} = \mathbf{1}_X = \sigma^{-1}\sigma.$$

Let $\sigma \in S_X$. An element $x \in X$ for which $\sigma(x) = x$ is said to be *fixed* by σ. Otherwise we say it is *transient* under σ or that it has been *moved* by σ. Set

$$M_\sigma := \{x \in X : \sigma(x) \neq x\}.$$

Observe that $M_{\mathbf{1}_X} = \emptyset$. Trivially

$$\text{if } x \in M_\sigma \text{ then } \sigma(x) \in M_\sigma. \tag{9.4}$$

For indeed, otherwise $\sigma(x)$ is fixed by σ so that $\sigma(\sigma(x)) = \sigma(x)$. This then means that both x and $\sigma(x)$ are now mapped to $\sigma(x)$ by σ contradicting the fact that σ is one-to-one.

Theorem 9.5 (Cancellation law for permutations)
Let $\alpha, \beta, \gamma \in S_n$. If either $\alpha\beta = \alpha\gamma$ or $\beta\alpha = \gamma\alpha$ then $\beta = \gamma$.

Proof. Let us assume that $\alpha\beta = \alpha\gamma$ and let us fix $i \in [n]$. We prove that $\beta(i) = \gamma(i)$. For suppose otherwise then owing to α being one-to-one

$$\alpha\beta(i) = \alpha(\beta(i)) \neq \alpha(\gamma(i)) = \alpha\gamma(i)$$

which is a contradiction. ■

Two permutations τ and σ are said to be *disjoint* if $M_\sigma \cap M_\tau = \emptyset$. In § 9.1 we prove that every permutation admits an essentially unique *factorisation* into disjoint permutations (of a special type) we take interest in results pertaining to the products of disjoint permutations that will facilitate our results of § 9.1.

Theorem 9.6 *If $\sigma, \tau \in S_X$ are disjoint then they commute.*

Proof. Fix $x \in X$. we seek to prove that $\tau\sigma(x) = \sigma\tau(x)$. As $M_\sigma \cap M_\tau = \emptyset$ there are three cases for the whereabouts of x to consider.

1. If $x \in M_\sigma$ then $\sigma(x) \in M_\sigma$, by (9.4). In particular, both x and $\sigma(x)$ do not lie in M_τ and are thus fixed by τ. Then $\tau(x) = x$ and $\tau(\sigma(x)) = \sigma(x)$. We may then write
$$\tau\sigma(x) = \tau(\sigma(x)) = \sigma(x) = \sigma(\tau x) = \sigma\tau(x)$$
as required.
2. The case that $x \in M_\tau$ is analogous to the former case.
3. The final case to consider is that $x \notin M_\sigma \cup M_\tau$. Then $\sigma(x) = x$ and $\tau(x) = x$ so that
$$\tau\sigma(x) = \tau(\sigma(x)) = \tau(x) = x = \sigma(x) = \sigma(\tau(x)) = \sigma\tau(x).$$

■

The converse of Theorem 9.6 is false. Indeed σ and its inverse σ^{-1} commute but these are surely not disjoint.

If $\alpha, \beta \in S_n$ are disjoint then we note that, say, $\alpha|_{M_\beta}$ coincides with $\mathbf{1}_{M_\beta}$ (in fact $\alpha|_{[n]\setminus M_\alpha} = \mathbf{1}_{[n]\setminus M_\alpha}$) so that $\alpha(M_\alpha) = M_\alpha$. The same holds for β. That is to say,
$$\alpha(M_\alpha) = M_\alpha,\ \alpha(M_\beta) = M_\beta \text{ and } \beta(M_\beta) = M_\beta,\ \beta(M_\alpha) = M_\alpha.$$
Consequently, the product $\alpha\beta$ is given by
$$\alpha\beta(i) = \begin{cases} \alpha(i), & i \in M_\alpha, \\ \beta(i), & i \in M_\beta, \\ i, & i \notin M_\alpha \cup M_\beta. \end{cases}$$
This in particular implies that $M_{\alpha\beta} \subseteq M_\alpha \cup M_\beta$. The above observations have several implications that we now collect.

Corollary 9.7 *If $\alpha, \beta \in S_n$ are disjoint and $\alpha\beta = \mathbf{1}_{[n]}$ then $\alpha = \mathbf{1}_{[n]} = \beta$.*

Write $\alpha^0 := \mathbf{1}_X$, $\alpha^1 := \alpha$ and for $k \geq 1$ write α^k to denote the k-fold product of α with itself and call α^k the *kth power of α*.

Corollary 9.8 *If $\alpha, \beta \in S_n$ are disjoint, then $(\alpha\beta)^k = \alpha^k\beta^k$.*

Proof. Fix $i \in [n]$. We show that $(\alpha\beta)^k(i) = \alpha^k\beta^k(i)$. If $i \notin M_\alpha \cup M_\beta$ then i is fixed by both α and β and the required equality follows trivially as i will remain fixed in any alternating series of invocations of α and β on it.

If $i \in M_\alpha$ then all invocations of β can be ignored on both sides of the required equality as these will always fix their argument owing to $\beta|_{M_\alpha}$ coinciding with $\mathbf{1}_{M_\alpha}$. Then on both sides of the required equality we attain $\alpha^k(i)$. The case that $i \in M_\beta$ is symmetrical and thus omitted. ■

Corollary 9.8 is false for non-disjoint permutations.

Corollary 9.9 *Let $\alpha = \beta\gamma \in S_n$ where β and γ are disjoint. If $i \in M_\beta$, then $\alpha^k(i) = \beta^k(i)$ for all $k \geq 0$.*

Proof. Disjointness of β and γ and the assumption that $i \in M_\beta$ implies that all invocations of γ made through α^k can be ignored as $\gamma|_{M_\beta}$ coincides with $\mathbf{1}_{M_\beta}$. Then for the elements of M_β, α^k coincides with β^k. ■

§9.1. CYCLES

Definition 9.10 *Let $\sigma \in S_X$. If $M_\sigma = \{i_1, \ldots, i_r\}$ and*

$$i_1 \xrightarrow{\sigma} i_2, \ldots, i_{r-1} \xrightarrow{\sigma} i_r, i_r \xrightarrow{\sigma} i_1$$

*then σ is called an r-*cycle *(or a* cycle of length r*) and is written $(i_1, \ldots, i_r)$.*

Every 1-cycle fixes all elements of X and thus coincides with $\mathbf{1}_X$; that is, $\mathbf{1}_X$ is the only 1-cycle. A 2-cycles interchanges a pair of elements and is referred to as a *transposition*.

Example 9.11 The permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

is a 4-cycle and as such we write it more concisely as $(1\ 2\ 3\ 4)$. The permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 2 & 3 \end{pmatrix}$$

is a 5-cycles written more economically as $(1\ 5\ 3\ 4\ 2)$. The previous two examples had no fixed points. The permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$$

is a 3-cycle which we write as $(1\ 2\ 3)(4)(5) = (1\ 2\ \ 3)$.

The *shorthand* notations used in Example 9.11 are real handy when it comes to taking the product of permutations.

Example 9.12 Let $\alpha = (1\ 2)$ and let $\beta = (1\ 3\ 4\ 2\ 5)$. Then

$$\alpha\beta = (1\ 2)(1\ 3\ 4\ 2\ 5) = (1\ 3\ 4)(2\ 5)$$

and the two resulting cycles are disjoint.

Example 9.13 Observe that

$$S_3 = \{\mathbf{1}_{[3]}, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}$$

so S_3 consists of cycles.

Reversing the action of a cycle amounts to traversing the cycle in the opposite direction.

Observation 9.14. *If σ is an r-cycle then σ^{-1} is an r-cycle as well. More precisely, if $\sigma = (i_1, \ldots, i_r)$ then $\sigma^{-1} = (i_r, \ldots, i_1)$.*

The following ambiguity arises now. Given $\sigma = (1\ 2\ 4)$ is it in S_4 (fixing 3) or is it in S_5 (fixing 3 and 5) and so on? The convention that we shall employ is that it simply does not matter. In particular, every member of S_n can be regarded as a member of S_{n+1} fixing $n+1$; that is,

$$S_1 \subseteq S_2 \subseteq S_3 \subseteq \cdots.$$

Not every permutation is a cycle naturally. As the next example demonstrates.

Example 9.15 Consider

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 7 & 6 & 10 & 4 & 2 & 5 & 9 & 8 \end{pmatrix}$$

in which we trace the pairwise-disjoint cycles $(1\ 3\ 7\ 2)$, $(4\ 6)$, $(5\ 10\ 8)$, and (9). Moreover, we notice that σ is in fact the product of all these cycles, that is

$$\sigma = (1\ 3\ 7\ 2)(4\ 6)(5\ 10\ 8)(9)$$

holds.

Cycles are more complicated than they seem. For instance, the power of a cycle need not be a cycle. Consider $\alpha := (1\ 2\ 3\ 4)$ and note that $\alpha^2 := (1\ 3)(2\ 4)$. On the other hand we case use powers to force two cycles to coincide.

Lemma 9.16 *Let α and β be cycles in S_n. If there is an $i \in M_\alpha \cap M_\beta$ and if $\alpha^k(i) = \beta^k(i)$ for all $k \geq 1$, then $\alpha = \beta$.*

Proof. Observe first that $M_\alpha = M_\beta$ must hold. Indeed, for suppose that there is an element $j \in M_\alpha \setminus M_\beta$ so that j is fixed by β yet not by α. Then there exists a k such that $\alpha^k(i) = j$ and by assumption $\beta^k(i) = j$ as well. As j is fixed by β and not by α it follows that $\alpha^{k+1}(i) \neq \beta^{k+1}(j)$; a contradiction.

With $M_\alpha = M_\beta$ established the assumption that $\alpha^k(i) = \beta^k(i)$ for all $k \geq 1$ asserts that each element in that set must be positioned at the same 'distance' from i 'along' the cycles leading to α and β to coincide as stipulated. ■

Permutations of finite sets have the property that each element of the set is either fixed by them or it lies in a cycle. The following is of no surprise then.

Theorem 9.17 (The cycle decomposition theorem)
Every permutation $\alpha \in S_n$ is either a cycle or a product of disjoint cycles.

Proof. The proof is by induction on $|M_\alpha|$. When $|M_\alpha| = 0$ the claim is true as then $\alpha = \mathbf{1}_{[n]}$. If, however, $|M_\alpha| \geq 1$, then let $i_1 \in M_\alpha$ be arbitrary and let $(i_1, \ldots, i_r)$ be the[2] r-cycle containing i_1. If $r = n$ then α is a cycle. Let then $r < n$ hold and let Y denote the remaining $n - r$ points. Then $\alpha(Y) = Y$ and $\alpha(\{i_1, \ldots, i_r\}) = \{i_1, \ldots, i_r\}$. By the inductive hypothesis, $\alpha|_Y$ is a product of disjoint cycles. Disjointness of $\{i_1, \ldots, i_r\}$ and Y then implies that $\alpha = (\alpha|_Y)(i_1\ i_2\ \cdots\ i_r)$ and the claim follows. ■

The expression of a permutation as a product of disjoint cycles is referred to as a *factorisation* of the permutation. Theorem 9.17 asserts that every permutation (of a finite set) admits such a factorisation. In such factorisations it is not clear whether one suppresses or not the fixed points. The term *complete factorisation* is often used in the literature in order to denote a factorisation in which each fixed point i appears as (i) in the factorisation. In what follows, unless otherwise stated, we always assume a factorisation to be complete. The next result asserts that such factorisations are essentially unique.

[2] The existence of such a cycle is trivial as we may choose $r \geq 1$ to be the least integer satisfying $\alpha(i_1) = i_2, \alpha(i_2) = i_3, \ldots, \alpha(i_r) = i_1$; finiteness of n stipulates that r exists.

Theorem 9.18 (Uniqueness of permutation factorisation)
Let $\alpha \in S_n$ and let $\alpha = \beta_1 \cdots \beta_t$ be a factorisation of α into disjoint cycles. Up to the order of the cycles β_i this factorisation is unique.

Proof. Let $\alpha = \gamma_1 \cdots \gamma_s$ be a second factorisation of α. Owing to the cancellation law of permutations (see Theorem 9.5) we may assume w.l.o.g. that none of cycles γ_i coincide with any of the cycles β_i. Let $i \in M_{\beta_t}$, say. By Corollary 9.9, $\beta_t^k(i) = \alpha^k(i)$ for every $k \geq 0$. As $M_{\beta_t} \subseteq M_\alpha$ then $i \in M_{\beta_t}$ necessarily implies that there exists a cycle γ_j, say, s.t. $i \in M_{\gamma_j}$. As, again by Corollary 9.9, $\gamma_j^k(i) = \alpha^k(i)$ for every $k \geq 0$, it now follows by Lemma 9.16 that $\beta_s = \gamma_j$; a contradiction. ■

Let $\alpha \in S_n$ be an r-cycle. A nice feature of such cycles is that α^r coincides with $\mathbf{1}_{[n]}$. In fact $\alpha^k = \mathbf{1}_{[n]}$ whenever $r \mid k$. More generally, if $\beta = \alpha_1 \ldots \alpha_t$ where α_i is an r_i-cycle, then $\beta^k = \mathbf{1}_{[n]}$ whenever $r_i \mid k$ for every $i \in [s]$. We have just proved the following.

Observation 9.19. *Let $\beta \in S_n$ be a permutation and let $\beta = \alpha_1 \ldots \alpha_t$ be its factorisation where α_i is an r_i-cycle. Then, the least integer ℓ such that $\beta^\ell = \mathbf{1}_{[n]}$ satisfies $\ell = \operatorname{lcm}(r_1, \ldots, r_s)$.*

§9.2. Transpositions

Recall that by *transposition* we mean a 2-cycle. 2-cycles have the form $\delta = (i\ j)$ and admit the certainly appealing property of being self-inverse in the sense that

$$\delta^2 = \mathbf{1}_{[n]} \text{ and } \delta^{-1} = \delta.$$

Unfortunately, this property does not characterise transpositions, as demonstrated by $\sigma = (1\ 2)(3\ 4)$ which also satisfies $\sigma^2 = \mathbf{1}_{[n]}$ and $\sigma = \sigma^{-1}$.

Our interest in transpositions arises from the fact that permutations can be decomposed into products of transpositions and not merely cycles of arbitrary length.

Theorem 9.20 *Every cycle of length $r > 1$ is a product of $r - 1$ transpositions:*

$$(k_1\ k_2\ \cdots\ k_r) = (k_1\ k_2)(k_2\ k_3) \cdots (k_{r-2}\ k_{r-1})(k_{r-1}\ k_r).$$

The proof of Theorem 9.20 is left to the reader. More importantly, Theorem 9.17 and 9.20 now imply the following.

Corollary 9.21 *Every permutation is a product of transpositions (assuming we omit fixed points from the description)*

In contrast to the factorisations into cycles, the factorisation into transpositions is not unique; for instance, consider

$$(2\ 3)(1\ 2)(2\ 5)(1\ 3)(2\ 4) = (1\ 2\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2).$$

Here we in fact also used the observation that

$$(1\ 2\ \cdots\ r) = (1\ r)(1\ r-1) \cdots (1\ 2).$$

Another issue with the decomposition into transposition is that the transposition occurring in the decomposition need not commute; for instance, $(1\ 3)(1\ 2) = (1\ 2\ 3)$ while $(1\ 2)(1\ 3) = (1\ 3\ 2)$.

Is there any uniqueness at all involved in such decompositions? It turns out that the answer is positive in that the parity of the number of 'factors' is always invariant. We now make this precise.

Definition 9.22 *A permutation is said to be* even *of it is a product of an even number of transpositions; otherwise it is said to be* odd.

We have seen in the examples above that $(1\ 2\ 3)$ is even; it is not clear whether it is also odd. In view of our examples so far, are there any odd permutations at all?

The following lemma takes a transposition $(a\ b)$ and considers, first, the outcome of multiplying it by a cycle containing both its points, and second, considers the outcome of multiplying it by two cycles each containing a single point of the transposition. This will facilitate subsequent arguments.

Lemma 9.23 *If $k, \ell \geq 0$, then*

$$(a\ b)(a\ c_1\ \cdots\ c_k\ b\ d_1\ \cdots\ d_\ell) = (a\ c_1\ \cdots\ c_k)(b\ d_1\ \cdots\ d_\ell)$$

and

$$(a\ b)(a\ c_1\ \cdots\ c_k)(b\ d_1\ \cdots\ d_\ell) = (a\ c_1\ \cdots\ c_k\ b\ d_1\ \cdots\ d_\ell).$$

Proof. Consider the l.h.s. of the first equality. Here the action of the permutation is

$$\begin{aligned}
&a \mapsto c_1 \mapsto c_1 && \\
&c_i \mapsto c_{i+1} \mapsto c_{i+1} && \text{whenever } i < k \\
&c_k \mapsto b \mapsto a && \\
&b \mapsto d_1 \mapsto d_1 && \\
&d_j \mapsto d_{j+1} \mapsto d_{j+1} && \text{whenever } j < \ell \\
&d_\ell \mapsto a \mapsto b. &&
\end{aligned}$$

One may examine the r.h.s. of the first equality to witness that the same mappings take place. The verification of the second equality is left to the reader as well. ■

Definition 9.24 *If $\alpha \in S_n$ has factorisation $\alpha = \beta_1 \cdots \beta_t$ then the* sign *of α is defined to be*

$$\operatorname{sgn}(\alpha) := (-1)^{n-t}$$

By Corollary 9.21, every permutation has a sign. However, it is not clear from the outset that a permutation has a unique sign. Put another way it is not clear whether $\operatorname{sgn}(\cdot)$ is in fact a function. In what follows we prove that it is. For instance, the sign of transpositions is clear.

Example 9.25 Let $\tau \in S_n$ be a transposition. Then it moves two elements and fixes the other $n-2$. Therefore $t = (n-2)+1 = n-1$ and thus

$$\operatorname{sgn}(\tau) = (-1)^{n-(n-1)} = -1.$$

Observe that no other value is possible for $\operatorname{sgn}(\tau)$ for it always fixes $n-2$ elements in any decomposition of it into transpositions.

The sgn 'function' has several pleasant features.

Lemma 9.26 *If $\beta, \tau \in S_n$ and τ is a transposition, then*

$$\operatorname{sgn}(\tau\beta) = -\operatorname{sgn}(\beta)$$

COMMENT: Note that in this lemma, it is not yet clear what $\mathrm{sgn}(\beta)$ is. One treats $\mathrm{sgn}(\tau\beta) = -\mathrm{sgn}(\beta)$ as a symbolic manipulation only at this stage.

PROOF. Let $\tau = (a\ b)$ and let $\beta = \gamma_1 \cdots \gamma_t$ be the factorisation of β. Either a and b occur in the same γ_i or they do not. In the former case, then by the commutativity of disjoint cycles we may assume w.l.o.g. that both occur in γ_1 so that

$$\gamma_1 := (a\ c_1\ \cdots c_k\ b\ d_1\ \cdots d_\ell)$$

for some $k, \ell \geq 0$. Lemma 9.23 (first equality) now yields that

$$\tau\gamma_1 = (a\ c_1\ \cdots c_k)(b\ d_1\ \cdots d_\ell).$$

Then, the factorisation of $\tau\beta$ is given by $\tau\beta = (\tau\gamma_1)\gamma_2 \cdots \gamma_t$. Consequently, $\mathrm{sgn}(\tau\beta) = (-1)^{n-(t+1)} = -\mathrm{sgn}(\beta)$.

In the latter case, that a and b do not reside in a single cycle of the factorisation of β, we may assume w.l.o.g. that $\gamma_1 = (a\ c_1\ \cdots c_k)$ and that $\gamma_2 = (b\ d_1\ \cdots d_\ell)$ for some $k, \ell \geq 0$. Appealing to Lemma 9.23 (second equality) we reach

$$\tau\gamma_1\gamma_2 = (a\ c_1\ \cdots c_k\ b\ d_1\ \cdots d_\ell)$$

which in turn implies that $\tau\beta = (\tau\gamma_1\gamma_2)\gamma_3 \cdots \gamma_t$ so that $\mathrm{sgn}(\tau\beta) = (-1)^{n-(t-1)} = -\mathrm{sgn}(\beta)$. ■

THEOREM 9.27 *For all $\alpha, \beta \in S_n$,*

$$\mathrm{sgn}(\alpha\beta) = \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta).$$

COMMENT: As in Lemma 9.26, it is not yet clear what $\mathrm{sgn}(\alpha)$ and $\mathrm{sgn}(\beta)$ are. Again the treatment here is still symbolic only.

PROOF. Let $\alpha = \tau_1 \cdots \tau_m$ be a decomposition of α into transposition with m minimal (and with fixed points suppressed). We prove by induction on m that

$$\mathrm{sgn}(\alpha\beta) = \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta) \text{ for all } \beta \in S_n.$$

For $m = 1$, the claim is true by Example 9.25 and Lemma 9.26. Let $m > 1$ then. In which case the permutation given by $\tau_2 \cdots \tau_m$ has the property that this decomposition of it into transposition is minimal as well. For indeed, suppose that we had $\tau_2 \cdots \tau_m = \sigma_1 \cdots \sigma_q$ for some $q < m - 1$. Then the the decomposition $\tau\sigma_1 \cdots \sigma_q$ would be a decomposition for α with less than m transpositions; contradicting the definition of m.

We may now write as follows.

$$\mathrm{sgn}(\alpha\beta) = \mathrm{sgn}(\tau_1 \cdots \tau_m\beta) = -\mathrm{sgn}(\tau_2 \cdots \tau_m\beta)$$

where here we appealed to Lemma 9.26. Then by the induction hypothesis we may write

$$\begin{aligned} &= -\mathrm{sgn}(\tau_2 \cdots \tau_m)\mathrm{sgn}(\beta) \\ &= \mathrm{sgn}(\tau_1\tau_2 \cdots \tau_m)\mathrm{sgn}(\beta) \end{aligned}$$

where here we again appealed to Lemma 9.26; concluding with

$$= \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta).$$

■

The functional behaviour of $\mathrm{sgn}(\cdot)$ now makes its appearance. Let $\alpha = \tau_1 \cdots \tau_q$ be a decomposition of α into transpositions. We have seen that $\mathrm{sgn}(\tau_i) = -1$; Theorem 9.27 then yields

$$\mathrm{sgn}(\alpha) = \prod_{i=1}^{q} \mathrm{sgn}(\tau_i) = (-1)^q. \tag{9.28}$$

Theorem 9.29 *A permutation $\alpha \in S_n$ is even if and only if* $\operatorname{sgn}(\alpha) = 1$.

Proof. If α is even then there is a decomposition $\alpha = \tau_1 \cdots \tau_q$ into transpositions with q even so that $\operatorname{sgn}(\alpha) = 1$.

Conversely, if $1 = \operatorname{sgn}(\alpha)$ then there is a decomposition of α into an even number of transpositions by (9.28). ■

The proof of the characterisation of odd permutations naturally depends on the characterisation of even ones, namely Theorem 9.29 as follows.

Theorem 9.30 *A permutation $\alpha \in S_n$ is odd if and only if it is a product of an odd number of transpositions.*

Proof. If α is odd then it has no decomposition into an even number of transposition, by definition; consequently, every decomposition of it into transpositions must contain an odd number of transpositions.

Conversely, if $\alpha = \tau_1 \cdots \tau_q$ with q odd then, by (9.28), $\operatorname{sgn}(\alpha) = -1$; Theorem 9.29 then asserts that α is not even and is consequently odd. ■

§9.3. Semigroups and monoids

In this section we cast certain of the features seen for permutations and their products into a more general framework referred to as a *semigroup*.

Definition 9.31 *A (binary) operation on a non-empty set G is a function $* : G \times G \to G$.*

Instead of using the cumbersome notation $*(a, b)$ we employ the more pleasant notation $a * b$. The use of $*$ conveys a *multiplicative* flavour to binary operations. This is misleading. One could of course use $ab, a + b, a \circ b$ instead. One should treat $*$ as a placeholder at this stage; in the sequel we shall use more intuitive notation depending on context. For now we use $*$.

If we let $G = S_n$, then the product of permutations is a binary operation on G. From our experience with S_n we note that $a * b$ and $b * a$ can be different elements. When they are not, i.e., when $a * b = b * a$, then we say that a and b *commute* w.r.t. $*$.

Definition 9.32 *Let G be a set and $*$ be a binary operation defined on it. If $a * b = b * a$ for every $a, b \in G$ then $*$ is said to be* commutative.

Given $a, b, c \in G$ and a binary operation $*$ over G, the term $a * b * c$ is currently ambiguous as it is not clear at all which $*$ operation should be performed first. Moreover, $(a * b) * c$ may differ from $a * (b * c)$. For instance, let $G = \mathbb{Z}$ and set $a * b = a - b$ and note that if we pick $c \neq 0$ then we can have $(a - b) - c \neq a - (b - c)$.

Definition 9.33 *An operation $*$ on G is said to be* associative *if*

$$(a * b) * c = a * (b * c)$$

for every $a, b, c \in G$.

We have seen that the operation of taking a product of permutations over S_X is associative. For associative operations expressions like

$$a_1 * a_2 * \cdots * a_n$$

make sense and does not need to be parenthesised. This last statement actually requires a proof which at this point is too technical and we choose to omit it from our exposition.

Definition 9.34 *A* semigroup *is a pair* $(G, *)$ *consisting of a set* G *and an associative binary operation* $*$ *over* G.

Usually one writes: "let G be a semigroup..." omitting $*$ as the latter is usually clear from the context. But of course if it is not one is mandated to specifying this as well.

Often we shall abbreviate and write ab instead of $a * b$ if $*$ is clear from the context.

Let $(G, *)$ be a semigroup. An element $e \in G$ is said to be a *unity* or an *identity* w.r.t. $*$ if $a * e = a = e * a$ for every $a \in G$.

Theorem 9.35 *If a binary operation* $*$ *has a unity then that unity is unique.*

Proof. For if e and f are both unities w.r.t. $*$ then $f = e * f$ and $e * f = e$ so that $f = e$. ■

Definition 9.36 *A semigroup* $(G, *)$ *is said to be a* monoid *if* $*$ *admits a unity.*

The pairs $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \cdot)$ are all commutative monoids. If Ω is a set, then the pairs $(\mathcal{P}\Omega, \cap)$ and $(\mathcal{P}\Omega, \cup)$ are both commutative monoids with unities $\emptyset$ and U, respectively. The pair $(S_n, \circ)$ where $n \geq 3$ is a non-commutative monoid.

Example 9.37 Consider the pair $(\mathbb{N}, *)$ where $* : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is given by $n * m := n^m$. This operation is not commutative as indeed $2 * 3 = 8$ while $3 * 2 = 9$. This operation is also not associative as $(2 * 3) * 2 = 64$ yet $2 * (3 * 2) = 512$. Moreover, this operation has no unity as $m = x * m$ for all m is impossible. It follows that $(\mathbb{N}, *)$ is not a monoid. However, this operation comes very close at having a unity as indeed $m * 1 = m$ for all $m \in \mathbb{N}$.

Definition 9.38 *Let* $(G, *)$ *be a monoid with unity* e *and let* $a \in G$. *Define* $a^0 := e$, $a^1 := a$. *For* $n \geq 1$, *define* $a^{n+1} := a * a^n$.

Corollary 9.39 *Let* $(G, *)$ *be a monoid with unity* e, *let* $a \in G$, *and let* $m, n \in \mathbb{Z}_{\geq 0}$. *Then*

1. $a^m a^n = a^{m+n} = a^n a^m$;
2. $(a^m)^n = a^{mn} = (a^n)^m$; *and*
3. *if* $ab = ba$ *then* $(ab)^n = a^n b^n$.

Proof.

1. Fix $m \geq 0$. We prove the claim by induction on n. For $n = 0$, we have $a^0 a^m = ea^m = a^m$. If $n \geq 1$, then $a^n a^m = (aa^{n-1})a^m = a(a^{n-1}a^m)$. By the induction hypothesis $a^{n-1}a^m = a^{n-1+m}$. This gives $a^n a^m = a(a^{n-1+m}) = a^{n+m}$.

2. Fix $n \geq 0$ and induct on m. If $m = 0$, then $(a^0)^m = e = a^{n \cdot 0}$. If $m \geq 1$, then $(a^n)^m = a^n \cdot (a^n)^{m-1} = a^{n+n(m-1)} = a^{mn}$, where for the second equality we used the first part of this claim.

3. First we prove that $ba^k = a^k b$; this we do by induction on k. To see this note that for $k = 1$ this is true by assumption. Then we may write that $ba^k = ba^{k-1}a \overset{\text{I.H.}}{=} a^{k-1}ba = a^{k-1}ab = a^k b$ where in the second to last equality we use the assumption that $ab = ba$.

   With the above established, we prove the main assertion of here by induction on n. For $n = 1$ the claim is trivially true. For $n \geq 1$ we may write $(ab)^n = ab(ab)^{n-1} \overset{\text{I.H.}}{=} aba^{n-1}b^{n-1} = aa^{n-1}bb^{n-1} = a^n b^n$, where here in the second to last equality we used the property proved earlier asserting that $ba^{n-1} = a^{n-1}b$.

■

The notation a^n is of course borrowed from the special case where $*$ is *multiplicative*. But this notation is also used when $*$ is *additive* in which case we have $a^n = a + a + \ldots + a$ and is sometimes replaced by na. If we choose to do so then we have $ma + na = (m+n)a$ and $(mn)a = m(na)$.

In the reals, if s is a nonzero real number, then its inverse, namely $1/s$ is the solution to the equation $xs = 1$. This idea extends to monoids.

Definition 9.40 *If a is an element of a monoid $(G, *)$ with unity e, then an element $b \in G$ satisfying $a * b = e = b * a$ is called an* inverse *of a. An element with an inverse is called a* unit.

Theorem 9.41 *Let $(G, *)$ be a monoid with unity e and let $a \in G$ be a unit. Then the inverse of a is unique.*

Proof. If both b and b' are inverses of a, then $ab = e = ba$ and $ab' = e = b'a$. Hence, we may use associativity of $*$ to write $b' = b'e = b'(ab) = (b'a)b = eb = b$. ■

The inverses of elements a in multiplicative monoids are written a^{-1}; in additive ones these are written $-a$.

Example 9.42

1. All elements of the additive monoids $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$ are units.
2. In the multiplicative monoid $(\mathbb{R}, \cdot)$ all elements bu 0 are units.
3. The units of the monoid $(\{\alpha : a : X \to X\}, \circ)$ are the bijections. In particular if $X = [n]$ then the set of units is S_n.

We observe the following properties of units.

Theorem 9.43 *Let $a, b, a_1, \ldots, a_n$ be elements of a monoid with unity e.*

1. *e is a unity and $e^{-1} = e$.*
2. *If a is a unit then so is a^{-1}; in particular $(a^{-1})^{-1} = a$.*
3. *If a and b are units then so is ab; in particular $(ab)^{-1} = b^{-1}a^{-1}$.*
4. *If $a_1, \ldots, a_n$ are units then so is $a_1 a_2 \cdots a_n$ and $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$ holds.*
5. *If a is a unit then so is a^n and $(a^n)^{-1} = (a^{-1})^n$.*

Proof.

1. The first assertion is a triviality.
2. Note that $(a^{-1})^{-1}$ is that element $g \in G$ such that $a^{-1}g = e = ga^{-1}$. As a is such an element the claim follows by the uniqueness of inverses.
3. We seek to prove that

$$(ab)(b^{-1}a^{-1}) = e \text{ and } e = (b^{-1}a^{-1})(ab).$$

Appealing to associativity we may write

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = e;$$

the second equality can be proved in a similar fashion.

4. The fourth assertion stems from the third by induction and we omit its treatment here.

5. The fifth assertion is a special case of the fourth when all elements are equal.

■

Every monoid has at least one unit and that is its unity.

By Theorem 9.43, $(a^{-1})^n = (a^n)^{-1}$ for any unit a. We define the negative powers a^{-n}, $n \geq 1$, of a unit a to be

$$a^{-n} := (a^{-1})^n = (a^n)^{-1}.$$

The laws of exponents met before extend naturally to cover negative powers as follows.

Theorem 9.44 *Let a, b be units in a monoid G.*

1. $a^n a^m = a^{n+m}$ *for all* $m, n \in \mathbb{Z}$.
2. $(a^n)^m = a^{nm}$ *for all* $m, n \in \mathbb{Z}$.
3. *If* $ab = ba$ *then* $(ab)^n = a^n b^n$ *for all* $m, n \in \mathbb{Z}$.

Lecture 10

Groups

Definition 10.1 *A* group *is a monoid with all its elements being units.*

The importance of this definition merits that reiterate this definition at a slower pace. A pair $(G, *)$ consisting of a set G and a binary operation $* : G \times G \to G$ is said to be a group if:

1. G is closed under $*$ (although this is clear from the definition of $*$ we stress this again for future reference).
2. $*$ is associative.
3. There is a unity in G w.r.t. $*$.
4. Every element in G has an inverse w.r.t. $*$.

The group is called *abelian* if the operation is commutative. If G is finite we write $|G|$ to denote its cardinality and refer to the latter as the *order* of G.

For an integer $n \geq 2$, define

$$\mathbb{Z}_n := \{[0]_n, [1]_n, \ldots, [n-1]_n\}.$$

Endowing this set with the binary operation of addition modulo n gives rise to the additive abelian group $(\mathbb{Z}_n, +)$ with unity $[0]_n$. Set

$$\mathbb{Z}_n^* := \{[a]_n \in \mathbb{Z}_n : (a, n) = 1\}.$$

Then $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{[0]_n\}$ if and only if n is prime. Endowing this set with the binary operation of multiplication modulo n results in the multiplicative abelian group $(\mathbb{Z}_n^*, \cdot)$ whose unity is $[1]_n$ and where here inverses are modular inverses per § 6.2.1.

We already have enough in place to give a more conceptual proof of Wilson's theorem appearing in Theorem 7.1 asserting that $(p-1)! \equiv -1 \pmod{p}$ whenever p is a prime. Wilson's theorem stems from the more general principle captured by the following observation.

Observation 10.2. *Let $G := \{g_1, \ldots, g_r\}$ be an abelian group and set $a := g_1 g_2 \cdots g_r$. Then $a^2 = e$.*

Applying this observation to the elements of $\mathbb{Z}_p^*$ for a prime p yields Wilson's theorem.

Proof of Theorem 7.1. Observation 10.2 applied to the elements of $\mathbb{Z}_p^*$ implies that

$$\prod_{g \in \mathbb{Z}_p^*} g = \prod_{\substack{g \in \mathbb{Z}_p^* \\ g^2 = e}} g.$$

By Lemma 6.40, the latter product contains precisely two elements, namely $\overline{1}$ and $\overline{p-1}$. The theorem now follows. ■

The pair $(S_n, \circ)$ of all permutations over $[n]$ is a group called the *symmetric group of degree* n.

Throughout, if the operation of a group is understood from the context we omit it.

The assumption that every element of a group has an inverse is a powerful one leading to the following so called *cancellation laws* not guaranteed in monoids.

Theorem 10.3 *Let g, h, f be elements of a group.*

1. *if $gh = gf$ then $h = g$ (left cancellation).*
2. *if $hg = fg$ then $h = g$ (right cancellation).*

Proof. Let $gh = gf$. Multiply by g^{-1} on the left on both sides and the first assertion follows. ■

Example 10.4 Let G be a finite group and let $g \in G$. Then $g^n = e$ for some $n \geq 1$. The elements $g, g^2, \ldots$ cannot all be distinct as G is finite. Then there exist $m, n \geq 1$ such that $g^m = g^{m+n}$ so that $g^m e = g^m g^n$. The claim follows by cancellation.

Another powerful consequence arising from the fact that all elements in a group is that the equations $gx = h$ and $xg = h$ are always soluble.

Theorem 10.5 *Let g, h be elements of a group G.*

1. *the equation $gx = h$ has a unique solution $x = g^{-1}h$ in G.*
2. *the equation $xg = h$ has a unique solution $x = hg^{-1}$ in G.*

Proof. That x is a solution in both cases one can easily verify. Let us argue for uniqueness for the first case. For suppose that there is a y such that $gy = h$ so that $gy = gx$. Then $y = x$ by cancellation. ■

If $G_1, \ldots, G_n$ are groups then their *direct product* $G_1 \times G_2 \times \cdots \times G_n$ coupled with the *component-wise operation* defined by

$$(g_1, \ldots, g_n) \cdot (g_1', \ldots, g_n') = (g_1 g_1', \ldots, g_n g_n')$$

where $g_i g_i'$ are taken in G_i, forms a group whose unity is $(e_{G_1}, \ldots, e_{G_n})$ and whose inverses obey $(g_1, \ldots, g_n)^{-1} = (g_1^{-1}, \ldots, g_n^{-1})$. The proof of this is left to the reader.

§10.1. Subgroups

Definition 10.6 *A non-empty subset S of a group G is called a* subgroup *of G, denoted $S \leq G$ if*

1. *$s \in S \implies s^{-1} \in S$; and*
2. *$s, t \in S \implies st \in S$.*

If G is a group then G and $\{e\}$ are always subgroups of G. Any subgroup of G other than G is called a *proper* subgroup. The subgroup $\{e\}$ is called the *trivial* subgroup.

Theorem 10.7 *If $S \leq G$ then S is a group in its own right.*

Proof. The hypothesis $s, t \in S \Rightarrow st \in S$ equips S with an operation under which S is closed. More specifically, if $\mu : G \times G \to G$ is the operation of G then its restriction $\mu|_{S\times S}$ is the operation on S. Since S is non-empty it contains an element, say, s. The hypothesis that $s^{-1} \in S$ now implies that $e = ss^{-1} \in S$. Finally, the operation on S is associative as it is associative over all of G. ■

The following is often much more convenient to use in order to test whether a set forms a subgroup.

Theorem 10.8 *A subset S of a group G is a subgroup if and only if $e \in S$ and $s, t \in S$ implies $st^{-1} \in S$.*

Proof.

- $\Leftarrow$ We verify that S satisfies the definition of a subgroup. Given $s \in S$ then as $1 \in S$ by assumption then we may write $1s^{-1} = s^{-1} \in S$ by the second property of S. Next if $s, t \in S$ then $s(t^{-1})^{-1} = st \in S$ and we are done.
- $\Rightarrow$ Trivial.

■

Example 10.9 $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$ yet the multiplicative group $(\mathbb{Q}^*, \cdot)$ is not a subgroup of $(\mathbb{R}, \cdot)$ because the operations are different.

Definition 10.10 *The set of all even permutations in S_n are denoted A_n.*

Lemma 10.11 *If $n \geq 2$ then $A_n \leq S_n$.*

Proof. We prove that $\mathbf{1}_{[n]} \in A_n$ and that if $\sigma, \tau \in A_n$ then both σ^{-1} and $\sigma\tau \in A_n$. Note first that $\mathbf{1}_{[n]} = (1\ 2)(1\ 2)$. Next let $\sigma, \tau \in A_n$ and write $\sigma = \gamma_1\gamma_2 \ldots \gamma_n$ and $\tau = \delta_1\delta_2 \cdots \delta_m$ where both m and n are even and where the γ_is and δ_is are transpositions. Then $\sigma\tau = \gamma_1\gamma_2 \ldots \gamma_n\delta_1\delta_2 \cdots \delta_m$ and is a product of $m + n$ transpositions and so is even. Finally, observe that

$$\sigma\mu = \underbrace{\gamma_1\gamma_2 \ldots \gamma_n}_{\sigma}\underbrace{\gamma_n\gamma_{n-1} \ldots \gamma_1}_{\mu} = \mathbf{1}_{[n]}$$

due to $\gamma_i^2 = \mathbf{1}_{[n]}$. Hence,

$$\sigma^{-1} = \sigma^{-1}\mathbf{1}_{[n]} = \sigma^{-1}\sigma\mu = \mathbf{1}_{[n]}\mu = \mu.$$

As μ is even so is σ^{-1}. ■

Definition 10.12 *A_n is called the* alternating group of order n.

Example 10.13 If $n \geq 0$ write $n\mathbb{Z} := \{nk : k \in \mathbb{Z}\}$. We show that $n\mathbb{Z} \subseteq \mathbb{Z}$. The unity of $\mathbb{Z}$ is $0 = n \cdot 0 \in n\mathbb{Z}$. If $a, b \in n\mathbb{Z}$, write these as $a = nk$ and $b = nm$; then $a + b = n(k + m) \in n\mathbb{Z}$. Finally, $-a = n(-k) \in n\mathbb{Z}$.

Testing whether finite sets form a subgroup is even simpler.

Theorem 10.14 *If H is a finite non-empty subset of a group G then $H \leq G$ if and only if H is closed under the operation of G.*

Proof. Let H be closed under the operation of G and let $h \in H$. Then $h, h^2, h^3, \ldots \in H$. As H is finite these elements cannot all be distinct. Hence there exist $n, m \geq 1$ such that $h^n = h^{n+m}$. This means that $e = h^m$ by cancellation so $e \in H$. Then $e = h^{m-1}h$ implies that $h^{-1} = h^{m-1}$ so $h^{-1} \in H$ as well. All this coupled with the closure of H under the operation of G implies that $H \subseteq G$.

The converse is trivial. ■

Abelian groups are of interest as every group contains an abelian subgroup.

Definition 10.15 *Let G be a group. The* zentrum *or* center *of G is given by*

$$Z(G) := \{z \in G : zg = gz \text{ for all } g \in G\}.$$

The elements of $Z(G)$ are said to be central *in G.*

Theorem 10.16 *Let G be a group. Then $Z(G)$ is an abelian subgroup of G.*

Proof. If we prove that $Z(G) \leq G$ then it is clearly abelian. To prove that it is a subgroup note first that $e \in Z(G)$. Next we show that $Z(G)$ is closed under taking inverse. That is, we seek to show that $z^{-1}g = gz^{-1}$ for all $g \in G$. Fix $z \in Z(G)$. Then $zg = gz$ for all $g \in G$ so that $g = z^{-1}gz$ holds. Multiplying this by z^{-1} on the right gives $gz^{-1} = z^{-1}g$ so that $z^{-1} \in Z$. Finally, we seek to show that $Z(G)$ is closed under the operation of G. Fix $y, z \in Z(G)$. then

$$(yz)g = y(zg) = y(gz) = (yg)z = (gy)z = g(yz)$$

holds for all g, where here we used associativity and the fact that $y, z \in Z(G)$. ■

Example 10.17 If $n \geq 3$ then $Z(S_n) = \{\mathbf{1}_{[n]}\}$. That is for any $\sigma \in S_n \setminus \{\mathbf{1}_{[n]}\}$ there exists a $\tau \in S_n$ such that $\sigma\tau \neq \tau\sigma$. As $\sigma \neq \mathbf{1}_{[n]}$ we may pick a $k, m \in [n]$ such that $\sigma(k) = m \neq k$. As $n \geq 3$, let ℓ, k, m be distinct and set τ to be the transposition $(k\ \ell)$. Then $(\tau\sigma)(k) = \tau(m) = m$ and $(\sigma\tau)(k) = \sigma(\ell)$. It suffices to show that $\sigma(\ell) \neq m$. Suppose equality holds. Then $m = \sigma(\ell) = \sigma(k)$ so that $k = \ell$ as σ is one-to-one; a contradiction.

Observation 10.18. *Let G be a group and let $H, K \leq G$. Then $H \cap K \leq G$*

Note that $H \cap K$ is the has the property that $X \subseteq H \cap K$ whenever $X \leq H \cap K$. Note however, that the union of two subgroups of a group is almost never a subgroup.

Theorem 10.19 *The intersection of any family of subgroups of a group G is again a subgroup of G.*

Proof. Let $\{S_i : i \in I\}$ be a family of subgroups of G. The $e \in S_i$ for every $i \in I$ implies that $e \in \bigcap_{i \in I} S_i$. Next, given $a, b \in \bigcap_{i \in I} S_i$, then $a, b \in S_i$ for every $i \in I$ and so $ab^{-1} \in S_i$ for every $i \in S_i$ and hence $ab^{-1} \in \bigcap_{i \in I} S_i$ and it follows that $\bigcap_{i \in I} S_i \leq G$. ■

For a subset X of a group G we say that $X \subseteq H \leq G$ is the *smallest* subgroup of G containing X if whenever $X \subseteq S \leq G$ holds then $S \leq H$. Theorem 10.19 implies the following.

Corollary 10.20 *For every subset X of a group G there is a smallest subgroup of G containing it.*

Proof. The set of subgroups of G containing G is non-empty as in particular G is such a subgroup. Set $:= \{S : X \subseteq S \leq G\}$ and set $H := \bigcap_{S\in} S$. Then $X \subseteq H \leq G$, where the latter claim is owing to Theorem 10.19. As any subgroup containing X is a member of , H is in fact the smallest subgroup of G containing X. ■

For $H \leq G$, sets of the form

$$gHg^{-1} := \{ghg^{-1} : h \in H\}$$

where $g \in G$ are called the *conjugates* of H in G.

Theorem 10.21 *Let G be a group, let $H \leq G$, and let $g \in G$. Then $gHg^{-1} \leq G$.*

Proof. Cleary $e = geg^{-1} \in gHg^{-1}$. Given ghg^{-1} with $h \in H$, we start by noting that

$$(gh^{-1})^{-1} = (g^{-1})^{-1}h^{-1}g^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$$

and thus closure under taking inverses is satisfied. To see that the conjugate of H is closed under the operation of G we observe that

$$(gh_1g^{-1})(gh_2g^{-1}) = g(h_1h_2)g^{-1}$$

for every $h_1, h_2 \in H$, and as $h_1h_2 \in H$ then $g(h_1h_2)g^{-1} \in gHg^{-1}$. ■

If $H \leq G$, then $H = eHe^{-1}$ so that H is always a conjugate of itself. If H is the only conjugate of H in G then H is said to be *self-conjugate* (or *normal*) in G.

Example 10.22 Recall that

$$S_3 = \{\mathbf{1}_{[3]}, (1\ 2\ 3), (1\ 3\ 2), (1\ 2), (1\ 3), (2\ 3)\}.$$

If we denote $\sigma := (1\ 2\ 3)$ and $\tau := (1\ 2)$ then one can verify that $\sigma^2 = (1\ 3\ 2)$, $\tau\sigma = (2\ 3)$, and $\tau\sigma^2 = (1\ 3)$. Then we can write S_3 parametrically as

$$S_3 = \{\mathbf{1}_{[3]}, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}.$$

One can also verify, for instance, that

$$\sigma^3 = \mathbf{1}_{[3]} = \tau^2 \text{ and } \sigma\tau\sigma = \tau.$$

Then $H := \{\mathbf{1}_{[3]}, \tau\} \leq S_3$. We find all conjugates of H in S_3. The first one is clearly $\mathbf{1}_{[3]}H\mathbf{1}_{[3]}^{-1} = H$. Next we consider $\sigma H\sigma^{-1}$ and observe that

$$\sigma H\sigma^{-1} = \{\sigma\mathbf{1}_{[3]}\sigma^{-1}\}, \sigma\tau\sigma^{-1}\} = \{\mathbf{1}_{[3]}, \sigma\tau\sigma^{-1}\}$$

Noting that $\sigma^{-1} = \sigma^2$ we may write

$$\sigma H\sigma^{-1} = \{\mathbf{1}_{[3]}, \sigma\tau\sigma^2\} = \{\mathbf{1}_{[3]}, \underbrace{\sigma\tau\sigma}_{\tau}\sigma\} = \{\mathbf{1}_{[3]}, \tau\sigma\}.$$

In a similar manner we can determine that

$$\sigma^2 H \sigma^{-2} = \{\mathbf{1}_{[3]}, \tau\sigma^2\}.$$

We we continue in this fashion we discover that $H, \sigma H \sigma^{-1}$ and $\sigma^2 H \sigma^{-2}$ are all the conjugates of H in G.

§10.2. Cyclic groups and the order of an element

Definition 10.23 *If G is a group and $a \in G$ then the* cyclic subgroup generated by a *denoted $\langle a \rangle$ is the set of all powers of a. The element a is called the* generator *of $\langle a \rangle$. A group G is called* cyclic *if there is an $a \in G$ such that $G = \langle a \rangle$; that is G consists of all powers of a.*

That $\langle a \rangle \leq G$ for every $a \in G$ is trivial and follows from the laws of exponents. Also note that the same cyclic subgroup can be generated by different elements; most notable is the example that $\langle a \rangle = \langle a^{-1} \rangle$.

Example 10.24 If G is any group, then $\langle e \rangle = \{e\}$ is a cyclic subgroup of G.

Example 10.25 The group $(\mathbb{Z}, +)$ is a cyclic subgroup having precisely two generators, namely 1 and -1. If $k \in \mathbb{Z}$ then $k = k \cdot 1 \in \langle 1 \rangle$ so $\mathbb{Z} = \langle 1 \rangle$. Similarly, $\mathbb{Z} = \langle -1 \rangle$ as $k = (-k) \cdot (-1)$. No other generator is possible as $n\mathbb{Z} \neq \mathbb{Z}$ whenever $|n| > 1$.

Example 10.26 The group $(\mathbb{Z}_n, +)$ is a cyclic group with generator $\overline{1}$. Indeed, given $\overline{k} \in \mathbb{Z}_n$ we have that $\overline{k} = k\overline{1}$ and thus $\overline{k} \in \langle \overline{1} \rangle$. That $\mathbb{Z}_n = \langle \overline{1} \rangle$ follows.

Definition 10.27 *If G is a group and $a \in G$, then the number of elements in $\langle a \rangle$ (which could of course be infinite) is called the* order *of a in G.*

Theorem 10.28 *If G is a group and $a \in G$ has finite order m then m is the least positive integer satisfying $a^m = e$.*

Proof. If $a = e$ then $m = 1$. Suppose then that $a \neq e$. There is a $k > 1$ such that

$$e, a^1, a^2, \ldots, a^{k-1}$$

are all distinct and $a^k = a^i$ for some $0 \leq i \leq k-1$. That is k is the least positive integer for which the above sequence of powers of a "intersects" itself. We claim that $a^k = e = a^0$ in fact holds. For if $a^k = a^i$ for some $i \geq 1$ then $k - i \leq k - 1$ and $a^{k-i} = e$ contradicting the minimality of k.

It remains to prove that $k = m$; that is, $\langle a \rangle = \{e, a, a^2, \ldots, a^{k-1}\}$. That $\langle a \rangle \supseteq \{e, a, a^2, \ldots, a^{k-1}\}$ is clear. For the reverse inclusion let a^ℓ be a power of a and write $\ell = qk + r$ where $0 \leq r \leq k-1$, which is possible by Theorem 4.1. Then $a^{qk+r} = a^{qk}a^r = a^r$ (as $a^k = e$), implying that $a^\ell = a^r \in \{e, a, a^2, \ldots, a^{k-1}\}$. ■

We may extract the following from the proof of Theorem 10.28.

Observation 10.29. *Let G be a group and let $g \in G$ have order n. Then $\langle g \rangle = \{e, g, \ldots, g^{n-1}\}$ where all elements in this set are distinct. Moreover, if G is a finite group and it admits an element of order $|G|$ then G is cyclic.*

We illustrate this last observation using the following example.

Example 10.30 Is $\mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$ cyclic? If $\mathbb{Z}_8^*$ is cyclic then it must admit an element whose order is 4 (i.e., equal to its size). So we examine the order of each of its elements. The order of $\overline{1}$ is of course 1. As $3^2 \equiv 9 \equiv 1 \pmod 8$ the order of $\overline{3}$ is 2. In a similar manner we can discover that the order of both $\overline{5}$ and $\overline{7}$ is 2 for both. Hence, no element has order 4 so $\mathbb{Z}_8^*$ is not cyclic.

Example 10.31 For the group $\mathbb{Z}_7^*$, we naturally appeal to Fermat's little theorem (namely Theorem 7.10) and note that $a^6 \equiv 1 \pmod 7$ for every $a \in \mathbb{Z}_7^*$. Question is though whether any of the elements of this group has order 6 which is the order of $\mathbb{Z}_7^*$. Some thought reveals that indeed 3 is such an element.

$$\begin{aligned}
3^1 &\equiv 3 \pmod 7\\
3^2 &\equiv 2 \pmod 7\\
3^3 &\equiv 6 \pmod 7\\
3^4 &\equiv 4 \pmod 7\\
3^5 &\equiv 5 \pmod 7\\
3^6 &\equiv 1 \pmod 7
\end{aligned}$$

It follows that $\mathbb{Z}_7^*$ is cyclic.

Example 10.32 Let $\gamma := (k_1\ k_2\ \cdots\ k_r)$ be a cycle in S_n. Then the order of γ is r; which is its length.

Observation 10.33. *The orders of any element of a group and its inverse coincide.*

Proof. Let g be an element of a group G. If $k \in \mathbb{Z}$, then $(g^k)^{-1} = (g^{-1})^k$ by the laws of exponents. It follows that $(g^{-1})^k = e$ if and only if $g^k = e$. The claim follows. ■

Observation 10.34. *If G is a finite group then every $g \in G$ has finite order.*

Proof. As G is finite the powers $g, g^2, g^3, \ldots$ are not all distinct and there are $1 \le k < m$ s.t. $g^k = g^m$. Then by cancellation $g^{m-k} = e$ and the order of g is at most $m - k$ and thus finite. ■

Computing the order of an element is made simple by the following.

Theorem 10.35 *Let G be a group and let $g \in G$ have order n. Then*

1. $g^k = e \iff n \mid k$.
2. $g^k = g^m \iff k \equiv m \pmod n$

Proof.

1. If $n \mid k$ then $k = qn$ and then $g^k = (g^n)^k = e$. Conversely, if $g^k = e$, then write $k = qn + r$ with $0 \le r < n$ so that $g^r = g^k(g^n)^{-q} = e$ with $0 \le r < n$ contradicting the minimality of n unless $r = 0$. But if the latter occurs then $n \mid k$.
2. W.l.o.g., $m \ge k$. Then $g^k = g^m$ holds if and only if $g^{m-k} = e$, by cancellation. This occurs by the first part of the theorem if and only if $n \mid m - k$ which in turn implies $k \equiv m \pmod n$.

■

A handy corollary of the first part of Theorem 10.35 reads as follows.

Corollary 10.36 *Let $G = \langle a \rangle$ have order n. Then $g^n = e$ for every $g \in G$.*

Proof. While we could appeal to the first part of Theorem 10.35, let us simply note that given $g \in G$ we may write $g = a^k$ for some k. Then $g^n = (a^k)^n = (a^n)^k = e$. ■

Example 10.37 Determine the order of $\overline{2}$ in $\mathbb{Z}_{19}^*$. We start with the following auxiliary computations:

$$\begin{aligned} 2^3 &\equiv 8 \pmod{19} \\ 2^6 &\equiv 64 \equiv 7 \pmod{19} \\ 2^9 &\equiv 56 \equiv -1 \pmod{19}. \end{aligned}$$

Then $2^{18} \equiv 1 \pmod{19}$. By Theorem 10.35, the order of $\overline{2}$ must be a divisor of 18 and thus lies in $\{1, 2, 3, 6, 9, 18\}$. We have already eliminated $3, 6, 9$. Eliminating 1 and 2 is easy so all we are left with is 18. So the order of $\overline{2}$ is 18. Noting that $|\mathbb{Z}_{19}^*| = 18$ it follows that $\mathbb{Z}_{19}^*$ is cyclic by Observation 10.29.

Next, we present the "infinite compnaion" of Theorem 10.35 and its proof is left to the reader.

Theorem 10.38 *Let G be a group and let $g \in G$ have infinite order. Then*

1. $g^k = e \iff k = 0$.
2. $g^k = g^m \iff k = m$.
3. $\langle g \rangle = \{\cdots, g^{-2}, g^{-1}, e, g, g^2, \cdots\}$ *with all elements distinct.*

Observation 9.19, Example 10.32, and Theorem 10.35 now yield the following.

Corollary 10.39 *Let $\sigma \in S_n$ with (cycle) factorisation $\sigma = \gamma_1\gamma_2\cdots\gamma_r$ of lengths $r_1, \ldots, r_r$, respectively. Then the order of σ is $\operatorname{lcm}(r_1, \ldots, r_r)$.*

10.2.1 *Subgroups of cyclic groups*

Exponent laws and the fact that, say, $\mathbb{Z}_8^*$ is abelian yet not cyclic (see Example 10.30) establish the following.

Observation 10.40. *Every cyclic group is abelian, but the converse does not hold.*

Proposition 10.41 *Every subgroup of a cyclic group is cyclic.*

Proof. Let $H \leq G := \langle g \rangle$. If H is trivial then it is cyclic. Otherwise there is $k \neq 0$ s.t. $g^k \in H$. As H is a subgroup then $g^{-k} = (g^k)^{-1} \in H$ so we may assume that $k > 0$. Let m be the smallest positive integer s.t. $g^m \in H$. We prove that $\langle g^m \rangle = H$. To see this, let $g^k \in H$ and write $k = qm + r$ with $0 \leq r < m$. As $g^r = (g^m)^{-q} g^k \in H$ we attain a contradiction to the minimality of m unless $r = 0$. Having $r = 0$ implies that $g^k = (g^m)^q$. This asserts that every element of H is a power of g^m and the claim follows. ■

Cyclic groups can have several generators. Previously we mentioned the somewhat degenerate example that if $G = \langle g \rangle$ then $G = \langle g^{-1} \rangle$. More can be said actually, and the following result describes all generators a cyclic group may have.

Proposition 10.42 *Let $G = \langle g \rangle$ and let it have order n. Then $G = \langle g^k \rangle$ if and only if $(k, n) = 1$.*

Proof. If $G = \langle g^k \rangle$, then $g \in \langle g^k \rangle$, and let us write $g = (g^k)^m$. Thus $g^1 = g^{km}$ implying that $g^{km-1} = e$ so that $n \mid km - 1$ so we may write $km - 1 = qn$ and thus $1 = km - qn$ implying that $(k, n) = 1$ by Proposition 4.30.

Conversely, if $(k, n) = 1$ then we may write $1 = xk + yn$ by Proposition 4.30 so that

$$g = g^1 = (g^k)^x (g^n)^y = (g^k)^x e \in \langle g^k \rangle.$$

■

Corollary 10.43 *If G is a cyclic group of order n then it has $\varphi(n)$ generators.*

Put another way, if G is a cyclic group of order n then there are precisely $\varphi(n)$ elements of G having order n.

Theorem 10.45 describes all subgroups of finite cyclic groups G. In particular it show that G has a unique subgroup of order k for every divisor k of $|G|$ and that these are the only subgroups of G. The following lemma facilitates in the proof of the forthcoming Theorem 10.45.

Lemma 10.44 *Let G be a group and let $g \in G$ have order n. If $d \mid n$, $d \geq 1$, then the order of g^d is n/d.*

Proof. Put $k := n/d$. Then $(g^d)^k = g^n = e$. We seek to show that k is the least positive integer with this property. Suppose that $(g^d)^r = e$, $r \geq 1$. Then $g^{dr} = e$ so that $n \mid dr$. Let $dr = qn$, $q \geq 1$. Then $dr = q(dk)$ so that $r = qk$ as these are integers and $d \neq 0$. It follows that $r \geq k$ as required. ■

Theorem 10.45 *Let $G = \langle g \rangle$ have order n.*

1. *If $H \leq G$ then $H = \langle g^d \rangle$ for some $d \mid n$; hence $|H| \mid |G| = n$.*
2. *Conversely, if $k \mid n$ then $\langle g^{n/k} \rangle$ is the unique subgroup of G of order k.*

Proof.

1. By Proposition 10.41, $H = \langle g^m \rangle$ for some m. Let $d = (m, n)$. We show that $H = \langle g^d \rangle$. As $d \mid m$, we may write $m = qd$ so that $g^m = (g^d)^q \in \langle g^d \rangle$ implying that $H \subseteq \langle g \rangle^d$. On the other hand, we may write $d = xm + yn$ and then have

$$g^d = (g^m)^x (g^n)^y = (g^m)^x e \in \langle g^m \rangle = H.$$

This establishes that $H = \langle g^d \rangle$. By Lemma 10.44, H has order n/d and thus $|H| \mid |G|$.

2. Let $K \leq G$ have order k where $k \mid n$. By the first part of this theorem, $K = \langle g^d \rangle$ where $d \mid n$. Lemma 10.44 then yields $k = |K| = n/d$ implying that $d = n/k$ so that $K = \langle g^{n/k} \rangle$.

■

The following generalises Lemma 10.44.

Lemma 10.46 *Let G be a group and let $g \in G$ have order t. If $u \in \mathbb{Z}^n$, then the order of a^u is $t/(t,u)$.*

Proof. Let s be the order of g^u and let $d = (t,u)$ so that $t = t_1 d$ and $u = u_1 d$ with $(t_1, u_1) = 1$. We start by proving that $s \mid \frac{t}{d}$ so that $s \leq \frac{t}{d}$. To see this, observe that

$$(g^u)^{t/d} = (g^{u_1 d})^{t/d} = g^{tu_1} = (g^t)^{u_1} = e_G;$$

then $s \mid \frac{t}{d}$, by Theorem 10.35.

Next, we prove that $\frac{t}{d} \mid s$ so that $\frac{t}{d} \leq s$. To see this, note that

$$(g^u)^s = g^{us} = e_G$$

so that $t \mid us$. Then, $t_1 d \mid u_1 ds$ implying that $t_1 \mid u_1 s$. As $(t_1, u_1) = 1$, it follows that $\frac{t}{d} = t_1 \mid s$, by Lemma 4.37, as required. ■

10.2.2 *Subgroups generated by sets*

Definition 10.47 *If X is a subset of a group G, then the smallest subgroup of G containing X is denoted $\langle X \rangle$ and is called the subgroup* generated *by X. One also says that X* generates *$\langle X \rangle$.*

If $X = \{a_1, \ldots, a_n\}$ is a finite set then we write $\langle a_1, \ldots, a_n \rangle$ instead of $\langle \{a_1, \ldots, a_n\} \rangle$.

Definition 10.48 *Let G be a group. If $\emptyset \neq X \subseteq G$, then a* word *on X is an element $w \in G$ having the form*

$$w = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$$

where $x_i \in X$, $e_i = \pm 1$ and $n \geq 1$.

Theorem 10.49 *Let X be a subset of a group G. If $X = \emptyset$ then $\langle X \rangle = e$ (as a subgroup). If $X \neq \emptyset$ then $\langle X \rangle$ is the set of all words on X.*

Proof. If $X = \emptyset$ then the subgroup $\{e\}$ contains X and so $\langle X \rangle = e$. If $X \neq \emptyset$, let $\mathcal{W}$ denote the set of all words on W. Then $X \subseteq \mathcal{W} \leq G$ ($e = x^{-1}x \in \mathcal{W}$, the inverse of a word is a word, and the product of two words is a word). As $\langle X \rangle$ is the smallest subgroup of G containing X it follows that $\langle X \rangle \subseteq \mathcal{W}$. The reverse inclusion also holds for every subgroup $H \leq G$ containing X must contain every word on X. Then $\mathcal{W} \leq H$ for every H containing X so $\mathcal{W}$ is the smallest subgroup of G containing X and thus coincides with $\langle X \rangle$. ■

If a group G has the form $G = \langle X \rangle$ for some $X \subseteq G$ we say that G is *generated* by X and that the members of X are the *generators* of G. If X is finite we say that G is a *finitely generated group*.

§10.3. On the cyclicity of $\mathbb{Z}_n^*$

The purpose of this section is twofold; first, we seek to introduce the notion of a *primitive root*; second, we would like to demonstrate the usefulness of the abstract algebraic terminology set thus far.

Let $a, n \in \mathbb{Z}^+$ such that $n > 1$ and $(a, n) = 1$. Then, by Euler's theorem (namely Theorem 8.15), $a^{\varphi(n)} \equiv 1 \pmod{n}$. The well-ordering principle then asserts that there is a least positive integer x such that $a^x \equiv 1 \pmod{n}$ called the *order of a modulo n* and denoted $\mathrm{ord}_n(a)$. This notion of an order of an

integer was first introduced by Gauss in 1801. We identify this notion as simply the order of $[a]_n$ in $\mathbb{Z}_n^*$. Recalling that $\mathbb{Z}_n^*$ need not be cyclic (see Example 10.30) we do however concede that one ought to treat orders of its elements with care.

Consider the number theoretic 'daunting' task of finding all solutions to the congruence $a^x \equiv 1 \pmod{n}$. The first part of Theorem 10.35 asserts that x is a solution if and only if $\mathrm{ord}_n(a) \mid x$. This in particular implies that $\mathrm{ord}_n(a) \mid \varphi(n)$. For dramatic effect, let us record these facts in their number theoretic formulation.

Proposition 10.50 *Let $a, n \in \mathbb{Z}^+$ such that $n > 1$ and $(a, n) = 1$. Then,*

1. *x is a solution for $a^x \equiv 1 \pmod{n}$ if and only if $\mathrm{ord}_n(a) \mid x$;*
2. *in particular, $\mathrm{ord}_n(a) \mid \varphi(n)$.*

Proposition 10.51 *Let $a, n \in \mathbb{Z}^+$ such that $n > 1$ and $(a, n) = 1$. Let $0 \leq j \leq i$ be integers. Then,*

$$a^i \equiv a^j \pmod{n} \iff i \equiv j \pmod{\mathrm{ord}_n(a)}.$$

Proof. We carry out the proof in $\mathbb{Z}_n^*$.

$\Leftarrow$ If $i \equiv j \pmod{\mathrm{ord}_n(a)}$, then we may write $i = j + k\mathrm{ord}_n(a)$ so that

$$\overline{a}^i = \overline{a}^{j+k\mathrm{ord}_n(a)} = \overline{a}^j(\overline{a}^{\mathrm{ord}_n(a)})^k = \overline{a}^j.$$

$\Rightarrow$ In this direction there is a subtlety in the algebraic proof that we wish to highlight by first providing a purely number theoretic proof for the claim in this direction. The latter proceeds as follows. If $a^i \equiv a^j \pmod{n}$ then we may write

$$a^j \equiv a^i \equiv a^j a^{i-j} \pmod{n}. \tag{10.52}$$

As $(a, n) = 1$ it follows that $(a^j, n) = 1$ so that we may reduce both sides by a_j, owing to Corollary 6.15, and obtain

$$a^{i-j} \equiv 1 \pmod{n}$$

so that $\mathrm{ord}_n(a) \mid i - j$, by Proposition 10.50, implying that $i \equiv j \pmod{\mathrm{ord}_n(a)}$.

Let us proceed to an algebraic proof in the context of $\mathbb{Z}_n^*$ for the same claim. The assumption now is that $[a^i]_n = [a_j]_n$. Already here we have to stop as this is only partially the assumption in the premise. The equality $[a^i]_n = [a^j]_n$ is a number theoretic formulation actually replacing $a^i \equiv a^j \pmod{n}$. Our algebraic assumption should be that $[a^i]_n$ and $[a^j]_n$ are equal in $\mathbb{Z}_n^*$. However it is not at all clear that these are actually elements of these group; recall that unlike $\mathbb{Z}_n$, the multiplicative group $\mathbb{Z}_n^*$ does not contain all congruence classes modulo n.

Noticing this hurdle we restart our argument as follows. Owing to $(a, n) = 1$, it follows that $(a^k, n) = 1$ for every $k \in \mathbb{Z}^+$, and thus $[a^k]_n \in \mathbb{Z}^*n$ for every k. In the number theoretic argument we employed this argument by invoking Corollary 6.15 in order to cancel a^j without changing the modulo n; this in algebraic terms simply means that $[a^j]_n \in \mathbb{Z}_n^*$ and thus has an inverse.

With the above understood we commence our algebraic proof by rewriting (10.52) as to read

$$[a^j]_n = [a^i]_n = [a^j a^{i-j}]_n = [a^j]_n[a^{i-j}]_n$$

and so far we only used modular arithmetics. As $[a^k]_n \in \mathbb{Z}_n^*$ for all k the equation

$$[a^j]_n = [a^j]_n[a^{i-j}]_n$$

can be viewed over $\mathbb{Z}_n^*$. As such $[a^j]_n \in \mathbb{Z}_n^*$ and has an inverse in that group. Cancellation laws allow us to write

$$[a^{i-j}]_n = [1]_n.$$

Modular arithmetics allows us to write

$$([a]_n)^{i-j} = [1]_n$$

and we note that as $(a, n) = 1$ then $[a]_n \in \mathbb{Z}_n^*$ so that $([a]_n)^{i-j}$ is a valid member of that group as well. Now we invoke the first part of Theorem 10.35 as to obtain that $\text{ord}_n(a) \mid i - j$ as in the number theoretic proof.

■

In 1773, Euler coined the term *primitive root*.

Definition 10.53 *Let $r, n \in \mathbb{Z}^+$ s.t. $n > 1$ and $(r, n) = 1$. If $\text{ord}_n(r) = \varphi(n)$, then r is called a* primitive root *modulo n and we say that n has a* primitive root.

Algebraically, for $n > 1$, the generators of $\mathbb{Z}_n^*$ (if there are any) are the primitive roots of n. For instance, the fact that $\mathbb{Z}_8^*$ is not cyclic (see Example 10.30) implies that 8 has no primitive roots. On the other hand we learn from Example 10.31 that 7 has primitive roots. More generally if n has a primitive root r, then $\mathbb{Z}_n^* = \langle r \rangle$; number theoretically, this means that

$$r^1, r^2, \ldots, r^{\varphi(n)}$$

forms a reduced system of residues modulo n.

If r is a primitive root of $n > 1$ then its powers are also primitive roots of n. In group theoretic terms this reads as follows.

Proposition 10.54 *Let $n > 1$. If $\mathbb{Z}_n^* = \langle r \rangle$ (i.e., admits at least one generator and thus cyclic), then $\mathbb{Z}_n^* = \langle r^u \rangle \iff (u, \varphi(n)) = 1$.*

Proof. By Lemma 10.46,

$$\begin{aligned} \text{ord}_n(r^u) &= \frac{r}{(u, \text{ord}_n(r))} \\ &= \frac{\varphi(n)}{(u, \varphi(n))}. \end{aligned}$$

Consequently, $\text{ord}_n(r^u) = \varphi(n)$ (and thus a generator of $\mathbb{Z}_n^*$) if and only if $(u, \varphi(n)) = 1$. ■

As there are $\varphi(\varphi(n))$ integers in $[1, \varphi(n)]$ that are co-prime with $\varphi(n)$ we have the following consequence.

Corollary 10.55 *Let $n \geq 1$. If $\mathbb{Z}_n^*$ is cyclic, then it has $\varphi(\varphi(n))$ denerators.*

§10.4. Group Homomorphisms

Mappings between groups that *preserve* the group operations are referred to as *homomorphisms*.

Definition 10.56 *Let $(G, *)$ and $(H, \cdot)$ be groups. A mapping $\alpha : G \to H$ satisfying*

$$\alpha(a * b) = \alpha(a) \cdot \alpha(b)$$

for all $a, b \in G$ is called a homomorphism *from G to H.*

Example 10.57 The mapping $\alpha : \mathbb{Z} \to \mathbb{Z}$ given by $\alpha(a) = 3a$ is a homomorphism as $\alpha(a + b) = 3(a + b) = 3a + 3b = \alpha(a) + \alpha(b)$.

Example 10.58 If a is an element of a group G then the *exponent map* $\alpha\mathbb{Z} \to \langle a \rangle$ given by $n \mapsto a^n$ is a homomorphism.

Example 10.59 The identity map $G \to G$ given by $g \mapsto g$ is a homomorphism.

For groups G and G there is always at least one homomorphism $G \to H$ and that is the *trivial* homomorphism given by $g \mapsto e_H$ for all $g \in G$ and where e_H denotes the unity of H.

Observation 10.60. *Let $\alpha : G \to H$ and $\beta : H \to K$ be group homomorphisms. Then their composition $\beta\alpha := \beta \circ \alpha : G \to K$ is also a group homomorphism.*

Proof. Fix $a, b \in G$ and note that

$$\beta\alpha(ab) = \beta(\alpha(ab)) = \beta(\alpha(a)\alpha(\beta)) = \beta\alpha(a)\beta\alpha(b).$$

■

The following result makes the preservation of algebraic structure by homomorphisms more clear.

Proposition 10.61 *Let $\alpha : G \to H$ be a group homomorphism. Then*

1. $\alpha(e_G) = e_H$.
2. $\alpha(g^{-1}) = \alpha(g)^{-1}$ *for all* $g \in G$.
3. $\alpha(g^k) = \alpha(g)^k$ *for all* $g \in G$.

Proof.

1. Observe that
$$\alpha(e_G)\alpha(e_G) = \alpha(e_G^2) = \alpha(e_G) = \alpha(e_G)e_H$$
and the claim follows by cancellation (in H).

2. Observe that
$$\alpha(g^{-1})\alpha(g) = \alpha(g^{-1}g) = \alpha(e_G) = e_H,$$
where for the last equality we used the first part of this proposition.

3. Lets first consider $k \geq 0$ and proceed by induction on k. For $k = 0$, $\alpha(g^0) = \alpha(e_G) = e_H = \alpha(g)^0$. For the inductive step we write
$$\alpha(g^{k+1}) = \alpha(gg^k) = \alpha(g)\alpha(g^k) \overset{\text{I.H.}}{=} \alpha(g)(\alpha(g))^k = \alpha(g)^{k+1}.$$
If $k < 0$, then write $k = -m$, $m > 0$, and proceed in a similar manner as to yield
$$\alpha(g^k) = \alpha((g^m)^{-1}) = \alpha(g^m)^{-1} = (\alpha(g)^m)^{-1} = \alpha(g)^{-m} = \alpha(g)^k.$$

■

Corollary 10.62 *Let $\alpha : G \to H$ be a group homomorphism. If $g \in G$ has finite order then $\alpha(G)$ has finite order and the order of $\alpha(g)$ divides the order of g.*

Proof. Let n be the order of g; then $g^n = e_G$. Hence, $\alpha(g)^n = \alpha(g^n) = \alpha(e_G) = e_H$. This establishes that $\alpha(g)$ has finite order. By (the first part of) Theorem 10.35 the order of $\alpha(g)$ must divide n. ■

For a group homomorphism $\alpha : G \to H$, write $\alpha(G) := \{\alpha(g) : g \in G\}$ to denote the *image* of G under α.

Corollary 10.63 *Let $\alpha : G \to H$ be a group homomorphism. Then $\alpha(G) \leq H$.*

Proof. First we note that $e_H = \alpha(e_G) \in \alpha(G)$. Next, given $\alpha(g_1), \alpha(g_2) \in \alpha(G)$, then $\alpha(g_1)\alpha(g_2) = \alpha(g_1 g_2) \in \alpha(G)$. Finally, given $\alpha(g) \in \alpha(G)$ we observe that $\alpha(g)^{-1} = \alpha(g^{-1}) \in \alpha(G)$. ■

A group homomorphism $\alpha : G \to H$ is onto if and only if $\alpha(G) = H$. For such mappings we have the following.

Proposition 10.64 *Let $\alpha : G \to H$ be an onto group homomorphism.*

1. *If G is abelian then H is abelian.*
2. *If $G = \langle a \rangle$ then $H = \langle \alpha(a) \rangle$.*

Proof. Let $h_1, h_2 \in H$. Since α is onto we may write $h_1 = \alpha(g_1)$ and $h_2 = \alpha(g_2)$ where $g_1, g_2 \in G$.

1. If G is abelian then we may write
$$h_1 h_2 = \alpha(g_1)\alpha(g_2) = \alpha(g_1 g_2) = \alpha(g_2 g_1) = \alpha(g_2)\alpha(g_1) = h_2 h_1.$$
2. If $h \in H$ then there is a k such that $h = \alpha(a^k) = \alpha(a)^k$.

■

In order to show that two mappings $\alpha, \beta : G \to H$ are equal we need to check all images of members of G. If in addition it is known that α and β are homomorphisms then we only need to examine the images of the generating set of G to determine equality of the mappings.

Proposition 10.65 *Let $\alpha, \beta : G \to H$ be group homomorphism and suppose that $G = \langle X \rangle$. Then $\alpha = \beta$ if and only if $\alpha(x) = \beta(x)$ for all $x \in X$.*

Proof.

$\Rightarrow$ Trivial.

$\Leftarrow$ Let $g = x_1^{k_1} \cdots x_n^{k_n} \in \langle X \rangle = G$. Then
$$\alpha(g) = \alpha(x_1)^{k_1} \cdots \alpha(x_n)^{k_n} = \beta(x_1)^{k_1} \cdots \beta(x_n)^{k_n} = \beta(g).$$
The claim follows.

■

10.4.1 *Isomorphisms*

Definition 10.66 *A group homomorphism that is also a bijection is called an* isomorphism.

Two groups G and H for which an isomorphism exists are called *isomorphic* and we write $G \cong H$ to denote this. If $\alpha : G \to H$ is an isomorphism then the message is that G and H are the same group under the change of names $g \mapsto \alpha(g)$. Clearly, $G \cong G$ for any G.

Example 10.67 The set $2\mathbb{Z}$ (i.e., the even numbers) forms and additive group that is isomorphic to $\mathbb{Z}$; i.e., $2\mathbb{Z} \cong \mathbb{Z}$. To see this simply define $\sigma : \mathbb{Z} \to 2\mathbb{Z}$ by setting $x \mapsto 2x$. This mapping clearly a bijection and

$$\sigma(x+y) = 2(x+y) = 2x + 2y = \sigma(k) + \sigma(y)$$

so it is a homomorphism as well.

Example 10.68 Let us prove that $(\mathbb{R}, \cdot) \cong (\mathbb{R}^+, +)$. Define $\sigma : \mathbb{R} \to \mathbb{R}^+$ to be given by $\sigma(r) = e^r$. To show that this mapping is one-to-one let $\sigma(r) = \sigma(s)$ for some $r, s \in \mathbb{R}$. Then $e^r = e^s$ leading to $r = \ln(e^r) = \ln(e^s) = s$. To see that this function is onto let $t \in \mathbb{R}^+$, then $t > 0$, so that $\ln t \in \mathbb{R}$ and $\sigma(\ln t) = t$. We have established that σ is a bijection. Finally note that

$$\sigma(r+s) = e^{r+s} = e^r e^s = \sigma(r)\sigma(s)$$

for all $r, s \in \mathbb{R}$ so σ is a homomorphism.

Homomorphisms we have seen to preserve unity, inverses, and powers. Isomorphisms also preserve order.

Proposition 10.69 *Let $\sigma : G \to H$ be an isomorphism. Then for all $g \in G$ the order of g and the order of $\sigma(g)$ are the same.*

Proof. Suffice to show that $g^k = e_G$ if and only if $\sigma(g)^k = e_H$. If $g^k = e_G$, then $\sigma(g)^k = \sigma(g^k) = \sigma(e_G) = e_H$. Conversely, if $\sigma(g)^k = e_H$ then $\sigma(g^k) = \sigma(g)^k = e_H = \sigma(e_G)$ so that $g^k = e_G$ as σ is one-to-one. ■

Direct products preserve isomorphism.

Proposition 10.70 *If $G \cong G_1$ and $H \cong H_1$ then $G \times G_1 \cong H \times H_1$.*

Proof. Let $\sigma : G \to G_1$ and $\tau : H \to H_1$ be isomorphisms and define $\mu : G \times H \to G_1 \times H_1$ by setting $\mu(g,h) = (\sigma(g), \tau(h))$. The proof that this is a bijection is left to the reader. We prove that this is a homomorphism.

$$\begin{aligned}
\mu((g,h)(g',h')) &= \mu(gg', hh') \\
&= (\sigma(gg'), \tau(hh')) \\
&= (\sigma(g), \tau(h))(\sigma(g'), \tau(h')) \\
&= \mu(g,h)\mu(g',h').
\end{aligned}$$

■

Example 10.71 $(\mathbb{Q}, +) \ncong (\mathbb{Q}^*, \cdot)$. To see this assume towards a contradiction that $\sigma : \mathbb{Q} \to \mathbb{Q}^*$ is an isomorphism between these two groups. As σ is onto we may choose $q \in \mathbb{Q}$ satisfying $\sigma(q) = 2$ and write $a := \sigma(\frac{1}{2}q)$. As σ is a homomorphism we may write

$$a^2 = \sigma(\frac{1}{2}q)\sigma(\frac{1}{2}q) = \sigma(\frac{1}{2}q + \frac{1}{2}q) = \sigma(q) = 2$$

which is impossible as 2 is irrational.

Example 10.72 Let G and H be cyclic groups of orders 9 and 3, respectively. Even though G and $H \times H$ both have order 9, one still has $G \ncong H \times H$. For suppose that an isomorphism $\sigma : G \to H \times H$ was to exist. If $G = \langle a \rangle$ (so that the order of a is 9) we may write $a = \sigma(x)$ for some $x \in H \times H$. By Corollary 10.36, $x^3 = e_{H \times H}$ (as this holds for any element of $H \times H$). If so we may write

$$a^3 = \sigma(x^3) = e_G$$

contradicting the fact that the order of G is 9.

The following is not hard to verify now.

Proposition 10.73 *Let G, H, K be groups.*

1. *The identity map $\mathbf{1}_G : G \to G$ is an isomorphism for every G.*
2. *If $\sigma : G \to H$ is an isomorphism then $\sigma^{-1} : H \to G$ is an isomorphism as well.*
3. *If $\sigma : G \to H$ and $\tau H \to K$ are isomorphisms then their composition $\tau\sigma : G \to K$ is an isomorphism as well.*

Theorem 10.74 *The isomorphic relation is an equivalence relation for groups.*

10.4.2 The Chinese remainder theorem revisited

In this section we aim at formulating the Chinese remainder theorem (see Theorem 6.64) in a group theoretic setting is to crystallise it further still. Our starting point is the following generalisation of Observation 10.29.

Proposition 10.75 *Let $G = \langle g \rangle$ and $H = \langle H \rangle$ have orders n and m, respectively, and such that $(n, m) = 1$. Then $G \times H$ is cyclic.*

Proof. By Observation 10.29, it suffice to prove that there exists an element of $G \times H$ whose order is $mn = |G \times H|$. We prove that (g, h) is such an element. Trivially, we note that

$$(g, h)^{mn} = (g^{mn}, h^{mn}) = ((g^n)^m, (h^m)^n) = (e_G, e_H).$$

Next, we note that only common multiples k of n and m can yield $(g, h)^k = (e_G, e_H)$. The least of these multiples is then the order of (g, h) in $G \times H$. As $(n, m) = 1$ we have that $\operatorname{lcm}(n, m) = mn$, by Corollary 4.73. The claim follows. ■

Induction, Lemma 4.76, and Proposition 10.75 yield the following extension of the latter.

Corollary 10.76 *Let $G_1, \ldots, G_r$ be cyclic groups where G_i has order n_i and such that $(n_1, \ldots, n_r) = 1$. Then $G_1 \times \cdots \times G_r$ is cyclic.*

The next observation we require reads as follows.

Observation 10.77. *Let $m \mid n$. If $x \in [r]_n$ then $x \in [r]_m$ (surely, $r \geq m$ is possible).*

PROOF. We may write $x = qn + r$ for some $0 \leq r < n$. As $m \mid n$ we may write $n = km$ and thus obtain $x = m(kq) + r$ and the claim follows. ■

The main point behind Observation 10.77 is that given $\mathbb{Z}_n$ and $\mathbb{Z}_m$ with $m \mid n$ then the mapping $[a]_n \mapsto [a]_m$ is a well-defined function which is in fact surjective (i.e., onto).

Let us apply our new found knowledge. In particular, let m and n be co-prime and consider $\mathbb{Z}_n \times \mathbb{Z}_m$ (which we now know to be cyclic) and $\mathbb{Z}_{mn}$. Observation 10.77 along with the trivialities $m \mid mn$ and $n \mid mn$, we have that $\sigma : \mathbb{Z}_{mn} \to \mathbb{Z}_n \times \mathbb{Z}_m$ given by $\sigma([a]_{mn}) := ([a]_n, [a]_m)$ is a well-defined function. In fact, it is an isomorphism. To see that σ is a homomorphism one notes that

$$\begin{aligned}
\sigma([a]_{mn} + [b]_{mn}) &= \sigma([a+b]_{mn}) = ([a+b]_n, [a+b]_m) \\
&= ([a]_n + [b]_n, [a]_m + [b]_m) \\
&= ([a]_n, [a]_m) + ([b]_n, [b]_m) \qquad \text{(pointwise addition)} \\
&= \sigma([a]_{mn}) + \sigma([b]_{mn}).
\end{aligned}$$

That σ is surjective we attain from Observation 10.77. To see that σ is injective (i.e., one-to-one) let $[a]_{mn}$ and $[b]_{mn}$ be distinct in $\mathbb{Z}_{mn}$, i.e., $a \not\equiv b \pmod{mn}$. If $\sigma([a]_{mn}) = \sigma([b]_{mn})$ then $([a]_n, [a]_m) = ([b]_n, [b]_m)$ implying that

$$\begin{aligned}
a &\equiv b \pmod{n} \\
a &\equiv b \pmod{m}
\end{aligned}$$

which in turn implies that $a \equiv b \pmod{mn}$, by Proposition 6.54, owing to m and n being co-prime; contradiction to the original assumption that $[a]_{mn} \neq [b]_{mn}$.

Inverting σ yields that for every $[r]_n \in \mathbb{Z}_n$ and for every $[s]_m \in \mathbb{Z}_m$ there is a *unique* $[x]_{mn} \in \mathbb{Z}_{mn}$ such that $\sigma([x]_{mn}) = ([r]_n, [s]_m)$. A number theoretic formulation of this last statement amounts to saying that for all $r, s \in \mathbb{Z}$ there exists an $x \in \mathbb{Z}$ such that

$$\begin{aligned}
x &\equiv r \pmod{n} \\
x &\equiv s \pmod{m};
\end{aligned}$$

moreover, such an x is unique modulo mn, as indeed σ is a bijection. This is the Chinese remainder theorem (see Theorem 6.64) stated for two equations.

A group theoretic formulation of the Chinese remainder theorem then modulo the uniqueness part reads as follows.

THEOREM 10.78 (Chinese remainder theorem; two equations)
Let m and n be co-prime. Then $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{mn}$. In particular $\mathbb{Z}_n \times \mathbb{Z}_m$ is cyclic.

The group theoretic formulation of the Chinese remainder theorem fitting for r equations arises then from Corollary 10.76.

10.4.3 *Automorphisms*

Let G be a group. An isomorphism of the form $G \to G$ is called an *automorphism*. Moreover, the set of all automorphisms of G, denoted $\mathrm{aut}G$ forms a group under composition.

EXAMPLE 10.79 Let G be an abelian group and let $\sigma : G \to G$ be given by $\sigma(g) := g^{-1}$. Then σ is an automorphism.

If G is a group and $a \in G$, define $\sigma_a : G \to G$ by $g \mapsto aga^{-1}$.

Proposition 10.80 *Let G be a group.*

1. *σ_a is an automorphism of G for every $a \in G$.*
2. *If $\vartheta : G \to \mathrm{aut}G$ is defined by $\vartheta(a) = \sigma_a$ for every $a \in G$, then ϑ is a homomorphism; i.e., $\sigma_{ab} = \sigma_a\sigma_b$ for all $a, b \in G$.*

Proof.

1. That σ_a is a bijection we leave to the reader to verify. That it is a homomorphism we see through
$$\sigma_a(g)\sigma_a(h) = aga^{-1} \cdot aha^{-1} = agha^{-1} = \sigma_a(gh)$$
whenever $g, h \in G$.
2. Fix $g \in G$. Then
$$\sigma_a\sigma_b(g) = \sigma_a(bgb^{-1}) = a(bgb^{-1})a^{-1} = (ab)g(ab)^{-1} = \sigma_{ab}(g).$$

■

This mapping σ_a is called the *inner automorphism* of G.

10.4.4 *Cayley's theorem*

We conclude this section with the so called *Cayley's theorem* asserting that every finite group is isomorphic to a group of permutations.

Theorem 10.81 (Cayley's theorem)
Every group of order n is isomorphic to a subgroup of S_n.

Prior to proving this result we require the following observation.

Observation 10.82. *Let X, Y be finite sets. If there is a bijection $X \to Y$ then $S_X \cong S_Y$. In particular, $S_X \cong S_n$ whenever $|X| = n$.*

Proof. Let $\sigma : X \to Y$ be a bijection. If $\lambda \in S_X$ then we have
$$Y \overset{\sigma^{-1}}{\to} X \overset{\lambda}{\to} X \overset{\sigma}{\to} Y.$$
That is, the composition $\sigma\lambda\sigma^{-1} : Y \to Y \in S_Y$. Then the mapping $\varphi : S_X \to S_Y$ given by $\varphi(\lambda) = \sigma\lambda\sigma^{-1}$ is an isomorphism. We leave all annoying verifications to the reader. ■

Proof of Theorem 10.81. Let G be a group of order n. By Observation 10.82, and while treating G as a set, there is an isomorphism $\vartheta : S_G \to S_n$. Then, if one can find a one-to-one homomorphism $\sigma : G \to S_G$ then $\vartheta\sigma$ is an isomorphism $G \to \vartheta\sigma(G)$. Then $G \cong \vartheta\sigma(G) \leq S_n$ and Cayley's theorem is established.

For $a \in G$, define $\mu_a : G \to G$ by $\mu_a(g) = ag$ for all $g \in G$. One may verify that μ_a is a bijection. As such, $\mu_a \in S_G$ holds. Define $\sigma : G \to S_G$ by setting $\sigma(a) = \mu_a$ for all $a \in G$. Then one may verify that σ is a homomorphism as $\mu_{ab} = \mu_a\mu_b$ for all $a, b \in G$. Moreover, one can also verify that σ is one-to-one as $\mu_a = \mu_b$ implies $a = \mu_a(e) = \mu_b(e) = b$. It follows that σ is a one-to-one homomorphism as required. ■

§10.5. Lagrange's theorem

Let H be a subgroup of a group G and let $a \in G$. We identify two subsets of G:

$$Ha := \{ha : h \in H\} \text{ and } aH := \{ah : h \in H\}$$

referred to as the *right coset of H generated by a* and the *left coset of H generated by a*. Trivially, $He = H = eH$ and $a \in Ha$ and $a \in aH$ always. If G is abelian these two subsets coincide. As the unity may not lie in a coset (left or right) neither are necessarily subgroups of G. The following asserts that the cosets of H partition G. We state the following for right cosets but the same holds for left ones as well.

Theorem 10.83 *let $H \leq G$ and let $a, b \in G$.*

1. *$H = He$.*
2. *$Ha = Hb$ if and only if $ab^{-1} \in H$.*
3. *$Ha = H$ if and only if $a \in H$.*
4. *If $a \in Hb$ then $Ha = Hb$.*
5. *Either $Ha = Hb$ or $Ha \cap Hb = \emptyset$.*
6. *The distinct right cosets of H form a partition of G.*

Proof.

1. Trivial.
2. If $Ha = Hb$ then $a \in Ha = Hb$ so that $a = hb$ for some $h \in H$. Hence $ab^{-1} = h \in H$. Conversely, if $ab^{-1} \in H$ then $ha = hab^{-1}b = h(ab^{-1})b \in Hb$ as $h(ab^{-1}) \in H$ owing to $ab^{-1} \in H$. This establishes that $Ha \subseteq Hb$. Noting that $ba^{-1} = (ab^{-1})^{-1} \in H$ as well then a similar argument establishes that $Hb \subseteq Ha$.
3. This is a special case of the second part of this theorem with b being the unity.
4. If $a \in Hb$ then we have seen that this implies that $ab^{-1} \in H$. By the second part of this theorem this implies that $Ha = Hb$.
5. Let $Ha \cap Hb$ be non-empty. We prove that $Ha = Hb$. Consider $x \in Ha \cap Hb$. Then $x \in Ha$ so $Hx = Hb$ by the fourth part of this theorem. In a similar manner $Hx = Hb$. The claim follows.
6. The fifth part of this theorem along with the fact that every element of G lies in some right coset of H yields the claim.

■

Two sets are said to have the same cardinality if there is a bijection from one to the other. In which case, let us write $|X| = |Y|$ even if the sets are infinite.

Proposition 10.84 *Let $H \leq G$.*

1. *$|aH| = |H| = |Ha|$ for every $a \in H$.*
2. *The map $Ha \mapsto a^{-1}H$ is a bijection $\{Ha : a \in G\} \to \{bH : b \in G\}$.*

PROOF.

1. The mapping $h \mapsto ah$ is a bijection $H \to aH$, hence $|H| = |aH|$.
2. We have that
$$Ha = Hb \iff ab^{-1} \in H \iff a^{-1} \in H \iff a^{-1}H = b^{-1}H.$$
so the mapping defined is indeed a bijection.

■

The second part of Proposition 10.84 asserts that the number of distinct right and distinct left cosets of H in G is the same (and possibly infinite). This common value is called the *index* of H in G and is denoted $|G : H|$. For finite groups this has a profound implication.

THEOREM 10.85 (Lagrange's theorem)
Let H be a subgroup of a finite group G. Then, $|H| \mid |G|$; in particular, $|G : H| = |G|/|H|$.

PROOF. Let $k := |G : H|$ and let $Ha_1, \ldots, Ha_k$ be the distinct right cosets of H in G. Then $G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k$ and $|H| = |Ha_i|$ for every $i \in [k]$. The claim follows. ■

Lagrange's theorem has several implications. As $\langle g \rangle \leq G$ for every $g \in G$ it follows now that $|\langle g \rangle| \mid |G|$ for every $g \in G$. We may rewrite this fact as follows.

COROLLARY 10.86 *If G is a finite group and $g \in G$ then the order of g divides $|G|$.*

We can now extend Corollary 10.36, known for finite cyclic groups, to all finite groups.

COROLLARY 10.87 *If G is a group of order n then $g^n = e$ for every $g \in G$.*

PROOF. Let m be the order of g. Then $m \mid n$, by Corollary 10.86. Then $m = qn$ so that $g^n = (g^m)^q = e$. ■

COROLLARY 10.88 *Every group G of prime order p is cyclic with its sole subgroups being G and $\{e\}$.*

PROOF. The sole non-triviality at this point in this claim is that G is cyclic. But this follows from the fact that all non-trivial subgroups of G coinciding with G and this holds for any $\langle a \rangle$, $a \in G$, as well. ■

COROLLARY 10.89 *Let $H, K \leq G$ with G a finite group If $(|H|, |K|) = 1$ then $H \cap K = \{1\}$.*

PROOF. As $H \cap K \leq H, K$ then $|H \cap K|$ divides both $|H|$ and $|K|$. As 1 is the sole common divisor of $|H|$ and $|K|$ it follows that $|H \cap K| = 1$. ■

COROLLARY 10.90 *Let $K \leq H \leq G$ be finite groups. If $|G : K|$ is prime then $H = K$ or $H = G$.*

PROOF. Start by noticing that $|G : H| \cdot |H : K| = \frac{|G|}{|H|}\frac{|H|}{|K|} = \frac{|G|}{|K|} = |G : K|$. As $|G : K|$ is prime then either $|G : H| = 1$ of $|H : K| = 1$ and the claim follows. ■

We conclude this section with an exceedingly short proof of Euler's theorem stated in Theorem 8.15 asserting that if $n \geq 2$ and $(a, n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

PROOF OF THEOREM 8.15. Given a as in the theorem we have that $\overline{a} \in \mathbb{Z}_n^*$. As $|\mathbb{Z}_n^*| = \varphi(n)$ it follows, by Corollary 10.87, that $\overline{a}^{\varphi(n)} = \overline{1}$ establishing Euler's theorem. ■

§10.6. On the cyclicity of $\mathbb{Z}_p^*$

The main result of this section reads as follows.

Theorem 10.91 *$\mathbb{Z}_p^*$ is cyclic for every prime p. Moreover, it has $\varphi(p-1)$ generators.*

Let us be reminded that a function of the form

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

is called a *polynomial*. For a polynomial $f(x)$ with integral coefficients, an integer c is said to be a *root of $f(x)$ modulo m* if $f(c) \equiv 0 \pmod{m}$. Clearly, if c is a root of $f(x)$ modulo then so is every member of $[c]_m$. For primes p, for instance, Fermat's little theorem, namely Theorem 7.10, asserts that the polynomial $x^{p-1} - 1$ has exactly $p-1$ incongruent roots modulo p. This is a special case of Theorem 8.5. We use the latter in order to deliver the following.

Proposition 10.92 *Let p be prime and let d satisfy $d \mid p-1$. Then, the polynomial $x^d - 1$ has exactly d incongruent roots modulo p.*

Proof. Write $p - 1 = de$. Then,

$$\begin{aligned} x^{p-1} - 1 &= (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1) \\ &= (x^d - 1)g(x). \end{aligned}$$

By Fermat's little theorem, namely Theorem 7.10, $x^{p-1} - 1$ has $p-1$ incongruent roots modulo p. Moreover, any root of $x^{p-1} - 1$ modulo p is either a root of $x^d - 1$ modulo p or a root of $g(x)$ modulo p.

Lagrange's theorem, namely Theorem 8.5, asserts that $g(x)$ has at most $d(e-1) = p - d - 1$ roots modulo p. Every root of $x^{p-1} - 1$ that is not a root of $g(x)$ must then be a root of $x^d - 1$; by now we know there are at least $(p-1) - (p-d-1) = d$ of those. Lagrange's theorem, namely Theorem 8.5 asserts that there can be no more than d. It follows that $x^d - 1$ has precisely d roots. ■

We now relate our knowledge of roots of polynomials modulo a prime to $\mathbb{Z}_p^*$.

Lemma 10.93 *Let p be a prime and let d be a positive divisor of $p-1$. Then, the number of elements in $\mathbb{Z}_p^*$ having order d is at most $\varphi(d)$. Moreover, if there is an element $a \in \mathbb{Z}_p^*$ of order d, then there are $\varphi(d)$ such elements; all residing in $\langle a \rangle$.*

Proof. For a positive divisor d of $p-1$, set

$$F(d) := \{x \in \mathbb{Z}_p^* : \text{ order of } x \text{ is } d\}.$$

If $|F(d)| = 0$, then trivially $|F(d)| \leq \varphi(d)$. Otherwise, there is an element $a \in \mathbb{Z}_p^*$ of order d. Then, each of the members of $\langle a \rangle := \{a, a^2, \ldots, a^d = 1\}$ is a root of the polynomial $x^d - 1$ modulo p (as indeed a is[1]). Proposition 10.92 asserts that the members of $\langle a \rangle$ in fact constitute all of the roots of this polynomial modulo p. This then implies that $F(d) \subseteq \langle a \rangle$.

It remains to argue as to the quantity of order d elements. By Lemma 10.46, the powers of a of the form a^k that have order d are precisely those satisfying $(k, d) = 1$. This establishes that $|F(d)| \leq \varphi(d)$, and in fact that equality holds if a exists. ■

We can refine Lemma 10.93 even further.

[1] Alternatively, just note that $(a^k)^d \equiv (a^d)^k \equiv 1 \pmod{p}$.

Proposition 10.94 *Let p be a prime and let d be a positive divisor of $p-1$. Then the number of elements of $\mathbb{Z}_p^*$ of order d is precisely $\varphi(d)$.*

Proof. For a positive divisor d of p, let $F(d)$ be as above. By Corollary 10.86, the order of any element in $\mathbb{Z}_p^*$ must divide $|\mathbb{Z}_p^*|$. This, in particular, implies that

$$\mathbb{Z}_p^* = \bigcup_{d \mid p-1} F(d).$$

The sets $\{F(d) : d \mid p-1\}$ are disjoint so, that

$$\mathbb{Z}_p^* = \dot{\bigcup_{d \mid p-1}} F(d)$$

in fact holds; i.e., we have a partition of the group. We may rewrite this as

$$p-1 = \sum_{d \mid p-1} |F(d)|.$$

We couple this with Theorem 7.58 asserting that

$$p-1 = \sum_{d \mid p-1} \varphi(d);$$

as well as with Lemma 10.93 asserting that $|F(d)| \leq \varphi(d)$ and derive that $|F(d)| = \varphi(d)$ whenever $d \mid p-1$. The claim now follows. ■

We are now ready to prove the main result of this section.

Proof of Theorem 10.91. Let p be prime. Proposition 10.94 asserts that $\mathbb{Z}_p^*$ has $\varphi(p-1) \geq 1$ elements of order $p-1$ which are generators of the group. ■

Conjecture 10.95 (Artin)

The integer a is a primitive root of infinitely many primes whenever $a \neq \pm 1$ and a is not a perfect square.

10.6.1 *The Korselt criterion*

We recall that a composite integer n satisfying $a^n \equiv a \pmod{n}$ is called a Carmichael number. In Theorem 7.33 we proved that every composite square-free number n having the property that each of its factors p satisfies $p-1 \mid n-1$ is Carmichael. This is, in fact, a characterisation.

Theorem 10.96 (Korselt criterion)
An integer n is a Carmichael number if and only if $n = q_1 \cdot q_2 \cdots q_k$ is a product of distinct primes such that

$$(q_j - 1) \mid (n-1) \; \forall j \in [k]$$

Proof. In view of Theorem 7.33, it suffices to prove that any Carmichael number has the stipulated form. Let n be Carmichael, and let p be a factor of n. Then, $p^n \equiv p \pmod{n}$, by definition, yielding $n \mid p^n - p$. Then $p^2 \nmid n$ for if so then $p^2 \mid p^n - p$ leading to $p \mid p^{n-1} - 1$ which is impossible. It follows that n is square-free. To verify the second property, let a be a generator of $\mathbb{Z}_p^*$; such an a exists by Theorem 10.91. By the definition of n we have that $a^n \equiv a \pmod{n}$, then $a^n \equiv a \pmod{p}$, by the first part of Proposition 6.54 applied to n and its square-free factorisation. Then $a^{n-1} \equiv 1 \pmod{p}$. The order of a in $\mathbb{Z}_p^*$ is $p-1$; the latter then divides $n-1$, by the first part of Theorem 10.35. ■

We can refine Theorem 10.96 further still and insist on all factors being odd primes.

Observation 10.97. *Carmichael numbers are odd.*

Proof. Let n be Carmichael. We may assume $n \geq 4$ as none of $1, 2, 3$ is Carmichael. Assume n is even. Then,

$$(n-1)^{n-1} \equiv (-1)^{n-1} \equiv -1 \pmod{n}.$$

As $(n-1, n) = 1$, it follows that n fails the condition of Fermat's little theorem (namely Theorem 7.10). ■

We can deduce further information from Theorem 10.96 regarding the factorisation of Carmichael numbers.

Corollary 10.98 *A Carmichael number must have at least three distinct odd prime factors.*

Proof. As n is composite and square-free it cannot have a single factor and thus cannot be a prime power. It must have at least two distinct prime factors; by Observation 10.97 we may assume these are also odd. So assume that $n = pq$ for some two primes p and q s.t. $p > q$. Then,

$$n - 1 = pq - 1 = (p-1)q + (q-1) \equiv q - 1 \pmod{p-1}.$$

Note also that $q - 1 \not\equiv 0 \pmod{p-1}$ for indeed $p - 1 > q - 1$ so $p - 1 \mid q - 1$ is impossible. It follows that $n - 1 \not\equiv 0 \pmod{p-1}$; implying that $p - 1 \nmid n - 1$. Hence, n is not Carmichael, by Theorem 10.96; a contradiction. ■

§10.7. Normal subgroups

§10.8. Quotient subgroups

§10.9. The isomorphism theorems

Lecture 11

Fields

Lecture 12

Polynomials

Part IV

Computational number theory

Lecture 13

Primality testing

Lecture 14

Discrete logarithms

Lecture 15

Algebraic algorithms

Part V

Analytic number theory

Lecture 16

Arithmetic functions

Early estimates for the primes

§17.1. Euler's proof for the infinitude of primes

By (a real) *power series* we mean a (real) function of the form

$$x \mapsto \sum_{n=0}^{\infty} a_n (x-c)^n$$

where $c \in \mathbb{R}$ as well as all the coefficients (a_n). A specific power series called the *Taylor series* is of special interest to us. For function $f : \mathbb{R} \to \mathbb{R}$ and $a \in \mathbb{R}$ we write $f^{(n)}(a)$ to denote its nth derivative at point a. With this notation $f(a) = f^{(0)}(a)$. A function f is said to be *infinitely derivable* at $a \in \mathbb{R}$ if $f^{(n)}(a)$ exists for every $n \in \mathbb{N}$.

Definition 17.1 *The Taylor series of an infinitely derivable at function $f : \mathbb{R} \to \mathbb{R}$ a point $a \in \mathbb{R}$ is the given by*

$$\sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)^n = \\ f(a) + \frac{f^{(1)}(a)}{1!}(x-a) + \frac{f^{(2)}(a)}{2!}(x-a)^2 + \frac{f^{(3)}(a)}{3!}(x-a)^3 + \cdots$$

When $a = 0$ the series is called a Maclaurin series. *We write $T(f;a)(x)$ to denote the Taylor series of f about a.*

Infinitely derivable functions f satisfying $f(x) = T(f;a)(x)$ for each point a in their domain are called *analytic functions*. A cornerstone result in calculus is that of Taylor asserting that subject to certain conditions one can approximate a function using its Taylor series.

Theorem 17.2 (Taylor's theorem in one real variable - abridged)
Let $k \geq 1$ be an integer an let $f : \mathbb{R} \to \mathbb{R}$ be k times derivable at $a \in \mathbb{R}$. Then

$$f(x) = \sum_{n=0}^{k} \frac{f^{(n)}(a)}{n!}(x-a)^n + o(x^k).$$

We should remark that the term $o(x^k)$ here is slightly different than the one in Definition **??**. Here by $o(x^k)$ we mean a function going to 0 as x tends to a.

It is through results like these that we have the following well known expansions:

1. Let $-1 < x < 1$. Then

$$(1-x)^{-1} = \sum_{n=0}^{\infty} x^n = 1 + x + x^2 + x^3 + \cdots .$$

2. For the exponential function

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots . \tag{17.3}$$

For a prime p then we may than write

$$\frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots \tag{17.4}$$

and for any fixed integer K then

$$\frac{1}{1-\frac{1}{p}} \geq 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots \frac{1}{p^K} \tag{17.5}$$

We are now in position to provide Euler's analytic proof for the infinitude of primes.

Proof of Theorem 5.23-Euler's proof. Assume for the sake of contradiction that there are only finitely many primes, namely $2 = p_1, \ldots, p_r$. Set

$$X := \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right)^{-1}.$$

Then, by (17.5), for any fixed $K > 0$,

$$\begin{aligned} X \geq & \left(1 + \frac{1}{2} + \cdots + \frac{1}{2^K}\right) \cdot \\ & \left(1 + \frac{1}{3} + \cdots + \frac{1}{3^K}\right) \cdot \\ & \left(1 + \frac{1}{5} + \cdots + \frac{1}{5^K}\right) \cdot \\ & \cdots\cdots\cdots\cdots\cdots\cdots \\ & \left(1 + \frac{1}{p_r} + \cdots + \frac{1}{p_r^K}\right) \\ = & \sum_{n \in \mathcal{N}(K)} \frac{1}{n}. \end{aligned}$$

where

$$\mathcal{N}(K) := \left\{ n \in \mathbb{N} : n = p_1^{e_1} \cdots p_r^{e_r},\ e_i \leq K,\ \forall i \in [r] \right\}.$$

Having $X \geq \sum_{n \in \mathcal{N}(K)} \frac{1}{n}$ for every $K \in \mathbb{N}$ implies $X \geq \sum_{n=1}^{M} \frac{1}{n}$ for every $M \in \mathbb{N}$. Indeed, given $M \in \mathbb{N}$ there exists a $K = K(M)$ such that $\{1, \ldots M\} \subseteq \mathcal{N}(K)$. The series $\left(\sum_{n=1}^{M} \frac{1}{n}\right)$ is the Harmonic series and is known to diverge (see practical sessions). We attain a contradiction to the assumption that X is a fixed number. ■

Let us linger a tad more on an idea emanating from Euler's proof. Fix $N \in \mathbb{N}$ and set

$$\mathfrak{N}(N) := \left\{ n \in \mathbb{Z} : \text{ all factor of } n \ \leq N \right\}. \tag{17.6}$$

Then

$$\prod_{p\le N}(1-p^{-1})^{-1} = \prod_{p\le N}\left(1+p^{-1}+p^{-2}+p^{-3}+\cdots\right)$$
$$= \sum_{n\in\mathfrak{N}(N)}\frac{1}{n}. \tag{17.7}$$

§17.2. $\sum \frac{1}{p}$ DIVERGES

We write $\sum_p$ to denote the sum ranging over all primes. For $x\in\mathbb{R}$ we write $\sum_{p\le x}$ to denote a sum ranging over all primes not exceeding x, and write $\sum_{p\ge x}$ to denote a sum of the primes at least x.

In this section, we consider the series of reciprocals of the primes, namely $\sum_p \frac{1}{p}$. If there are finitely many primes in $\mathbb{Z}$, then surely $\sum_p \frac{1}{p}\le M<\infty$ for some $M\in\mathbb{N}$. If so the sequence $\left(\sum_{p\le N}\frac{1}{p}\right)_{N\in\mathbb{N}}$ is bounded and monotonically increasing and thus convergent by the monotone convergence theorem . Hence, proving that the series $\sum_p \frac{1}{p}$ diverges would imply the infinitude of primes. This is the goal of this section.

The divergence of $\sum_p \frac{1}{p}$ goes beyond the infinitude of primes. For indeed, if this is all one seeks to prove using the reciprocals of primes the following modest argument can be offered.

Proof of Theorem 5.23. Suppose that $p_1,\ldots,p_n$ consist of all primes, and set $N:=\prod_i p_i$. Set

$$a=\sum_{i=1}^{n}\frac{1}{p_i}$$

and then

$$aN=\sum_{i=1}^{n}\frac{N}{p_i};$$

holds. Moreover, aN is a positive integer; as such it has a prime factor (we may assume $aN>1$ of course) which must be p_j for some $j\in[n]$. Then, $p_j\mid aN$ and also $p_j\mid \frac{N}{p_i}$ for every $i\in[n]\setminus\{j\}$. Then

$$p\mid aN=\sum_{i\ne j}\frac{N}{p_i}+\frac{N}{p_j} \text{ and } p\mid \sum_{i\ne j}\frac{N}{p_i}.$$

Then, $p_j\mid \frac{N}{p_j}$, by Lemma 4.40, which is a contradiction. ■

We return to the main result of this section.

Theorem 17.8 *The series $\sum\frac{1}{p}$ diverges.*

Proof. Suppose the series $\sum_p 1/p$ is convergent which in particular means $\sum_p\frac{1}{p}\le M<\infty$ for some $M\in\mathbb{N}$. This upper bound on the whole sum together with the fact that the sequence $\left(\sum_{p<n}\frac{1}{p}\right)_{n\in\mathbb{N}}$ is ever increasing implies that the sequence of tails $\left(\sum_{p\ge n}\frac{1}{p}\right)_{n\in\mathbb{N}}$ is ever decreasing. Hence there exists an integer j for which

$$\frac{1}{p_{j+1}}+\frac{1}{p_{j+2}}+\cdots<\frac{1}{2} \tag{17.9}$$

holds. We show that this implies that the set $\mathbb{N}$ is finite.

For let us consider an arbitrary integer x and observe the quantity $x-|N(x,j)|$ for it. The $x-|N(x,j)|$ quantity denotes the number of integers n not exceeding x that are divisible by at least one of the primes $p_{j+1}, p_{j+2}, \ldots$. The number of integers n not exceeding x divisible by an arbitrary prime p surely does not exceed x/p. Hence,

$$x - |N(x,j)| \leq \frac{x}{p_{j+1}} + \frac{x}{p_{j+2}} + \cdots = x\left(\frac{1}{p_{j+1}} + \frac{1}{p_{j+2}} + \cdots\right) \overset{(17.9)}{<} \frac{x}{2}.$$

Rearranging we arrive at

$$x/2 < |N(x,j)| \leq 2^j\sqrt{x},$$

where the upper bound is owing to Lemma 5.26. This in turn implies $x < 2^{2j+2}$. As x is arbitrary we have just proved that all natural numbers do not exceed 2^{2j+2}; this is clearly false as the number $2^{2j+2}+1$ surely shows. ■

17.2.1 $\sum_p \frac{1}{p}$ diverges: a proof via the Harmonic series

Theorem 17.8 is a fundamental result in number theory. As such it has many proofs in the literature. We consider two additional proofs.

Proof of Theorem 17.8. For suppose the series converges; then for some N we have

$$\sum_{p>N} \frac{1}{p} < \frac{1}{2} \tag{17.10}$$

(this is simply a reiteration of (17.9) see explanation there). Set $Q := \prod_{p\leq N} p$ and note that for every $n \in \mathbb{N}$

$$p \not| 1 + nQ, \text{ for every prime } p \leq N. \tag{17.11}$$

(for if such a p were to divide $1+nQ$ then $p \mid (Qn+1-Q) = 1$).

$$\sum_{t=1}^{\infty}\left(\sum_{p>N}\frac{1}{p}\right)^t \overset{(17.10)}{<} \sum_{t=1}^{\infty}\frac{1}{2^t} \overset{(??)}{\leq} 2.$$

Owing to (17.11) we have,

$$\sum_{n=1}^{\infty}\frac{1}{1+nQ} \leq \sum_{t=1}^{\infty}\left(\sum_{p>N}\frac{1}{p}\right)^t.$$

This as each term on the left-hand side appears at least once on the right hand side. To see this fix $1+nQ$ for some $n \in \mathbb{N}$. All its factors are $> N$ by (17.11). For t sufficiently large we can form the prime-power factorisation of $1+nQ$ on the right hand side. Then

$$\sum_{n=1}^{\infty}\frac{1}{1+nQ} \leq 2.$$

On the other hand, for every $K \in \mathbb{N}$

$$\sum_{n=1}^{K}\frac{1}{1+nQ} \geq \sum_{n=1}^{K}\frac{1}{2nQ} = \frac{1}{2Q}\sum_{n=1}^{K}\frac{1}{n}.$$

The sequence $\left(\sum_{n=1}^{K}\frac{1}{n}\right)_{K\in\mathbb{N}}$ is the Harmonic series which diverges (see Example **??**); we reached a contradiction. ■

17.2.2 $\sum_{p\le N}\frac{1}{p}=\Omega(\log\log N)$

Our last proof of Theorem 17.8 establishes a stronger result; in that it provides a lower bound on the rate in which the series $\sum 1/p$ diverges. In particular we shall see in this section that $\sum 1/p$ goes to infinity at least as fast as $\log\log n$; (note that $\ln\ln n\le 10$ for all $n\le 10^{9565}$ so this function although it does go to infinity it does so very slowly. In § **??** we have seen that for $N\in\mathbb{N}$

$$\ln(N+1)\le\sum_{n=1}^{N}\frac{1}{n}\le 1+\ln N,$$

holds. In particular we have

$$\ln N\le\sum_{n=1}^{N}\frac{1}{n}. \tag{17.12}$$

The reciprocals of the primes are all captured by the interval $[0,1/2]$. Above we have frequently encountered terms of the form $(1-p^{-1})^{-1}$. It makes sense to have an upper bound for such terms.

Lemma 17.13 *For any $v\in[0,1/2]$*

$$(1-v)^{-1}\le e^{v+v^2}. \tag{17.14}$$

Proof. Set $f(v):=(1-v)e^{v+v^2}$. Then $f'(v)=v(1-2v)e^{v+v^2}\ge 0$ for all $v\in[0,1/2]$. This coupled with the fact that $f(0)=1$ implies that $f(v)\ge 1$ for all $v\in[0,1/2]$. ■

Theorem 17.15 *Let K be an integer. Then*

$$\sum_{p\le K}\frac{1}{p}=\Omega(\log\log K).$$

Proof. Fix $N\in\mathbb{N}$. Recall $\mathfrak{N}(N)$ from (17.6). Then

$$\begin{aligned}\ln N &\overset{(17.12)}{\le}\sum_{n\le N}\frac{1}{n}\le\sum_{n\in\mathfrak{N}(N)}\frac{1}{n}\overset{(17.7)}{=}\prod_{p\le N}(1-p^{-1})^{-1}\\ &\overset{(17.14)}{\le}\prod_{p\le N}e^{p^{-1}+p^{-2}}.\end{aligned}$$

Taking ln on both sides yields

$$\ln\ln N\le\ln\left(\prod_{p\le N}e^{p^{-1}+p^{-2}}\right)=\sum_{p\le N}\ln\left(e^{p^{-1}+p^{-2}}\right)=\sum_{p\le N}\left(p^{-1}+p^{-2}\right)$$

Write

$$\ln\ln n\le\sum_{p\le N}\frac{1}{p}+\sum_{p\le N}\frac{1}{p^2}.$$

For the second sum on the right hand side we have

$$\sum_{p\le N}\frac{1}{p^2}\le\sum_{p\le\mathbb{Z}}\frac{1}{p^2}\le\sum_{n=1}^{\infty}\frac{1}{n^2}\overset{(??)}{\le}2$$

that is we have bounded the contribution of $\sum_{p\le N}\frac{1}{p^2}$ by a constant (independent of N). The claim now follows. ■

One may observe that our proof of Theorem 17.15 establishes much more than $\sum_{p\le N} 1/p = \Omega(\log\log N)$; indeed it establishes that $\sum_{p\le N} 1/p \ge \ln\ln N - 2$. A well known result by Mertens asserts that the upper bound for this sum is not far off.

Theorem 17.16 (Mertens' theorem)

$$\sum_{p\le N}\frac{1}{p} = \log\log N + O(1)$$

§17.3. Tchebyshev's theorem: $\pi(x) = O(x\log x)$

A landmark result then is the so called *prime number theorem*.

Theorem 17.17 (The prime number theorem)

$$\pi(x) \sim \frac{x}{\log x}.$$

Put another way, the prime number theorem asserts that $p_n \sim n\log n$. Compare this with the estimates we had so far for p_n. In fact it is known that the so called *logarithmic integral* given by

$$\mathrm{li}(x) = \int_2^x \frac{\mathrm{d}\,t}{\log t} = x/\log x + O\left(x/(\log x)^2\right)$$

approximates $\pi(x)$ better than $x/\log x$. To date the best known approximation for $\pi(x)$ is

$$\pi(x) = \mathrm{li}(x) + O(xe^{-c\kappa(x)})$$

where c is some absolute constant and $\kappa(x) := (\log x)^{3/5}\cdot(\log\log x)^{-1/5}$.

Conjecture 17.18

For $x \ge 2.01$

$$\left|\pi(x) - \mathrm{li}(x)\right| < \sqrt{x}\log x$$

holds.

Proofs of any of these results lie beyond the scope of these notes. As a substitute we focus on the following earlier result by Tchebyshev.

Theorem 17.19 (Tchebyshev's theorem)

$$\pi(x) \asymp \frac{x}{\log x}.$$

We only prove the upper bound in Tchebyshev's theorem. The lower bound is delegated to exercises.

Proposition 17.20

$$\pi(x) = O(x/\log x).$$

A close "relative" of $\pi(x)$ is the so called *Tchebyshev function* given by

$$\vartheta(x) = \sum_{p \leq x} \log p$$

for all $x \in \mathbb{R}$. A motivation for considering $\vartheta(x)$ is delivered by the fact

$$\vartheta(x) = \Theta(\pi(x) \log x) \tag{17.21}$$

proof of which is delegated to exercises. Through (17.21) we see how estimates for $\vartheta(x)$ translate to estimates for $\pi(x)$. In particular, owing to (17.21) the following then implies Proposition 17.20.

Lemma 17.22

$$\vartheta(x) = O(x).$$

Proof. Let us first study a property of $\vartheta(x)$; in particular its behaviour over powers of 2. To that end let us fix $n \in \mathbb{N}$ and observe

$$N := \binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \frac{(n+1) \cdot (n+2) \cdots 2n}{1 \cdot 2 \cdots n}.$$

By the binomial theorem $N \leq 2^{2n}$. It is easily seen that all prime factors of N are $< 2n$. In particular $p \mid \binom{2n}{n}$ for every prime $n < p < 2n$. Then

$$\prod_{p>n}^{p<2n} p \leq N < 2^{2n}.$$

Taking log on both sides yields

$$2n = 2n \log 2 > \log \left(\prod_{p>n}^{p<2n} p \right) = \sum_{p>n}^{p<2n} \log p = \vartheta(2n) - \vartheta(n). \tag{17.23}$$

We use (17.23) to make the following observation. Fix $0 < m \in \mathbb{N}$. Then

$$\begin{aligned} \vartheta(2^m) &< \vartheta(2^{m-1}) + 2^m \\ &< \vartheta(2^{m-2}) + 2^{m-1} + 2^m \\ &< \vartheta(2^{m-3}) + 2^{m-2} + 2^{m-1} + 2^m \\ &< \dots . \end{aligned}$$

Continuing (inductively[1]) in this fashion leads to

$$\vartheta(2^m) \leq \sum_{i=1}^{m} 2^i \overset{(2.20)}{\leq} 2^{m+1}. \tag{17.24}$$

With the behaviour of $\vartheta(x)$ over powers of 2 understood we proceed now with the asymptotic analysis of $\vartheta(x)$. We partition $\mathbb{R}$ into intervals of the form $[2^{m-1}, 2^m]$ for $1 \leq m \in \mathbb{N}$ and show that whenever

[1] We leave the tedious details of this to the reader.

$x \in (2^{m-1}, 2^m]$ then $\vartheta(x) \leq Cx$ where C is a constant independent of m. To see this fix $0 < m \in \mathbb{N}$ and fix $2^{m-1} \leq x \leq 2^m$. Then

$$\vartheta(x) \leq \vartheta(2^m) \overset{(17.24)}{\leq} 2^{m+1} = 4 \cdot 2^{m-1} \leq 4x.$$

As 4 is independent of m (as promised for C above) the claim follows. ■

For future reference let us record here that we have in fact proved

$$\vartheta(x) \leq 4x \tag{17.25}$$

for $x \in \mathbb{R}$ sufficiently large. In fact one can prove

$$\vartheta(x) \leq 2x; \tag{17.26}$$

this is delegated to the exercises.

§17.4. Bertrand's postulate

(for n sufficiently large)

In this section we prove Theorem 5.49 for n sufficiently large. That is we prove Theorem 17.37 stated below.

17.4.1 *The* $\mathrm{ord}_p(\cdot)$ *function*

Definition 17.27 *For a prime p we define the function $\mathrm{ord}_p : \mathbb{Z}^+ \to \mathbb{N}$ given by $\mathrm{ord}_p(n) := t$ if $n = p^t m$ and $n \not| m$.*

The definition given here for $\mathrm{ord}_p(\cdots)$ is somewhat enigmatic. Suppose $n = 5^5$, say. Then we may write $n = 5^4 \cdot 5 = 5^3 \cdot 5^2$ and surely $5^5 \not| 5^3$ and $5^5 \not| 5^2$. The definition above however states $\mathrm{ord}_5(5^5) = 5$. A more revealing way to define $\mathrm{ord}_p(\cdot)$ then is the following.

Definition 17.28 *Let p be a prime. For $n \in \mathbb{Z}^+$ we let $\mathrm{ord}_p(n)$ denote the largest integer t such that $p^t \mid n$ yet $p^{t+1} \not| n$.*

We thus refer to $\mathrm{ord}_p(n)$ as the *order of n at p*. With this understood we may write the factorisation of any $n \in \mathbb{Z}$ as

$$n = \pm \prod_p p^{\mathrm{ord}_p(n)}$$

where $\prod_p$ denotes a product over all primes. It will be convenient to extend the definition of ord_p to include 0 by setting $\mathrm{ord}_p(0) = \infty$ for every p. Notice that $\mathrm{ord}_p(n) = 0$ if and only if $p \not| n$.

The function $\mathrm{ord}_p(\cdot)$ admits several pleasant properties. For a, b non-zero integers,

$$\mathrm{ord}_p(a \cdot b) = \mathrm{ord}_p(a) + \mathrm{ord}_p(b) \tag{17.29}$$

holds for every prime p. If $a/b \in \mathbb{Z}$ then

$$\mathrm{ord}_p(a/b) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b) \tag{17.30}$$

holds for every prime p. Through (17.29) and (17.30) we see that $\mathrm{ord}_p(\cdot)$ has properties seen in the logarithmic function. In addition,

$$a \mid b \iff \mathrm{ord}_p(a) \leq \mathrm{ord}_p(b), \text{ for all primes } p. \tag{17.31}$$

We may use (17.31) to rewrite (5.16) as

$$(a, b) = \prod_p p^{\min(\mathrm{ord}_p(a), \mathrm{ord}_p(b))}.$$

17.4.2 Proof of Bertrand's postulate

Prior to doing so let us reconsider

$$N := \binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \frac{(n+1)\cdot(n+2)\cdots 2n}{1\cdot 2\cdots n}$$

for $n \geq 1$ yet again. To prove Lemma 17.22 we used the estimations

$$\prod_{p>n}^{p<2n} p \leq N \leq 2^2 n.$$

To prove Theorem 17.37 our starting point is a different set of estimations for N which we now develop.

N is the largest binomial coefficient amongst $\{\binom{2n}{k} : 0 \leq 2n\}$ and as such we have pleasant lower and upper bounds for it.

$$\frac{2^{2n}}{2n+1} \leq N \leq 2^{2n}.$$

In fact we can write

$$2^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} = 1 + \sum_{k=1}^{2n-1} \binom{2n}{k} + 1 \leq 2 + (2n-1)N \leq 2nN$$

so that

$$2^{2n}/2n \leq N$$

in fact holds improving the naive lower bound $\frac{2^{2n}}{2n+1} \leq N$ arising from simple averaging. As mentioned once already, the prime factors of N are all $< 2n$. In particular

$$N \leq \prod_{p<2n} p^{\mathrm{ord}_p(N)}$$

holds Combining this upper bound with the lower bound just seen for N yields

$$\log\left(\frac{2^{2n}}{2n}\right) \leq \log\left(\prod_{p<2n} p^{\mathrm{ord}_p(N)}\right).$$

Properties of the logarithmic function then give

$$2n\underbrace{\log 2}_{=1} - \log 2n \leq \sum_{p<2n} \mathrm{ord}_p(N)\log p;$$

so that

$$2n < \sum_{p<2n} \mathrm{ord}_p(N)\log p + \log 2n. \tag{17.32}$$

The fact that $\log 2n = o(n)$ shifts the interest towards estimations of $\sum_{p<2n} \mathrm{ord}_p(N)\log p$ which in turn prompts questions regarding estimations for the quantity $\mathrm{ord}_p(N)$. A key result (established in Exercise 7) relating to this quantity is that

$$\mathrm{ord}_p(N) \leq \frac{\log 2n}{\log p}. \tag{17.33}$$

Example 17.34 One way to use (17.33) is to attain estimations for sums of the form

$$\sum_{\substack{p<2n:\\ \mathrm{ord}_p(N)\geq k}} \mathrm{ord}_p(N)\log p$$

for some given constant k. Primes p with $\mathrm{ord}_p(N)\geq k$ satisfy

$$k\log p \leq \mathrm{ord}_p(N)\log p \leq \frac{\log 2n}{\log p}\log p = \log 2n.$$

That is such primes p satisfy

$$p^k \leq 2n.$$

Put another way the primes p with $\mathrm{ord}_p(N)\geq k$ must satisfy $p\leq (2n)^{1/k}$. That is there are not "so many" of them. In particular this means that

$$\sum_{\substack{p<2n:\\ \mathrm{ord}_p(N)\geq k}} \mathrm{ord}_p(N)\log p \leq (2n)^{1/k}\log 2n. \tag{17.35}$$

Returning to (17.32), we note that already for $k\geq 2$, say, $(2n)^{1/k}\log 2n = o(n)$ so that (17.32) can be further decomposed into

$$\begin{aligned} 2n &< \sum_{\substack{p<2n:\\ \mathrm{ord}_p(N)<k}} \log p + \sum_{\substack{p<2n:\\ \mathrm{ord}_p(N)\geq k}} \mathrm{ord}_p(N)\log p + \log 2n. \\ &\leq \sum_{\substack{p<2n:\\ \mathrm{ord}_p(N)<k}} \log p + \underbrace{(2n)^{1/k}\log 2n}_{o(n)} + \underbrace{\log 2n}_{o(n)}. \end{aligned} \tag{17.36}$$

We now put the above understandings to work by proving the following result.

Theorem 17.37 *Let n be sufficiently large. Then there exists a prime number p satisfying*

$$n < p \leq 2n. \tag{17.38}$$

Proof. Assume for the sake of contradiction that (17.38) does not hold for some n sufficiently large and set $N := \binom{2n}{n}$. Then

$$\begin{aligned} 2n &\overset{(17.32)}{<} \sum_{p<2n} \mathrm{ord}_p(N)\log p + \log 2n \\ &= \sum_{\substack{p:\\ \mathrm{ord}_p(N)=1}} \log p + \sum_{\substack{p:\\ \mathrm{ord}_p(N)\geq 2}} \mathrm{ord}_p(N)\log p + \log 2n \\ &\overset{(17.35)}{\leq} \sum_{p|N} \log p + (\sqrt{2n}+1)\log 2n \end{aligned}$$

To attain a contradiction it suffices to prove

$$\sum_{p|N} \log p \leq \frac{4}{3}n; \tag{17.39}$$

for indeed proving so implies that

$$2n < 4n/3 + (\sqrt{2n} + 1)\log 2n$$

which is false for n sufficiently large. To prove (17.39) suffice to show

$$N \text{ has no prime factors } p \text{ satisfying } \frac{2}{3}n < p \leq n. \tag{17.40}$$

Indeed, (17.40) implies that

$$\sum_{p|N} \log p \leq \sum_{p \leq \frac{2}{3}n} \log p = \vartheta(2n/3) \overset{(17.26)}{\leq} \frac{4}{3}n.$$

Using the assumption that the assertion fails for n we prove (17.40). This we do by showing that $\mathrm{ord}_p(N) = 0$ for every prime $2n/3 < p \leq n$. All prime factors of N are $\leq 2n$; however the additional assumption that (17.38) fails for n implies that all factors of N are $\leq n$. In the practical sessions we prove that

$$\mathrm{ord}_p(N) = \sum_{k \geq 1} \left(\left\lfloor \frac{2m}{p^k} \right\rfloor - 2 \left\lfloor \frac{m}{p^k} \right\rfloor \right). \tag{17.41}$$

Prior to analysing this sum let us observe a couple of bounds for primes p satisfying $2n/3 < p \leq n$ which will be useful for us in the sequel. In particular that

$$2p \leq 2n < 3p \text{ and } p^2 > \frac{4}{9}n^2 > 2n$$

where the last inequality is owing to n being sufficiently large. To evaluate $\mathrm{ord}_p(N)$ we consider the summands of (17.41); we analyse each term in a summand.

1. Consider the term $\left\lfloor \frac{2n}{p^k} \right\rfloor$ in a single summand. For $k = 1$ the assumption $\frac{2}{3}n < p \leq n$ yields

$$2 = \frac{2n}{n} \leq \frac{2n}{p} < \frac{2n}{\frac{2}{3}n} = 3$$

   so that $\left\lfloor \frac{2n}{p} \right\rfloor = 2$. The inequality $p^2 > 2n$ yields $\left\lfloor \frac{2n}{p^k} \right\rfloor = 0$ for every $k > 1$.

2. Consider the term $2\left\lfloor \frac{n}{p^k} \right\rfloor$ in a single summand. For $k > 1$ this term is zero (again by $p^2 > 2n$). For $k = 1$ the assumption of the car that $\frac{2}{3}n < p \leq n$ implies that $1 = \frac{n}{n} \leq \frac{n}{p} < \frac{n}{\frac{2}{3}n} = \frac{3}{2}$ so that $\left\lfloor \frac{n}{p} \right\rfloor = 1$ so that $2\left\lfloor \frac{n}{p} \right\rfloor = 2$.

It follows that if $\frac{2}{3}n < p \leq n$ then $\mathrm{ord}_p(N) = 0$; hence (17.40) follows. ■

§17.5. Exercises

Exercise 1. In Proposition 17.20 we proved that $\pi(x) = O(x/\log x)$. In this exercise you are asked to prove that $\pi(x) = \Omega(x/\log x)$ and thus complete the result of Tchebyshev asserting that $\pi(x) \asymp x/\log x$. Recall that for the proof of Bertrand's postulate we used

$$\frac{2^{2n}}{2n} \leq \binom{2n}{n} \leq \prod_{p<2n} p^{\mathrm{ord}_p(\binom{2n}{n})}.$$

For the upper bound in Tclebyshev's theorem one only needs

$$2^n \leq \binom{2n}{n} \leq \prod_{p<2n} p^{\mathrm{ord}_p(\binom{2n}{n})} \tag{17.42}$$

which holds for n sufficiently large as $2^n = o(2^{2n}/2n)$. The purpose of this exercise is for you to explore (17.42).

1. Use (17.42) to prove

$$n \leq \sum_{p\leq\sqrt{2n}} \left\lceil \frac{\log 2n}{\log p} \right\rceil \log p + \sum_{p>\sqrt{2n}}^{p<2n} \log p$$

   and use the latter to prove

$$\vartheta(2n) \geq n - \sqrt{2n}\log 2n \tag{17.43}$$

   holds for n sufficiently large.

   Hint. Let $p < 2n$. If $\log p > \log 2n/2$ then trivially $\lceil \log 2n/\log p \rceil = 1$.

2. (a) Use (17.43) to establish that $\vartheta(x) = \Omega(x)$ for $x \in \mathbb{R}$ sufficiently large.
   (b) Prove that $\pi(x) \geq \vartheta(x)/\log x$. So that $\vartheta(x) = \Omega(x)$ implies $\pi(x) = \Omega(x/\log x)$.

Exercise 2. In Exercise 1 you proved $\vartheta(x) \leq \pi(x)\log x$ which in particular implies that $\vartheta(x) = O(\pi(x)\log x)$. In this exercise you are asked to prove that $\vartheta(x) = \Omega(\pi(x)\log x)$ and thus attain $\vartheta(x) \asymp \pi(x)\log x$.

Hint: First write $\vartheta(x) \geq \sum_{\sqrt{x}<p\leq x} \log p$. Second, recall the result of Exercise 1 that $\pi(x) = \Omega(x/\log x)$ which in turn implies that $\sqrt{x}\log\sqrt{x} = o(\pi(x)\log\sqrt{x})$.

Exercise 3. We have seen that $\vartheta(x) = O(x)$ and in particular we have seen that $\vartheta(x) \leq 4x$ for x sufficiently large (see (17.25)). In this exercise you asked to prove $\vartheta(x) \leq 2x$ for $x \geq 2$ and thus prove (17.26). To prove this it is sufficient to prove that for every $2 \leq k \in \mathbb{Z}$

$$\vartheta(k) \leq 2k. \tag{17.44}$$

Use the following questions as a guide to this goal.

1. Let $1 \leq m \in \mathbb{Z}$. Prove that $M := \binom{2m+1}{2} \leq 2^{2m}$.
2. Given $1 \leq m \in \mathbb{Z}$, use the fact that $\prod_{m+1<p\leq 2m+1} p \mid \binom{2m+1}{m}$ to prove

$$\sum_{p\leq 2m+1} \log p - \sum_{p\leq m+1} \log p < 2m \tag{17.45}$$

3. Prove (17.44) by induction on k. One way to do this is to separate the induction step into two cases: either k is even or it is odd.

Exercise 4. Let p be a prime and let $n \in \mathbb{Z}^+$. Prove that

$$\mathrm{ord}_p(n!) = \sum_{k\geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Exercise 5. Let p be a prime and let $m \in \mathbb{Z}^+$. Prove that

$$\operatorname{ord}_p\left(\binom{2m}{m}\right) = \sum_{k\geq 1}\left(\left\lfloor \frac{2m}{p^k}\right\rfloor - 2\left\lfloor \frac{m}{p^k}\right\rfloor\right) \tag{17.46}$$

Exercise 6. Let $x \in \mathbb{R}$. Show that $2\lfloor x\rfloor \leq \lfloor 2x\rfloor \leq 2\lfloor x\rfloor + 1$. This in turn implies

$$\lfloor 2x\rfloor \in \{2\lfloor x\rfloor, 2\lfloor x\rfloor + 1\}. \tag{17.47}$$

Exercise 7. Let p be a prime and let $m \in \mathbb{Z}^+$. Prove that

$$\operatorname{ord}_p\left(\binom{2m}{m}\right) \leq \frac{\log(2m)}{\log p}.$$

§17.6. Solutions

Solution for Exercise 1.

1. For n sufficiently large $2^n \leq \prod_{p<2n} p^{\operatorname{ord}_p(\binom{2n}{n})}$ holds by (17.42). Taking log (base 2 as usual) on both sides yields the following.

$$\begin{aligned} n &\leq \log\left(\prod_{p<2n} p^{\operatorname{ord}_p(\binom{2n}{n})}\right) \\ &= \sum_{p<2n} \log\left(p^{\operatorname{ord}_p(\binom{2n}{n})}\right) \\ &= \sum_{p<2n} \operatorname{ord}_p(\binom{2n}{n})\log p \\ &\leq \sum_{p<2n}\left\lceil \frac{\log 2n}{\log p}\right\rceil \log p, \end{aligned}$$

where for the last equality we used the fact that $\operatorname{ord}_p(\binom{2n}{n}) \leq \lceil \log 2n/\log p\rceil$. If $\log p > \log 2n/2$, i.e., $p > \sqrt{2n}$, then $\lceil \log 2n/\log p\rceil = 1$. That is

$$\begin{aligned} n &\leq \sum_{p\leq\sqrt{2n}}\left\lceil \frac{\log 2n}{\log p}\right\rceil \log p + \sum_{p>\sqrt{2n}}^{p<2n} \log p \\ &\leq \sqrt{2n}\log 2n + \vartheta(2n). \end{aligned}$$

   (a) Owing to $\sqrt{2n}\log 2n = o(n)$, we have that $\vartheta(2n) \geq n - \sqrt{2n}\log 2n = \Omega(n)$, i.e., there exists a constant $C >$ such that $\vartheta(2n) \geq Cn$ for n sufficiently large. Then for any x sufficiently large let n satisfy $2n \leq x \leq 2n+1$. For such an x

$$\vartheta(x) \geq \vartheta(2n) \geq Cn \geq C(x-1)/2 \geq C'x$$

   for some constant $C' > 0$. This shows that $\vartheta(x) = \Omega(x)$.

   (b) As $\vartheta(x) = \sum_{p\leq x}\log p \leq \pi(x)\log x$ it follows that $\pi(x) \geq \vartheta(x)/\log x$. Hence $\vartheta(x) = \Omega(x)$ implies $\pi(x) = \Omega(x/\log x)$.

Solution for Exercise 2. The upper bound is clear (and is already present in Exercise 1):

$$\vartheta(x) = \sum_{p\le x} \log p \le \log x \sum_{p\le x} 1 = \pi(x)\log x.$$

For the lower bound we write

$$\begin{aligned}\vartheta(x) &\ge \sum_{\sqrt{x}<p\le x} \log p \\ &\ge \big(\log\sqrt{x}\big)\big(\pi(x)-\pi(\sqrt{x})\big);\end{aligned}$$

as $\pi(\sqrt{x}) \le \sqrt{x}$ we arrive at

$$\ge \big(\log\sqrt{x}\big)\pi(x) - \big(\log\sqrt{x}\big)\sqrt{x}$$

Owing to $\pi(x) = \Omega(x/\log x)$, by the result of Exercise 1, we have $\sqrt{x}\log\sqrt{x} = o\big(\pi(x)\log\sqrt{x}\big)$. The desired lower bound then follows.

Solution for Exercise 3.

1. As $2m+1$ is odd we have that $\binom{2m+1}{m} = \binom{2m+1}{m+1}$ so that

$$\binom{2m+1}{m} \le \frac{\sum_{k=0}^{2m+1}\binom{2m+1}{k}}{2} \le \frac{2^{2m+1}}{2} = 2^{2m}.$$

2. As $\prod_{m+1<p\le 2m+1} p \mid \binom{2m+1}{m}$ then in particular $\prod_{m+1<p\le 2m+1} p \le \binom{2m+1}{m}$ so that

$$\sum_{p\le 2m+1}\log p - \sum_{p\le m+1}\log p \le \sum_{p>m+1}^{p\le 2m+1}\log p \le \log M \le \log 2^{2m} = 2m.$$

3. The proof is by induction on k. For $k=2$ the claim is trivial. Assume the claim holds for all $n \le k-1$ and consider the claim for k. If k is even then

$$\vartheta(k) = \sum_{p\le k}\log p = \sum_{p\le k-1}\log p \le 2(k-1) \le 2k,$$

where in the next to last inequality we used the induction hypothesis. Suppose then that k is odd and write $k = 2m+1$. Then

$$\vartheta(k) = \underbrace{\sum_{p\le 2m+1}\log p - \sum_{p\le m+1}\log p}_{I} + \underbrace{\sum_{p\le m+1}\log p}_{II}$$

Using (17.45) to estimate term I and the induction hypothesis to estimate term II we arrive at

$$\begin{aligned}\vartheta(k) &\le 2m + 2(m+1) \\ &= 4m+2 \\ &= 2(2m+1) \\ &= 2k.\end{aligned}$$

Solution for Exercise 4. By (17.29),

$$\mathrm{ord}_p(n!) = \sum_{j=1}^{n} \mathrm{ord}_p(j) = \sum_{j=1}^{n} \sum_{k\geq 1} d_{j,k} = \sum_{k\geq 1} \sum_{j=1}^{n} d_{j,k}, \tag{17.48}$$

where

$$d_{i,j} = \begin{cases} 1, & p^k \mid j, \\ 0, & p^k \nmid j. \end{cases}$$

Notice that $\sum_{j=1}^{n} d_{j,k}$ is the number of multiples of p^k in the interval $[1, n]$. Consequently, $\sum_{j=1}^{n} d_{j,k} = \left\lfloor \frac{n}{p^k} \right\rfloor$. The claim then follows.

Solution for Exercise 5. We may write

$$\mathrm{ord}_p((m!)^2) \overset{(17.29)}{=} 2\mathrm{ord}_p((m!)) \overset{(17.48)}{=} 2\sum_{k\geq 1} \left\lfloor \frac{m}{p^k} \right\rfloor,$$

and

$$\mathrm{ord}_p((2m)!) \overset{(17.48)}{=} \sum_{k\geq 1} \left\lfloor \frac{2m}{p^k} \right\rfloor$$

. As

$$\binom{2m}{m} = \frac{(2m)!}{(m!)^2} \in \mathbb{Z},$$

the claim no follows by (17.30).

Solution for Exercise 6. For $y \in \mathbb{R}$ we write $\{y\}$ to denote the fractional part of y. Assume $x > 0$ (the complementary case is identical) and write $x = z + \varepsilon$ where $z \in \mathbb{Z}$ and $\varepsilon \in [0, 1)$. Then

$$\{2x\} = \{2z + 2\varepsilon\} = 2\varepsilon - \lfloor 2\varepsilon \rfloor = 2\{x\} - \lfloor 2\varepsilon \rfloor,$$

implying that

$$\{2x\} \leq 2\{x\}.$$

However, as $\varepsilon < 1$, then $2\varepsilon < 2$ so that $0 \leq \lfloor 2\varepsilon \rfloor \leq 1$ implying that

$$\{2x\} + 1 = 2\{x\} - \lfloor 2\varepsilon \rfloor + 1 \geq 2\{x\}.$$

We thus have

$$\{2x\} \leq 2\{x\} \leq \{2x\} + 1. \tag{17.49}$$

By the upper bound in (17.49) we have

$$\lfloor 2x \rfloor = 2x - \{2x\} \leq 2x - 2\lfloor x \rfloor + 1 = 2\lfloor x \rfloor + 1$$

giving us the desired upper bound. By the lower bound in (17.49) we have

$$\lfloor 2x \rfloor = 2x - \{2x\} \geq 2x - 2\{x\} = 2\lfloor x \rfloor$$

giving us the desired lower bound.

Solution for Exercise 7. By (17.46)

$$\operatorname{ord}_p\left(\binom{2m}{m}\right) = \sum_{k\geq 1}\left(\left\lfloor\frac{2m}{p^k}\right\rfloor - 2\left\lfloor\frac{m}{p^k}\right\rfloor\right).$$

Each summand in this sum is either 0 or 1 by (17.47). A summand for which $p^k > 2m$ must be zero as indeed $\binom{2m}{m} = (2m)!/(m!)^2$ cannot be divided by numbers exceeding $2m$. Hence, the number of ks for which the summand may be non-zero is given by the equation $p^k \leq 2m$ leading to the upper bound of $k \leq \log(2m)/\log p$. The claim now follows.