MATH 312
AN INTRODUCTION TO
NUMBER THEORY

NUNO FREITAS and ADELA GHERGA

November 22, 2017
The University of British Columbia

An Introduction to Number Theory is an introductory undergraduate text designed to initiate the study of the integer numbers together with some of their elementary properties and applications. The exposition is aimed at students who have some (but not necessarily much) experience with reading and writing proofs. Specifically, it will be assumed that students are familiar with basic techniques of mathematical proof and reasoning such as induction and proof by contradiction. We will introduce basic concepts of number theory, such as prime numbers, factorization, and congruences, as well as some of their applications, particularly to cryptography.

Contents

1. The Integers

In this section, we will recall some basic notation and properties of the integers. Throughout the remainder of this book, we will use this information as axioms without further explanation. The properties listed here are not necessarily independent; that is, it is possible to prove some of these properties from the others.

We will denote the integer numbers by

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

Given $a, b \in \mathbb{Z}$ we will write $a + b$ for their sum and $a \cdot b$ for their product. We also denote the product by ab. We will write $a - b$ to denote $a + (-b)$.

We call the *positive integers*, to the numbers

$$\mathbb{Z}_{>0} = \{1,\ 2,\ 3,\ 4, \ldots\}.$$

Given two integers a, b, we will say that a *is greater than* b if $a - b \in \mathbb{Z}_{>0}$; this is denoted $a > b$. We also say that b *is smaller than* a, writing $b < a$.

The integers satisfy the following properties:

Closure: If $a, b \in \mathbb{Z}$ then $a + b \in \mathbb{Z}$ and $ab \in \mathbb{Z}$.

Commutativity: If $a, b \in \mathbb{Z}$ then $a + b = b + a$ and $ab = ba$.

Associativity: If $a, b, c \in \mathbb{Z}$ then $(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$.

Distributivity: If $a, b, c \in \mathbb{Z}$ then $a(b + c) = ab + ac$.

Identity: If $a \in \mathbb{Z}$ then $a + 0 = 0 + a = a$ and $1 \cdot a = a \cdot 1 = a$.

Additive inverse: For all $a \in \mathbb{Z}$ there is a unique element $x \in \mathbb{Z}$ such that $a + x = 0$. We denote x by $-a$ and call it the additive inverse of a.

Cancellation law for multiplication: If $a, b, c \in \mathbb{Z}$, $c \neq 0$ and $ca = cb$ then $a = b$.

Trichotomy law: If $a \in \mathbb{Z}$ then exactly one of the following holds:

$$(i)\ \ a < 0, \qquad (ii)\ \ a = 0, \qquad (iii)\ \ a > 0.$$

Closure for the positive integers: If a and b are positive integers then $a + b$ and $a \cdot b$ are positive integers.

Example 1.1. We will use the axioms above to show that, for all $a \in \mathbb{Z}$, we have $a \cdot 0 = 0$. Indeed, since 0 is the identity element for addition we have $0 + 0 = 0$, hence

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

by the distributivity property. Adding the inverse of $a \cdot 0$ to both sides and applying the associativity law, we obtain

$$0 = a \cdot 0 - a \cdot 0 = a \cdot 0 + (a \cdot 0 - a \cdot 0) = a \cdot 0 + 0 = a \cdot 0,$$

where the first equality comes from the definition of inverse and the last by the identity element of addition. Thus $a \cdot 0 = 0$, as desired.

The Well Ordering Principle (WOP): Every non-empty subset $S \subset \mathbb{Z}_{>0}$ of the positive integers contains a least element.

That is, given a subset S of $\mathbb{Z}_{>0}$, there is an $m \in S$ such that $m \leq n$ for all $n \in S$. The following examples illustrate this property.

Examples 1.2.

(1) Given $S = \mathbb{Z}_{>0}$, the smallest element of S is 1.
(2) Let S be the set of even integers. Then 2 is the smallest element of S.
(3) Let S be the set of all prime numbers. Then 2 is the smallest element of S.

Remark 1.3. The WOP does not hold for other sets of numbers like $\mathbb{Q}$ or $\mathbb{R}$. Indeed, consider the set

$$S = \left\{ \frac{1}{n} \ : \ n \in \mathbb{Z}_{>0} \right\}.$$

This is a non-empty set of positive elements which does not have a smallest element in either $\mathbb{Q}$ or $\mathbb{R}$.

For an integer k we will write $\mathbb{Z}_{>k}$ to denote the set of integers greater than k. Similarly, we will also write $\mathbb{Z}_{\geq k}$, $\mathbb{Z}_{<k}$, $\mathbb{Z}_{\leq k}$ or $\mathbb{Z}_{\neq k}$ to denote the sets with the natural analogous definition.

We conclude this section by defining the rational numbers $\mathbb{Q}$ as fractions of integers. Formally, we have the following definition.

Definition 1.4. Consider pairs (p, q) where $p, q \in \mathbb{Z}$ and $q \neq 0$ and the following equivalence relation on them: two such pairs (p, q) and (p', q') are equivalent if and only if $pq' = p'q$ in $\mathbb{Z}$.

We define the rational numbers $\mathbb{Q}$ as the set of equivalence classes for this relation. The equivalence class of (p, q) is denoted by the fraction $\frac{p}{q}$.

Exercises.

Exercise 1.5. Let $a, b \in \mathbb{Z}$ with $ab = 0$. Show that either $a = 0$ or $b = 0$.

Exercise 1.6. Let $a, b, c \in \mathbb{Z}$ with $a < b$. Show that $a + c < b + c$.

Exercise 1.7. Let $a, b, c \in \mathbb{Z}$ with $a < b$ and $c > 0$. Show that $ac < bc$.

2. Mathematical Induction

In this section, we recall the first and second principles of mathematical induction, an important proof technique. The first principle is also known as *weak induction* while the second is also known as *strong induction*, because it seems to use a stronger assumption (compare parts (b) of Theorems 1 and 2). However, they are equivalent; we shall see in Theorem 3 that they are both equivalent to the Well Ordering Principle.

Theorem 1 (First Principle of Mathematical Induction)**.**

Let m be an integer and S a subset of $\mathbb{Z}$ satisfying

(a) $m \in S$ and
(b) if $k \geq m$ and $k \in S$ then $k+1 \in S$.

Then S contains all integers greater or equal to m, that is $S = \mathbb{Z}_{\geq m}$.

Proof. Let $m = 1$ and S be as in the statement. Assume, for contraction, that there exists an integer greater or equal to $m = 1$ which is not in S. Then the set of positive integers which are not in S is non-empty. By the WOP, this set has a minimal element s. Since $1 \in S$, we have that $s \neq 1$ so that s is a positive integer strictly greater than 1. Now, the integer $s-1$ is a positive integer smaller than s. By minimality of s, we must have that $s - 1 \in S$. Then, from property (b), it follows that $s = (s-1)+1 \in S$, a contraction.

Finally, let m be any integer and S as in the statement; we will reduce this situation to the case $m = 1$ and apply the previous paragraph. Indeed, consider the translated set

$$S' = \{k - m + 1 \mid k \in S\}.$$

Since $m \in S$ we have $1 \in S'$. Let $k \geq 1$ be in S'. Then, there is $k_0 \geq m$ in S such that $k = k_0 - m + 1$; since S satisfies (b) we have $k_0 + 1 \in S$, hence $k + 1 = (k_0 + 1) - m + 1$ is in S'. We conclude that S' satisfies (a) and (b) with $m = 1$, so by the first part of the proof we have $S' = \mathbb{Z}_{\geq 1}$. Then $S = \mathbb{Z}_{\geq m}$, as desired. ☕

Theorem 2 (Second Principle of Mathematical Induction)**.**

Let m be an integer and S a subset of $\mathbb{Z}$ satisfying

(a) $m \in S$ and
(b) if $k \geq m$ and $\{m, m+1, m+2, \ldots, k\} \subset S$ then $k+1 \in S$.

Then S contains all integers greater or equal to m, that is $S = \mathbb{Z}_{\geq m}$.

Proof. Let m and S be as in the statement. Consider the set T of all the integers $n \geq m$ such that every integer in the interval $[m, n]$ belongs to S. In particular, $m \in T$.

Suppose that $n \in T$. Then $\{m, m+1, m+2, \ldots, n\} \subset S$ by definition of T. The hypotheses on S now imply $n+1 \in S$. Then all the integers in the interval $[m, n+1]$ are in S, so $n + 1 \in T$ also.

We have shown that T satisfies hypothesis (a) and (b) of Theorem 1, so T contains all the integers greater or equal to m. Since $T \subset S$ the same is true for S, as desired. ☕

In practice, induction is used to show that a statement is true for all integers $\geq m$ for some $m \in \mathbb{Z}_{\geq 0}$. This is done via two steps. The first step is the *base case*, where we prove the desired statement is true for $n = m$. The second is the *induction step*, where, assuming that the desired statement is true for n (the *induction hypothesis*), we prove it is also true for $n+1$. Letting S denote the set of positive integers for which the statement is true, these two steps show S satisfies (a) and (b) of Theorem 1. Hence, S must contain all the integers $\geq m$. Note that the only difference between strong and weak induction is that in strong induction, the induction hypothesis becomes that the statement is true for all integers in the interval $[m, n]$. We now give a few examples.

Proposition 1. *Let $n \in \mathbb{Z}_{>0}$. The sum of the first n integers is given by the formula*

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

Proof. Let $S \subset \mathbb{Z}$ be the set of positive integers for which the formula holds. We use weak induction on S.

Base: Let $n = 1$. Then $\sum_{k=1}^{1} k = 1 = 1 \cdot (1+1)/2$, so $1 \in S$.

Hypothesis: Suppose that the formula holds for $n > 1$, that is $n \in S$.

Step: We will show that $n + 1 \in S$. We have that

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

where in the second equality we have used the induction hypothesis. This shows that $n+1 \in S$. We conclude that S satisfies both properties (a) with $m = 1$ and (b) in Theorem 1, therefore $S = \mathbb{Z}_{\geq 1}$, as desired. ☕

Proposition 2. *Consider the geometric series $\sum_{k=0}^{\infty} ar^k$ where $a, r \in \mathbb{R}$ with $r \neq 1$. For $n \in \mathbb{Z}_{\geq 0}$, its partial sum is given by the formula*

$$\sum_{k=0}^{n} ar^k = a\left(\frac{1 - r^{n+1}}{1 - r}\right).$$

Proof. We will use weak induction to prove the case $a = 1$.

Base: Let $n = 0$. Then $\sum_{k=0}^{n} r^k = 1 = \frac{1 - r^{0+1}}{1 - r}$.

Hypothesis: Suppose that the formula holds for $n > 1$.

Step: We have that

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

It follows that the formula holds for $a = 1$. Finally, multiply the above formula on both sides by a to obtain the general case. ☕

Example 2.1 (Strong induction)**.** We will show that any amount of postage more than one cent can be formed using just two-cent and three-cent stamps.

Base: For $n = 2$ cents we use one two-cent stamp; for $n = 3$ we use one three-cent stamp.

Hypothesis: Let $n \geq 3$ and suppose that every amount of postage in the interval $[2, n]$ can be formed using two-cent and three-cent stamps.

Step: We can write $n+1 = 2+(n-1)$. By the induction hypothesis, $n-1 \geq 2$ can be obtained by using just two-cent and three-cent stamps; then $n+1$ can be obtained by using those stamps plus an extra two-cent stamp.

Theorem 3. *The Well Ordering Principle is equivalent to both weak and strong induction.*

Proof. We have seen in the previous proofs that WOP implies weak induction and that weak induction implies strong induction. We will now show that strong induction implies WOP.

Suppose there exist $S \subset \mathbb{Z}_{>0}$ without a smallest element. We will prove that S is empty. Let T be the complement of S in $\mathbb{Z}_{>0}$. That is, T is the set of positive integers which are not in S.

Clearly, $1 \in T$ otherwise $1 \in S$ is the smallest element of S since 1 is the smallest positive integer. Let $n > 1$ and write $S_n = \{1, \ldots, n\}$. Suppose $S_n \subset T$, hence $S_n \cap S = \varnothing$. Therefore, if $n+1 \in S$ then $n+1$ is the smallest integer in S, which is a contradiction to our hypothesis, so $n+1 \notin S$. We conclude that $n+1 \in T$, hence T satisfies properties (a) and (b) of Theorem 2 and we have $T = \mathbb{Z}_{>0}$ by strong induction. Thus $S = \varnothing$, as desired. ☕

Exercises.

Exercise 2.2. Let $n \in \mathbb{Z}_{>0}$. Use induction to show that the sum of the first n^2 integers is given by the formula

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

Exercise 2.3. Define a sequence $x_1, x_2, \ldots$ by

$$\begin{cases} x_1 = 1 \\ x_2 = 3 \\ x_{k+2} = 3x_{k+1} - 2x_k & \text{for } k \geq 1. \end{cases}$$

Use induction to show that for all positive integers n, we have $x_n = 2^n - 1$.

3. Divisibility

Definition 3.1. Let $a, b \in \mathbb{Z}$. We say that a *divides* b, denoted $a \mid b$, if there exists $c \in \mathbb{Z}$ such that $b = a \cdot c$. In this case, we also say that a is a *factor* of b and b is a *multiple* of a. We write $a \nmid b$ to denote that a does not divide b.

Examples 3.2.

(1) $3 \mid 6$ since $6 = 3 \cdot c$ with $c = 2$.
(2) $3 \nmid 5$ since $5 = 3 \cdot c$ with $c = \frac{5}{3} \notin \mathbb{Z}$.
(3) $a = 1 \cdot a = (-1)(-a) \Rightarrow \pm 1, \pm a$ divide a.
(4) $0 = a \cdot 0 \Rightarrow a \mid 0 \quad \forall a \in \mathbb{Z}$.
(5) $b = 0 \cdot c \Rightarrow b = 0$. That is, only 0 is divisible by 0.

Remark 3.3. From (4) in the example above, it follows that $0 \mid 0$. However, the fraction $\frac{0}{0}$ makes no sense as a rational number.

In subsequent sections, we will need some simple properties of divisibility, which we now state and prove.

Proposition 3. *Let a, b, c be integers. If $a \mid b$ and $b \mid c$ then $a \mid c$.*

Proof. By hypothesis, $b = ab_0$ and $c = bc_0$ for some $b_0, c_0 \in \mathbb{Z}$. Then,

$$c = bc_0 = (ab_0)c_0 = a(b_0c_0) \iff a \mid c.$$

☕

Proposition 4. *Let $a, b, c, m, n \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$ then $c \mid ma + nb$.*

Proof. By hypothesis, $a = ca_0$ and $b = cb_0$ for some $a_0, b_0 \in \mathbb{Z}$. Then,

$$ma + nb = m(ca_0) + n(cb_0) = c(ma_0 + nb_0) \iff c \mid ma + nb.$$

☕

An expression of the form $ma + nb$ as in the previous proposition is called a *(integral) linear combination of a and b.* A very useful consequence of this proposition is that if a and b are divisible by an integer d, then their sum and difference are also divisible by d.

Corollary 1. *Let $a, b, c \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$, then $c \mid a + b$ and $c \mid a - b$.*

The above examples and definitions give a consice meaning to an exact division, but we are also used to division with a remainder. For example, we know that 4 fits into 15 exactly 3 times, with a remainder of 3. The following theorem makes this idea precise.

Theorem 4 (Division Algorithm/Division with Remainder)**.** *Let $n, a \in \mathbb{Z}$ with $a > 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that*

$$n = q \cdot a + r \qquad \textit{where} \qquad 0 \le r < a.$$

We say that q is the quotient and r the remainder of the division of n by a.

Proof. The proof consists of two parts: first we find some q, r with the desired properties and then we prove they are unique with those properties. Let $n, a \in \mathbb{Z}$ with $a > 0$.

Existence. Consider

$$T = \{m \in \mathbb{Z}_{>0} \mid m = n - ka \text{ for some } k \in \mathbb{Z}\},$$

that is, the set of non-negative numbers that differ from n by a multiple of a. Note that $T \neq \varnothing$ because we can choose a negative k with large enough absolute value to make $m > 0$. Then, by the WOP we can choose r to be the smallest positive integer in T. In particular, we have $0 \leq r = n - qa$ for some $q \in \mathbb{Z}$ by definition of T.

This gives our candidates for r and q. It remains to show that $r < a$. Indeed, suppose $r \geq a > 0$. Then

$$r - a = n - (q+1)a \geq 0 \implies r - a \in T \text{ with } 0 \leq r - a < r.$$

This contradicts the fact that r is the smallest positive element of T, hence $r < a$, as desired.

Uniqueness. Suppose, in addition to q and r, there exist q' and r' with

$$n = q' \cdot a + r' \quad \text{where} \quad 0 \leq r' < a.$$

Now

$$n = q \cdot a + r = q' \cdot a + r' \quad \text{with} \quad 0 \leq r, r' < a.$$

Suppose first $r = r'$. Then $(q - q')a = 0$ and, since $a \neq 0$, we have $q = q'$. We conclude that, to finish the proof, we need to show $r = r'$. We proceed by contraction.

Suppose WLOG that $r' > r$. Then $r' - r = (q - q')a > 0$ implies $r' - r \geq a$ but

$$a > r' \geq r' - r \geq a,$$

a contradiction. Hence $r = r'$, as desired. ☕

Corollary 2. *Let $n, a \in \mathbb{Z}$ with $a > 0$. Then $a \mid n$ if and only if the remainder of the division of n by a is $r = 0$.*

Examples 3.4.

(1) Take $n = 6$ and $a = 3$; then $6 = 2 \cdot 3 + 0$. That is $q = 2$ and $r = 0$.
(2) Take $n = 30$ and $a = 7$; then $30 = 4 \cdot 7 + 2$. That is $q = 4$ and $r = 2$.

Exercises.

Exercise 3.5. Let $n \in \mathbb{Z}$. Prove that $5 \mid n^5 - n$.

Exercise 3.6. Let $n \in \mathbb{Z}$. Is it true that $4 \mid n^4 - n$? Provide a proof or counterexample.

4. Representation of Integers

When writing down integers, we typically use decimal notation, also called 'base 10'. For example, 37465 means that

$$37465 = 3 \cdot 10^4 + 7 \cdot 10^3 + 4 \cdot 10^2 + 6 \cdot 10 + 5 \cdot 10^0.$$

We have also heard that computers use 'base 2,' representing numbers by using only a series of 1's and 0's. For instance, 36 can be written as

$$36 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0,$$

or more simply, $36 = (100100)_2$. Here, $(100100)_2$ is the collection of the coefficients in front of the exponents of 2 in the representation of 36. Of course, these coefficients can only be either 1 or 0, since, for example $2 = 1 \cdot 2^1 + 0 \cdot 2^0$, or more concisely, $2 = (10)_2$.

The following theorem makes this notion precise and shows that other bases, aside from 10 and 2, may also be used.

Theorem 5. *Let $b \geq 2$ be an integer. Every positive integer n can be uniquely written in base b. More precisely,*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 \quad \textit{with} \;\; a_k \neq 0 \;\; \textit{and} \;\; 0 \leq a_i \leq b-1 \;\; \textit{for} \;\; i = 0, \ldots, k.$$

We denote n in base b by $(a_k a_{k-1} \ldots a_1 a_0)_b$.

Proof. The proof uses strong induction and is divided into two parts: first we prove the existence of a description of n as in the statement and then we show that such a description is unique. Note that in the base step of induction, we must consider several cases. This is because these cases are all independent of each other, in contrast to the induction step, where each case follows from previous cases.

Existence.

Base: For the cases $n = 1, \ldots, b-1$, take $k = 0$ and $a_0 = n$.

Hypothesis: There exists a description in base b for all positive integers less than n.

Step: Suppose $n \geq b$. We divide n by b using the division algorithm (Theorem 4) to obtain

$$n = b \cdot q + a_0 \quad \text{with} \quad 0 \leq a_0 \leq b-1.$$

Note that $1 \leq q < n$, so by the induction hypothesis

$$q = c_s b^s + c_{s-1} b^{s-1} + \cdots + c_0 \quad \text{with} \;\; c_s \neq 0 \;\; \text{and} \;\; 0 \leq c_i \leq b-1.$$

Then

$$n = b \cdot q + a_0 = b\big(c_s b^s + c_{s-1} b^{s-1} + \cdots + c_0\big) + a_0 = c_s b^{s+1} + \cdots + c_0 b + a_0.$$

Taking $k = s+1$ and $a_i = c_{i-1}$ for $i = 1, \ldots, k$ we obtain the claimed description.

Uniqueness. Suppose

$$(4.1) \qquad n = a_k b^k + \cdots + a_1 b + a_0 = a'_l b^l + \cdots + a'_1 b + a'_0 \quad \text{with} \;\; a_k, a'_l \neq 0 \;\; \text{and} \;\; 0 \leq a_i, a'_i \leq b-1.$$

Base: If $n \leq b-1$, then $k = l = 0$ and $a'_0 = a_0 = n$.

Hypothesis: There is an unique description in base b for all positive integers less than n.

Step: Suppose $n \geq b$. From equation (4.1) we see that both a_0 and a_0' satisfy the properties of being the remainder of the divsion of n by b. From the uniqueness part of Theorem 4 we conclude $a_0 = a_0'$. We thus have

$$\frac{n - a_0}{b} = a_k b^{k-1} + \cdots + a_2 b + a_1 = a_l' b^{l-1} + \cdots + a_2' b + a_1'$$

and since, $1 \leq \frac{n-a_0}{b} < n$, by the induction hypothesis, we have $k = \ell$ and

$$a_k = a_l', \ \ldots, \ a_1 = a_1',$$

completing the proof. ☕

Example 4.2. Let $n = 67$.

(1) $n = (67)_{10}$ since $67 = 6 \cdot 10 + 7 \cdot 10^0$
(2) $n = (235)_5$ since $67 = 2 \cdot 5^2 + 3 \cdot 5 + 2 \cdot 5^0$
(3) $n = (2111)_3$ since $67 = 2 \cdot 3^3 + 1 \cdot 3^2 + 1 \cdot 3 + 1 \cdot 3^0$

Exercises.

Exercise 4.3. Convert $(101001000)_2$ to base 7.

Exercise 4.4. Consider a balance scale with 2 pans, A and B. Let $k \in \mathbb{Z}_{>0}$. Show that any weight not exceeding $2^k - 1$ that is placed on pan A may be measured, by placing on pan B, a subset of weights of $\{1, 2, 2^2, \ldots, 2^{k-1}\}$.

5. The Greatest Common Divisor

Definition 5.1. Let $a, b \in \mathbb{Z}$ not both zero. The *greatest common divisor* of a and b is the largest positive integer d such that $d \mid a$ and $d \mid b$. We denote it by (a, b) or $\gcd(a, b)$. When $(a, b) = 1$, we say that a and b are *coprime*.

Since the set of positive divisors of n and $-n$ are the same, it is clear that

$$(-a, b) = (a, -b) = (-a, -b) = (a, b).$$

Therefore, we can restrict the coming discussion to non-negative integers a, b.

Examples 5.2.

(1) The set of all common divisors of 12 and 18 is $\{1, 2, 3, 6\}$, so $(12, 18) = \gcd(12, 18) = 6$.
(2) For all $a > 0$, since $a \mid 0$, we have $(a, 0) = a$.

The following theorem provides an alternative description of the greatest common divisor.

Theorem 6. *Let $a, b \in \mathbb{Z}$ not both zero. Then (a, b) is the smallest positive integral linear combination of a and b. That is, the smallest positive integer of the form*

$$ax + by \qquad \textit{where} \qquad x, y \in \mathbb{Z}.$$

Proof. Let $a, b \in \mathbb{Z}$ be non-negative and not both 0. Consider

$$I = \{ax + by \mid x, y \in \mathbb{Z}\},$$

that is, the set of all integral linear combinations of a, b. Clearly, $\pm a, \pm b \in I$, so that I contains positive integers. By the WOP, let d be the smallest such positive integer. By definition of I, we have $d = ax_0 + by_0$, for some $x_0, y_0 \in \mathbb{Z}$. To complete the proof, we must show that $d = (a, b)$.

Let n be a common divisor of a and b. By Proposition 4, we have $n \mid ax + by$ for all $x, y \in \mathbb{Z}$, i.e. n divides all the elements of I. In particular, $n \mid d$. Choosing $n = (a, b)$ we conclude that $(a, b) \leq d$.

Suppose for a moment that d divides all the elements of I. In particular, $d \mid a$ and $d \mid b$ so $d \leq (a, b)$ by definition of (a, b). Since $(a, b) \leq d \leq (a, b)$, we may conclude that $d = (a, b)$.

Now, to finish the proof, we will now show that d divides every element of I. Indeed, let $n \in I$. Dividing n by d with the division algorithm gives

$$n = q \cdot d + r, \quad 0 \leq r < d, \; q \in \mathbb{Z}.$$

We claim that I is closed under addition and multiplication by scalars. More precisely, if $x, y \in I$ and $\lambda \in \mathbb{Z}$ then $x + y$ and λx belong to I. In particular, $qd \in I$ and, since $r = n - qd$ with $n \in I$, we conclude $r \in I$. Thus $r = 0$, otherwise I would contain a positive number smaller than d. It follows that $d \mid n$, where $n = (a, b)$.

We now prove the claim. Let $x = ax_0 + bx_1$ and $y = ay_0 + by_1$ be elements of I and $\lambda \in \mathbb{Z}$. Then,

$$x + y = ax_0 + bx_1 + ay_0 + by_1 = a(x_0 + y_0) + b(x_1 + y_1) \in I$$

and

$$\lambda x = \lambda(ax_0 + bx_1) = a(\lambda x_0) + b(\lambda x_1) \in I,$$

as claimed. ☕

Examples 5.3.

(1) $(5,7) = 10 \cdot 5 + (-7) \cdot 7 = 1$.
(2) $(3,15) = 3 \cdot 6 + (-1) \cdot 15 = 3 \cdot 1 + 0 \cdot 15 = 3$.

The second example illustrates that the values x, y given by Theorem 6 are not unique. In what follows, we look at how to find all the possible choices for x, y.

Corollary 3. *Let $a, b \in \mathbb{Z}$ not both zero. If $(a,b) = 1$, then $ax + by = 1$ for some $x, y \in \mathbb{Z}$.*

Proof. This is a direct consequence of Theorem 6. ☕

Corollary 4. *Let $a, b \in \mathbb{Z}$ not both zero. Every common divisor of a and b divides (a,b).*

Proof. Let d be a common divisor of a, b. We have $a = da'$ and $b = db'$ for some $a', b' \in \mathbb{Z}$. From Theorem 6, there are $x, y \in \mathbb{Z}$ such that

$$(a,b) = ax + by = d(a'x) + d(b'y) = d(a'x + b'y) \implies d \mid (a,b)$$

☕

Corollary 5. *Let $a, a', b, b' \in \mathbb{Z}$ satisfy $a = da'$ and $b = db'$ where $d = (a,b)$. Then $(a', b') = 1$.*

Proof. From Theorem 6, there are $x_0, y_0 \in \mathbb{Z}$ such that

$$ax_0 + by_0 = d \iff d(a'x_0) + d(b'y_0) = d \implies a'x_0 + b'y_0 = 1.$$

By Theorem 6, (a', b') is the smallest positive integer that can be written as a linear combination of a' and b'. It follows that $(a', b') = 1$. ☕

The notion of greatest common divisor also makes sense for more than two integers.

Definition 5.4. Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ not all zero. The *greatest common divisor of* $a_1, \ldots, a_n$, denoted $\gcd(a_1, \ldots, a_n)$ or $(a_1, \ldots, a_n)$, is the largest positive integer dividing all the a_i.

When $(a_1, \ldots, a_n) = 1$ we say that the a_i are *coprime* and if $(a_i, a_j) = 1$ for all $i \neq j$, we say they are *pairwise coprime*.

Example 5.5. Note that $7 \nmid 24$, $7 \nmid 60$ and it is the unique prime factor of $49 = 7^2$, so $(24, 60, 49) = 1$; however, $(24, 60) = 12$. This shows that 24, 60 and 49 are coprime but not pairwise coprime.

We complete this section with an useful generalization of Corollary 4.

Proposition 5. *Let $k \geq 2$ and $a_1, \ldots, a_k \in \mathbb{Z}_{\neq 0}$. Every common divisor of all the a_i divides their greatest common divisor $(a_1, \ldots, a_k)$.*

Proof. We will use induction.

Base: Suppose $k = 2$. The result follows directly by Corollary 4.

Hypothesis: Assume the result is true for any set of $k \geq 2$ non-zero integers.

Step: Suppose $d \mid a_i$ where $a_i \neq 0$ for $i = 1, \ldots, k+1$. In particular, d divides a_1 and, by the induction hypothesis, d divides $\gcd(a_2, a_3, \ldots, a_{k+1})$. Then, by Corollary 4 it also divides

$$\gcd(a_1, \gcd(a_2, a_3, \ldots, a_{k+1})).$$

To complete the proof, we will now show that $\gcd(a_1, \gcd(a_2, a_3, \ldots, a_{k+1})) = \gcd(a_1, a_2, \ldots, a_{k+1})$. Indeed, let d_0 be a common divisor of all the a_i. In particular, by the induction hypothesis, d_0 divides $\gcd(a_2, \ldots, a_{k+1})$, and since d_0 also divides a_1, we have that

$$d_0 \mid \gcd(a_1, \gcd(a_2, a_3, \ldots, a_{k+1}))$$

by Corollary 4. By choosing $d_0 = \gcd(a_1, \ldots, a_{k+1})$, we conclude that

$$\gcd(a_1, \gcd(a_2, a_3, \ldots, a_{k+1})) \geq \gcd(a_1, a_2, \ldots, a_{k+1})$$

by definition of the GCD. Conversely, suppose d_0 divides a_1 and $\gcd(a_2, \ldots, a_{k+1})$; hence d_0 also divides $a_2, \ldots a_{k+1}$. It follows that d_0 divides $\gcd(a_1, a_2, \ldots, a_{k+1})$, and as above, we conclude that

$$\gcd(a_1, \gcd(a_2, a_3, \ldots, a_{k+1})) \leq \gcd(a_1, a_2, \ldots, a_{k+1}).$$

☕

Exercises.

Exercise 5.6. Let a, b be coprime integers not both zero. Determine with proof the possible values of $(a^2 + b^2, a + b)$.

NOTE: You may use the fact that every integer has a prime divisor (Lemma 2 below).

6. The Euclidean Algorithm

In Example 5.2 we have computed $(12,18) = 6$ by first listing all common divisors of 12 and 18. We now compute $(18,30)$ in the same way. Indeed, the positive divisors of 30 are $\{1,2,3,5,6,10,15,30\}$ and those of 18 are $\{1,2,3,6,9,18\}$. Then their common divisors are $\{1,2,3,6\}$, therefore $(30,18) = 6$. Though this method is effective, it is not practical when dealing with large numbers. In this section, we introduce the Euclidean algorithm which, given integers a, b, allows one to compute (a,b) in an efficient way. We will first need the following auxiliary result.

Lemma 1. *Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$. Suppose*

$$a = q \cdot b + r \qquad \text{with} \;\; q, r \in \mathbb{Z}.$$

Then $(a,b) = (b,r)$.

Proof. Let c be a common divisor of a and b. Since $r = a - q \cdot b$, we have $c \mid r$ by Proposition 4 so that c is a common divisor of b and r. Conversely, suppose c is a common divisor of b and r. Then c divides $a = b \cdot q + r$, thus it is also a common divisor of a and b. We conclude that a, b and b, r have the same set of common divisors. Then $(a,b) = (b,r)$, as desired. ☕

Theorem 7 (The Euclidean Algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$. By the Division Algorithm, there exist $q_1, r_1 \in \mathbb{Z}$ such that*

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b.$$

If $r_1 > 0$, there exist (again, by the Division Algorithm) $q_2, r_2 \in \mathbb{Z}$ such that

$$b = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1.$$

If $r_2 > 0$, there exist (again, by the Division Algorithm) $q_3, r_3 \in \mathbb{Z}$ such that

$$r_1 = r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2.$$

Continue this process. Then $r_n = 0$ for some n. Moreover, if $n > 1$, then $(a,b) = r_{n-1}$; if $n = 1$, we have $(a,b) = b$.

Proof. Note that the $r_i \geq 0$ satisfy $r_1 > r_2 > r_3 > \dots$. If $r_n \neq 0$ for all n, then we obtain a strictly decreasing sequence of positive integers, which is impossible. Thus $r_n = 0$ for some $n \geq 1$.

Suppose $n > 1$. Repeated applications of Lemma 1 gives

$$(a,b) = (b, r_1) = (r_1, r_2) = \dots = (r_{N-1}, r_n) = (r_{n-1}, 0) = r_{n-1},$$

as desired. If $n = 1$, then $r_1 = 0$ and $b \mid a$, thus $(a,b) = b$. ☕

Example 6.1. For $a = 30$, $b = 18$, we compute

(1) $30 = 1 \cdot 18 + 12$, so $r_1 = 12 \implies (30,18) = (18,12)$.
(2) $18 = 1 \cdot 12 + 6$, so $r_2 = 6 \implies (18,12) = (12,6)$.
(3) $12 = 2 \cdot 6 + 0$, so $r_3 = 0 \implies (12,6) = (6,0) = 6$.

Thus $(30,18) = 6$, as expected.

Example 6.2. Compute $(803, 154)$:

(1) $803 = 154 \cdot 5 + 33$, so $r_1 = 33 \implies (803, 154) = (154, 33)$.
(2) $154 = 33 \cdot 4 + 22$, so $r_2 = 22 \implies (154, 33) = (33, 22)$.
(3) $33 = 22 \cdot 1 + 11$, so $r_3 = 11 \implies (33, 22) = (22, 11)$.
(4) $22 = 11 \cdot 2 + 0$, so $r_4 = 0 \implies (22, 11) = (11, 0) = 11$.

Thus $(803, 154) = 11$.

Recall that (a, b) is the smallest positive integer of the form $ax+by$ with $x, y \in \mathbb{Z}$ (Theorem 6). The following method, called *back substitution*, allows one to find $x_0, y_0 \in \mathbb{Z}$ such that

$$(a, b) = ax_0 + by_0.$$

This method is also known as *extended Euclidean algorithm* since it mostly consists of reverting the steps of the Euclidean algorithm. We illustrate this with a few examples.

Example 6.3. In Example 6.2, we computed $(803, 154) = 11$. We can revert the steps of the Euclidean algorithm as follows:

$$\begin{aligned}(803, 154) = 11 = 33 - 22 &= 33 - (154 - 33 \cdot 4) = 33 \cdot 5 - 154 \\ &= (803 - 154 \cdot 5) \cdot 5 - 154 = 803 \cdot 3 - 154 \cdot 26 \\ &= 803 \cdot 3 + 154 \cdot (-26),\end{aligned}$$

hence

$$(803, 154) = 803 \cdot 3 + 154 \cdot (-26) \implies x_0 = 3 \quad \text{and} \quad y_0 = -26.$$

Example 6.4. Compute $(154, 35)$ and x_0, y_0 satisfying $154x_0 + 35y_0 = (154, 35)$.

First apply the Euclidean Algorithm:

(1) $154 = 4 \cdot 35 + 14$, so $r_1 = 14 \implies (154, 35) = (35, 14)$;
(2) $35 = 2 \cdot 14 + 7$, so $r_2 = 7 \implies (35, 14) = (14, 7)$;
(3) $14 = 2 \cdot 7 + 0$, so $r_3 = 0 \implies (14, 7) = (7, 0) = 7$,

to conclude $(154, 35) = 7$. Now we apply back substitution:

$$\begin{aligned}(154, 35) = 7 &= 35 - 2 \cdot 14 = 35 - 2 \cdot (154 - 4 \cdot 35) \\ &= 35 \cdot 9 + 154 \cdot (-2) = 154 \cdot (-2) + 35 \cdot 9.\end{aligned}$$

That is $x_0 = -2$ and $y_0 = 9$.

Proposition 6. *Let a and b be non-zero integers satisfying $a \mid b$ and $b \mid a$.*

Then, $a = b$ or $a = -b$. In particular, if a and b are positive, then $a = b$.

Proof. By hypothesis we have $a = bk$ and $b = ak'$ for some integers $k, k' \in \mathbb{Z}$. Then,

$$a = bk = akk' \implies kk' = 1 \implies k = k' = 1 \quad \text{or} \quad k = k' = -1$$

and we have $a = b$ or $a = -b$ accordingly. The last statement is clear since $a = -b$ and b have different signs. ☕

Exercises.

Exercise 6.5. Use the Euclidean algorithm to prove that 7 has no expression as an integral linear combination of 18209 and 19043.

Exercise 6.6. Use the Euclidean algorithm and back substitution to find two rational numbers with denominators 11 and 13, respectively, and a sum of $\frac{7}{143}$.

7. Prime Numbers

The prime numbers function as the 'building blocks' of the integers in the sense that they cannot be divided any further.

Definition 7.1. Let $p > 1$ be an integer. Then p is a *prime number* if its only positive divisors are 1 and p. An integer $n > 1$ which is not prime is called *composite*.

Examples 7.2.

(1) $2, 3, 5, 7$ are prime numbers.
(2) $6 = 2 \cdot 3$ is composite.
(3) 34052881 is a prime.
(4) $2^{74207281} - 1$ is the largest prime number known as of May 2017. It is a number with 22338618 digits.

The last examples show that there are enormous prime numbers. In fact, a theorem of Euclid states that there are infinitely many primes. It is a consequence of this theorem (see Theorem 8) that we can always find larger and larger primes. Before we prove Euclid's theorem, we need to introduce the following important auxiliary result.

Lemma 2. *Every integer $n > 1$ has a prime divisor.*

Proof. Let $n > 1$ be an integer. If n is prime, since $n \mid n$, then n is its own prime divisor and we are done. Suppose now that n is composite. Assume further that n is the smallest composite number without any prime divisors. Then, there are integers a, b such that

$$n = a \cdot b \quad \text{with} \quad 1 < a, b < n.$$

By minimality of n, there exists a prime p dividing a; that is $a = pa'$ for some $a' \in \mathbb{Z}$. Then, $n = ab = p(a'n)$, so that $p \mid n$, a contraction. ☕

Theorem 8 (Euclid)**.** *There are infinitely many prime numbers.*

Proof of Euclid's Theorem. Suppose, for contradiction, that there are only finitely many primes numbers. Denote them $p_1, p_2 \ldots, p_k$ and consider the the number

$$n = p_1 p_2 \cdots p_k + 1.$$

By Lemma 2, n has a prime divisor p, hence $p = p_i$ for some i. Since p divides n and $p_1 p_2 \cdots p_k$, from Corollary 1, p divides the difference

$$n - p_1 p_2 \cdots p_k = 1$$

which is impossible. Hence there are infinitely many primes. ☕

The following two theorems are classical results on the distribution of prime numbers. They are beyond the scope of these notes, so we restrict ourselves to their statements.

Theorem 9 (The Prime Number Theorem)**.** *Let $\pi(x)$ denote the function giving the number of primes $\leq x$. Then, when x gets closer to infinity, the function $\frac{x}{\log(x)}$ gets closer to $\pi(x)$.*

Theorem 10 (Dirichlet Density Theorem)**.** *Let $a, b \in \mathbb{Z}$ satisfy $(a, b) = 1$. Then, there are infinitely many primes of the form $a + bk$ with $k \in \mathbb{Z}$.*

In later discussions about cryptographic applications, it will be clear that it is important to find and use extremely large primes. Given a large odd integer it can be very hard to decide if it is a prime number, therefore tests distinguishing between primes and composite integers will be crucial. The most basic such test is trial division; the following proposition tells us that, given an integer n, we need only test its divisibility by all the primes up to $\sqrt{n}$. If n is not divisible by any of these primes, then n must be a prime number.

Proposition 7. *Let n be composite. Then n has a prime divisor $p \le \sqrt{n}$.*

Proof. Since n is composite, we have $n = a \cdot b$ for $1 < a, b < n$. WLOG, suppose $b \ge a$. Suppose $a > \sqrt{n}$. Then

$$n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n,$$

a contradiction. Hence $a \le \sqrt{n}$. In particular, the prime factors of a are $\le \sqrt{n}$ and, since they are also prime factors of n, the result follows. ☕

This method, though effective, is not practical when n is large. In later sections, we shall study alternative methods to deal with such cases.

Exercises.

Exercise 7.3. Using Euclid's proof that there are infinitely many primes, show that the n-th prime p_n does not exceed $2^{2^{n-1}}$ whenever n is a positive integer. Conclude that when n is a positive integer, there are at least $n + 1$ primes less than 2^{2^n}.

8. The Fundamental Theorem of Arithmetic

The main objective of this section is to prove the following result, which justifies the expression 'the primes are the building blocks of the integers'.

Theorem 11 (The Fundamental Theorem of Arithmetic)**.** *Let $n \neq 0, 1$ be an integer. Then n has a prime factorization of the form*

$$n = \pm p_1^{a_1} \cdots p_r^{a_r}, \quad a_i \geq 1,$$

where the p_i are distinct prime numbers. Furthermore, up to the order of the p_i, this factorization is unique.

We remark that, however familiar this statement sounds, it is non-trivial. Suppose, for example, that instead of the integers, we work with only with the even integers. In this setting, the numbers $6, 10, 30, 50$ are 'primes', in the sense that they cannot be decomposed into a product of smaller even numbers. Moreover, we have $300 = 10 \cdot 30 = 6 \cdot 50$, showing that the number 300 has two different 'prime decompositions' in the universe of even numbers.

To prove the FTA some preparation is required.

Lemma 3. *Let $a, b \in \mathbb{Z}_{>0}$ satisfy $(a, b) = 1$. If $a \mid bc$, then $a \mid c$.*

Proof. By hypothesis, there exists $k \in \mathbb{Z}$ such that $bc = ak$. Additionally, by Corollary 3, we have

$$(a, b) = 1 = ax + by \quad \text{for some } x, y \in \mathbb{Z}.$$

Then,

$$c = cax + cby = a(cx) + (ak)y = a(cx + ky)$$

so that $a \mid c$ as required. ☕

Remark 8.1. The condition $(a, b) = 1$ in Lemma 3 is necessary. Indeed, if $a = 6,\ b = 3$, and $c = 4$, we have $6 \mid 3 \cdot 4 = 12$ but $6 \nmid 4$ and $6 \nmid 3$.

Corollary 6. *Let $a_1, \ldots, a_n, p$ be integers with p prime. If $p \mid a_1 \cdots a_n$ then $p \mid a_i$ for some i.*

Proof. We will use induction on the number n of integers a_i.

Base: Let $n = 1$. If $p \mid a_1$, then $p \mid a_i$ for $i = 1$;

Hypothesis: Assume that, for any n integers $a_1, \ldots, a_n$, if $p \mid a_1 \cdots a_n$ then $p \mid a_i$ for some i.

Step: We consider now $n + 1$ integers $a_1 \cdots a_n a_{n+1}$. Suppose $p \mid a_1 \cdots a_n a_{n+1} = (a_1 \cdots a_n) \cdot a_{n+1}$.

If $(p, a_1, \ldots, a_n) = 1$. Then, by Lemma 3, we have $p \mid a_{n+1}$. Suppose now $(p, a_1, \ldots, a_n) \neq 1$ Since p is prime, we have $p \mid a_1 \cdots a_n$ and, by the induction hypothesis, we have $p \mid a_i$ for some $i = 1, \ldots, n$ as desired. ☕

We are now in position to prove the Fundamental Theorem of Arithmetic.

Proof of FTA. The proof is divided into two parts. Namely, we first prove that a prime factorization exists and then we show this factorization is unique. For $n < 1$ the result follows from the factorization of $-n$. Let $n > 1$ be an integer.

Existence.

If n is prime, then taking $p_1 = n$ and $a_1 = 1$ gives the desired factorization.

Suppose n is composite. For contradiction, suppose n is the smallest integer without a prime decomposition. We have

$$n = a \cdot b \quad \text{with} \quad 1 < a, b < n,$$

and, by minimality of n, we have $a = p_1 \ldots p_k$ and $b = q_1 \ldots q_t$ where the p_i and q_j are primes. (Here we allow repetition of primes in these factorizations.) Thus

$$n = a \cdot b = p_1 \ldots p_k \cdot q_1 \cdots q_t,$$

is a prime factorization for n, a contradiction.

Uniqueness. Suppose $n = p_1 \ldots p_s = q_1 \ldots q_t$ are two prime decompositions of n. After cancelling common factors and relabeling the remaining primes, we obtain

$$p_1 \cdots p_{s'} = q_1 \cdots q_{t'} \quad \text{with} \quad 0 \leq s' \leq s, \;\; 0 \leq t' \leq t.$$

We will now show by contradiction that $s' = t' = 0$. This means that the previous equality is $1 = 1$; that is, the initial decompositions of n are the same up to ordering of the prime factors. Indeed, suppose there is at least one prime on the left side, that is $s' \geq 1$ and $p_1 \neq 1$. Then, $t' \geq 1$ and $p_i \neq q_j$ for all i, j since common primes were cancelled out. Moreover, since p_1 divides the product on the right hand side, by Corollary 6, we have $p_1 \mid q_j$ for some j. Since q_j is prime, we must have $p_1 = q_j$, contradicting the fact that $p_i \neq q_j$ for all i, j. Thus $s' = t' = 0$. ☕

Example 8.2.

$$\begin{aligned} 756 &= 2 \cdot 378 = 2 \cdot 2 \cdot 189 = 2 \cdot 2 \cdot 3 \cdot 63 \\ &= 2 \cdot 2 \cdot 3 \cdot 7 \cdot 3 \cdot 3 = 2^2 \cdot 3^3 \cdot 7. \end{aligned}$$

Proposition 8. *Let $n \in \mathbb{Z}_{>0}$ have prime factorization $n = p_1^{a_1} \cdots p_n^{a_n}$. Suppose that $d \mid n$. Then, the prime factorization of d is of the form*

$$d = p_1^{b_1} \cdots p_n^{b_n} \quad \textit{with} \quad 0 \leq b_i \leq a_i.$$

Proof. Let $n > 0$ and $d \mid n$. We have $n = dk$ for some integer k. Clearly, any prime divisor of d is a prime divisor of n, so $d = p_1^{b_1} \cdots p_n^{b_n}$ with $b_i \geq 0$. WLOG suppose that $b_1 > a_1$. Then, $b_1 - a_1 \geq 1$ and

$$n = dk \iff p_1^{a_1} \cdots p_n^{a_n} = (p_1^{b_1} \cdots p_n^{b_n})k \iff p_2^{a_2} \cdots p_n^{a_n} = p_1(p_1^{b_1 - a_1 - 1} p_2^{n_2} \cdots p_n^{b_n} k),$$

showing that p_1 divides the left hand side, which is impossible because the $p_i \neq p_1$ for all $i \geq 2$. Thus, $b_1 \leq a_1$, as desired. ☕

Exercises.

Exercise 8.3. An integer $n > 0$ is a *square* if there is $c \in \mathbb{Z}$ such that $n = c^2$. A *square-free integer* is an integer that is not divisible by any squares other than 1. Show that every positive integer can be written as the product of a square (possibly 1) and a square-free integer.

Exercise 8.4. An integer n is called *powerful* if, whenever a prime p divides n, p^2 also divides n. Show that every powerful number can be written as the product of square and a cube (i.e. an integer of the form c^3 for some integer c).

9. The Least Common Multiple

Definition 9.1. Let $a_1, a_2, \dots, a_k \in \mathbb{Z}_{>0}$. The *least common multiple* of $a_1, a_2, \dots, a_k$ is the smallest positive integer that is divisible by all of the a_i. We denote this by $\operatorname{lcm}(a_1, \dots, a_k)$.

Remark 9.2. Let $a_1, a_2, \dots, a_k \in \mathbb{Z}_{>0}$. Note that $\operatorname{lcm}(a_1, \dots, a_k)$ is the smallest positive multiple of all of the a_i. In addition, since the product $a_1 a_2 \cdots a_k > 0$ is a common multiple of all the a_i, the Well Ordering Principle guarantees that $\operatorname{lcm}(a_1, \dots, a_k)$ exists.

Examples 9.3.

(1) The positive multiples of 2 and 3 are, respectively, $\{2, 4, \underline{6}, 8, \dots\}$ and $\{3, \underline{6}, 9, \dots\}$. Then, $\operatorname{lcm}(2, 3) = 6$.
(2) The positive multiples of 6 and 9 are, respectively, $\{6, 12, \underline{18}, \dots\}$ and $\{9, \underline{18}, 27, \dots\}$. Then, $\operatorname{lcm}(6, 9) = 18$.

Proposition 9. *Let $a_1, a_2, \dots a_k \in \mathbb{Z}_{>0}$ have prime decompositions*

$$a_i = p_1^{s_{i,1}} \cdots p_n^{s_{i,n}} \qquad \text{for } i = 1, \dots, k,$$

where $s_{i,j} \geq 0$ for all i, j and the p_i are distinct primes. Then,

$$(a_1, a_2, \dots, a_k) = p_1^{\min(s_{i,1})} \cdots p_n^{\min(s_{i,n})} \qquad \text{and} \qquad \operatorname{lcm}(a_1, a_2, \dots, a_k) = p_1^{\max(s_{i,1})} \cdots p_n^{\max(s_{i,n})},$$

where $\min(s_{i,j})$ and $\max(s_{i,j})$ denote the minimum and maximum element of the set of exponents $\{s_{1,j}, \dots, s_{n,j}\}$ respectively.

Proof. Let p be a prime and let p^s denote the largest power of p dividing $(a_1, \dots, a_k)$. For $i = 1, \dots, k$, write

$$a_i = p^{e_i} m_i \qquad \text{with} \qquad (m_i, p) = 1.$$

Since $p^s \mid (a_1, \dots, a_k)$, we have $p^s \mid a_i$ for all i. By Proposition 8, it we have $s \leq \min(e_1, \dots, e_k)$. Conversely, $p^{\min(e_1, \dots, e_k)} \mid a_i$ for all i. It now follows from Proposition 5 that

$$p^{\min(e_1, \dots, e_k)} \mid (a_1, \dots, a_k),$$

hence $s = \min(e_1, \dots, e_k)$, as desired. Repeating this argument for each p_i establishes

$$(a_1, a_2, \dots, a_k) = p_1^{\min(s_{i,1})} \cdots p_n^{\min(s_{i,n})}.$$

Now, to prove the second part of the proposition, write $\ell = \operatorname{lcm}(a_1, a_2, \dots, a_k)$ and

$$\ell' = p_1^{\max(s_{i,1})} \cdots p_n^{\max(s_{i,n})}.$$

If $s_{i,j}$ denotes the exponent of the j^{th} prime, p_j, in the decomposition of a_i,

$$a_i = p_1^{s_{i,1}} \cdots p_n^{s_{i,n}} \qquad \text{for } i = 1, \dots, k,$$

then clearly $p_j^{s_{i,j}} \mid \ell'$ for all i, j. Therefore, ℓ' is a multiple of all the a_i. Since ℓ is the smallest multiple of all of the a_i, this means that $\ell \leq \ell'$.

Suppose now that $\ell < \ell'$. Clearly, ℓ does not have any prime factor different from the p_i. Indeed, suppose ℓ contained a prime factor different from $p_1, \dots, p_n$, say

$$\ell = p_1^{b_1} \cdots p_n^{b_n} \cdot p^b,$$

for some integers $b_1, \dots, b_n, b$ and p a prime distinct from $p_1, \dots, p_n$. Since the a_i are made up only of the primes $\{p_1, \dots, p_n\}$ and ℓ denotes the smallest multiple of all of the a_i, dropping p from ℓ would yield a smaller multiple of the a_i, a contradiction.

Now, if

$$\ell < \ell' = p_1^{\max(s_{i,1})} \cdots p_n^{\max(s_{i,n})},$$

it is because one of the exponents in the factorization of ℓ, say (WLOG) the exponent of p_1, is strictly smaller than $\max(s_{i,1})$. Suppose $\max(s_{i,1}) = s_{r,1}$ for some $1 \le r \le k$. But then, the above implies that $a_r \nmid \ell$ because the exponent $s_{r,1}$ of p_1 in the factorization of a_r is strictly larger than the exponent of p_1 in ℓ. This is a contradiction. Thus $\ell = \ell'$ as desired. ☕

The particular case of only two integers a, b is very useful and deserves to be highlighted.

Proposition 10. *Let $a, b \in \mathbb{Z}_{>0}$ have prime decompositions*

$$a = p_1^{a_1} \cdots p_n^{a_n} \quad \textit{and} \quad b = p_1^{b_1} \cdots p_n^{b_n},$$

where $a_i, b_i \ge 0$, and the p_i are distinct primes. Then,

(i) $(a, b) = p_1^{\min(a_1,b_1)} \cdots p_n^{\min(a_n,b_n)}$.
(ii) $\operatorname{lcm}(a, b) = p_1^{\max(a_1,b_1)} \cdots p_n^{\max(a_n,b_n)}$.
(iii) $a \cdot b = (a, b) \cdot \operatorname{lcm}(a, b)$.

Proof. Parts (i) and (ii) follow by Proposition 9 with $k = 2$.

We will prove (iii). Let $a, b \in \mathbb{Z}_{>0}$ have prime decompositions

$$a = p_1^{a_1} \cdots p_n^{a_n} \quad \text{and} \quad b = p_1^{b_1} \cdots p_n^{b_n},$$

where $a_i, b_i \ge 0$ and the p_i are the primes dividing a or b.

Note that $a_i + b_i = \min(a_i, b_i) + \max(a_i, b_i)$. Then, from (i) and (ii) we have

$$\begin{aligned}(a, b) \cdot \operatorname{lcm}(a, b) &= (p_1^{\min(a_1,b_1)} \cdots p_n^{\min(a_n,b_n)}) \cdot (p_1^{\max(a_1,b_1)} \cdots p_n^{\max(a_n,b_n)}) \\ &= p_1^{\min(a_1,b_1)+\max(a_1,b_1)} \cdots p_n^{\min(a_n,b_n)+\max(a_n,b_n)} \\ &= p_1^{a_1+b_1} \cdots p_n^{a_n+b_n} = (p_1^{a_1} \cdots p_n^{a_n})(p_1^{b_1} \cdots p_n^{b_n}) \\ &= a \cdot b.\end{aligned}$$

☕

Remark 9.4. Unlike parts (i) and (ii), which have an analogous version for more than two integers (Proposition 9), part (iii) of Proposition 10 does not generalize in the more direct way; this is illustrated by the exercises at the end of this section.

Example 9.5. We will compute $(756, 2205)$ and $\operatorname{lcm}(756, 2205)$.

We have the prime factorizations $756 = 2^2 \cdot 3^3 \cdot 5^0 \cdot 7^1$ and $2205 = 2^0 \cdot 3^2 \cdot 5^1 \cdot 7^2$, hence

$$(756, 2205) = 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^1 = 63 \quad \text{and} \quad \operatorname{lcm}(756, 2205) = 2^2 \cdot 3^3 \cdot 5^1 \cdot 7^2 = 26460.$$

We note that the above formulas for (a,b) and $\operatorname{lcm}(a,b)$ are great theoretical tools but not practical for computation when large values of a and b are involved. Both formulas require one to compute the prime factorization of both a and b, which is a very hard problem computationally. Instead, we compute ab and use the Euclidean algorithm to compute (a,b) and the third formula to find $\operatorname{lcm}(a,b)$.

Proposition 11. *Let $a_1, a_2 \ldots, a_n \in \mathbb{Z}$. Then* $\operatorname{lcm}(a_1, a_2, \ldots, a_n) = \operatorname{lcm}(a_1, \operatorname{lcm}(a_2, \ldots, a_n))$.

Proof. This follows directly from the formula for the least common multiple in Proposition 9. ☕

Proposition 12. *Let $n, a_1, \ldots, a_k \in \mathbb{Z}$. Suppose that $a_i \mid n$ for all i. Then* $\operatorname{lcm}(a_1, \ldots, a_k) \mid n$.

Proof. Clearly, $a_i \mid n$ for all i if $\operatorname{lcm}(a_1, \ldots, a_k) \mid n$ since $a_i \mid \operatorname{lcm}(a_1, \ldots, a_k)$. For the other direction, we use induction on $k \geq 2$.

Base: Let a_1, a_2, n be integers such that both a_1 and a_2 divide n. Then, we can write their factorizations as follows

$$a_1 = p_1^{e_1} \cdots p_n^{e_n} \qquad a_2 = p_1^{b_1} \cdots p_n^{b_n} \qquad n = p_1^{c_1} \cdots p_n^{c_n} \quad \text{with } e_i, b_i, c_i \geq 0$$

and p_i distinct primes. From Proposition 8, we have $e_i, b_i \leq c_i$, hence $\max(e_i, b_i) \leq c_i$ for all i. Thus, by Propositions 10 and 8, we conclude $\operatorname{lcm}(a_1, a_2) \mid n$.

Hypothesis: The result is true for $k > 2$ integers a_i.

Step: Suppose $a_i \mid n$ for $1 \leq i \leq k+1$ and write $\ell = \operatorname{lcm}(a_1, \ldots, a_k)$. Then, $a_{k+1} \mid n$ and by hypothesis $\ell \mid n$, therefore $\operatorname{lcm}(\ell, a_{k+1}) \mid n$ by the base case. Now from Proposition 11 we have $\operatorname{lcm}(\ell, a_{k+1}) = \operatorname{lcm}(a_1, \ldots, a_{k+1}) \mid n$, as desired. ☕

Proposition 13. *Let $a_1, \ldots, a_n \in \mathbb{Z}$ be pairwise coprime. Then* $\operatorname{lcm}(a_1, \ldots, a_n) = a_1 \cdots a_n$.

Proof. We use induction on n.

Base: Let a_1, a_2 be coprime. Then $(a_1, a_2) = 1$ and Proposition 10 (iii) gives $\operatorname{lcm}(a_1, a_2) = a_1 a_2$.

Hypothesis: Assume $\operatorname{lcm}(a_1, \ldots, a_n) = a_1 \cdots a_n$ for any choice of n pairwise coprime integers.

Step: Let $a_1, \ldots, a_{n+1}$ be pairwise coprime integers. We have,

$$\operatorname{lcm}(a_1, \ldots, a_{n+1}) = \operatorname{lcm}(\operatorname{lcm}(a_1, \ldots, a_n), a_{n+1}) = \operatorname{lcm}(a_1 \cdots a_n, a_{n+1}) = a_1 \cdots a_{n+1},$$

where the first equality follows from Proposition 11, the second by induction hypothesis, and the third by the base case (because $(a_1 \cdots a_n, a_{n+1}) = 1$). ☕

Proposition 14. *Let n_1, n_2 be coprime integers. If $d \mid n_1 n_2$, then there are unique integers $d_1 \mid n_1$ and $d_2 \mid n_2$ such that $d = d_1 d_2$. Conversely, any such product is a divisor of $n_1 n_2$.*

Proof. Consider the prime factorizations

$$n_1 = p_1^{a_1} \cdots p_k^{a_k} \quad \text{and} \quad n_2 = q_1^{b_1} \cdots q_r^{b_r}.$$

Since $(n_1, n_2) = 1$ we have that $p_i \neq q_i$ for all i, j and the prime factorization of $n_1 n_2$ is

$$n_1 n_2 = p_1^{a_1} \cdots p_k^{a_k} q_1^{b_1} \cdots q_r^{b_r}.$$

Let d be a divisor of n_1n_2. Then, by Proposition 8, we have

$$d = p_1^{s_1} \cdots p_k^{s_k} q_1^{e_1} \cdots q_r^{e_r},$$

where $0 \le s_i \le a_i$ and $0 \le e_j \le b_j$. Now let $d_1 = (n_1, d)$ and $d_2 = (n_2, d)$. From Proposition 10 (i), we have

$$d_1 = p_1^{s_1} \cdots p_k^{s_k} \quad \text{and} \quad d_2 = q_1^{e_1} \cdots q_r^{e_r},$$

which clearly satisfy $d_i \mid n_i$ and $d = d_1d_2$. Suppose now $d = d'_1d'_2$ and $d'_i \mid n_i$. Since $(n_1, n_2) = 1$ we have also $(d'_1, n_2) = 1$ and $(d'_2, n_1) = 1$, therefore $d'_i = (d, n_i) = d_i$, showing the decomposition $d = d_1d_2$ is unique.

Conversely, let d_1 and d_2 be divisors of n_1 and n_2, respectively. Then, by Proposition 8 we have

$$d_1 = p_1^{s_1} \cdots p_k^{s_k} \quad \text{and} \quad d_2 = q_1^{e_1} \cdots q_r^{e_r},$$

where $0 \le s_i \le a_i$ and $0 \le e_j \le b_j$. Moreover, from the same proposition and the prime factorizations of the products d_1d_2 and n_1n_2 (which are the product of the factorizations of each factor) we conclude that $d_1d_2 \mid n_1n_2$, as desired. ☕

Exercises.

Exercise 9.6. Show that, $abc = \gcd(a, b, c) \operatorname{lcm}(a, b, c)$ does not hold for general $a, b, c \in \mathbb{Z}$ by finding a counterexample.

Exercise 9.7. Prove that, for all $a, b, c \in \mathbb{Z}_{>0}$, we have $abc = \gcd(bc, ac, ab) \operatorname{lcm}(a, b, c)$.

10. Primes of the Form $4k+3$

In this section, we will prove the following particular case of Dirichlet's Density Theorem (Theorem 10).

Theorem 12. *There are infinitely many primes of the form $4k+3$ for $k \in \mathbb{Z}$.*

We will need the following two auxiliary results.

Lemma 4. *Let n be an integer. Then n is of the form $4k$, $4k+1$, $4k+2$, or $4k+3$. In particular, if n is odd, then it is of the form $4k+1$ or $4k+3$.*

Proof. Dividing n by 4 via the division algorithm (Theorem 4) yields

$$n = 4k + r, \quad 0 \le r \le 3.$$

Clearly, the four possible forms in the statement are in correspondence with the value of r. Suppose now $n = 4k$ or $n = 4k+2$. Then $2 \mid n$, hence n is even. ☕

Lemma 5. *Let a, b be integers of the form $4k+1$. Then ab is also of the form $4k+1$.*

Proof. Write $a = 4k_a + 1$ and $b = 4k_b + 1$. Then,

$$a \cdot b = (4k_a + 1)(4k_b + 1) = 16k_ak_b + 4k_a + 4k_b + 1 = 4(4k_ak_b + k_a + k_b) + 1.$$

☕

Proof of Theorem 12. We will proceed using proof by contradiction. Indeed, suppose there are only finitely many primes of the form $4k+3$. Denote these primes $p_0 = 3, p_1, p_2, \dots, p_s$ and consider the number

$$Q = 4p_1p_2 \cdots p_s + 3.$$

Clearly, $2 \nmid Q$, hence the prime factorization of Q (which exists by Theorem 11) contains only odd primes. By Lemma 4, the primes in this factorization are all of the form $4k+1$ or $4k+3$. If all the primes occurring in the prime factorization of Q are of the form $4k+1$, by Lemma 5, we conclude that Q is also of the form $4k+1$. Here, Q is of the form $4k+3$, so that there is at least one prime factor of Q which is of the form $4k+3$.

Let $p \mid Q$ be of the form $4k+3$. Thus $p = p_i$ for some i. If $p = 3$, then $3 \mid (Q-3) = 4p_1 \cdots p_s$, a contradiction. If $p = p_i \neq 3$, then $p \mid (Q - 4p_1 \cdots p_s) = 3$, a contradiction. Hence there are infinitely many primes of the form $4k+3$. ☕

Example 10.1. The first few values of $4k+3$ are $3, 7, 11, 15, 19, 23, 27$, so that clearly the formula generates both primes and composite numbers. Theorem 12 guarantees that we will always find larger and larger values of k giving rise to new primes.

Exercises.

Exercise 10.2. Give a counterexample to show that Lemma 5 is false if we replace $4k+1$ by $4k+3$.

11. Linear Diophantine Equations

Definition 11.1. Any equation with one or more variables to be solved in the integers is called a *Diophantine Equation.*

Examples 11.2. The equations

$$3x = 1, \qquad 2x + 2y = 3, \qquad x^2 + z^2 = y^2$$

are Diophantine equations when we are only interested in integer solutions. For example, the first equation has solution $x = 1/3$. However, viewed as a Diophantine equation in $\mathbb{Z}$, this equation has no solutions.

Definition 11.3. Let $a_1, \dots, a_n \in \mathbb{Z}_{\neq 0}$. A Diophantine equations of the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \qquad \text{with } b \in \mathbb{Z}$$

is a *linear Diophantine equation in n variables $x_1, \dots, x_n$.*

Examples 11.4.

(1) $3x = 1$ and $2x + 2y = 3$ are linear.
(2) $x^2 + z^2 = y^2$ and $3xy = 10$ are non-linear.

Our objective in this section is to prove Theorem 14 which gives a complete resolution of linear Diophantine equations in two variables. The case of one variable follows directly from the definition of divisibility.

Theorem 13. *Let $a, b \in \mathbb{Z}$ with $a \neq 0$. The equation $ax = b$ has a unique solution if and only if $a \mid b$. When a solution exists, necessarily, it is given by $x = \frac{b}{a}$.*

Theorem 14. *Let $a, b, c \in \mathbb{Z}$, with $a, b \neq 0$. Write $d = (a, b)$. Consider the equation*

$$ax + by = c. \tag{11.5}$$

(A) The equation (11.5) has an integer solution (x_0, y_0) if and only if $d \mid c$.
(B) Suppose $d \mid c$ so that there is a solution (x_0, y_0) by part (A). Then, all the solutions to (11.5) are given by the formulas

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t \quad \textit{with} \;\; t \in \mathbb{Z}.$$

Proof. We have $a = da'$ and $b = db'$ with $a', b' \in \mathbb{Z}$. By Corollary 5 we know that $(a', b') = 1$.

We will now prove part (A). Suppose first that $ax + by = c$ has a solution (x_0, y_0). Then,

$$ax_0 + by_0 = c \iff d(a'x_0) + d(b'y_0) = d(a'x_0 + b'y_0) = c \implies d \mid c.$$

Conversely, suppose $d \mid c$. That is, $c = dt$ with $t \in \mathbb{Z}$. From Theorem 6, we know there are $x_1, y_1 \in \mathbb{Z}$ such that

$$ax_1 + by_1 = d \iff a(tx_1) + b(ty_1) = dt = c.$$

Then, $x_0 = tx_1$, $y_0 = ty_1$ is a solution to $ax + by = c$.

We now prove (B). Suppose $d \mid c$ and (x_0, y_0) is a solution to $ax + by = c$. Let $t \in \mathbb{Z}$. We compute

$$a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t = ax_0 + by_0 = c,$$

showing that the formula in the statement produces solutions to $ax + by = c$. To finish the proof, it remains to show that all solutions are given by the formula above. Let (x_1, y_1) be another solution. We define the quantities $t_x = x_1 - x_0$ and $t_y = y_1 - y_0$ and compute

$$at_x + bt_y = ax_1 - ax_0 + by_1 - by_0 = (ax_1 + by_1) - (ax_0 + by_0) = c - c = 0.$$

Then,

$$\begin{aligned} bt_y = -at_x &\iff d\left(\frac{b}{d}\right)t_y = -d\left(\frac{a}{d}\right)t_x \quad \text{ where } d = (a,b) \\ &\iff b't_y = -a't_x, \quad \text{ where } a' = \frac{a}{d}, b' = \frac{b}{d}. \end{aligned}$$

Since $(a', b') = 1$, by Lemma 3, we have $b' \mid t_x$, that is $t_x = b't$ for some $t \in \mathbb{Z}$. Then, $b't_y = -a'b't \implies t_y = -a't$. Therefore,

$$x_1 = x_0 + t_x = x_0 + b't = x_0 + \frac{b}{d}t \quad \text{ and } \quad y_1 = y_0 + t_y = y_0 - a't = y_0 - \frac{a}{d}t,$$

showing that (x_1, y_1) is obtained from (x_0, y_0) by the formula in the statement, as desired. ☕

Example 11.6. We will solve the equation $154x + 35y = 7$.

In Example 6.4, we have computed $d = (154, 35) = 7$ and, since $d \mid 7$, there exist solutions by part (A) of Theorem 14. Indeed, in the same example, we also computed the particular solution $(x_0, y_0) = (-2, 9)$. Therefore, by part (B) of Theorem 14, the general solution is given by

$$x = -2 + 5t, \qquad y = 9 - 22t, \quad t \in \mathbb{Z}.$$

In particular, taking $t = 1$ gives the particular solution $(x_1, y_1) = (3, -13)$.

Example 11.7. Consider the equation $154x + 35y = 24$.

Since $d = (154, 35) = 7 \nmid 24$, there are no solutions by part (A) of Theorem 14.

Example 11.8. Consider the equation $154x + 35y = 21$.

Since $d = (154, 35) = 7 \mid 21$, this equation has solutions in $\mathbb{Z}$. Example 11.6 shows that $154x + 35y = 7$ has the solution $x_1 = -2$ and $y_1 = 9$. Then, $154x + 35y = 21$ has the solution $x_0 = 3x_1 = -6$, $y_0 = 3y_1 = 27$. We conclude that the general solution is given by

$$x = -6 + 5t, \quad y = 27 - 22t \quad \text{ for } t \in \mathbb{Z}.$$

Exercises.

Exercise 11.9. A shopper spends a total of \$5.49 for oranges, which cost 18¢ each, and grapefruit, which cost 33¢ each. What is the minimum number of pieces of fruit the shopper could have bought?

12. Irrational Numbers

Any element in the set rational numbers $\mathbb{Q}$ is denoted as a fraction, a/b, where $a, b \in \mathbb{Z}$ with $b \neq 0$. By cancelling out the common factors of a and b we may obtain another fraction, a'/b'. This new fraction a'/b' represents the same rational number $a/b = a'/b'$, but with a' and b' now coprime. Recall the inclusions $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Definition 12.1. We say that a real number $x \in \mathbb{R}$ is *irrational* if $x \notin \mathbb{Q}$.

We will prove the following standard fact using two techniques we have learned so far.

Theorem 15. *The number $\sqrt{2}$ is irrational.*

Proof 1. Suppose, for contradiction, that $\sqrt{2}$ is rational. Then, by definition of the rationals, $\sqrt{2} = a/b$ with a, b positive integers. Consider the set

$$S = \{k\sqrt{2} \mid k \text{ and } k\sqrt{2} \text{ are positive integers }\}.$$

Note that this set is non-empty since $a = b\sqrt{2} \in S$. It follows by the WOP that there exists a smallest positive element in S, say $s = t\sqrt{2}$ with $t \in \mathbb{Z}_{>0}$. We claim that $s\sqrt{2} - s \in S$ and $s\sqrt{2} - s < s$, obtaining a contradiction with minimality of s, and completing the proof.

Indeed, note that $s \in S$ is an integer by definition of S. Additionally, since $t \in \mathbb{Z}_{>0}$, it follows that

$$s\sqrt{2} = t\sqrt{2} \cdot \sqrt{2} = 2t \quad \text{and} \quad s - t$$

are integers. Moreover,

$$s\sqrt{2} - s = s\sqrt{2} - t\sqrt{2} = (s-t)\sqrt{2},$$

so that $s\sqrt{2} - s \in S$, provided that we show $s - t$ is positive. This is the same as showing that $(s-t)\sqrt{2}$ is positive, which is true because

$$(s-t)\sqrt{2} = s\sqrt{2} - s = s(\sqrt{2} - 1) \quad \text{and} \quad (\sqrt{2} - 1), s > 0.$$

Therefore, $s\sqrt{2} - s \in S$ and since $\sqrt{2} - 1 < 1$ we also have $s\sqrt{2} - s < s$, as desired. ☕

Proof 2. Suppose, for contradiction, that $\sqrt{2}$ is rational. Then, by definition of the rationals, $\sqrt{2} = a/b$ with a, b coprime positive integers. Hence,

$$\sqrt{2} = a/b \implies 2b^2 = a^2 \implies 2 \mid a$$

because 2 is a prime dividing the product $a^2 = a \cdot a$, so it divides one of the factors. Therefore, $a = 2k$ for some $k \in \mathbb{Z}$ and, replacing the above gives,

$$2b^2 = a^2 = (2k)^2 \iff b^2 = 2k^2 \implies 2 \mid b,$$

showing that both a, b are divisible by 2, contradicting the fact that $(a, b) = 1$. ☕

The following theorem provides a criterion to decide if a number is irrational.

Theorem 16. *Let $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ be a polynomial with coefficients $c_i \in \mathbb{Z}$. Suppose that the real number α satisfies $f(\alpha) = 0$. Then α is either an integer or irrational.*

Proof. Let $\alpha \in \mathbb{R}$ satisfy $f(\alpha) = 0$. If α is irrational we are done. Suppose that $\alpha = a/b \in \mathbb{Q}$; we shall show that $\alpha \in \mathbb{Z}$. That is, $b = \pm 1$.

From $f(\alpha) = 0$, we see that

$$\left(\frac{a}{b}\right)^n + c_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + c_1\left(\frac{a}{b}\right) + c_0 = 0$$

and, multiplying by b^n, we obtain

$$a^n + c_{n-1}a^{n-1}b + \cdots + c_1ab^{n-1} + c_0b^n = 0 \iff a^n = b(-c_{n-1}a^{n-1} - \cdots - c_1ab^{n-2} - c_0b^{n-1}),$$

showing that $b \mid a^n$. Now, if $b \neq \pm 1$, any prime factor of b is also a prime factor of a, a contraction with $(a, b) = 1$. Thus $b = \pm 1$ and $\alpha = \pm a \in \mathbb{Z}$, as desired. ☕

Corollary 7. *Let $a, m \in \mathbb{Z}_{>0}$ satisfy $a \neq k^m$ for $k \in \mathbb{Z}$ so that the real number $\sqrt[m]{a}$ is not an integer. Then, $\sqrt[m]{a}$ is irrational.*

Proof. The number $\sqrt[m]{a}$ satisfies $f(\sqrt[m]{a}) = 0$ where $f(x) = x^m - a$. By hypothesis, $\sqrt[m]{a} \notin \mathbb{Z}$ then $\sqrt[m]{a}$ is irrational by Theorem 16. ☕

Using this corollary, we can easily give examples of irrational numbers; in particular, we obtain another proof of Theorem 15.

Example 12.2. The numbers $\sqrt{2}$, $\sqrt{6}$, $\sqrt[3]{5}$ and $\sqrt[10]{19}$ are irrational.

Exercises.

Exercise 12.3. Show that $\sqrt{5} + \sqrt{3}$ is irrational.

Exercise 12.4. Show that $\log_2 3$ is an irrational number.

13. Congruences

Definition 13.1. Let $a, b, m \in \mathbb{Z}$ with $m > 0$. We say that a *is congruent to* b *modulo* m if and only if $m \mid a - b$. We will write $a \equiv b \pmod{m}$ to denote that a and b are congruent modulo m and $a \not\equiv b \pmod{m}$ if they are not. We call m the *congruence modulus*.

Examples 13.2.

(a) $9 \equiv 3 \pmod{3}$ because $3 \mid (9 - 3) = 6$.
(b) $7 \equiv 1 \pmod{2}$ because $2 \mid (7 - 1)$.
(c) $8 \equiv 0 \pmod{2}$ because $2 \mid 8 - 0 = 8$.
(d) If $n = 4k + 3$, then $4 \mid (n - 3)$ and $n \equiv 3 \pmod{4}$.
(e) If $n = 4k + 1$, then $4 \mid (n - 1)$ and $n \equiv 1 \pmod{4}$.
(f) For all $a, b \in \mathbb{Z}$ we have $a \equiv b \pmod{1}$ because $1 \mid a - b$.
(g) $a \equiv 1 \pmod{2}$ for all odd integer $a = 2k + 1$.
(h) $a \equiv 0 \pmod{2}$ for all even integer $a = 2k$.

Using the language of congruences we can often state theorems in a more compact way; in particular, we can now rephrase Lemma 5 and Theorem 12 as follows:

Lemma 6. *Let $a, b \in \mathbb{Z}$ satisfy $a, b \equiv 1 \pmod{4}$. Then $ab \equiv 1 \pmod{4}$.*

Theorem 17. *There are infinitely many primes p such that $p \equiv 3 \pmod{4}$.*

We will show that Lemma 6 is a special case of a general basic property of congruences (see Corollary 10), but first we need to introduce other elementary properties and definitions.

Proposition 15. *Let $m \in \mathbb{Z}_{>0}$. Then, the relation of congruence modulo m is an equivalence relation in $\mathbb{Z}$. More precisely, for all $a, b, c \in \mathbb{Z}$, we have*

(i) $a \equiv a \pmod{m}$ **(reflexivity)**;
(ii) $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$ **(symmetry)**;
(iii) $a \equiv b,\ b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$ **(transitivity)**.

Proof. Let $a, b, c, m \in \mathbb{Z}$ with $m > 0$.

(i) Clearly $m \mid (a - a) = 0$, so $a \equiv a \pmod{m}$.

(ii) Since $a \equiv b \pmod{m}$, we have $a - b = mk$ for some $k \in \mathbb{Z}$. Then $b - a = m(-k)$, so that $m \mid b - a \iff b \equiv a \pmod{m}$.

(iii) We have $a - b = mk_1$, $b - c = mk_2$ for $k_1, k_2 \in \mathbb{Z}$; then

$$a - c = (a - b) + (b - c) = mk_1 + mk_2 = m(k_1 + k_2) \iff a \equiv c \pmod{m}.$$

☕

Fix a congruence modulus $m > 0$. Since the relation of congruence mod m is an equivalence relation, it divides $\mathbb{Z}$ into disjoint equivalence classes. The equivalence class of an integer a is the set of integers which are congruent to a modulo m. We call it the *congruence class of a mod m* and denote it by $[a]$. That is, for an integer a, we have

$$[a] := \Big\{ x \in \mathbb{Z} \,:\, x \equiv a \pmod{m} \Big\}.$$

We say that a is a *representative* of the class; we can choose any element $y \in [a]$ as a representative, in which case we have $[y] = [a]$. This is illustrated by the following examples.

Example 13.3. Let $m = 4$. We have $\mathbb{Z} = [0] \cup [1] \cup [2] \cup [3]$, where

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} \ : \ x \equiv 0 \pmod 4\} = \{x \in \mathbb{Z} \ : \ x - 0 = 4k \text{ with } k \in \mathbb{Z}\} \\
&= \{\ldots, -8, -4, 0, 4, 8, \ldots\} \\
[1] &= \{x \in \mathbb{Z} \ : \ x \equiv 1 \pmod 4\} = \{x \in \mathbb{Z} \ : \ x - 1 = 4k \text{ with } k \in \mathbb{Z}\} \\
&= \{x \in \mathbb{Z} \ : \ x = 1 + 4k \text{ with } k \in \mathbb{Z}\} = \{\ldots, -7, -3, 1, 5, 9, \ldots\} \\
[2] &= \{\ldots, -6, -2, 2, 6, \ldots\} \\
[3] &= \{\ldots, -5, -1, 3, 7, 11, \ldots\}
\end{aligned}$$

In particular, $[0] = [-4]$, $[1] = [9]$, $[2] = [6]$ and $[3] = [-1]$.

Example 13.4. Let $m = 3$. We have $\mathbb{Z} = [0] \cup [1] \cup [2]$, where

$$[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

$$[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$

$$[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

In particular, $[0] = [3]$, $[1] = [-2]$ and $[2] = [-1]$.

Example 13.5. Let $m = 2$. We have $\mathbb{Z} = [0] \cup [1]$, where

$$[0] = \{ \text{ even integers } \}$$

$$[1] = \{ \text{ odd integers } \}$$

In particular, $[0] = [4]$ and $[1] = [3]$.

It follows from the previous discussion that every integer a belongs to an unique congruence class modulo m. Given a, the next proposition determines the smallest non-negative representative of the congruence class, $[a]$.

Proposition 16. *Let $a, m \in \mathbb{Z}$ with $m > 0$. Then $a \equiv r \pmod m$, where r is the remainder of the division of a by m.*

In particular, $[a] = [r]$ and a is congruent to exactly one integer in $\{0, 1, 2, \ldots, m-1\}$.

Proof. Let $S = \{0, 1, 2, \ldots, m-1\}$. By the division algorithm we obtain

$$a = m \cdot q + r \qquad \text{with} \qquad r \in S.$$

Then, $a - r = m \cdot q \iff a \equiv r \pmod m$, which proves the first statement.

Suppose now $a \equiv r_1 \pmod m$ and $a \equiv r_2 \pmod m$ with $r_1, r_2 \in S$. Then, $r_1 \equiv r_2 \pmod m$ and $m \mid r_1 - r_2$. Moreover, since r_1, r_2 are in S, we see that $-(m-1) \le r_1 - r_2 \le m - 1$. But now we have just shown that these two conditions

$$m \mid r_1 - r_2, \qquad \text{and} \qquad -(m-1) \le r_1 - r_2 \le m - 1$$

are simultaneously satisfied. Since the only multiple of m in the range $[-(m-1), m+1]$ is zero, we must have $r_1 - r_2 = 0$, hence $r_1 = r_2$. ☕

The following two results follow from the theory so far. We highlight them in a format that we will use several times later on.

Corollary 8. *Let $a, b, m \in \mathbb{Z}$ with $m > 0$. If $a \equiv b \pmod{m}$ and $0 \le a, b \le m-1$, then $a = b$.*

Corollary 9. *Let $a, m \in \mathbb{Z}$ with $m > 0$. Suppose $a \equiv r \pmod{m}$ with $0 \le r \le m-1$. Then,*

$$(a, m) = 1 \iff (r, m) = 1.$$

Proof. We have $a = mk + r$ for some integer k. Then $(a, m) = (m, r)$ by Lemma 1. ☕

Definition 13.6. A set $S \subset \mathbb{Z}$ such that every integer is congruent mod m to exactly one integer in S is called a *complete residue system modulo m*.

Example 13.7. From Proposition 16 it follows that $S = \{0, 1, \dots, m-1\}$ is a complete residue system modulo m.

Definition 13.8. We define $\mathbb{Z}/m\mathbb{Z}$, the *integers modulo m*, to be the set of congruence classes modulo m, i.e

$$\frac{\mathbb{Z}}{m\mathbb{Z}} := \Big\{[0], [1], \dots, [m-1]\Big\}.$$

Example 13.9. Let $m = 3$. Then,

$$\frac{\mathbb{Z}}{3\mathbb{Z}} = \Big\{[0], [1], [2]\Big\} = \Big\{[3], [7], [2]\Big\},$$

where the second equality holds because we have only changed the representative of the congruence classes $[0]$ and $[1]$.

In what follows, we will see that $\mathbb{Z}/m\mathbb{Z}$ has properties similar to the integers. In particular, we shall soon define addition and multiplication in $\mathbb{Z}/m\mathbb{Z}$. However, let us first observe a very important difference between $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}$: there is no cancellation law in $\mathbb{Z}/m\mathbb{Z}$. More precisely, in the integers we have

$$\text{if } \ a, b \in \mathbb{Z} \ \text{ satisfy } \ ab = 0, \ \text{ then } a = 0 \ \text{ or } \ b = 0$$

whilst, for example, in $\mathbb{Z}/4\mathbb{Z}$ we have

$$2 \cdot 2 \equiv 4 \equiv 0 \pmod{4} \quad \text{ and } \quad 2 \not\equiv 0 \pmod{4}.$$

To define addition and multiplication in $\mathbb{Z}/m\mathbb{Z}$ we will need the following result.

Theorem 18. *Let $m \in \mathbb{Z}_{>0}$. Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then,*

(i) $a + c \equiv b + d \pmod{m}$;
(ii) $a - c \equiv b - d \pmod{m}$;
(iii) $ac \equiv bd \pmod{m}$.

Proof. By hypothesis, we have $b = a + km$ and $d = c + k'm$ for some $k, k' \in \mathbb{Z}$.

(i) Adding the two equalities gives

$$\begin{aligned} a + c + (k + k')m = b + d &\iff (a + c) - (b + d) = m(-k - k') \\ &\iff a + c \equiv b + d \pmod{m}. \end{aligned}$$

(ii) Similar to (i).

(iii) We conpute

$$\begin{aligned} bd = (a+km)(c+k'm) = ac + ak'm + ckm + kk'm^2 \\ \iff bd - ac = m(ak' + ck + kk'm) \\ \iff bd \equiv ac \pmod{m} \end{aligned}$$

☕

Corollary 10. *The Lemma 6 holds.*

Proof. Take $m = 4$ and let $a, c \in \mathbb{Z}$ satisfy $a, c \equiv 1 \pmod{4}$. Then, by part (iii) of Theorem 18 with $b = d = 1$, we conclude $ac \equiv 1 \cdot 1 \equiv 1 \pmod{4}$, as desired. ☕

Example 13.10. Let $m = 5$. To compute $49^2 \pmod{5}$ we calculate that $49^2 = 2401 = 480{\cdot}5{+}1$ and by Proposition 16, it follows that $49^2 \equiv 1 \pmod{5}$. However, Theorem 18 allows for the much quicker calculations

$$49^2 \equiv 4^2 \equiv 16 \equiv 1 \pmod{5} \quad \text{or} \quad 49^2 \equiv (-1)^2 \equiv 1 \pmod{5}.$$

Remark 13.11. Theorem 18 does not hold for exponentiation. That is,

$$c \equiv d \pmod{m} \not\Longrightarrow a^c \equiv a^d \pmod{m}.$$

For example, taking $m = 3$, $a = 2$, $d = 3$, and $c = 6$, we have $3 \equiv 6 \pmod{3}$ but

$$2^3 \equiv 8 \equiv 2 \pmod{3} \quad \text{and} \quad 2^6 \equiv 2^3 \cdot 2^2 \equiv 4 \equiv 1 \pmod{3}$$

are not congruent mod 3.

We can now define arithmetic operations in $\mathbb{Z}/m\mathbb{Z}$.

Definition 13.12. Define the addition, multiplication and multiplication by scalar operations in $\mathbb{Z}/m\mathbb{Z}$ as follows. Let $[r], [s] \in \mathbb{Z}/m\mathbb{Z}$ and $\lambda \in \mathbb{Z}$.

Addition: $[r] + [s] := [r + s]$;
Multiplication: $[r] \cdot [s] := [r \cdot s]$;
Multiplication by scalar: $\lambda \cdot [r] := [\lambda \cdot r]$.

Note that, in the above definitions, we use the concrete representatives $r, s \in \mathbb{Z}$ to calculate the result of the operation. For example, for $m = 5$, we have $[2] + [3] = [2 + 3] = [5]$, but, since $[2] = [7]$ and $[3] = [-7]$, in order for the definition to make sense, we also need that $[7] + [-7] = [7 + (-7)] = [0]$ is equal to $[5]$, which is the case. Clearly, for the operations to be well defined, we need a similar compatibility for any other choice of representatives. This is the content of the next proposition.

Proposition 17. *The operations in Definition 13.12 are well defined. That is, their output is independent of the choice of representatives.*

Proof. Let $r' \in [r]$ and $s' \in [s]$, that is, $r' \equiv r \pmod{m}$ and $s' \equiv s \pmod{m}$. Then, by part (i) of Theorem 18, we have

$$r + s \equiv r' + s' \pmod{m} \iff [r + s] = [r' + s'],$$

hence

$$[r] + [s] := [r + s] = [r' + s'] =: [r'] + [s'].$$

This shows that addition is well defined. Similar arguments show that the other operations are also well-defined. ☕

Example 13.13. We can write tables of addition and multiplication in $\mathbb{Z}/m\mathbb{Z}$. For example, the table of addition in $\mathbb{Z}/3\mathbb{Z}$:

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

Example 13.14. In $\mathbb{Z}/7\mathbb{Z}$, we have $[3]\cdot[6] = [18] = [4] = [-10]$, but since $[3] = [10]$ and $[6] = [-1]$ we also have, more directly, $[3]\cdot[6] = [10]\cdot[-1] = [-10]$.

We have mentioned that, in general, there is no cancellation law in $\mathbb{Z}/m\mathbb{Z}$. For example, when $m = 4$, we have $2\cdot 2 \equiv 0 \pmod 4$ and $2 \not\equiv 0 \pmod 4$. The following is another example of the failure of the cancellation law. For all $a, b \in \mathbb{Z}$ we have $6a \equiv 6b \pmod 3$, because both sides of the congruence are congruent to 0 since $3 \mid 6$. If we just cancel out the 6 (like we do in $\mathbb{Z}$), we get $a \equiv b \pmod 3$ for all a, b, which of course is false since $1 \not\equiv 2 \pmod 3$.

The following lemma can be interpreted as a cancellation law in $\mathbb{Z}/m\mathbb{Z}$ where we allow changing the congruence modulus.

Lemma 7. *Let $a, b, c, m \in \mathbb{Z}$ with $m > 0$ and $c \neq 0$. Write $d = (c, m)$. Then,*

$$c\cdot a \equiv c\cdot b \pmod m \iff a \equiv b \pmod{\frac{m}{d}}.$$

Proof. Suppose first $a \equiv b \pmod{\frac{m}{d}}$. That is, $a - b = \frac{m}{d}\cdot k$ for some $k \in \mathbb{Z}$. Then,

$$da - db = m\cdot k \iff \frac{c}{d}(da - db) = \frac{c}{d}mk \iff ca - cb = m\left(\frac{c}{d}k\right) \iff ca \equiv cb \pmod m.$$

Conversely, suppose $ca \equiv cb \pmod m$. That is $ca - cb = mk$ for $k \in \mathbb{Z}$. Therefore, we also have

$$\frac{m}{d}\cdot k = \frac{c}{d}(a - b) \quad \text{with} \quad \left(\frac{c}{d}, \frac{m}{d}\right) = 1,$$

where the second condition follows from Corollary 5. Then, Lemma 3 implies that

$$\frac{m}{d} \mid a - b \iff a \equiv b \pmod{\frac{m}{d}}.$$

☕

Example 13.15. From Lemma 7, for all $a, b \in \mathbb{Z}$, we have

$$6a \equiv 6b \pmod 3 \iff a \equiv b \pmod{\frac{3}{(3,6)}} \iff a \equiv b \pmod 1,$$

which is true (see Examples 13.2 (f)).

Exercises.

Exercise 13.16. Let $m \in \mathbb{Z}_{>0}$ and let $[r], [s] \in \mathbb{Z}/m\mathbb{Z}$. Prove that multiplication, as defined by

$$[r] \cdot [s] := [r \cdot s],$$

is a well-defined operation on $\mathbb{Z}/m\mathbb{Z}$.

Exercise 13.17. Prove or disprove that $\{-39, 72, -23, 50, -15, 63, -52\}$ is a complete residue system modulo 7.

Exercise 13.18. Find a complete residue system modulo 7 consisting entirely of even integers.

Exercise 13.19. Determine all least positive integers k modulo 16 satisfying $k \equiv 2 \pmod 4$.

14. Fast Modular Exponentiation

In this section, we describe an efficient procedure to deal with exponentials modulo m. More precisely, given $a, k, m \in \mathbb{Z}$ with $m, k \geq 2$, we will describe how to compute $a^k \pmod{m}$ quickly.

The following method, know as *fast modular exponentiation*, consists of 3 main steps.

Step 1: Write the exponent in base 2. That is,

$$k = 2^{r_1} + 2^{r_2} + \cdots + 2^{r_l}, \quad r_1 > r_2 > \cdots > r_l.$$

Step 2: For all powers of 2 which are less than or equal to 2^{r_1}, compute

$$a \pmod{m},\ a^2 \pmod{m},\ a^4 \pmod{m}, \ldots, a^{2^{r_1}} \pmod{m}$$

by successively squaring and reducing the result modulo m.

Step 3: Compute

$$a^k = a^{2^{r_1}+2^{r_2}+\cdots+2^{r_l}} \equiv a^{2^{r_1}} \cdot a^{2^{r_2}} \cdot \ldots \cdot a^{2^{r_l}} \pmod{m},$$

where we use the values computed in Step 2 to obtain the right hand side of the congruence.

Example 14.1. Compute $7^{51} \pmod{17}$.

Step 1: $51 = 2^5 + 2^4 + 2 + 1 = 32 + 16 + 2 + 1$.

Step 2:

$$\begin{aligned} 7 &\equiv 7 \pmod{17} & 7^2 &\equiv 49 \equiv 15 \equiv -2 \pmod{17} \\ 7^4 &\equiv (-2)^2 \equiv 4 \pmod{17} & 7^8 &\equiv 4^2 \equiv 16 \equiv -1 \pmod{17} \\ 7^{16} &\equiv (-1)^2 \equiv 1 \pmod{17} & 7^{32} &\equiv 1^2 \equiv 1 \pmod{17}. \end{aligned}$$

Step 3:

$$7^{51} = 7^{32+16+2+1} = 7^1 \cdot 7^2 \cdot 7^{16} \cdot 7^{32} = 7 \cdot (-2) \cdot 1 \cdot 1 \equiv -14 \equiv 3 \pmod{17}.$$

Example 14.2. In this example, we demonstrate why working with base 2 is efficient in fast modular exponentiation. Suppose we want to compute $7^{51} \pmod{17}$ using base 3, for instance.

We first compute 51 in base 3, obtaining

$$51 = 3^3 + 2 \cdot 3^2 + 2 \cdot 3 = 27 + 18 + 6.$$

Now, by successively taking cubes and reducing modulo 17, we obtain

$$\begin{aligned} 7 &\equiv 7 \pmod{17} & 7^3 &\equiv 3 \pmod{17} \\ 7^9 &\equiv 3^3 \equiv 9 \pmod{17} & 7^{27} &\equiv 9^3 \equiv 14 \pmod{17}. \end{aligned}$$

Now, since

$$7^{51} = 7^{27+18+6} = 7^{27} \cdot 7^{18} \cdot 7^6 \equiv 14 \cdot \left(7^9\right)^2 \cdot \left(7^3\right)^2 \equiv 14 \cdot 9^2 \cdot 3^2 \pmod{17},$$

we see that the above pre-calculations are insufficient, since we must also compute $\left(7^9\right)^2$ and $\left(7^3\right)^2$ modulo 17. Note that this is due to the fact that representations of integers in base 3 (or any other base ≥ 3) can have coefficients other than 0 and 1, which is not the case in base 2.

Exercises.

Exercise 14.3. Find the least positive residue of each of the following.

(a) $3^{10} \pmod{11}$
(b) $5^{16} \pmod{17}$
(c) $2^{12} \pmod{13}$
(d) $3^{22} \pmod{23}$
(e) Can you propose a theorem from the above congruences?

15. The Congruence Method

Before we proceed with the study of congruences, in this section, we will describe an application of congruences to the solution of Diophantine equations.

The following method, called *the congruence method*, may sometimes be used to conclude that certain Diophantine equations have no solutions in $\mathbb{Z}$. The idea behind this method is that if an equation is satisfied in $\mathbb{Z}$, then it has to be satisfied modulo m for all $m > 0$. If, however, we can find a value of m for which it is not satisfied mod m, then we can conclude that there are no solutions in $\mathbb{Z}$. We illustrate this with two examples.

Example 15.1. We will show that $3x^3 + 2 = y^2$ has no integer solutions. Indeed, suppose there are $x_0, y_0 \in \mathbb{Z}$ satisfying $3x_0^3 + 2 = y_0^2$. Since every integer is congruent to itself (see Proposition 15 (i)) we conclude that, for all integers $m > 0$, we have the congruence

$$y_0^2 \equiv y_0^2 = 3x_0^3 + 2 \pmod{m}. \tag{15.2}$$

In particular, taking $m = 3$, we have

$$y_0^2 \equiv 2 \pmod{3},$$

where we have used the fact that $3 \equiv 0 \pmod{3}$.

On the other hand, every integer is congruent modulo 3 to one of $\{0, 1, 2\}$; in particular, $y_0 \equiv 0, 1$ or $2 \pmod{3}$ and we respectively obtain

$$y_0^2 \equiv 0, 1, 4 \equiv 0, 1, 1 \pmod{3}.$$

Thus $y_0^2 \not\equiv 2 \pmod{3}$ and the integer solution x_0, y_0 to equation (15.2) cannot exist, otherwise y_0 satisfies an impossible congruence.

We note that there can be solutions mod m for other values of m. For example, if instead we work modulo $m = 2$, from (15.2) we obtain

$$3x_0^2 + 2 \equiv y_0^2 \pmod{2} \iff x_0^2 \equiv y_0^2 \pmod{2},$$

which is satisfied whenever $x_0 \equiv y_0 \pmod{2}$. For example, take $x_0 = y_0 = 1$. This shows that the existence of solutions mod m says nothing about the existence of solutions in $\mathbb{Z}$.

Example 15.3. We will show that $20y^2 + 2x = 3$ has no integer solutions. Indeed, suppose $x_0, y_0 \in \mathbb{Z}$ is a solution. Taking $m = 2$ and arguing as in the previous example, we get

$$20y_0^2 + 2x_0 \equiv 3 \pmod{2} \iff 0 \equiv 1 \pmod{2},$$

which is impossible. If instead we take $m = 5$, we obtain

$$20y_0^2 + 2x_0 \equiv 3 \pmod{5} \iff 2x_0 \equiv 3 \pmod{5}. \tag{15.4}$$

We have that $x_0 \equiv 0, 1, 2, 3, 4 \pmod{5}$ which implies, respectively,

$$2x_0 \equiv 0, 2, 4, 1, 3 \pmod{5},$$

so $x_0 \equiv 4 \pmod{5}$ satisfies (15.4) and there is no contradiction. We conclude that every integer $x_0 = 4 + 5k$ satisfies the congruence equation (15.4). However, we have shown above that no integer x_0 will satisfy the original equation in $\mathbb{Z}$.

Exercises.

Exercise 15.5. Prove or disprove the following statements

(a) The Diophantine equation $3x^2 - 7y^2 = 2$ has no integral solutions.
(b) The Diophantine equation $x^2 + y^2 + 1 = 4z$ has no integral solutions.

16. Linear Congruences in One Variable

Let $a, b, m \in \mathbb{Z}$ with $m > 0$. Here we consider congruence equations of the form

$$ax \equiv b \pmod{m}, \tag{16.1}$$

which are called *linear congruences in one variable.* Note that in Example 15.3 we have already found a congruence of this type. More precisely, we have shown that the congruence equation $2x \equiv 3 \pmod 5$ admits the unique solution $x \equiv 4 \pmod 5$. We now give further examples.

Example 16.2. Consider the linear congruence equation $10x \equiv 3 \pmod 4$. We have

$$x \equiv 0, 1, 2, 3 \pmod 4 \implies 10x \equiv 0, 10, 20, 30 \equiv 0, 2, 0, 2 \pmod 4,$$

respectively. Hence this equation has no solutions.

Example 16.3. We consider $3x \equiv 9 \pmod 6$. Note that $9 \equiv 3 \pmod 6$ and

$$x \equiv 0, 1, 2, 3, 4, 5 \pmod 6 \implies 3x \equiv 0, 3, 6, 9, 12, 15 \equiv 0, 3, 0, 3, 0, 3 \pmod 6,$$

hence there are three non-congruent solutions

$$x \equiv 1 \pmod 6, \quad x \equiv 3 \pmod 6, \quad x \equiv 5 \pmod 6.$$

The previous examples show that an equation of the form (16.1) can have sets of solutions with different behaviours. This is explained by the following theorem.

Theorem 19. *Let $a, b, m \in \mathbb{Z}$, with $m > 0$. Write $d = (a, m)$.*

(i) If $d \nmid b$ then the equation (16.1) has no solutions.
(ii) Suppose $d \mid b$. Then equation (16.1) has exactly d non-congruent solutions modulo m, which are given by

$$x \equiv x_0 - \frac{m}{d}t, \qquad \textit{where} \qquad 0 \le t \le d - 1,$$

and x_0 is a particular solution.

Proof.

(i) Suppose for contradiction that $x_0 \in \mathbb{Z}$ satisfies $ax_0 \equiv b \pmod m$. By definition of congruence, there exists some $y_0 \in \mathbb{Z}$ such that

$$ax_0 - b = my_0 \iff ax_0 + m(-y_0) = b,$$

meaning that $ax + my = b$ has the solution $(x_0, -y_0)$. Then $(a, m) = d \mid b$ by Theorem 14.

(ii) Suppose $d \mid b$. Then $ax - my = b$ has solutions by Theorem 14. Let (x_0, y_0) be a particular solution. By Theorem 14, the general solution is

$$x = x_0 - \frac{m}{d}t, \quad y = y_0 - \frac{a}{d}t, \quad t \in \mathbb{Z},$$

which gives all the integer solutions satisfying $ax \equiv b \pmod m$.

To finish the proof, we must show that the above formula for x produces exactly d incongruent values modulo m. Indeed, suppose we choose $t_1, t_2 \in \mathbb{Z}$ giving the same value for x modulo m, that is,

$$x_0 - \frac{m}{d}t_1 \equiv x_0 - \frac{m}{d}t_2 \pmod{m}.$$

From here, we see that

$$\begin{aligned} x_0 - \frac{m}{d}t_1 \equiv x_0 - \frac{m}{d}t_2 \pmod{m} &\iff \frac{m}{d}(t_2 - t_1) \equiv 0 \equiv \frac{m}{d}\cdot 0 \pmod{m} \\ &\iff t_2 - t_1 \equiv 0 \pmod{\frac{m}{(m, m/d)}} \quad \text{by Lemma 7} \\ &\iff t_1 \equiv t_2 \pmod{d}, \end{aligned}$$

where we used $\left(m, \frac{m}{d}\right) = \frac{m}{d}$ in the last step. In other words, for t_1, t_2 giving the same value of x modulo m, we must have that $t_1 \equiv t_2 \pmod{d}$. Therefore taking $t \in \{0, 1, \dots, d-1\}$ gives the desired d non-congruent solutions mod m.

☕

We highlight the following special case.

Corollary 11. *Let $a, m \in \mathbb{Z}$, with $m > 0$. The congruence equation*

$$ax \equiv 1 \pmod{m}$$

has exactly one solution modulo m if and only if $(a, m) = 1$.

The solutions to the congruence in this corollary will play a crucial role in everything that follows, so they deserve a special name.

Definition 16.4. Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. We call any integer solution of the congruence $ax \equiv 1 \pmod{m}$ *an inverse of a modulo m.*

Suppose that $x_0 \in \mathbb{Z}$ is an inverse of a mod m. Then $ax_0 \equiv 1 \pmod{m}$ and we have the following equalities in $\mathbb{Z}/m\mathbb{Z}$

$$[ax_0] = [1] \iff [a]\cdot[x_0] = [1].$$

Suppose x_1 is another inverse of a mod m. Corollary 11 shows that x_1 is congruent to x_0 mod m so that $[x_1] = [x_0]$. In other words, the inverse of a mod m is unique when viewed as an element of $\mathbb{Z}/m\mathbb{Z}$. This is summarized by the following definition.

Definition 16.5. Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. The congruence class $[x_0]$ in $\mathbb{Z}/m\mathbb{Z}$ which satisfies $[a]\cdot[x_0] = [1]$ is called *the inverse of $[a]$ in $\mathbb{Z}/m\mathbb{Z}$.* We denote it by $[a]^{-1}$.

Remark 16.6. We note that the use of the term 'inverse' and the notation a^{-1} is analogous to that of the real numbers. Indeed, for all $a \in \mathbb{R}_{\neq 0}$, we call $1/a$ the 'inverse' of a, which we also denote as a^{-1}. This number is also the unique number satisfying $a\cdot(1/a) = 1$.

In practice, despite the fact that a^{-1} makes no sense as an integer, we write $a^{-1} \pmod{m}$ to denote the smallest positive representative of the congruence class $[a]^{-1}$. As an example, in the following tables, we list the inverses modulo $m = 10$ and $m = 5$.

Examples 16.7.

(1) For $m = 10$,

$a \pmod{10}$	0	1	2	3	4	5	6	7	8	9
$a^{-1} \pmod{10}$	–	1	–	7	–	–	–	3	–	9

(2) For $m = 5$,

$a \pmod 5$	0	1	2	3	4
$a^{-1} \pmod 5$	–	1	3	2	4

Note that there are many integers $a \not\equiv 0 \pmod{10}$ which are not invertible, while for $m = 5$, only those congruent to zero have no inverse. This behavior for $m = 5$ holds more generally for all prime numbers.

Corollary 12. *Let $a, p \in \mathbb{Z}$ with p a prime and $a \not\equiv 0 \pmod p$. Then a has an inverse mod p.*

Proof. Since p is prime and $a \not\equiv 0 \pmod p$ we have $(a, p) = 1$. The result follows from Corollary 11. ☕

To find the inverses for $m = 5, 10$ we only have to try a few possibilities due to the small size of m. In general, to compute $a^{-1} \pmod m$, we need to solve the linear Diophantine equation $ax + my = 1$ using the Euclidean Algorithm and back substitution.

Example 16.8. We will compute $17^{-1} \pmod{55}$. Here, we need to solve $17x \equiv 1 \pmod{55}$. We will do this by finding x_0, y_0 satisfying $17x_0 + 55y_0 = 1$, because taking this equality mod 55 gives precisely $17x_0 \equiv 1 \pmod{55}$. This means that $x_0 \pmod{55}$ will be the inverse of 17 mod 55 that we are looking for. First, we find $(17, 55)$ using the Euclidean Algorithm:

$$55 = 17 \cdot 3 + 4$$

$$17 = 4 \cdot 4 + 1$$

$$4 = 1 \cdot 4 + 0,$$

so $(17, 55) = 1$. Secondly, we find a solution (x_0, y_0) to $17x + 55y = (17, 55) = 1$ using back substitution:

$$\begin{aligned}(17, 55) = 1 = 17 - 4 \cdot 4 &= 17 - 4(55 - 17 \cdot 3)\\ &= 17 - 4 \cdot 55 + 12 \cdot 17\\ &= 17 \cdot 13 - 55 \cdot 4,\end{aligned}$$

so $x_0 = 13$ and $y_0 = -4$. We conclude that $17 \cdot 13 \equiv 1 \pmod{55}$ and

$$[17]^{-1} = [13] \quad \text{in } \mathbb{Z}/55\mathbb{Z}.$$

Proposition 18. *Let a, m be coprime integers with $m > 0$ and let $k \in \mathbb{Z}_{>0}$.*
Then $(a^k)^{-1} \equiv (a^{-1})^k \pmod m$.

Proof. We use induction.

Base: For $k = 1$ the result is clear.

Hypothesis: Suppose the result holds for $k \geq 2$.

Step: We have

$$(a^{k+1})^{-1} \equiv (a^k \cdot a)^{-1} \equiv (a^k)^{-1}a^{-1} \equiv (a^{-1})^k a^{-1} \equiv (a^{-1})^{k+1} \pmod{m},$$

as desired, where we used Exercise 16.10 for the second congruence. ☕

In other words, the previous proposition shows that mod m the inverse of a power is the same power of the inverse; therefore, we may use the notation $a^{-k} \pmod{m}$ to denote both $(a^k)^{-1}$ and $(a^{-1})^k$ mod m.

Exercises.

Exercise 16.9. Prove that the inverse of the inverse of a modulo m is a. More precisely, let a^{-1} be an inverse of a modulo m and prove that $(a^{-1})^{-1} \equiv a \pmod{m}$.

Exercise 16.10. Let a^{-1} be an inverse of a modulo m and let b^{-1} be an inverse of b modulo m. Prove that $a^{-1}b^{-1}$ is an inverse of ab modulo m.

Exercise 16.11. Find all least non-negative incongruent solutions of $623x \equiv 511 \pmod{679}$.

17. The Chinese Remainder Theorem

In the previous section, we studied a single congruence in one variable, so it is natural to wonder if something can be said about several congruences in one variable. As motivation, let us consider the following problem:

> *"Find a positive integer having remainder* 2 *when divided by* 3*, remainder* 1 *when divided by* 4*, and remainder* 3 *when divided by* 5*."*

In the language of congruences, this problem translates into finding a positive integer solution x to the following system of congruences

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 1 \pmod 4 \\ x \equiv 3 \pmod 5. \end{cases}$$

The Chinese Remainder Theorem (CRT) is a tool that allows us to solve this and many other systems of congruences.

Theorem 20 (Chinese Remainder Theorem)**.** *Let $n_1, n_2, \dots, n_k \in \mathbb{Z}_{>0}$ be pairwise coprime and $b_1, b_2, \dots, b_k \in \mathbb{Z}$. Consider the system of congruences*

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \\ \quad\vdots \qquad\quad \vdots \\ x \equiv b_k \pmod{n_k}. \end{cases} \tag{17.1}$$

Write $m = n_1 n_2 \dots n_k$. Then, any two solutions x, x' to the system satisfy $x \equiv x' \pmod m$, that is, there is a unique solution modulo m.

Before we give a proof of CRT, let us analyze the congruence equations

$$x \equiv 3 \pmod 7 \qquad \text{and} \qquad x \equiv 2 \pmod 3.$$

From the first congruence, we have $x = 3 + 7k$ for some $k \in \mathbb{Z}$. Substituting this equation into the second congruence yields

$$x = 3 + 7k \equiv 2 \pmod 3 \iff k \equiv 2 \pmod 3.$$

Then $k = 2 + 3t$ for $t \in \mathbb{Z}$ and replacing this for k gives

$$x = 3 + 7k = 3 + 7(2 + 3t) = 17 + 21t.$$

In particular, taking $t = 0$ and $t = 1$ gives, respectively, $x = 17$ and $x = 38$, and we can easily double-check that these values satisfy the two initial congruences. Note that 21 is the modulus predicted by the conclusion of CRT. Hence $x = 17 + 21t \equiv 17 \pmod{21}$ must be the unique solution modulo 21 predicted by CRT.

For the proof of CRT, we will need the following basic fact, which will come of use in the remainder of these notes.

Proposition 19. *Let $a, b, m, n \in \mathbb{Z}$ with $m, n > 0$ and $n \mid m$. If $a \equiv b \pmod m$, then $a \equiv b \pmod n$.*

Proof. We have $m = nm'$ for some $m' \in \mathbb{Z}$ and

$$a - b = mk = (nm')k \implies n \mid a - b \iff a \equiv b \pmod{n}.$$

☕

We will now prove the Chinese Remainder Theorem.

Proof of CRT. This proof has two parts. Namely, we first show that a solution exists by constructing it explicitly, and then we show that this solution is unique modulo $(n_1 n_2 \cdots n_k)$.

Existence. Let $m = n_1 n_2 \cdots n_k$ and $m_i = m/n_i$. Since $(n_i, n_j) = 1$ for all $i \neq j$, we have $(m_i, n_i) = 1$, therefore the congruence equation $m_i y \equiv 1 \pmod{n_i}$ has a solution y_i. Consider the integer

$$x = b_1 m_1 y_1 + b_2 m_2 y_2 + \cdots + b_k m_k y_k$$

and observe that $n_i \mid m_i$ for all $i \neq j$. Proposition 19 now implies

$$\begin{aligned} x &\equiv 0 + 0 + \cdots + b_i m_i y_i + \cdots + 0 \equiv b_i m_i y_i \pmod{n_i} \\ &\equiv b_i \pmod{n_i}, \end{aligned}$$

where the last congruence follows because $m_i y_i \equiv 1 \pmod{n_i}$.

Uniqueness. Suppose $x, x' \in \mathbb{Z}$ are two solutions to the system in the statement of CRT. This means that $x \equiv b_i \equiv x' \pmod{n_i}$ for all i, and hence $n_i \mid x - x'$ for all i. From Proposition 12 we conclude that $x - x'$ is divisible by $\operatorname{lcm}(n_1, n_2, \ldots, n_k)$. Since n_i are pairwise coprime, Proposition 13 tells us that

$$m = n_1 n_2 \cdots n_k = \operatorname{lcm}(n_1, n_2, \ldots, n_k).$$

Then $m \mid (x - x') \iff x \equiv x' \pmod{m}$ as desired. ☕

We extract the following useful consequence of CRT.

Corollary 13. *Let $n_1, n_2, \ldots, n_k \in \mathbb{Z}_{>0}$ be pairwise coprime. Then the systems*

$$\begin{cases} x \equiv 1 \pmod{n_1} \\ x \equiv 1 \pmod{n_2} \\ \quad\vdots \qquad\quad \vdots \\ x \equiv 1 \pmod{n_k} \end{cases} \quad \textit{and} \quad \begin{cases} x \equiv -1 \pmod{n_1} \\ x \equiv -1 \pmod{n_2} \\ \quad\vdots \qquad\quad \vdots \\ x \equiv -1 \pmod{n_k} \end{cases}$$

have respectively the unique solution $x \equiv 1 \pmod{n_1 \cdots n_k}$ and $x \equiv -1 \pmod{n_1 \cdots n_k}$.

Proof. Clearly $x = 1$ and $x = -1$ satisfy the above systems, respectively. It follows from the uniqueness part of the CRT that there are no other solutions modulo $(n_1 \cdots n_k)$. ☕

We observe that the proof of the CRT is an effective proof. That is, the proof of existence provides us with a method to compute the solution $x \bmod n_1 \cdots n_k$.

Corollary 14. *Consider a system of congruences as in (17.1). Let $m = n_1 n_2 \cdots n_k$ and $m_i = m/n_i$. Since $(n_i, n_j) = 1$ for all $i \neq j$, we have $(m_i, n_i) = 1$, so that $m_i y \equiv 1 \pmod{n_i}$ has a solution y_i. Then*

$$x = b_1 m_1 y_1 + b_2 m_2 y_2 + \cdots + b_k m_k y_k$$

is a solution to (17.1).

We illustrate this method with a few examples.

Example 17.2. Consider again

$$x \equiv 3 \pmod 7 \qquad \text{and} \qquad x \equiv 2 \pmod 3.$$

In the notation of the theorem and its proof we have $b_1 = 3$, $b_2 = 2$,

$$n_1 = 7 \quad n_2 = 3, \quad m = 3 \cdot 7 = 21, \quad m_1 = m/n_1 = 3, \quad m_2 = m/n_2 = 7$$

and for $i = 1, 2$ we have to solve $m_i y \equiv 1 \pmod{n_i}$. Indeed,

$$i = 1: \quad 3y \equiv 1 \pmod 7 \implies y_1 = 5 \pmod 7.$$

$$i = 2: \quad 7y \equiv 1 \pmod 3 \implies y_2 = 1 \pmod 3.$$

Thus

$$x = b_1 m_1 y_1 + b_2 m_2 y_2 \equiv 3 \cdot 3 \cdot 5 + 2 \cdot 7 \cdot 1 \equiv 45 + 14 \equiv 17 \pmod{21},$$

as expected.

Example 17.3. Find $17^{-1} \pmod{55}$. We have to solve $17x \equiv 1 \pmod{55}$. Since $55 = 5 \cdot 11$, by Proposition 19, any solution to the previous congruence will also satisfy the following congruences

$$\begin{cases} 17x \equiv 1 \pmod 5 \\ 17x \equiv 1 \pmod{11} \end{cases} \iff \begin{cases} 2x \equiv 1 \pmod 5 \\ 6x \equiv 1 \pmod{11}. \end{cases}$$

Observe that the latter system is not yet ready to be solved using CRT, because the variable x appears with coefficients different from 1. To make the coefficients equal to 1, we have to multiply each equation by the corresponding inverse. Note that $3 \cdot 2 \equiv 1 \pmod 5$, hence

$$2x \equiv 1 \pmod 5 \iff x \equiv 3 \pmod 5,$$

and using $6 \cdot 2 \equiv 1 \pmod{11}$, we proceed similarly for the second congruence. This leads to the equivalent system

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod{11} \end{cases}$$

to which we can now apply the CRT. In this case, we have

$$n_1 = 5, \quad n_2 = 11, \quad b_1 = 3, \quad b_2 = 2,$$

so

$$m = 5 \cdot 11 = 55, \quad m_1 = m/n_1 = 11, \quad m_2 = m/n_2 = 5$$

and we have to solve $m_i x \equiv 1 \pmod{n_i}$ for $i = 1, 2$. Indeed,

$$i = 1: \quad 11x \equiv 1 \pmod 5 \implies y_1 = 1,$$

$$i = 2: \quad 5x \equiv 1 \pmod{11} \implies y_2 = -2,$$

and the solution is given by

$$\begin{aligned} x &\equiv b_1 m_1 y_1 + b_2 m_2 y_2 \pmod m \\ &\equiv 3 \cdot 11 \cdot 1 + 2 \cdot 5 \cdot (-2) \pmod{55} \\ &\equiv 33 - 20 \equiv 13 \pmod{55} \end{aligned}$$

as computed in Example 16.8.

Example 17.4. In Section 14 we computed $8^{10003} \pmod{105}$ by using fast modular exponentiation; here, we give an alternative calculation using CRT. We want to find an integer $x \equiv 8^{10003} \pmod{105}$ such that $0 \le x < 105$. In particular, since $105 = 3{\cdot}5{\cdot}7$, by Proposition 19, we know that x satisfies

$$\begin{cases} x \equiv 8^{10003} \pmod 3 \\ x \equiv 8^{10003} \pmod 5 \\ x \equiv 8^{10003} \pmod 7 \end{cases}$$

and applying CRT will give the number we need. Before we proceed, we will simplify the congruences above. First note that

$$\begin{cases} 8 \equiv -1 \pmod 3 \\ 8 \equiv -2 \pmod 5 \\ 8 \equiv 1 \pmod 7 \end{cases} \implies \begin{cases} x \equiv (-1)^{10003} \equiv -1 \pmod 3 \\ x \equiv (-2)^{10003} \equiv r \pmod 5 \\ x \equiv 1^{10003} \equiv 1 \pmod 7. \end{cases}$$

To find r, we observe $(-2)^4 \equiv 16 \equiv 1 \pmod 5$, thus

$$x \equiv r \equiv (-2)^{10003} \equiv (-2)^{10000} \cdot (-2)^3 \equiv ((-2)^4)^{2500} \cdot (-2)^3 \equiv 1 \cdot (-8) \equiv 2 \pmod 5.$$

Therefore, we have to apply CRT to the congruences

$$x \equiv -1 \pmod 3, \qquad x \equiv 2 \pmod 5, \qquad x \equiv 1 \pmod 7.$$

In this case, we have $b_1 = -1$, $b_2 = 2$, $b_3 = 1$,

$$n_1 = 3, \quad n_2 = 5, \quad n_3 = 7, \quad m = 105, \quad m_1 = 35, \quad m_2 = 21, \quad m_3 = 15$$

and we need to solve the congruences

$$35y \equiv 1 \pmod 3, \qquad 21y \equiv 1 \pmod 5, \qquad 15y \equiv 1 \pmod 7.$$

We can take, respectively, the solutions $y_1 \equiv -1$, $y_2 \equiv 1$ and $y_3 \equiv 1$, from which we obtain

$$\begin{aligned} x &\equiv b_1 m_1 y_1 + b_2 m_2 y_2 + b_3 m_3 y_3 \pmod m \\ &\equiv (-1) \cdot 35 \cdot (-1) + 2 \cdot 21 \cdot 1 + 1 \cdot 15 \cdot 1 \pmod{105} \\ &\equiv 35 + 42 + 15 \equiv 92 \pmod{105}. \end{aligned}$$

Remark 17.5. Since $-1 \equiv 2 \pmod 3$, we could have rewritten the system in the previous example as

$$x \equiv 2 \pmod 3, \qquad x \equiv 2 \pmod 5, \qquad x \equiv 1 \pmod 7$$

and grouped the first two congruences together into

$$x \equiv 2 \pmod{15} \qquad x \equiv 1 \pmod 7$$

and applied CRT with these two congruences instead.

Exercises.

Exercise 17.6. Solve the following ancient Indian problem: If eggs are removed from a basket $2, 3, 4, 5$ and 6 at a time, there remain respectively, $1, 2, 3, 4$ and 5 eggs. But if the eggs are removed 7 at a time, no eggs remain. What is the least number of eggs that could have been in the basket?

18. Applications of Congruences

Here we will explore a couple of applications of the theory we have developed so far.

18.1. Divisibility Tests.

Here we will prove practical criteria to decide when a given integer n is divisible by 3, 9, 11, or a power of 2. In particular, we will understand why the following well known fact is true.

> *"A number is divisible by 3 if the sum of its digits is divisible by 3."*

Proposition 20. *Let $n \in \mathbb{Z}_{>0}$. Then n is divisible by 3 or 9 if and only if the sum of its digits (in base 10) is divisible by 3 or 9, respectively.*

Proof. Let $q = 3$ or $q = 9$. We have

$$10 \equiv 1 \pmod{q} \Rightarrow 10^k \equiv 1 \pmod{q} \quad \text{for all } k > 0.$$

In base 10,

$$\begin{aligned} n &= a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10 + a_0, \quad a_k \neq 0 \\ &\equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod{q}. \end{aligned}$$

Therefore,

$$\begin{aligned} q \mid n &\iff n \equiv 0 \pmod{q} \\ &\iff a_k + a_{k-1} + \cdots + a_1 + a_0 \equiv 0 \pmod{q}, \\ &\iff q \mid a_k + a_{k-1} + \cdots + a_1 + a_0, \end{aligned}$$

as desired. ☕

Proposition 21. *Let $n \in \mathbb{Z}_{>0}$. Then n is divisible by 11 if and only if the alternating sum of its digits (in base 10) is divisible by 11.*

Proof. Note that

$$10 \equiv -1 \pmod{11} \Rightarrow 10^k \equiv (-1)^k \pmod{11} \quad \text{for all } k > 0.$$

In base 10, we have

$$\begin{aligned} n &= a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10 + a_0, \quad a_k \neq 0 \\ &\equiv a_k(-1)^k + a_{k-1}(-1)^{k-1} + \cdots + a_2 - a_1 + a_0 \pmod{11}, \end{aligned}$$

therefore

$$\begin{aligned} 11 \mid n &\iff n \equiv 0 \pmod{11} \\ &a_k(-1)^k + a_{k-1}(-1)^{k-1} + \cdots + a_2 - a_1 + a_0 \equiv 0 \pmod{11}, \\ &\iff 11 \mid a_k(-1)^k + a_{k-1}(-1)^{k-1} + \cdots + a_2 - a_1 + a_0 \pmod{11}, \end{aligned}$$

as desired. ☕

Proposition 22. *Let $n, k \in \mathbb{Z}_{>0}$. Then, n is divisible by 2^k if and only if the integer obtained from the last k digits (in base 10) of n is divisible by 2^k.*

Proof. We have

$$10 \equiv 0 \pmod{2} \implies 10^j \equiv 0 \pmod{2^j} \text{ for all } j > 0.$$

From $n = a_k 10^k + \cdots + a_1 10 + a_0$, we obtain

$$n \equiv a_{j-1}10^{j-1} + \cdots + a_1 10 + a_0 \pmod{2^j}.$$

The number on the right hand side of this congruence has base 10 representation $(a_{j-1} \cdots a_1 a_0)_{10}$. Taking $j = k$, this is the integer obtained from the last k digits of n, as desired. ☕

Examples 18.1.

(1) Let $n = 4127835$. Consider

$$S = \text{ sum of the digits of } n = 4 + 1 + 2 + 7 + 8 + 3 + 5 = 30.$$

Since $3 \mid S$ but $9 \nmid S$, we conclude that $3 \mid n$ but $9 \nmid n$.

(2) Let $n = 723160823$. We have,

$$S = \text{ alternating sum of the digits of } n \ = 7 - 2 + 3 - 1 + 6 - 0 + 8 - 2 + 3 = 22.$$

Then $11 \mid n$.

(3) Let $n = 33678924$. We have,

$$S = 3 - 3 + 6 - 7 + 8 - 9 + 2 - 4 = -4,$$

so that $11 \nmid n$.

(4) Let $n = 32688048$. Since

$$2 \mid 8, \quad 4 \mid 48, \quad 8 \mid 048, \quad 16 \mid 8048, \quad 32 \nmid 88048,$$

we may conclude that $2, 4, 8, 16 \mid n$ and $32 \nmid n$.

18.2. **The ISBN10 Code.** In this section, we will apply congruences to describe the ISBN10 code and some of its properties. An ISBN10 code is a sequence of 10 digits, a_1, $a_2, \ldots, a_{10}$, used to identify books, where

(i) $0 \le a_i \le 9$ for $i = 1, \ldots, 9$;

(ii) a_{10} is an integer mod 11, where the letter X is used to denote $10 \pmod{11}$.

An ISBn10 code is called *valid* if

$$S = \sum_{i=1}^{10} i \cdot a_i \equiv 0 \pmod{11}.$$

Examples 18.2.

(1) The code is $0 - 321 - 50031 - 8$ is valid because it satisfies

$$\begin{aligned} S &= 1 \cdot 0 + 2 \cdot 3 + 3 \cdot 2 + 4 \cdot 1 + 5 \cdot 5 + 6 \cdot 0 + 7 \cdot 0 + 8 \cdot 3 + 9 \cdot 1 + 10 \cdot 8 \\ &\equiv 16 + 49 + 89 \equiv 5 + 5 + 1 \equiv 0 \pmod{11} \end{aligned}$$

(2) The code $1 - 100 - 00000 - X$ is invalid since

$$S = 1 \cdot 1 + 2 \cdot 1 + 10 \cdot 10 \equiv 103 \equiv 4 \not\equiv 0 \pmod{11}.$$

Proposition 23. *Let $a_1, a_2, \dots, a_9$ be integers such that $0 \leq a_i \leq 9$ for $i = 1, \dots, 9$ and take*

$$a_{10} = \sum_{i=1}^{9} i \cdot a_i \pmod{11},$$

where we write X for a_{10} if $a_{10} \equiv 10 \pmod{11}$. Then, $a_1 a_2 \cdots a_{10}$ is a valid ISBN10 code.

Proof.

$$S = \sum_{i=1}^{10} i \cdot a_i = \left(\sum_{i=1}^{9} i \cdot a_i\right) + 10a_{10} = \left(\sum_{i=1}^{9} i \cdot a_i\right) + 10\left(\sum_{i=1}^{9} i \cdot a_i\right) = 11\left(\sum_{i=1}^{9} i \cdot a_i\right) \equiv 0 \pmod{11}.$$

☕

Suppose that an ISBN10 code $x = x_1 \cdots x_{10}$ is transmitted and the code $y = y_1 \cdots y_{10}$ is received; the transmission is successful if $x = y$. We say that y contains *a single error* if there exists a single value of j such that

$$\forall i \neq j \text{ we have } x_i = y_i \quad \text{and} \quad y_j = x_j + a \text{ with } -10 \leq a \leq 10,\ a \neq 0.$$

We say that y contains a *transposition error* if there are $j \neq k$ such that

$$x_j \neq x_k, \quad y_j = x_k, \quad y_k = x_j \text{ and } y_i = x_i \quad \forall i \neq j, k.$$

Proposition 24. *The ISBN10 code detects both single errors and transposition errors.*

Proof. Let x be a valid code so that $S_x = \sum_{i=1}^{10} i \cdot x_i \equiv 0 \pmod{11}$.

We will assume that a single error has occurred in the transmission and will show that the received code y is not valid. Indeed, let j and a be as described above and compute

$$S_y = \sum_{i=1}^{10} i \cdot y_i = \sum_{i=1, i \neq j}^{10} i \cdot y_i + j \cdot y_j = \sum_{i=1, i \neq j}^{10} i \cdot x_i + jx_j + ja = S_x + j \cdot a \equiv ja \pmod{11}.$$

Since 11 is prime and $11 \nmid j$ and $11 \nmid a$,

$$S_y \equiv ja \not\equiv 0 \pmod{11},$$

hence y is not valid.

Suppose now that a transposition error has occurred in the transmission. We will show that y is not valid. Indeed, let j, k be as described above and compute

$$\begin{aligned} S_y = \sum_{i=1}^{10} i \cdot y_i &= \sum_{i=1}^{10} i \cdot y_i + kx_k - kx_k + jx_j - jx_j \\ &= \sum_{i=1, i \neq k, j}^{10} i \cdot y_i + ky_k + jy_j + kx_k - kx_k + jx_k - jx_j \\ &= \sum_{i=1}^{10} i \cdot x_i + kx_j + jx_k - kx_k - jx_j \\ &= S_x + (k - j)(x_j - x_k) \equiv 0 + (k - j)(x_j - x_k) \pmod{11}. \end{aligned}$$

Since $1 \leq |k - j|, |x_j - x_k| \leq 10$ and 11 is a prime we conclude that $11 \nmid (k - j)(x_j - x_k)$, hence $S_y \not\equiv 0$, as desired. ☕

Exercises.

Exercise 18.3. Suppose that $n = 81294358X$. Write down a digit in the slot marked X so that n is divisible by

(a) 11
(b) 9
(c) 4

Exercise 18.4. Suppose that one digit, indicated with a question mark, in each of the following ISBN10 codes has been smudged and cannot be read. What should this missing digit be?

(a) $0 - 19 - 8?3804 - 9$
(b) $? - 261 - 05073 - X$

19. Wilson's Theorem

Theorem 21 (Wilson's Theorem)**.** *Let p be a prime. Then* $(p-1)! \equiv -1 \pmod{p}$.

In order to prove this theorem, we will need the following result. Note that this result is also relevant on its own.

Lemma 8. *Let $a, p \in \mathbb{Z}$ with p a prime and a invertible mod p. That is $p \nmid a$. Then* $a \equiv a^{-1} \pmod{p}$ *if and only if* $a \equiv \pm 1 \pmod{p}$.

Proof. Suppose first that $a \equiv \pm 1 \pmod{p}$. Recall that a^{-1} is an integer satisfying $aa^{-1} \equiv 1 \pmod{p}$. Since $1{\cdot}1 \equiv 1 \pmod{p}$ and $(-1)(-1) \equiv 1 \pmod{p}$ we conclude, in both cases, that $a \equiv a^{-1} \pmod{p}$.

Conversely, suppose $a \equiv a^{-1} \pmod{p}$. Multiplying both sides by a then yields

$$\begin{aligned} a^2 \equiv 1 \pmod{p} &\iff a^2 - 1 = pk, \quad \text{for some } k \in \mathbb{Z} \\ &\iff p \mid (a-1)(a+1) \\ &\implies p \mid (a-1) \quad \text{or} \quad p \mid (a+1) \quad \text{by Corollary 6} \\ &\iff a \equiv 1 \pmod{p} \quad \text{or} \quad a \equiv -1 \pmod{p}. \end{aligned}$$

☕

Remark 19.1. In Lemma 8, the condition that p is prime is necessary. For example, take $a = 3$ and $p = 8$; since $3 \cdot 3 = 9 \equiv 1 \pmod{8}$, we have $a^{-1} \equiv 3 \equiv a \pmod{8}$ but $3 \not\equiv \pm 1 \pmod{8}$.

Before we prove Wilson's theorem, let us verify it via an example. This example illustrates the main idea of the proof.

Example 19.2. Let $p = 7$. Wilson's theorem tells us that $(7-1)! = 6! \equiv -1 \pmod{7}$. We now verify this by direct computation.

$$\begin{aligned} 6! &= 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \\ &= 1 \cdot 6 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \\ &\equiv 1 \cdot 6 \cdot 1 \cdot 1 \equiv -1 \pmod{7}, \end{aligned}$$

as expected. In the second equality, we note that we have reordered the integers in the product. This reordering pairs the numbers in the brackets with their inverses mod p.

Proof of Wilson's Theorem. For $p = 2, 3$ the theorem holds. Indeed,

$$(2-1)! = 1 \equiv -1 \pmod{2} \quad \text{and} \quad (3-1)! = 2 \equiv -1 \pmod{3}.$$

Suppose $p > 3$ is prime. We know that every $a \not\equiv 0 \pmod{p}$ has an inverse a^{-1} which is unique in the range $1 \leq a^{-1} \leq p-1$. Also, by Lemma 8, only 1 and $p-1$ are their own inverses. Therefore the set $S = \{2, \ldots, p-2\}$ contains $p-3 > 0$ elements which can be grouped into $(p-3)/2$ pairs of the form $\{a, a^{-1}\}$. This is the generalization of the situation in Example 19.2, where we have the pairs $\{a = 2, a^{-1} = 4\}$ and $\{a = 3, a^{-1} = 5\}$.

Now, the product of the elements of S satisfies

$$2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv (2 \cdot 2^{-1})(3 \cdot 3^{-1}) \cdots \equiv 1 \pmod{p}.$$

Multiplying this congruence by 1 on the left and $p - 1$ on the right gives

$$(p-1)! = 1 \cdot (2 \cdot 3 \cdot \ldots \cdot (p-2))(p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}.$$

☕

Exercises.

Exercise 19.3. For each of the following congruences, find the least nonnegative integer x that satisfies it.

(a)

$$\frac{60!}{31!} \equiv x \pmod{31}$$

(b)

$$\frac{59!}{30!} \equiv x \pmod{31}$$

20. Fermat's Little Theorem

Theorem 22 (Fermat's Little Theorem)**.**
Let p be a prime. If $a \in \mathbb{Z}$ satisfies $(a,p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. Let $a \in \mathbb{Z}$ be coprime to p and consider the sequence of integers

$$a,\ 2a,\ 3a, \ldots,\ (p-1)a. \tag{20.1}$$

Claim: The integers in (20.1) are all distinct mod p and not congruent to zero mod p.

It follows from the claim that the sequence

$$a \pmod{p},\ 2a \pmod{p},\ \ldots,\ (p-1)a \pmod{p}$$

is comprised of $p-1$ distinct integers in the interval $[1, p-1]$. Hence, they must be the integers $1, 2, \ldots, p-1$ in some order (i.e. multiplication by a mod p is reordering them). Therefore, by taking the product mod p of the elements in (20.1), we obtain

$$\begin{aligned} a \cdot (2a) \cdot (3a) \cdots (p-1)a &\equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p} \\ &= (p-1)! \pmod{p}. \end{aligned}$$

Since we also have

$$a(2a)(3a)\cdots(p-1)a \equiv a^{p-1}(1 \cdot 2 \cdot 3 \cdots p-1) = a^{p-1}(p-1)! \pmod{p},$$

it follows that

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

Now, by Wilson's theorem, we conclude that

$$a^{p-1}(-1) \equiv -1 \pmod{p} \iff a^{p-1} \equiv 1 \pmod{p},$$

as desired. To complete the proof, it remains to prove the claim.

Proof of Claim: Suppose $ka \equiv k'a \pmod{p}$. Note that a^{-1} exists since $(a,p) = 1$. Then, multiplying the previous congruence by a^{-1}, we obtain

$$ka \equiv k'a \pmod{p} \iff k(aa^{-1}) \equiv k'(aa^{-1}) \pmod{p} \implies k \equiv k' \pmod{p} \implies k = k',$$

where the last implication follows from Corollary 8 because $1 \le k, k' \le p-1$. Finally, since $p \nmid a$ and $p \nmid k$, we conclude $ka \not\equiv 0 \pmod{p}$ for all ka in (20.1), completing the proof. ☕

We have the following three corollaries of FLT.

Corollary 15. *Let p be prime and let a be any integer. Then $a^p \equiv a \pmod{p}$.*

Proof. Let $a \in \mathbb{Z}$. If $p \mid a$, then $p \mid a^p$ and we have $a \equiv 0 \equiv a^p \pmod{p}$.

Suppose $p \nmid a$. Then $(a,p) = 1$ and $a^{p-1} \equiv 1 \pmod{p}$ by FLT. Multiplying both sides by a gives $a^p \equiv a \pmod{p}$, as desired. ☕

Corollary 16. *Let p be prime and $a \in \mathbb{Z}$ coprime to p. Suppose $d \equiv e \pmod{p-1}$.*

Then $a^d \equiv a^e \pmod{p}$.

Proof. If $d = e$ then $a^d = a^e$ and the result is trivial. WLOG, suppose that $d > e$. We have $d - e = (p-1)k$ for some $k \in \mathbb{Z}_{>0}$. Thus

$$a^d = a^{e+(p-1)k} = a^e \cdot \left(a^{p-1}\right)^k \equiv a^e \cdot 1^k \equiv a^e \pmod{p},$$

where we used FLT to conclude $a^{p-1} \equiv 1 \pmod{p}$. ☕

Examples 20.2.

(1) Compute $3^{201} \pmod{11}$. By Fermat's Little Theorem, we have $3^{10} \equiv 1 \pmod{11}$, hence

$$3^{201} = \left(3^{10}\right)^{20} \cdot 3 \equiv 1^{20} \cdot 3 \equiv 3 \pmod{11}.$$

(2) Compute $2^{180} \pmod{89}$. Note that $p = 89$ is prime and $p - 1 = 88$. By Corollary 16, since $180 \equiv 4 \pmod{88}$, we have $2^{180} \equiv 2^4 \equiv 16 \pmod{89}$.

(3) Exercise 3.5 follows directly from Corollary 15 and the definition of congruence, that is $5 \mid n^5 - n$.

(4) Note that FLT and Corollary 15 do not hold for non prime modulus; indeed, we have $3^4 \equiv 1 \not\equiv 3 \pmod{4}$; this is a reformulation of Exercise 3.6.

Exercises.

Exercise 20.3. Let p and q be distinct odd prime numbers with $p - 1 \mid q - 1$. If $a \in \mathbb{Z}$ with $(a, pq) = 1$, prove that $a^{q-1} \equiv 1 \pmod{pq}$.

21. Primality Testing, Pseudoprimes, and Carmichael Numbers

Given a positive integer n it is important to decide if it is a prime number. From Proposition 7 we know that it is enough to test divisibility of n by primes up to $\sqrt{n}$; if no such prime divides n we conclude that n is a prime number. This test, however, is not practical when n is very large, so other tests are needed. In this section we will describe how the theorems in Sections 19 and 20 can be used to obtain more efficient primality tests.

We start by showing that the converse of Wilson's theorem provides a primality test.

Proposition 25. *Let $n \in \mathbb{Z}_{>1}$ satisfy $(n-1)! \equiv -1 \pmod{n}$. Then n is a prime number.*

Proof. Suppose that n is a composite number such that $(n-1)! \equiv -1 \pmod{n}$. In particular, say n factors into $n = a \cdot b$ where $1 < a, b < n$. We observe that $a \leq n-1$, so $a \mid (n-1)!$. Moreover,

$$(n-1)! \equiv -1 \pmod{n} \iff n \mid (n-1)! + 1.$$

Lastly, since $a \mid n$ and $n \mid (n-1)! + 1$, we have $a \mid (n-1)! + 1$, and in particular, a divides the difference,

$$a \mid ((n-1)! + 1 - (n-1)!) = 1 \implies a = 1.$$

This is a contradiction, hence n is prime. ☕

We remark that this proposition, together with Wilson's theorem, shows that the condition $(n-1)! \equiv -1 \pmod{n}$ is equivalent to n being prime. This can be very helpful for theoretical arguments, but in practice it is not a good test because computing $(n-1)! \bmod n$ is hard. The following test is much better in practice.

Theorem 23 (Fermat's Test)**.** *Let $n, b \in \mathbb{Z}_{>1}$ with $1 < b < n$.*

If $b^{n-1} \not\equiv 1 \pmod{n}$, then n is composite.

Proof. If n is prime, we have $(b, n) = 1$ and $b^{n-1} \equiv 1 \pmod{n}$ by FLT. ☕

Example 21.1. Consider $n = 91$. Since $2^{91-1} \equiv 64 \pmod{91}$ and $64 \not\equiv 1 \pmod{91}$, Fermat's test implies that 91 is composite; indeed $91 = 13 \cdot 7$.

Unlike the condition $(n-1)! \bmod n$, Fermat's test does not classify prime numbers. That is, the converse of the theorem does not imply that n is prime. For instance, $b^{n-1} \equiv 1 \pmod{n}$ does not necessarily mean that n is prime, as the following example illustrates.

Example 21.2. Taking $n = 341$ and $b = 2$, we observe that $2^{340} \equiv 1 \pmod{341}$ but $341 = 11 \cdot 31$ so that 341 is not prime.

Composite numbers which pass Fermat's test deserve a special name.

Definition 21.3. If $n \in \mathbb{Z}_{>1}$ is composite and satisfies $b^{n-1} \equiv 1 \pmod{n}$ for some $1 < b < n$, we say that n is a *pseudoprime* to the base b.

Examples 21.4.

(1) $2^{340} \equiv 1 \pmod{341}$ but $341 = 11 \cdot 31$, hence 341 is a pseudoprime for base $b = 2$.

(2) 341 is not a pseudoprime for base $b = 3$. Indeed, $3^{30} \equiv 1 \pmod{31}$ by Fermat's Little Theorem, therefore

$$3^{340} \equiv \left(3^{30}\right)^{11} \cdot 3^{10} \equiv 1^{11} \cdot 3^{10} \pmod{31}$$

and since

$$3^{10} \equiv \left(3^{3}\right)^{3} \cdot 3 \equiv (-4)^3 \cdot 3 \equiv 25 \pmod{31},$$

we conclude $3^{340} \not\equiv 1 \pmod{31}$. Because $31 \mid 341$, it follows from Proposition 19, that $3^{340} \not\equiv 1 \pmod{341}$, as desired.

The previous example show that 341 passes Fermat's test in base 2 but not in base 3. It is natural to wonder if there are integers n that pass Fermat's test in every base coprime to n.

Definition 21.5. We call an integer $n > 1$ a *Carmichael number* if it is a pseudoprime for every base $b \geq 2$ such that $(n, b) = 1$.

It is not easy to prove that Carmichael numbers actually exist. The following theorem classifies them, allowing us to decide if an integer is a Carmichael number without checking the definition. For now, we will only prove one implication of the theorem, as the other direction (Theorem 44) requires the notion of primitive roots, which will only be introduced in Section 26.

Definition 21.6. We say that an integer n is *squarefree* if no square number divides it. In particular, the prime factorization of n contains only primes with exponent one.

Theorem 24 (Korset). *A composite positive integer n is a Carmichael number if and only if*

(i) n is squarefree and
(ii) if $p \mid n$ is prime then $p - 1 \mid n - 1$.

Proof. For now, we will only prove one implication. Suppose (i) and (ii) hold for n. and let $b \in \mathbb{Z}$ satisfy $(b, n) = 1$.

From (i), we have $n = p_1 \cdots p_k$ with p_i distinct primes. Then $(b, p_i) = 1$ for $i = 1, \ldots, k$.

From (ii), we have, for $i = 1, .., k$, that $n - 1 = (p_i - 1)k_i$ for some $k_i \in \mathbb{Z}$. Then

$$b^{n-1} \equiv \left(b^{p_i - 1}\right)^{k_i} \equiv 1^{k_i} \equiv 1 \pmod{p_i},$$

where the second congruence follows from FLT. Therefore, the system of congruences

$$\begin{cases} x \equiv 1 \pmod{p_1} \\ \quad \vdots \\ x \equiv 1 \pmod{p_k} \end{cases}$$

has the solution $x = b^{n-1}$. Clearly, $x = 1$ is also a solution to the above system. From the uniqueness part of CRT, we have $b^{n-1} \equiv 1 \pmod{n = p_1 \cdots p_k}$. This shows that n is a pseudoprime for base b. Since b is arbitrary, we conclude that this holds for all values b such that $1 < b < n$ so that n is a Carmichael number. ☕

Remark 21.7. In the previous proof, we could replace CRT by the following argument. For all $i = 1, \dots, k$, we have $b^{n-1} \equiv 1 \pmod{p_i}$, hence $p_i \mid b^{n-1} - 1$. Then $\operatorname{lcm}(p_1, .., p_k) \mid b^{n-1} - 1$ by Proposition 12. Since the p_i are distinct primes,

$$\operatorname{lcm}(p_1, .., p_k) = p_1 \cdots p_k = n,$$

hence $b^{n-1} \equiv 1 \pmod{n}$.

Example 21.8. The number 561 is the smallest Carmichael number. Indeed, $561 = 3 \cdot 11 \cdot 17$ and $3 - 1 = 2$, $11 - 1 = 10$, and $17 - 1 = 16$ all divide $561 - 1 = 560 = 2^4 \cdot 5 \cdot 7$.

To conclude this section, we describe a primality test which is a refinement of Fermat's test.

21.1. **Miller's Test.** Let $n > 0$ be odd and suppose n is a pseudoprime for the base $b \geq 2$. That is,

$$b^{n-1} \equiv 1 \pmod{n}.$$

Write $x = b^{\frac{n-1}{2}} \pmod{n}$. If n is prime, since $x^2 \equiv b^{n-1} \equiv 1 \pmod{n}$, it follows from Lemma 8 that $x \equiv \pm 1 \pmod{n}$. So, if $b^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}$, then n is composite.

Suppose we failed to conclude that n is composite in the previous step. If $b^{\frac{n-1}{2}} \equiv 1 \pmod{n}$ and $n - 1$ is divisible by 4, then we can repeat the argument with $y = b^{\frac{n-1}{4}}$.

Indeed, $y^2 \equiv b^{\frac{n-1}{2}} \equiv 1 \pmod{n}$ implies $y \equiv \pm 1 \pmod{n}$ if n is prime. Then, if we have $b^{\frac{n-1}{4}} \not\equiv \pm 1 \pmod{n}$ we conclude that n is composite. If we fail again to conclude that n is composite we can repeat this procedure as long as $\frac{n-1}{2^k}$ is an integer and $b^{\frac{n-1}{2^{k-1}}} \equiv 1 \pmod{n}$.

Example 21.9. We have seen that $n = 561$ is the smallest Carmichael number. In other words,

$$b^{560} \equiv 1 \pmod{561} \quad \text{for all } b \geq 2 \quad \text{satisfying} \quad (b, n) = 1.$$

Let $b = 5$. Then $5^{280} \equiv 67 \not\equiv \pm 1 \pmod{561}$ so that n is composite by Miller's test.

Let $b = 2$; we have $2^{280} \equiv 1 \pmod{561}$ but $2^{140} \equiv 67 \not\equiv \pm 1 \pmod{561}$ and we conclude again that n is composite. Note, however, that depending on the base b we may need a different number of steps in Miller's test.

There are integers which fool the test, and we often refer to these integers as *strong pseudoprimes*.

Example 21.10. Let $n = 2047 = 23 \cdot 89$. Then

$$2^{2046} = \left(2^{11}\right)^{186} = (2048)^{186} \equiv 1 \pmod{2047},$$

so n is a pseudoprime in base $b = 2$. Moreover,

$$\frac{n-1}{2} = 1023 \quad \text{and} \quad 2^{1023} = \left(2^{11}\right)^{93} = 2048^{93} \equiv 1 \pmod{2047},$$

so 2047 fools Miller's Test for base $b = 2$.

It is convenient to summarize the conditions under which Miller's test fails.

Definition 21.11. Let $n \in \mathbb{Z}_{>2}$ be odd. Write $n - 1 = 2^s t$, where $s \geq 1$ and t is odd. We say that *n passes Miller's test for base b* if either $b^t \equiv 1 \pmod{n}$ or $b^{2^j t} \equiv -1 \pmod{n}$ for some j in $0 \leq j \leq s - 1$.

We have seen that Carmichael numbers fool Fermat's test for every base. The following theorem, which we will not prove, shows that this is not possible for Miller's test.

Theorem 25. *Let $n \in \mathbb{Z}_{>0}$ be odd and composite. Then n fools Miller's test for at most $\frac{n-1}{4}$ bases b such that $1 \leq b \leq n - 1$.*

Based on this theorem, there is the following very practical primality test.

Theorem 26 (Rabin's probabilistic test)**.** *Let $n \in \mathbb{Z}_{>0}$ be odd and composite. Choose $b_1, \ldots, b_k \in \mathbb{Z}$ such that $1 < b_i \leq n - 1$. If n is composite, then the probability that it passes Miller's test for all b_i is less than $\frac{1}{4^k}$.*

Exercises.

Exercise 21.12. Prove that 1729 is a Carmichael number.

Exercise 21.13. Use Miller's Test in base $b = 2$ to show that 1729 is composite.

22. Euler's ϕ-Function and Euler's Theorem

Fermat's Little Theorem tells us that the $(p-1)$-th power of any integer coprime to p is congruent to one mod p. In this section we will study Euler's theorem which generalizes this idea to any congruence modulus m. In other words, for any fixed m, Euler's theorem determines $y > 0$ (depending on m) such that, for all $a \in \mathbb{Z}$ coprime to m, we have $a^y \equiv 1 \pmod{m}$.

To state Euler's theorem we first need to introduce a very important function.

Definition 22.1. The *Euler ϕ-function* is the function $\phi : \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ defined by

$$\phi(n) = \#\{x \in \mathbb{Z} \; : \; 1 \le x \le n \text{ and } (x, n) = 1\}.$$

In words, it counts the number of positive integers up to n that are coprime to n.

Examples 22.2.

(1) $\phi(1) = \phi(2) = 1$;
(2) $\phi(3) = 2$ since both $\{1, 2\}$ are coprime to 3;
(3) $\phi(6) = 2$ since, from $\{1, 2, 3, 4, 5, 6\}$, only 1 and 5 are coprime to 6;
(4) For any prime p, since $p \nmid x$ if $x < p$, we have

$$\phi(p) = \#\{x \in \mathbb{Z} \; : \; 1 \le x \le p \text{ and } (x, p) = 1\} = \#\{x \in \mathbb{Z} \; : \; 1 \le x \le p - 1\} = p - 1.$$

Theorem 27 (Euler)**.** *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. Then,*

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

Observe that, as a direct consequence of Example 22.2 (4) and Euler's theorem, we recover FLT.

Corollary 17. *Let p be a prime. Then $\phi(p) = p - 1$ and $a^{p-1} \equiv 1 \pmod{p}$.*

Proof of Euler's Theorem. Let $a \in \mathbb{Z}$ satisfy $(a, m) = 1$. From the definition of $\phi(m)$, there are $\phi(m)$ distinct positive integers, $a_1, \dots, a_{\phi(m)}$, such that $a_i \le m$ and $(a_i, m) = 1$. Consider the sequence of integers

$$a \cdot a_1, \; a \cdot a_2, \; \dots, \; a \cdot a_{\phi(m)}. \tag{22.3}$$

Claim. The integers in (22.3) are all distinct mod m, satisfy $(a \cdot a_i, m) = 1$, and are not congruent to zero mod m.

It follows from the claim that, the mod m sequence,

$$a \cdot a_1 \pmod{m}, \; a \cdot a_2 \pmod{m}, \; \dots, \; a \cdot a_{\phi(m)} \pmod{m}.$$

is made of $\phi(m)$ distinct integers in the interval $[1, m-1]$ which are coprime to m (by Proposition 16). Since the integers with these properties are $a_1, a_2, \dots, a_{\phi(m)}$, we conclude that the mod m sequence must be the integers $a_1, a_2, \dots, a_{\phi(m)}$ in some order (i.e. multiplication by a is reordering them). Therefore, by taking their product, we get

$$\begin{aligned} (a \cdot a_1) \cdot (a \cdot a_2) \cdots (a \cdot a_{\phi(m)}) &\equiv a_1 \cdot a_2 \cdots a_{\phi(m)} \pmod{m} \\ \iff a^{\phi(m)} (a_1 a_2 \cdots a_{\phi(m)}) &\equiv a_1 a_2 \cdots a_{\phi(m)} \pmod{m}. \end{aligned}$$

Write $A = a_1 a_2 \cdots a_{\phi(m)}$. Clearly, $(A, m) = 1$, therefore A is invertible mod m, and multiplying the last congruence by A^{-1} yields

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

as desired. To complete the proof, we now prove the claim.

Proof of Claim. Suppose $a \cdot a_i \equiv a \cdot a_j \pmod{m}$. Since $(a, m) = 1$, the inverse a^{-1} exists so we can cancel the a in the previous congruence to obtain

$$a_i \equiv a_j \pmod{m} \quad \text{with} \quad 0 \le a_i, a_j \le m - 1.$$

It now follows from Corollary 8 that $a_i = a_j$. Suppose $(a \cdot a_i, m) > 1$ for some i. Then there exists p such that $p \mid aa_i$ and $p \mid m$; hence $(p \mid a$ and $p \mid m)$ or $(p \mid a_i$ and $p \mid m)$. This implies $(a, m) > 1$ or $(a_i, m) > 1$, a contraction. We conclude $(a \cdot a_i, m) = 1$. Clearly $a \cdot a_i \not\equiv 0 \pmod{m}$, otherwise $m \mid a \cdot a_i$, completing the proof. ☕

Remark 22.4. Since Euler's theorem implies FLT (see Corollary 17), the previous proof, when restricted to $m = p$ a prime, must also provide a proof of Fermat's Little Theorem. Indeed, comparing both proofs, we see that the main difference is that instead of using Wilson's theorem, we used the fact that $A = a_1 a_2 \cdots a_{\phi(m)}$ is invertible. Of course A is invertible in the proof of FLT, since $A \equiv -1 \pmod{m}$ by Wilson's theorem.

Definition 22.5. A set of integers with $\phi(m)$ elements which are coprime to m such that no two of them are congruent modulo m is called a *reduced residue system modulo m.*

We extract the following corollary from the previous proof.

Corollary 18. *Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. If $\{a_1, a_2, \dots, a_{\phi(m)}\}$ is a reduced residue system modulo m, then as is $\{a \cdot a_1, a \cdot a_2, \dots, a \cdot a_{\phi(m)}\}$.*

22.1. **A Formula for ϕ.** The following theorem gives a formula to compute $\phi(n)$. We will prove this formula in Section 23 when studying arithmetic functions. For the moment, we are interested in using the formula to illustrate different kinds of calculations involving the function $\phi(n)$.

Theorem 28. *Let $n \in \mathbb{Z}_{>1}$ have factorization $n = p_1^{a_1} \cdots p_k^{a_k}$, $a_j \ge 1$ and p_j distinct primes. Then, $\phi(n)$ is given by the formula,*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) = \prod_{j=1}^{k} p_j^{a_j - 1}(p_j - 1). \tag{22.6}$$

Examples 22.7.

(1) $\phi(100) = \phi\left(2^2 \cdot 5^2\right) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40.$

(2) We will determine the last two (decimal) digits of 3^{50}, i.e. $3^{50} \pmod{100}$. By Euler's Theorem, we have $3^{40} = 3^{\phi(100)} \equiv 1 \pmod{100}$. Then

$$3^{50} = 3^{40} \cdot 3^{10} \equiv 1 \cdot 3^{10} \equiv 3^4 \cdot 3^4 \cdot 3^2 \equiv (-19)^2 \cdot 9 \equiv 49 \pmod{100}.$$

Example 22.8. Find all integers $n > 0$ satisfying $\phi(n) = 1$. We know from Examples 22.2 that $\phi(2) = \phi(1) = 1$. We will now show that no other integer has this property.

Write $n = p_1^{a_1} \cdots p_k^{a_k}$ for the prime factorization of n and suppose $\phi(n) = 1$. Then, from the formula 22.6, we obtain

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

which implies $(p_i - 1) \mid 1$ for all i. That is, $p_i = 2$ for all i. Hence, if $n \neq 1$, we have $n = 2^{a_1}$ with $a_1 \geq 1$ and therefore

$$\phi(n) = 2^{a_1 - 1} = 1 \implies a_1 = 1 \implies n = 2.$$

Example 22.9. Find all integers $n > 0$ satisfying $\phi(n) = 3$.

Write $n = p_1^{a_1} \cdots p_k^{a_k}$ for the prime factorization of n and suppose $\phi(n) = 3$. Then, from the formula 22.6, we get

$$\phi(n) = \prod_{i=1}^{k} p^{a_i - 1}(p_i - 1) = 3,$$

which implies $p_i - 1 \mid 3$ for all i. Thus $p_i - 1 = 1$ or $p_i - 1 = 3$ for all i. Note that the second case is impossible, because $p_i = 4$ is not a prime. We conclude that $p_i = 2$ for all i. Hence, if $n \neq 1$, we have $n = 2^{a_1}$ with $a_1 \geq 1$, therefore $\phi(n) = 2^{a_1 - 1} = 3$, which is impossible. In addition, $n = 1$ clearly has $\phi(1) \neq 3$ so that there are no solutions to the equation.

Example 22.10. Find all integers $n > 0$ satisfying $\phi(n) = 8$.

Let n have prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$ and suppose $\phi(n) = 8$. If, for some j, $p_j > 9$ then, by the formula (22.6), we have $\phi(n) \geq p_j - 1 > 8$, a contradiction. If $p_j = 7 \mid n$ then $p_j - 1 = 6 \mid \phi(n) = 8$, another contradiction. We conclude that $n = 2^a \cdot 3^b \cdot 5^c$, where $a, b, c \geq 0$.

Suppose $b \geq 2$. Then $3^{b-1} \mid \phi(n) = 8$, a contraction. Thus $b = 0$ or $b = 1$. Similarly, if $c \geq 2$ we get $5^{c-1} \mid \phi(n) = 8$, a contradiction, hence $c = 0$ or $c = 1$.

We now have the following cases, according to the possible values of b and c:

(1) $b = c = 0$: then $n = 2^a$.
   (a) if $a \geq 1$, we have
$$\phi(n) = 2^{a-1} = 8 \implies a = 4 \implies n = 16;$$
   (b) if $a = 0$ then $n = 1$, hence $\phi(n) = 1 \neq 8$ is not a solution.

(2) $b = 0$, $c = 1$: then $n = 2^a \cdot 5$.
   (a) if $a \geq 1$,
$$\phi(n) = 2^{a-1} \cdot 4 = 8 \implies a = 2 \implies n = 20;$$
   (b) if $a = 0$ then $n = 5 \implies \phi(n) = 4 \neq 8$.

(3) $b = 1$, $c = 0$: then $n = 2^a \cdot 3$.
   (a) if $a \geq 1$,
$$\phi(n) = 2^{a-1} \cdot 2 = 8 \implies a = 3 \implies n = 24;$$
   (b) if $a = 0$ then $n = 3 \implies \phi(n) = 2 \neq 8$.

(4) $b = c = 1$: then $n = 2^a \cdot 3 \cdot 5$.
   (a) if $a \geq 1$,
$$\phi(n) = 2^{a-1} \cdot 2 \cdot 4 = 8 \implies a = 1 \implies n = 30;$$

(b) if $a = 0$ then $n = 15 \implies \phi(15) = (3-1)(5-1) = 8$.

We conclude that $\phi(n) = 8$ has solutions $n = 15, 16, 20, 24, 30$.

Exercises.

Exercise 22.11. Find a reduced residue system modulo each integer below

(i) 15
(ii) 18
(iii) p, where p is a prime number
(iv) 2^n, where n is a positive integer
(v) For each of (i) and (ii), give another solution sharing exactly one element with your previous solution

Exercise 22.12. Prove that $9^8 \equiv 1 \pmod{16}$ by following the steps in the proof of Euler's Theorem.

23. Arithmetic Functions

We have already encountered in Section 22.1 a very important function, the Euler-ϕ function. In this section, we will study other relevant functions in number theory; in particular, we'll focus on those which are 'multiplicative', a property that sometimes allows to derive formulas for the functions we consider.

Definition 23.1. A function whose domain is $\mathbb{Z}_{>0}$ is called an *arithmetic function.*

Examples 23.2.

(1) $f(n) = 1$ for all $n \in \mathbb{Z}_{>0}$;
(2) $f(n) = n$ for all $n \in \mathbb{Z}_{>0}$;
(3) $\phi(n)$, the Euler ϕ-function;
(4) $\tau(n)$ = the number of positive divisors of n;
(5) $\sigma(n)$ = the sum of the positive divisors of n.

Example 23.3. The positive divisors of 6 are $\{1, 2, 3, 6\}$. Therefore,

$$\tau(6) = 4 \quad \text{and} \quad \sigma(6) = 1 + 2 + 3 + 6 = 12.$$

Definition 23.4. Let f be an arithmetic function. We say that f is *multiplicative* if, for all $n_1, n_2 \in \mathbb{Z}_{>0}$ satisfying $(n_1, n_2) = 1$, we have

$$f(n_1 \cdot n_2) = f(n_1) \cdot f(n_2)$$

and we say f is *completely multiplicative* if

$$f(n_1 \cdot n_2) = f(n_1) \cdot f(n_2) \quad \text{for all } n_1, n_2 \in \mathbb{Z}_{>0}.$$

Clearly, both the constant function $f(n) = n$ and the identity function $f(n) = 1$ are completely multiplicative. We shall prove that the three functions ϕ, τ, and σ are multiplicative. We begin by showing that ϕ is multiplicative, which is a key ingredient to later establish the formula (22.6).

Theorem 29. *The Euler ϕ-function is multiplicative.*

Proof. Let n_1, n_2 be positive and coprime integers. By definition, we have

$$\phi(n_1 n_2) = \#\{x \in \mathbb{Z} \ : \ 1 \le x \le n_1 n_2 \text{ and } (x, n_1 n_2) = 1\}.$$

We want to show

$$\phi(n_1 \cdot n_2) = \phi(n_1) \cdot \phi(n_2).$$

To prove this equality, we will count the elements in the set above in such a way that the desired result becomes clear. The integers we need to count are between 1 and $n_1 n_2$. Begin by writing the positive integers up to $n_1 n_2$ in the form

$$\begin{array}{cccccc}
1 & n_1 + 1 & 2n_1 + 1 & \cdots & (n_2 - 1)n_1 + 1 \\
2 & n_1 + 2 & 2n_1 + 2 & \cdots & (n_2 - 1)n_1 + 2 \\
\vdots & \vdots & \vdots & \cdots & \vdots \\
r & n_1 + r & 2n_1 + r & \cdots & (n_2 - 1)n_1 + r \\
\vdots & \vdots & \vdots & \cdots & \vdots \\
n_1 & 2n_1 & 3n_1 & \cdots & n_1 n_2.
\end{array}$$

We now identify the integers in the above list which are coprime to n_1n_2.

Suppose $1 \leq r \leq n_1$ and $(r, n_1) = d > 1$. Then all the elements in the r-th row are divisible by d, hence are not coprime to n_1n_2. We conclude that all the integers coprime to n_1n_2 belong to the rows whose first number is coprime to n_1. Since there are n_1 rows, there are precisely $\phi(n_1)$ rows containing integers coprime to n_1n_2. To finish the proof, it remains to show that each of these $\phi(n_1)$ rows contains exactly $\phi(n_2)$ integers coprime to n_1n_2.

Suppose $(r, n_1) = 1$. It follows that the numbers in the r-th row are coprime to n_1. Indeed, if $d > 1$ divides both n_1 and a number of the form $kn_1 + r$, then it also divides r, a contradiction. Therefore, an integer in the r-th row is coprime to n_1n_2 if and only if it is coprime to n_2.

We claim that the n_2 elements in the r-th row are all distinct mod n_2. Thus, exactly $\phi(n_2)$ of them are coprime to n_2 by Corollary 9. Since these integers are also coprime to n_1, they are coprime to n_1n_2. There are $\phi(n_1)$ rows, each containing $\phi(n_2)$ integers coprime to n_1n_2, hence $\phi(n_1n_2) = \phi(n_1) \cdot \phi(n_2)$, as desired.

We now prove the claim. Suppose that

$$kn_1 + r \equiv k'n_1 + r \pmod{n_2} \quad \text{where } 1 \leq k, k' \leq n_2 - 1.$$

Since $(n_1, n_2) = 1$ there exists an inverse of n_1 mod n_2 and we have

$$kn_1 + r \equiv k'n_1 + r \pmod{n_2} \iff k \equiv k' \pmod{n_2} \implies k = k',$$

where the last implication follows from Corollary 8. ☕

The following theorem will play a central role in proving that τ and σ are multiplicative functions. This will yield a method to construct a new multiplicative function, provided that we start with a multiplicative function.

Theorem 30. *Let f be an arithmetic function and define the arithmetic function F by*

$$F(n) = \sum_{d|n, d>0} f(d), \quad \forall n \in \mathbb{Z}_{>0}.$$

If f is multiplicative, then F is multiplicative.

Proof. Let $n_1, n_2 > 0$ be coprime integers. We want to show that

$$F(n_1n_2) = F(n_1) \cdot F(n_2).$$

Since $(n_1, n_2) = 1$, from Proposition 14 we know that the divisors d of n_1n_2 are exactly the integers of the form $d = d_1d_2$, where $(d_1, d_2) = 1$, $d_1 \mid n_1$, $d_2 \mid n_2$. Then,

$$\begin{aligned} F(n_1n_2) &= \sum_{d|n_1n_2, d>0} f(d) = \sum_{\substack{d_1|n_1, d_2|n_2 \\ d_1>0, d_2>0}} f(d_1d_2) = \sum_{\substack{d_1|n_1, d_2|n_2 \\ d_1>0, d_2>0}} f(d_1)f(d_2) \\ &= \left(\sum_{\substack{d_1|n_1 \\ d_1>0}} f(d_1) \right) \left(\sum_{\substack{d_2|n_2 \\ d_2>0}} f(d_2) \right) = F(n_1)F(n_2), \end{aligned}$$

where we used that $f(d_1d_2) = f(d_1)f(d_2)$ as f is multiplicative. ☕

Theorem 31. *The functions $\sigma(n)$ and $\tau(n)$ are multiplicative.*

Proof. Note that we can write τ and σ as

$$\tau(n) = \sum_{d|n, d>0} 1 \quad \text{and} \quad \sigma(n) = \sum_{d|n, d>0} d.$$

In other words, they are of the form F as in Theorem 30 where we choose $f(n) = 1$ and $f(n) = n$, respectively. Since these two functions f are multiplicative, the result now follows from Theorem 30. ☕

Exercises.

Exercise 23.5. Prove that a completely multiplicative arithmetic function is completely determined by its values at prime numbers.

Exercise 23.6. Let $n \in \mathbb{Z}$ with $n > 0$. Define an arithmetic function ρ by $\rho(1) = 1$ and $\rho(n) = 2^m$ where m is the number of distinct prime factors dividing n. Prove that ρ is multiplicative but not completely multiplicative.

24. Formulas for the Functions ϕ, τ and σ

Let f be a multiplicative arithmetic function and let $n > 1$ be an integer with prime factorization $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Then

$$f(n) = f\left(p_1^{a_1}\right) f\left(p_2^{a_2}\right) \cdots f\left(p_k^{a_k}\right).$$

Thus, to determine the formula for f, it suffices to determine a formula for $f\left(p_i^{a_i}\right)$ and take the product.

Lemma 9. *Let p be a prime and $a \geq 1$. Then,*

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

In particular, $\phi(p) = p - 1$.

Proof. Since p is prime,

$$(n, p^a) = 1 \iff (n, p) = 1 \iff p \nmid n,$$

hence

$$\phi(p^a) = \#\left\{x \in \mathbb{Z} \;:\; 1 \leq x \leq p^a \text{ and } (x, p^a) = 1\right\} = \#\left\{x \in \mathbb{Z} \;:\; 1 \leq x \leq p^a \text{ and } p \nmid x\right\}.$$

The positive multiples of p which are $\leq p^a$ are the numbers of the form kp for $1 \leq k \leq p^{a-1}$. In particular, there are p^{a-1} of them and we conclude $\phi(p^a) = p^a - p^{a-1}$, as desired. ☕

We are now in position to prove the formula for $\phi(n)$.

Theorem 32. *Let $n \in \mathbb{Z}_{>1}$ have factorization $n = p_1^{a_1} \cdots p_k^{a_k}$, $a_j \geq 1$ and p_j distinct primes. Then, $\phi(n)$ is given by the formula,*

$$\phi(n) = n \prod_{j=1}^{k} \left(1 - \frac{1}{p_i}\right) = \prod_{j=1}^{k} p_j^{a_j - 1}(p_j - 1).$$

Proof. From Lemma 9 and the fact that ϕ is multiplicative, we have

$$\begin{aligned}
\phi(n) &= \phi\left(p_1^{a_1}\right) \phi\left(p_2^{a_2}\right) \cdots \phi\left(p_k^{a_k}\right) \\
&= p_1^{a_1}\left(1 - \frac{1}{p_1}\right) \cdots p_k^{a_k}\left(1 - \frac{1}{p_k}\right) \\
&= p_1^{a_1} \cdots p_k^{a_k}\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
&= n \prod_{j=1}^{k} \left(1 - \frac{1}{p_i}\right).
\end{aligned}$$

☕

Lemma 10. *Let p be a prime and $a \geq 1$. Then,*

$$\tau(p^a) = a + 1 \qquad \textit{and} \qquad \sigma(p^a) = \frac{1 - p^{a+1}}{1 - p}.$$

Proof. The positive divisors of p^a are $\{1, p, \ldots, p^a\}$. Clearly $\tau(p^a) = a + 1$ as there are $a + 1$ such divisors. Moreover, the formula for the sum of terms in a geometric progression (Proposition 2) gives

$$\sigma(p^a) = 1 + p + \cdots + p^a = \frac{1 - p^{a+1}}{1 - p}.$$

☕

Theorem 33. *Let $n \in \mathbb{Z}_{>1}$ have prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$. Then,*

$$\tau(n) = \prod_{i=1}^{k} (a_i + 1) \quad \text{and} \quad \sigma(n) = \prod_{i=1}^{k} \left(\frac{1 - p_i^{a_i+1}}{1 - p_i} \right).$$

Proof. The result follows from Lemma 10 and the fact that τ and σ are multiplicative functions. ☕

Proposition 26. *An integer $n > 0$ is prime if and only if $\sigma(n) = 1 + n$.*

Proof. Clearly, $\sigma(n) \geq 1 + n$ for all n. Furthermore, n is not a prime if and only if the set of its positive divisors contains at least one element c such that $1 < c < n$. That is,

$$\sigma(n) \geq 1 + n + c > n + 1.$$

☕

Example 24.1. Let $n = 100 = 2^2 \cdot 5^2$. Then $\tau(n) = (2 + 1)(2 + 1) = 9$ and

$$\sigma(n) = \frac{2^3 - 1}{2 - 1} \cdot \frac{5^3 - 1}{5 - 1} = 7 \cdot 31 = 217.$$

Theorem 34. *Let $n \in \mathbb{Z}_{>0}$. Then*

$$\sum_{\substack{d \mid n \\ d > 0}} \phi(d) = n.$$

Proof. Since ϕ is multiplicative, Theorem 30 yields

$$F(n) = \sum_{\substack{d \mid n \\ d > 0}} \phi(d),$$

a multiplicative function. In other words, $F(n) = F(p_1^{a_1}) \cdots F(p_k^{a_k})$, where $n = p_1^{a_1} \cdots p_k^{a_k}$ is the prime factorization of n. Lastly, we observe that

$$F(p^a) = \sum_{0 \leq i \leq a} \phi(p^i) = 1 + (p - 1) + (p^2 - p) + \cdots + (p^a - p^{a-1}) = p^a,$$

and therefore $F(n) = p_1^{a_1} \cdots p_k^{a_k} = n$, as desired. ☕

Example 24.2. The positive divisors of 12 are $\{1, 2, 3, 4, 6, 12\}$ and we have

$$\phi(1) = \phi(2) = 1, \quad \phi(3) = \phi(4) = \phi(6) = 2, \quad \phi(12) = 4.$$

Finally, we check $1 + 1 + 2 + 2 + 2 + 4 = 12$, as expected.

Exercises.

Exercise 24.3. Show that ϕ, τ and σ are not completely multiplicative by providing a counterexample in each case.

Exercise 24.4. Characterize the positive integers for which $\tau(n)$ is odd.

Exercise 24.5. Characterize the positive integers n such that

(i) $\phi(n)$ is odd
(ii) $4 \mid \phi(n)$

Exercise 24.6. Let p be a prime such that $p+2$ is also a prime (these are called *twin primes*). Prove that $\sigma(p+2) = \sigma(p) + 2$.

25. Perfect Numbers and Mersenne Primes

In this section, we study the relationship between so-called perfect numbers and Mersenne primes. We begin with a few definitions.

Definition 25.1. An integer $n > 0$ is called *perfect* if $\sigma(n) = 2n$.

Definition 25.2. Let $n > 1$ be an integer. We call the integer $M_n = 2^n - 1$ the *n-th Mersenne number*. If M_n is prime, we call it a *Mersenne prime*.

Examples 25.3.

(1) The positive divisors of $n = 6$ are $\{1, 2, 3, 6\}$ and we have
$$\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6,$$
so 6 is a perfect number;

(2) The positive divisors of $n = 28$ are $\{1, 2, 4, 7, 14, 28\}$ and we have
$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \cdot 28,$$
so 28 is a perfect number.

(3) $M_5 = 2^5 - 1 = 31$ is a Mersenne prime.

(4) $M_7 = 2^7 - 1 = 127$ is a Mersenne prime.

(5) $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ is not prime.

There are no known odd perfect numbers.[1] It is also unknown if there are infinitely many even ones, but the next theorem shows there is a one-to-one correspondence between Mersenne primes and even perfect numbers.

Theorem 35. *Let $n \in \mathbb{Z}_{>0}$. Then n is an even perfect number if and only if*
$$n = 2^{p-1}\left(2^p - 1\right) \quad \text{with } \; 2^p - 1 \; \text{ a Mersenne prime.}$$

Proof. We first suppose $n = 2^{p-1}(2^p - 1)$, where $2^p - 1$ is a Mersenne prime, and show that n must be an even perfect number. In other words, $2^p - 1$ is a prime number and we have $\sigma(2^p - 1) = (2^p - 1) + 1 = 2^p$ by Proposition 26. We now compute
$$\sigma(n) = \sigma(2^{p-1}(2^p - 1)) = \sigma(2^{p-1})\sigma(2^p - 1) = \sigma(2^{p-1})2^p,$$
where we used the fact that σ its multiplicative and $(2^{p-1}, 2^p - 1) = 1$. Now, from Lemma 10, it follows that
$$\sigma(n) = \left(\frac{2^p - 1}{2 - 1}\right) \cdot 2^p = (2^p - 1) \cdot 2^p = 2\left(2^{p-1}\left(2^p - 1\right)\right) = 2n.$$

Conversely, suppose now n is an even perfect number. Write $n = 2^a \cdot b$, where $a, b \in \mathbb{Z}_{>0}$, b is odd, and $a \geq 1$. Since σ is multiplicative, by Lemma 10,
$$\sigma(n) = \sigma\left(2^a\right)\sigma(b) = \left(\frac{2^{a+1} - 1}{2 - 1}\right)\sigma(b) = \left(2^{a+1} - 1\right)\sigma(b).$$

Since n is perfect,
$$\sigma(n) = 2n = 2\left(2^a \cdot b\right) = 2^{a+1}b,$$

[1] As of 2012 it is known that no odd perfect numbers were found up to 10^{1500}

we have

$$\left(2^{a+1}-1\right)\sigma(b)=2^{a+1}b \implies 2^{a+1}\mid\sigma(b) \iff \sigma(b)=2^{a+1}c \text{ with } c>0$$

and it follows that

$$\left(2^{a+1}-1\right)\sigma(b)=\left(2^{a+1}-1\right)2^{a+1}c=2^{a+1}b \implies \left(2^{a+1}-1\right)c=b.$$

We claim that $c=1$. Then $b=2^{a+1}-1$ and $\sigma(b)=2^{a+1}=b+1$, hence b is prime by Proposition 26. Thus $n=2^a b=2^a\left(2^{a+1}-1\right)$ with $2^{a+1}-1$ is a prime, as desired.

We will now prove the claim. Suppose $c>1$. Since $\left(2^{a+1}-1\right)c=b$, we see that b has at least the three positive divisors $1, c$, and b. Thus $\sigma(b)\geq 1+b+c$, but

$$\sigma(b)=2^{a+1}c=2^{a+1}c-c+c=\left(2^{a+1}-1\right)c+c=b+c,$$

a contradiction. ☕

To conclude this section, we establish the following two properties of Mersenne numbers.

Theorem 36. *Let $n\in\mathbb{Z}_{>1}$. If M_n is prime then n is prime.*

Proof. We prove the contrapositive. That is, suppose n is composite, so $n=a\cdot b$ with $1<a,b<n$. We have

$$2^n-1=2^{ab}-1=(2^a-1)\left(2^{a(b-1)}+2^{a(b-2)}+2^{a(b-3)}+\cdots+2^a+1\right),$$

with both factors >1. Thus M_n is not prime. ☕

From Example 25.3 (5), we see that M_{11} is not a prime despite the fact that 11 is a prime. The next theorem shows that, in this kind of situation, the divisors of M_p cannot be arbitrary. For this result, we require the following lemma.

Lemma 11. *Let a and b be positive integers. Then* $(2^a-1, 2^b-1)=2^{(a,b)}-1$.

Proof. Write $D=(2^a-1,2^b-1)$ and $d=(a,b)$. We want to show that $D=2^d-1$.

By Theorem 6, there exist $x,y\in\mathbb{Z}$ such that

$$d=ax+by.$$

Since $D=(2^a-1,2^b-1)$, we have

$$2^a\equiv 1 \pmod{D}, \quad\text{and}\quad 2^b\equiv 1 \pmod{D},$$

so

$$2^d=2^{ax+by}=(2^a)^x\left(2^b\right)^y\equiv(1^x)(1^y)\equiv 1 \pmod{D}.$$

That is, $D\mid(2^d-1)$.

Conversely, since $d|a$, we have that $2^d-1\mid 2^a-1$ (as in the proof of Theorem 36). Similarly, as $d|b$, we have $2^d-1\mid 2^b-1$, and so $2^d-1\mid(2^a-1,2^b-1)$. That is, $2^d-1\mid D$.

Since D and 2^d-1 are positive and satisfy $D\mid 2^d-1$ and $2^d-1\mid D$, Proposition 6 implies

$$(2^a-1,2^b-1)=D=2^d-1=2^{(a,b)}-1,$$

as desired. ☕

Theorem 37. *Let p be an odd prime and d a divisor of $M_p=2^p-1$. Then $d\equiv 1 \pmod{2p}$.*

Proof. Since the product of two numbers $q_1, q_2 \equiv 1 \pmod{2p}$ is $q_1 q_2 \equiv 1 \pmod{2p}$, it is enough to prove the theorem for the prime factors of M_p (any other divisor will be a product of prime factors).

Let $q \mid M_p$ be prime. By FLT, we have

$$2^{q-1} \equiv 1 \pmod{q} \iff q \mid 2^{q-1} - 1,$$

and, by Corollary 4, we also have $q \mid (2^p - 1, 2^{q-1} - 1)$. Now, Lemma 11 gives

$$\left(2^p - 1, 2^{q-1} - 1\right) = 2^{(p,q-1)} - 1 \implies q \mid 2^{(p,q-1)} - 1,$$

so $2^{(p,q-1)} - 1 \neq 1$. We conclude $(p, q-1) \neq 1$ and, since p is prime, we have $p \mid q - 1$. Thus $q - 1 = pk'$ with $k' = 2k$ because q is odd (since M_p is odd). That is, $q = 1 + 2pk$, as desired. ☕

Example 25.4. Is $M_{23} = 2^{23} - 1 = 8388607$ a prime? By the previous theorem, we need only test divisibility by primes of the form $q = 46k + 1$. The smallest such prime is 47, and dividing M_{23} by this number shows $M_{23} = 47 \cdot 178481$. So, M_{23} is not a Mersenne prime.

Exercises.

Exercise 25.5. Let $n \in \mathbb{Z}$ with $n > 1$. Then n is said to be *almost perfect* if $\sigma(n) = 2n - 1$. Show that, for $k \in \mathbb{Z}_{>0}$, the number 2^k is almost perfect.

26. Primitive Roots

We know from Euler's theorem that $a^{\phi(m)} \equiv 1 \pmod{m}$ for any integer a coprime to $m > 0$. Therefore, it is natural to ask if, fixed $m > 0$, there exists an integer $x < \phi(m)$ such that for all integer a coprime to m we have $a^x \equiv 1 \pmod{m}$. For example, for $m = 8$ we can easily compute that

$$1^2 \equiv 1, \quad 3^2 = 9 \equiv 1, \quad 5^2 = 25, \quad 7^2 = 49 \equiv 1 \pmod{8},$$

showing that $x = 2 < \phi(8) = 4$ has the desired property. Inverting the question, we are interested in understanding when the smallest value of x with the above property is $x = \phi(m)$. The complete answer to this question is provided by the Primitive Root Theorem (see Theorem 40).

We begin with the following definition.

Definition 26.1. Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. The *order of a modulo m*, denoted $\mathrm{ord}_m(a)$, is the least positive integer n such that $a^n \equiv 1 \pmod{m}$.

Example 26.2. Let $m = 7$, $a = 3$. We have

$$3^1 \equiv 3, \quad 3^2 \equiv 2, \quad 3^3 \equiv 6, \quad 3^4 \equiv 4, \quad 3^5 \equiv 5, \quad 3^6 \equiv 1 \pmod{7},$$

so $\mathrm{ord}_7(3) = 6 = \phi(7)$. Similarly, we can compute the order of every integer a coprime to 7:

$a \pmod{7}$	1	2	3	4	5	6
$\mathrm{ord}_7(a)$	1	3	6	3	6	2

Example 26.3. Let $m = 8$. Here, $\phi(8) = 4$ and the order of an integer a coprime to 8 is given in the table

$a \pmod{8}$	1	3	5	7
$\mathrm{ord}_8(a)$	1	2	2	2

It is clear from Euler's theorem that, for any a coprime to m, we have $\mathrm{ord}_m(a) \le \phi(m)$. In the examples above, we see that $\mathrm{ord}_7(3) = \mathrm{ord}_7(5) = \phi(7)$, while for $m = 8$ there is no a with the maximal order $\phi(8) = 4$. However, in both cases, all the orders occurring are divisors of $\phi(m)$. This is a general property.

Proposition 27. *Let $a, m \in \mathbb{Z}$ such that $m > 0$ and $(a, m) = 1$. Then $a^n \equiv 1 \pmod{m}$ for some $n \in \mathbb{Z}_{>0}$ if and only if $\mathrm{ord}_m(a) \mid n$. In particular, $\mathrm{ord}_m a \mid \phi(m)$.*

Proof. Suppose first that $a^n \equiv 1 \pmod{m}$ for some $n > 0$. Dividing n by $\mathrm{ord}_m(a)$ via the division algorithm yields

$$n = \mathrm{ord}_m(a)q + r, \quad 0 \le r < \mathrm{ord}_m(a).$$

Then

$$a^n = \left(a^{\mathrm{ord}_m(a)}\right)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \equiv 1 \pmod{m},$$

where we used the definition of order and our assumption. Suppose $r \neq 0$. Since $\mathrm{ord}_m(a)$ is the smallest integer for which $a^{\mathrm{ord}_m(a)} \equiv 1 \pmod{m}$ and $r < \mathrm{ord}_m(a)$, we obtain a contradiction. So $r = 0$ and hence $\mathrm{ord}_m(a) \mid n$.

Suppose now $\mathrm{ord}_m(a) \mid n$. That is, $n = \mathrm{ord}_m(a) \cdot k$ for some $k \in \mathbb{Z}$. Thus

$$a^n = \left(a^{\mathrm{ord}_m(a)}\right)^k \equiv 1^k \equiv 1 \pmod{m}.$$

☕

Example 26.4. Let $m = 11$ and $a = 2$. We have $\phi(11) = 10$, so $\mathrm{ord}_{11} 2 \in \{1, 2, 5, 10\}$ by Proposition 27. We compute

$$2^1 \equiv 2 \pmod{11}, \quad 2^2 \equiv 4 \pmod{11}, \quad 2^5 \equiv 32 \equiv 10 \pmod{11}$$

and since none of these are congruent to 1 mod 11, it follows that $\mathrm{ord}_{11}(2) = 10$. Note that, by using Proposition 27, we avoided computing $2^3, 2^4, 2^6, 2^7, 2^8, 2^9 \pmod{11}$.

Definition 26.5. Let $a, m \in \mathbb{Z}$ with $m > 0$ and $(a, m) = 1$. We say that a is *a primitive root modulo m* if $\mathrm{ord}_m(a)$ is maximal, that is $\mathrm{ord}_m(a) = \phi(m)$.

Examples 26.6. From the examples above, we already know the following:

(1) 3 and 5 are primitive roots modulo 7;
(2) 2 is a primitive root modulo 11;
(3) There are no primitive roots modulo 8.

We see now that the discussion in the first paragraph of this section can be summarized into the question: *which integers admit primitive roots?*. The answer is given by Theorem 40 to which we will not give a complete proof. In the remainder of this section, we will need the following result.

Proposition 28. *Let $a, m \in \mathbb{Z}$, $m > 0$, $(a, m) = 1$.*

(i) For $i, j \in \mathbb{Z}$, we have $a^i \equiv a^j \pmod{m} \iff i \equiv j \pmod{\mathrm{ord}_m(a)}$.
(ii) For $i > 0$, we have

$$\mathrm{ord}_m\left(a^i\right) = \frac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), i)}.$$

Proof. (i) Since $(a, m) = 1$, we know $a^{-1} \pmod{m}$ exists and

$$a^i \equiv a^j \pmod{m} \iff a^i\left(a^{-1}\right)^j \equiv a^j \cdot a^{-j} \equiv 1 \pmod{m} \iff a^{i-j} \equiv 1 \pmod{m}.$$

By Proposition 27, we thus have $\mathrm{ord}_m a \mid i - j \iff i \equiv j \pmod{\mathrm{ord}_m a}$.

(ii) Note that $a^{i \cdot \mathrm{ord}_m(a^i)} = (a^i)^{\mathrm{ord}_m(a^i)} \equiv 1 \pmod{m}$ so that $\mathrm{ord}_m(a) \mid i \cdot \mathrm{ord}_m(a^i)$ by Proposition 27. We claim that $i \cdot \mathrm{ord}_m(a^i) = \mathrm{lcm}(\mathrm{ord}_m(a), i)$. In this case,

$$i \cdot \mathrm{ord}_m\left(a^i\right) = \mathrm{lcm}(\mathrm{ord}_m(a), i) = \frac{i \cdot \mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), i)}$$

by Proposition 10 (iii), therefore

$$\mathrm{ord}_m\left(a^i\right) = \frac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), i)}$$

as required.

We now prove the claim. Suppose that $\mathrm{ord}_m(a) \mid ik$ for some $k > 0$. By Proposition 27, $(a^i)^k = a^{ik} \equiv 1 \pmod{m}$, hence $\mathrm{ord}_m(a^i) \mid k$ again by Proposition 27. It follows that

$k = \mathrm{ord}_m\left(a^i\right)$ is the smallest k such that ik is both a multiple of i and $\mathrm{ord}_m(a)$. That is, $i\,\mathrm{ord}_m\left(a^i\right) = \mathrm{lcm}(\mathrm{ord}_m(a), i)$, as claimed.

☕

Corollary 19. *Let a be a primitive root mod m and $S = \{1, a, a^2, \ldots, a^{\phi(m)-1}\}$. Then, the set S is a reduced residue system mod m.*

Proof. The set S has $\phi(m)$ elements. Additionally, because a is a primitive root, $(a, m) = 1$ so that all of these elements are coprime to m. It remains to show that no two of them are congruent mod m.

Suppose that $a^i \equiv a^j \pmod{m}$ for some $a^i, a^j \in S$. Then $i \equiv j \pmod{\mathrm{ord}_m(a)}$ by Proposition 28 (i). Then $i = j$ by Corollary 8 since $\mathrm{ord}_m(a) = \phi(m)$ and $0 \le i, j \le \phi(m) - 1$. ☕

Example 26.7. Let $m = 7$ and $a = 3$ which is a primitive root mod 7. For $0 \le i \le 6$, in Example 26.2, we computed $3^i \pmod 7$ and obtained the second row of the table

i	1	2	3	4	5	6
$3^i \pmod 7$	3	2	6	4	5	1
$\mathrm{ord}_7\left(3^i\right)$	6	3	2	3	6	1

which is a reduced residue system mod 7, as predicted by the previous corollary. To obtain the third row we can, for example, apply the formula in Proposition 28 (ii). For instance, to determine $\mathrm{ord}_7(2)$, we compute

$$\mathrm{ord}_7(2) = \mathrm{ord}_7\left(3^2\right) = \frac{\mathrm{ord}_7(3)}{(\mathrm{ord}_7(3), 2)} = \frac{6}{(6,2)} = \frac{6}{2} = 3.$$

Corollary 20. *Let m be an integer admitting a primitive root. Then there are $\phi(\phi(m))$ non-congruent primitive roots mod m.*

Proof. Let r be a primitive root mod m so $\mathrm{ord}_m(r) = \phi(m)$. By Corollary 19, any other primitive root must be congruent to r^i for some i such that $1 \le i \le \phi(m)$. If r^i is also a primitive root, then $\mathrm{ord}_m\left(r^i\right) = \mathrm{ord}_m(r) = \phi(m)$ and, by Proposition 28 (ii), we have

$$\mathrm{ord}_m\left(r^i\right) = \frac{\mathrm{ord}_m r}{(\mathrm{ord}_m(r), i)} \iff (\mathrm{ord}_m(r), i) = 1.$$

Clearly, there are $\phi(\mathrm{ord}_m(r)) = \phi(\phi(m))$ such i, giving the desired result. ☕

To understand which integers admit a primitive root it is convenient to first understand why certain integers cannot have a primitive root.

Examples 26.8.

(1) For $m = 15$, we have $\phi(m) = \phi(3)\phi(5) = 2 \cdot 4 = 8$ and

a such that $(a, 15) = 1$	1	2	4	7	8	11	13	14
$\mathrm{ord}_{15}(a)$	1	4	2	4	4	4	4	2

(2) For $m = 16$, we have $\phi(16) = 8$ and

a such that $(a, 16) = 1$	1	3	5	7	9	11	13	15
$\mathrm{ord}_{16}(a)$	1	4	4	2	2	4	4	2

(3) Recall there are no primitive roots mod 8.

We shall shortly prove results explaining what is behind these examples, but first let us have a closer look at the case $m = 15$. From Euler's theorem we know that $a^8 \equiv 1 \pmod{15}$ when $(a, 15) = 1$, hence, by Proposition 19, we have $a^8 \equiv 1 \pmod 3$ and $a^8 \equiv 1 \pmod 5$. Clearly, from these two congruences we recover that $a^8 \equiv 1 \pmod{15}$ by CRT. However, FLT gives us the sharper congruences $a^2 \equiv 1 \pmod 3$ and $a^4 \equiv 1 \pmod 5$ which, after squaring the first, leads to $a^4 \equiv 1 \pmod{15}$. Note that this is consistent with the orders in the table for $m = 15$ in Examples 26.8. The following theorem generalizes this idea.

Theorem 38. *Let $m \in \mathbb{Z}_{>0}$. Suppose $m = kn$ where $(k, n) = 1$ and $\phi(k)$, $\phi(n)$ are even. Then, for all $a \in \mathbb{Z}$ coprime to m, we have*

$$a^{\frac{\phi(m)}{2}} \equiv 1 \pmod m.$$

In particular, there are no primitive roots modulo m.

Proof. Let $\ell = \operatorname{lcm}(\phi(k), \phi(n))$. By Euler's Theorem, we have

$$a^{\phi(k)} \equiv 1 \pmod k \quad \text{and} \quad a^{\phi(n)} \equiv 1 \pmod n,$$

hence

$$a^{\ell} \equiv 1 \pmod k \quad \text{and} \quad a^{\ell} \equiv 1 \pmod n.$$

Thus $a^{\ell} \equiv 1 \pmod m$ by CRT. Finally, from Proposition 10 (iii), we have

$$\ell \cdot (\phi(k), \phi(n)) = \phi(k)\phi(n) \implies \ell \mid \frac{\phi(k)\phi(n)}{2} = \frac{\phi(m)}{2}$$

where we used the fact that $2 \mid (\phi(k), \phi(n))$ as both $\phi(k), \phi(n)$ are even. Then $a^{\frac{\phi(m)}{2}} \equiv 1 \pmod m$, as desired. The last statement is clear from $\phi(m)/2 < \phi(m)$. ☕

Corollary 21. *If $m > 0$ is divisible by two different odd primes then, there are no primitive roots modulo m.*

Proof. We can write $m = p^d q^{\ell} r$, where $p \neq q$ are two odd primes and $(r, p) = (r, q) = 1$. Let $k = p^d$ and $n = q^{\ell} r$, so that $m = kn$ and $(k, n) = 1$. By the formula for ϕ, we also have that

$$\phi(k) = p^{d-1}(p-1) \quad \text{and} \quad \phi(n) = q^{\ell-1}(q-1)\phi(r)$$

are even, so we can apply Theorem 38. ☕

Corollary 22. *If m is divisible by $4p$ with p an odd prime, then there are no primitive roots modulo m.*

Proof. We can write $m = 2^d p^{\ell} r$ with $d \geq 2$, $(2p, r) = 1$. Let $k = 2^d$ and $n = p^{\ell} r$, so that $m = kn$ and $(k, n) = 1$. By the formula for ϕ, we also have that

$$\phi(k) = 2^{d-1} \neq 1 \quad \text{and} \quad \phi(n) = p^{\ell-1}(p-1)\phi(r)$$

are even, so we can apply Theorem 38. ☕

Theorem 39. *Suppose $m = 2^d$, $d \geq 3$. Then*

(A) $a^{2^{d-2}} \equiv 1 \pmod m$ for all $a \in \mathbb{Z}$ odd.
(B) There is no primitive root modulo m.

Proof. We will use induction on $d \geq 3$ to prove (A).

Base: Let $d = 3$. Then $m = 8$ and $2^{d-2} = 2$. We check

$$1^2 \equiv 1 \pmod 8, \quad 3^2 \equiv 9 \equiv 1 \pmod 8, \quad 5^2 \equiv 25 \equiv 1 \pmod 8, \quad 7^2 \equiv 1 \pmod 8.$$

Hypothesis: Suppose the result is valid for $d-1$, that is, $a^{2^{d-3}} \equiv 1 \pmod{2^{d-1}}$.

Step: Let $d > 3$. The induction hypothesis is equivalent to $a^{2^{d-3}} = 1 + 2^{d-1}k$ for some $k \in \mathbb{Z}$. Squaring both sides gives

$$a^{2^{d-2}} = (1 + 2^{d-1}k)^2 = 1 + 2^d k + 2^{2d-2}k^2,$$

which, since $2d - 2 \geq d$ for $d \geq 3$, implies

$$a^{2^{d-2}} \equiv 1 \pmod{2^d}.$$

This completes the proof of (A). Finally, from (A) and $2^{d-2} < \phi(m) = 2^{d-1}$ it follows there is no integer of order $\phi(m)$, proving (B). ☕

Putting together these results we conclude that primitive roots may exist only for the integers $m = 1, 2, 4, p^d$ or $2p^d$, where $d \geq 1$ and p is an odd prime. The following theorem guarantees that primitive roots exist for all such integers.

Theorem 40 (Primitive Root Theorem)**.** *Let $m \in \mathbb{Z}_{>0}$. Then a primitive root modulo m exists if and only if $m = 1, 2, 4, p^d$ or $2p^d$, where $d \geq 1$ and p is an odd prime.*

This result is clear for $m = 1, 2, 4$ and, in the next section, we will prove it for $m = p$ a prime. To close this section, we will prove the above result for $m = 2p^d$ assuming it to be true for $m = p^d$. More precisely, we will prove that (1) implies (2) in the following result.

Theorem 41. *Let p be an odd prime and $d \geq 1$. Then,*

(1) there exist a primitive root modulo p^d;
(2) there exist a primitive root modulo $2p^d$.

Proof of part (2). Write $n = 2p^d$. Let r be a primitive root mod p^d which exists by part (1). Then $(r, p^d) = 1$ and, since $r \equiv r + p^d \pmod{p^d}$, if r is even we replace it by $r + p^d$ which is odd. So, we can assume r is odd and $(2p^d, r) = 1$.

We aim to show that r is also a primitive root mod n. Note that $\phi(2p^d) = \phi(2)\phi(p^d) = \phi(p^d)$. By Proposition 27, we have $\operatorname{ord}_n r \mid \phi(2p^d) = \phi(p^d)$. Moreover,

$$r^{\operatorname{ord}_n r} \equiv 1 \pmod{n = 2p^d} \implies r^{\operatorname{ord}_n r} \equiv 1 \pmod{p^d}$$

which, by Proposition 27, implies $\operatorname{ord}_{p^d} r = \phi(p^r) \mid \operatorname{ord}_n r$. Now, we have shown that $\operatorname{ord}_n r \mid \phi(p^d)$ and $\phi(p^d) \mid \operatorname{ord}_n r$, therefore $\operatorname{ord}_n r = \phi(p^d) = \phi(2p^d)$ because both $\operatorname{ord}_n r$ and $\phi(p^d)$ are positive. We conclude that r is a primitive root modulo $n = 2p^d$. ☕

Exercises.

Exercise 26.9.

(a) Show that 2 is a primitive root modulo 19.
(b) How many incongruent primitive roots modulo 19 are there?
(c) By Euler's Theorem, we know that $a^{18} \equiv 1 \pmod{19}$ for any a coprime to 19. Explain why a is not necessarily a primitive root modulo 19.
(d) Determine, with proof, a maximal set of incongruent primitive roots modulo 19.

27. Primitive Roots for Primes

The objective of this section is to prove the following result

Theorem 42. *Let p be a prime. Then there exists a primitive root modulo p.*

Consider a polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with integer coefficients $a_i \in \mathbb{Z}$. We call n the *degree* of f and we say that f is *monic* if $a_n = 1$. We call an integer c satisfying $f(c) \equiv 0 \pmod m$ a *root of f modulo m.*

Example 27.1. Let $f(x) = x^3 + x + 1$. We have

$$f(0) = 1 \equiv 1 \pmod 2 \quad \text{and} \quad f(1) = 3 \equiv 1 \pmod 2,$$

so f has no roots modulo 2. Now, working modulo 3, we obtain

$$f(0) = 1 \equiv 1 \pmod 3, \quad f(1) = 3 \equiv 0 \pmod 3, \quad f(2) = 11 \equiv 2 \pmod 3,$$

showing that 1 is a root modulo 3 but 0 and 2 are not. We also have $f(4) = 69 \equiv 0 \pmod 3$ so 4 is another root of f modulo 3, but $4 \equiv 1 \pmod 3$ is congruent to the root we already found. Since any integer is congruent mod 3 to $0, 1$ or 2 we conclude that f has exactly one root modulo 3.

The polynomial f of the previous examples has 0 and 1 roots modulo 2 and 3, respectively. In both cases, the number of roots is smaller than the degree of f which is 3. The following lemma shows this is a general fact.

Lemma 12 (Lagrange)**.** *Let f be a monic polynomial of degree n with integer coefficients. Then, f has at most n roots modulo p.*

Proof. We use induction on the degree n of f.

Base: For $n = 1$, then $f(x) = x + a_0$ has one root, namely $x \equiv -a_0 \pmod p$.

Hypothesis: Suppose the statement is true for polynomials of degree $n-1$. That is, every polynomial of degree $n-1$ has at most $n-1$ roots mod p.

Step: Let f be a polynomial of degree n. For contradiction, assume f has $n+1$ roots mod p. Denote these roots by $c_0, c_1, \ldots, c_n$. Therefore, $f(c_k) \equiv 0 \pmod p$ and $c_i \not\equiv c_j \pmod p$ for $i \neq j$.

We compute

$$\begin{aligned} f(x) - f(c_0) &= x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0 - (c_0^n + a_{n-1}c_0^{n-1} + \cdots + a_1 c_0 + a_0) \\ &= x^n - c_0^n + a_{n-1}(x^{n-1} - c_0^{n-1}) + \cdots + a_1(x - c_0). \end{aligned}$$

Note that $x^i - c_0^i = (x - c_0)h_{i-1}(x)$, where $h_{i-1}(x)$ is a monic polynomial of degree $i-1$, hence

$$\begin{aligned} f(x) - f(c_0) &= (x - c_0)h_{n-1}(x) + a_{n-1}(x - c_0)h_{n-2}(x) + \cdots + a_1(x - c_0) \\ &= (x - c_0)g(x). \end{aligned}$$

Here, $g(x)$ is a monic polynomial of degree $n-1$. Now, evaluating x at c_i in the previous equality gives

$$f(c_i) - f(c_0) \equiv (c_i - c_0)g(c_i) \pmod p \iff (c_i - c_0)g(c_i) \equiv 0 \pmod p$$

and, since p is prime, this implies

$$c_i - c_0 \equiv 0 \pmod p \quad \text{or} \quad g(c_i) \equiv 0 \pmod p.$$

For $i > 0$, the first equivalence cannot occur since $c_k \not\equiv c_0 \pmod p$ by hypothesis. Hence $g(c_i) \equiv 0 \pmod p$ for all $i = 1, .., n$. Thus, g has degree $n-1$ and n different roots mod p, a contraction. We conclude that f has at most n roots mod p, as desired. ☕

We can now prove the following statement which implies Theorem 42.

Theorem 43. *Let p be a prime and $d \geq 1$ a divisor of $p-1$. Then, there are $\phi(d)$ integers a such that $1 \leq a \leq p-1$ such that $\operatorname{ord}_p(a) = d$.*

In particular, there are $\phi(p-1)$ primitive roots $\pmod p$.

Proof. Let $F(d)$ denote the number of integers a such that $1 \leq a \leq p-1$ and $\operatorname{ord}_p(a) = d$. The proof is divided into two main parts:

(1) We will show that either $F(d) = 0$ or $F(d) = \phi(d)$;
(2) Using (1), we will show that $F(d) = \phi(d)$ when $d \mid p-1$.

We start by proving (1). If $F(d) = 0$ there are no integers of order d.

Suppose $F(d) \neq 0$, so that there is at least one integer of order d. Note that any a of order d is a root mod p of $f(x) = x^d - 1$; indeed, $a^d \equiv 1 \pmod p \iff f(a) \equiv a^d - 1 \equiv 0 \pmod p$.

Fix a of order d. Note that $f(a^i) = (a^i)^d - 1 \equiv (a^d)^i - 1 \equiv 0 \pmod p$ and $a^i \not\equiv a^j \pmod p$ if $i \neq j$ are in the range $0 \leq i, j \leq d-1$. Then, $a^0, a^1, \dots, a^{d-1}$ are d distinct mod p roots of f. Since f has degree d, it follows from Lemma 12 that these are all the mod p roots of f.

We conclude that all the elements of order d are among the a^i and so we need to determine how many a^i, $1 \leq i \leq d-1$ have order d. Suppose a^i has order d. Then, from Proposition 28 (ii), we know that

$$\operatorname{ord}_p a^i = \frac{\operatorname{ord}_p a}{(\operatorname{ord}_p a, i)} \iff d = \frac{d}{(d,i)} \iff (d,i) = 1,$$

which occurs for $\phi(d)$ values of i in $1 \leq i \leq d-1$. Then $F(d) = \phi(d)$, as desired.

We will now prove (2). Since every a in $1 \leq a \leq p-1$ has a unique order d dividing $\phi(p) = p-1$ (by Proposition 27), we can group these elements based on their orders. In doing so, we see that the total amount of integers, $p-1$, is equal to the sum of the number of integers $F(d)$ for each order d. Therefore,

$$p - 1 = \sum_{\substack{d \mid p-1 \\ d>0}} F(d) = \sum_{\substack{d \mid p-1 \\ d>0}} \phi(d),$$

where the second equality follows from by Theorem 34. We conclude that

$$\sum_{\substack{d \mid p-1 \\ d>0}} (F(d) - \phi(d)) = \sum_{\substack{d \mid p-1 \\ F(d)=0}} (F(d) - \phi(d)) = -\sum_{\substack{d \mid p-1 \\ F(d)=0}} \phi(d) = 0.$$

Here, we used part (1) to discard all the terms such that $F(d) \neq 0$ in the first equality. Since $\phi(d) \geq 1$ for all d, we conclude that the last sum runs over the empty set, otherwise we have a contradiction. Thus $F(d) = \phi(d)$ for all $d \mid p-1$. ☕

Example 27.2. Find all integers of order 6 modulo 19.

We first show that 2 is a primitive root. We have $\phi(19) = 18$, so the possible order mod 19 is among the values $\{1,2,3,6,9,18\}$. We compute

$$2 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^6 \equiv 7, \quad 2^9 \equiv 18 \pmod{19}.$$

Since all of the above congruences have $\not\equiv 1 \pmod{19}$, we conclude $\operatorname{ord}_{19} 2 = 18$, as desired.

Since $\phi(6) = 2$, by Theorem 43, there are two integers of order 6 mod 19. From Corollary 19 we know they are congruent mod 19 to 2^i for some $1 \le i \le 18$. We need to find the values of i in this interval satisfying

$$6 = \operatorname{ord}_{19} 2^i = \frac{\operatorname{ord}_{19} 2}{(\operatorname{ord}_{19} 2, i)} = \frac{18}{(18,i)} \iff (18,i) = 3.$$

Therefore $i = 3$ or $i = 15$, hence

$$2^3 \equiv 8 \pmod{19} \quad \text{and} \quad 2^{15} \equiv 12 \pmod{19}$$

are the two order 6 elements.

27.1. **Carmichael Numbers, Revisited.** Recall that a Carmichael number is a composite integer $n > 0$ such that, for all $a \in \mathbb{Z}$ coprime to n, we have $a^{n-1} \equiv 1 \pmod{n}$. In Section 21, we have introduced Korset's criterion which classifies Carmichael numbers (see Theorem 24), but we only proved one direction of this theorem. The proof of the other direction requires the use of primitive roots. In this section, we finally complete the proof of Korset's criterion. More precisely, we will show the following implication.

Theorem 44. *Let $n > 2$ be a Carmichael number. Then,*

(i) n is squarefree, i.e $n = p_1 \cdots p_k$ with p_i distinct primes;
(ii) if $p \mid n$ is prime then $p - 1 \mid n - 1$.

Proof. Let $n > 2$ be a Carmichael number and $p \mid N$ a prime factor. We can write $n = p^k n'$ with $(p, n') = 1$ for some $n' \in \mathbb{Z}$. Note that to prove (i) we need to show that $k = 1$. By CRT, the system of congruences

$$x \equiv 1 + p \pmod{p^k}, \qquad x \equiv 1 \pmod{n'}$$

admits a solution, that is, there is an integer a satisfying

$$a \equiv 1 + p \pmod{p^k}, \qquad a \equiv 1 \pmod{n'}. \tag{27.3}$$

We note that $(a, n) = 1$. Indeed, if a prime $q \mid (a, n)$ then, either $q = p$ or q is a prime factor of n'. Reducing the first congruence mod q if $q = p$ or the second if $q \mid n'$ leads to $0 \equiv 1 \pmod{q}$ in both cases, a contraction. Therefore, since n is a Carmichael number, we have

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

Suppose now $k \ge 2$ so that $p^2 \mid n$. Reducing this congruence mod p^2 gives

$$a^{n-1} \equiv 1 \pmod{p^2} \implies (1+p)^{n-1} \equiv 1 \pmod{p^2}$$

where we used (27.3) in the implication above. We have, by the Binomial theorem[2], that

$$(1+p)^{n-1} = (1+p)(1+p)\cdots(1+p) \equiv 1+(n-1)p \pmod{p^2}.$$

Since $p \mid N$, we also have

$$1+(n-1)p = 1+np-p \equiv 1-p \pmod{p^2},$$

therefore,

$$1 \equiv (1+p)^{n-1} \equiv 1+(n-1)p \equiv 1-p \pmod{p^2} \implies -p \equiv 0 \pmod{p^2},$$

which is impossible. Thus $k=1$, completing the proof of (i).

We will now prove (ii). Let $p \mid n$ be a prime. Since n is squarefree by part (i), we have $(p, n/p) = 1$. Let b be a primitive root mod p. This primitive root exists by Theorem 42. By CRT, the system of congruences

$$x \equiv b \pmod{p}, \qquad x \equiv 1 \pmod{n/p}$$

admits a solution. That is, there is an integer a satisfying

$$a \equiv b \pmod{p}, \qquad a \equiv 1 \pmod{n/p}.$$

A similar argument as above shows that $(a,n)=1$ and, since n is a Carmichael number, we have

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

By Proposition 27 and since b is a primitive root mod p, we conclude

$$\operatorname{ord}_p b = \phi(p) = p-1 \mid n-1,$$

completing the proof of (ii). ☕

Exercises.

Exercise 27.4. Show that, if $f(x)$ is a polynomial of degree n with integer coefficients, and p and q are prime numbers such that $p \neq q$, then the congruence $f(x) \equiv 0 \pmod{pq}$ has at most n^2 incongruent solutions modulo pq.

Exercise 27.5.

(a) How many elements of order 6 modulo 17 are there?
(b) How many elements of order 4 modulo 17 are there?
(c) Find all elements of order 4 modulo 17 using the fact that 3 is a primitive root modulo 17.

[2] The binomial theorem:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

28. Index Arithmetic and Discrete Logarithms

Let n be an integer admitting a primitive root. Recall that, if r is a primitive root, then the set $\{1, r, r^2, \dots, r^{\phi(n)-1}\}$ is a reduced residue system mod n. In particular, for all $a \in \mathbb{Z}$ such that $(a,n) = 1$ we have $r^i \equiv a \pmod{n}$ for some i in the range $1 \le i \le \phi(n)$.

Definition 28.1. Let r be a primitive root mod n and $a \in \mathbb{Z}$ coprime to n. The *index of a relative to r* is the least positive integer i such that $r^i \equiv a \pmod{n}$. We denote this by $\operatorname{ind}_r a$.

Example 28.2. We know that $r = 3$ is a primitive root mod $n = 7$. We have already computed the first two rows of the following table. Using them we can determine all the indices relative to 3 mod 7.

i	1	2	3	4	5	6
$3^i \pmod{7}$	3	2	6	4	5	1

a	1	2	3	4	5	6
$\operatorname{ind}_3 a$	6	2	1	4	5	3

Remark 28.3. Note that the existence of a primitive root is necessary for the definition of the index to make sense. For instance, consider $n = 12$ and $r = 5$

i	1	2	3	4	5	6	7	8	9	10	11
$5^i \pmod{12}$	5	1	5	1	5	1	5	1	5	1	5

This shows that there is no integer i such that $5^i \equiv a \pmod{n}$ for $a \neq 1, 5$. This occurs because 5 is not a primitive root modulo 12. In fact, since there is no primitive root mod 12, the index does not make sense in this setting.

It is common to also refer to indices as *discrete logs* since they share properties similar to those of the usual logarithms of real numbers. This is clear from the following proposition.

Proposition 29. *Let r be a primitive root mod n. Let $a, b \in \mathbb{Z}$ be coprime to n and $d \ge 1$.*

(a) $\operatorname{ind}_r 1 \equiv 0 \pmod{\phi(n)}$
(b) $\operatorname{ind}_r r \equiv 1 \pmod{\phi(n)}$
(c) $\operatorname{ind}_r ab \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \pmod{\phi(n)}$
(d) $\operatorname{ind}_r a^d \equiv d \cdot \operatorname{ind}_r a \pmod{\phi(n)}$.

Proof.

(a) By definition of the primitive root, we have $r^{\phi(n)} \equiv 1 \pmod{n}$ and no smaller positive exponent i satisfies $r^i \equiv 1 \pmod{n}$. Thus $\operatorname{ind}_r 1 = \phi(n) \equiv 0 \pmod{\phi(n)}$.

(b) Since $i = 1$ is the smallest positive exponent such that $r^i \equiv r \pmod{n}$, we have

$$\operatorname{ind}_r r = 1 \equiv 1 \pmod{\phi(n)}.$$

(c) By definition of index, we have

$$r^{\operatorname{ind}_r(ab)} \equiv ab \equiv r^{\operatorname{ind}_r a} \cdot r^{\operatorname{ind}_r b} \equiv r^{\operatorname{ind}_r a + \operatorname{ind}_r b} \pmod{n},$$

hence, by Proposition 28 (i), we have

$$\operatorname{ind}_r ab \equiv \operatorname{ind}_r a + \operatorname{ind}_r b \quad (\text{mod } \operatorname{ord}_n r = \phi(n)).$$

(d) Similarly to (c), we have

$$r^{\operatorname{ind}_r a^d} \equiv a^d \equiv (r^{\operatorname{ind}_r a})^d \equiv r^{d \cdot \operatorname{ind}_r a} \pmod{n},$$

hence, by Proposition 28 (i), $\operatorname{ind}_r a^d \equiv d \cdot \operatorname{ind}_r a \pmod{\operatorname{ord}_n r} = \phi(n)$.

☕

We will now see how index arithmetic can be used to solve certain congruence equations. Let r be a primitive root mod n, $a, b, d \in \mathbb{Z}$ with $d \geq 1$ and consider the congruence equation

$$ax^d \equiv b \pmod{n}.$$

We can rewrite this equation as $r^{\operatorname{ind}_r ax^d} \equiv r^{\operatorname{ind}_r b} \pmod{n}$. By Propositions 28 and 29, we also have

$$\operatorname{ind}_r a + d \cdot \operatorname{ind}_r x \equiv \operatorname{ind}_r b \pmod{\phi(n)}.$$

Relabeling $y = \operatorname{ind}_r x$, $a' = d$, and $b' = \operatorname{ind}_r b - \operatorname{ind}_r a$, the equation transforms into the linear congruence in one variable

$$a'y \equiv b' \pmod{\phi(n)},$$

which we know how to solve using Theorem 19.

We will now solve some concrete equations in a couple of examples. For that we need to have access to a table of indices.

Example 28.4. For $n = 17$, we check that $r = 3$ is a primitive root and compute the table of indices relative to 3.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\operatorname{ind}_3 a$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

In the next two examples, we will not refer to the previous table, though it should be understood that we are using the results listed there.

Example 28.5. Determine all the integers satisfying $6x^{12} \equiv 11 \pmod{17}$.

We have $\phi(17) = 16$. Taking indices on both sides gives

$$\begin{aligned}
6x^{12} \equiv 11 \pmod{17} &\iff \operatorname{ind}_3 6 + 12 \cdot \operatorname{ind}_3 x \equiv \operatorname{ind}_3 11 \pmod{16} \\
&\iff 15 + 12 \cdot \operatorname{ind}_3 x \equiv 7 \pmod{16} \\
&\iff 12 \cdot \operatorname{ind}_3 x \equiv 8 \pmod{16} \\
&\iff 3 \cdot \operatorname{ind}_3 x \equiv 2 \pmod{4} \\
&\iff \operatorname{ind}_3 x \equiv 2 \pmod{4} \\
&\iff \operatorname{ind}_3 x \equiv 2, 6, 10, 14 \pmod{16} \\
&\iff x \equiv 3^{\operatorname{ind}_3 x} \equiv 3^2, 3^6, 3^{10}, 3^{14} \pmod{17} \\
&\implies x \equiv 9, 15, 8, 2 \pmod{17}.
\end{aligned}$$

Here, we have changed from modulus 16 to 4 using Lemma 7. See also Exercise 13.19.

Example 28.6. Determine all the integers satisfying $7^x \equiv 6 \pmod{17}$.

Taking indices on both sides we get

$$\begin{aligned} 7^x \equiv 6 \pmod{17} &\iff x \cdot \operatorname{ind}_3 7 \equiv \operatorname{ind}_3 6 \pmod{16} \\ &\iff 11x \equiv 15 \pmod{16} \\ &\iff 33x \equiv 45 \pmod{16} \\ &\iff x \equiv 13 \pmod{16}. \end{aligned}$$

We note that, in this example, the original congruence is mod 17 but the final description of the integer solutions is mod 16.

The last two examples show that particular non-linear congruence equations can be solved using indices. As for a general theorem, we will prove the following criterion to decide if certain congruence equations have solutions.

Theorem 45. *Let n be an integer admitting a primitive root. Let $a, k \in \mathbb{Z}$ with $(a, n) = 1$ and $k \geq 1$. Consider the congruence equation*

$$x^k \equiv a \pmod{n}. \tag{28.7}$$

Write $d = (k, \phi(n))$. Then,

(a) if $a^{\frac{\phi(n)}{d}} \not\equiv 1 \pmod{n}$, then (28.7) has no solutions;
(b) if $a^{\frac{\phi(n)}{d}} \equiv 1 \pmod{n}$, then (28.7) has exactly d non-congruent solutions mod n.

Proof. Let r be a primitive root $\pmod{n}$. We have,

$$x^k \equiv a \pmod{n} \iff k \cdot \operatorname{ind}_r x \equiv \operatorname{ind}_r a \pmod{\phi(n)}.$$

By Theorem 19, the above linear congruence, in the variable $y = \operatorname{ind}_r x$, has no solutions if $d \nmid \operatorname{ind}_r a$ and d non-congruent solutions if $d \mid \operatorname{ind}_r a$. We show that the condition $d \mid \operatorname{ind}_r a$ is equivalent to $a^{\frac{\phi(n)}{d}} \equiv 1 \pmod{n}$ which proves (A) and (B) simultaneously. Indeed,

$$\begin{aligned} a^{\frac{\phi(n)}{d}} \equiv 1 \pmod{n} &\iff \operatorname{ind}_r a^{\frac{\phi(n)}{d}} \equiv \operatorname{ind}_r 1 \equiv 0 \pmod{\phi(n)} \\ &\iff \left(\frac{\phi(n)}{d}\right) \operatorname{ind}_r a \equiv 0 \pmod{\phi(n)} \\ &\iff d \mid \operatorname{ind}_r a. \end{aligned}$$

☕

We finish this section with the following example.

Example 28.8. Decide how many non-congruent solutions the equation $x^3 \equiv 6 \pmod{7}$ has.

In the notation of Theorem 45, we have

$$a = 6, \quad n = 7, \quad k = 3, \quad d = (3, \phi(7)) = (3, 6) = 3,$$

and computing

$$a^{\frac{\phi(n)}{d}} = 6^2 \equiv 36 \equiv 1 \pmod{7},$$

we conclude that $x^3 \equiv 6 \pmod{7}$ has $d = 3$ non-congruent solutions mod 7. Indeed, direct calculation shows the solutions are $x \equiv 3, 5, 6 \pmod{7}$.

Exercises.

Exercise 28.9. Given that $3^{18} \equiv 9 \pmod{17}$, explain why $\operatorname{ind}_3(9) \neq 18$.

Exercise 28.10. Prove that the congruence $x^5 \equiv 1 \pmod{52579}$ has exactly one solution, $x \equiv 1 \pmod{52579}$. Use the fact that 52579 is a prime.

29. Nonlinear Diophantine Equations

A Diophantine equation in one or more variables, which is not linear in the sense of Definition 11.3, is called *nonlinear*. In Section 11, we have studied linear Diophantine equations and completely solved the case of two variables. There is no analogous result for the nonlinear case. Moreover, it is a theorem that there is no algorithm that will solve all nonlinear Diophantine equation, and it is usually very hard to solve particular examples. Nevertheless, there are many methods that can be used for particular instances or families; for example, in Section 15, we have used the congruence method to prove that $3x^3+2=y^2$ has no integer solutions. Depending on the situation, other methods may find a partial or complete list of solutions and sometimes one finds all the solutions but has no proof there are no more.

Example 29.1. The following are examples of famous nonlinear Diophantine equations:

(1) The *Pythagorean Equation*
$$x^2+y^2=z^2;$$

(2) The *Fermat Equation*
$$x^n+y^n=z^n, \quad \text{where} \quad n\geq 3;$$

(3) The *Pell equation*
$$x^2-ny^2=1,$$
where $n\in\mathbb{Z}_{>0}$ is not a square.

In the next two sections, we will solve two classical examples of nonlinear Diophantine equations. More precisely, we will describe the complete set of solutions (a,b,c) satisfying $\gcd(a,b,c)=1$ of the equations $x^2+y^2=z^2$ and $x^4+y^4=z^4$.

Exercises.

Exercise 29.2. Which of the following equations are nonlinear?
$$x^2=1, \quad x+y+z=4, \quad xy=3, \quad y=1, \quad z+y^2=7$$

30. Pythagorean Triples

It is very well known that, given a right triangle, the square of the hypotenuse is equal to the sum of the squares of the other two sides. This statement can be made more precise in the following way.

Theorem 46 (Pythagora's theorem)**.** *Let x, y, z be the sides of a right triangle, where z corresponds to the hypothenuse. Then, $x^2 + y^2 = z^2$.*

Examples 30.1. Here are a few solutions to the Pythagorean equation:

(1) $1^2 + 1^2 = (\sqrt{2})^2$
(2) $3^2 + 4^2 = 5^2$
(3) $(-3)^2 + 4^2 = 5^2$
(4) $9^2 + 12^2 = 15^2$

We are interested in $x^2 + y^2 = z^2$ as a Diophantine equation, so example (1) above is not a solution for us since $\sqrt{2} \notin \mathbb{Z}$. Also, solutions (2) and (3) are related by a change of sign; indeed, we can flip the sign of any variable and obtain a new solution. This occurs because the exponents are even. Therefore, we will restrict ourselves to only positive values of x, y, z.

Definition 30.2. We call $x, y, z \in \mathbb{Z}$ a *Pythagorean triple* if $x, y, z > 0$ and $x^2 + y^2 = z^2$.

Note that solution (4) can be obtained by multiplying solution (2) by 3. In general, if x, y, z is a Pythagorean triple, then

$$(dx)^2 + (dy)^2 = d^2(x^2 + y^2) = d^2 z^2 = (dz)^2,$$

so dx, dy, dz is also a Pythagorean triple for all $d > 0$. Conversely, suppose x, y, z is a Pythagorean triple with a common factor $(x, y, z) = d$. Then, we can write

$$x = dx_0, \quad y = dy_0, \quad z = dz_0$$

to obtain

$$(dx_0)^2 + (dy_0)^2 = (dz_0)^2 \implies x_0^2 + y_0^2 = z_0^2$$

with $(x_0, y_0, z_0) = 1$. Thus we can restrict our attention to coprime triples.

Definition 30.3. We call a Pythagorean triple x, y, z *primitive* if $(x, y, z) = 1$.

We start by proving some elementary properties of Pythagorean triples.

Proposition 30. *If x, y, z is a primitive Pythagorean triple then*

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

Proof. Suppose $(x, y) \neq 1$. Then $p \mid x$ and $p \mid y$ for some prime p. Thus $p \mid (x^2 + y^2) = z^2$, hence $p \mid z$ and $(x, y, z) \neq 1$, a contradiction. Similarly for (x, z) and (y, z). ☕

Proposition 31. *If x, y, z is a primitive Pythagorean triple then $x \not\equiv y \pmod 2$. That is, exactly one of x, y is odd and the other is even.*

Proof. By the previous proposition, x, y are not both even, otherwise $2 \mid (x, y)$.

Suppose x, y are both odd, i.e. $x \equiv y \equiv 1 \pmod 2$. Then, $x, y \equiv 1, 3 \pmod 4$ and

$$z^2 = x^2 + y^2 \implies z^2 \equiv x^2 + y^2 \equiv 2 \pmod 4$$

which is impossible because

$$0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 0,\ 3^2 \equiv 1 \pmod 4,$$

shows that 2 is not a square mod 4. ☕

30.1. **Classification of Primitive Pythagorean Triples.** Given a primitive Pythagorean triple, x, y, z, we know from Proposition 31 that x, y must have different parity. From the symmetry of the equation $x^2 + y^2 = z^2$, we can further assume y to be even.

Theorem 47. *The positive integers x, y, z form a primitive Pythagorean triple with even y if and only if there are integers $m, n > 0$ such that*

(1) $(m, n) = 1$*;*
(2) $m > n$*;*
(3) m *and* n *have different parity, that is,* $m \not\equiv n \pmod 2$*;*
(4) the values of x, y, z *are given by*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2.$$

Proof. Suppose m, n are positive integers satisfying (1), (2), (3) and (4). Let x, y, z be as in (4). We compute

$$\begin{aligned} x^2 + y^2 &= (m^2 - n^2)^2 + (2mn)^2 = m^4 - 2m^2n^2 + n^4 + 4m^2n^2 \\ &= m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2 = z^2, \end{aligned}$$

so x, y, z form a Pythagorean triple. Suppose x, y, z are not primitive. That is, there exists a prime p such that $p \mid x$, $p \mid y$, and $p \mid z$.

Since $x = m^2 - n^2 \equiv m - n \not\equiv 0 \pmod 2$ by (3), it follows that x is odd, so $p \neq 2$. Note also that p divides both $x + z = 2m^2$ and $z - x = 2n^2$, so $p \mid m$ and $p \mid n$, contradicting (1). Thus, x, y, z form a primitive Pythagorean triple.

Conversely, let x, y, z be a primitive Pythagorean triple with even y. From Proposition 30, we know that $(x, y) = (x, z) = (y, z) = 1$. We also have

$$x^2 + y^2 = z^2 \iff y^2 = z^2 - x^2 = (z - x)(z + x),$$

and dividing both sides by 4 we get

$$\left(\frac{y}{2}\right)^2 = \left(\frac{z - x}{2}\right)\left(\frac{z + x}{2}\right).$$

Since x, z are odd and y is even, $\frac{z-x}{2}$, $\frac{z+x}{2}$ and $\frac{y}{2}$ are integers.

We note that $\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = 1$. Indeed, suppose $\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = d > 1$. Then d divides both the sum and the difference of the two numbers, that is

$$d \,\Bigg|\, \left(\frac{z - x}{2} + \frac{z + x}{2}\right) = z \quad \text{and} \quad d \,\Bigg|\, \left(\frac{z - x}{2} - \frac{z + x}{2}\right) = x,$$

contradicting $(x, z) = 1$. Note also that $z > x$ so $\frac{z-x}{2}$, $\frac{z+x}{2}$ are both positive. Now, from applying Proposition 32 with $a = \frac{x+z}{2}$, $b = \frac{z-x}{2}$, and $c = \frac{y}{2}$, there are $m, n \in \mathbb{Z}_{>0}$ such that

$$\frac{z-x}{2} = n^2 \quad \text{and} \quad \frac{z+x}{2} = m^2.$$

Writing x, y, z in terms of m, n gives $z = m^2 + n^2$, $x = m^2 - n^2$ and

$$y^2 = z^2 - x^2 = (z-x)(z+x) = (2n^2)(2m^2) = 4m^2n^2,$$

hence $y = \pm 2mn$. Choosing the positive value of y proves (4). Since $x > 0$, we have $m > n > 0$, proving (2). If p divides n and m, then p divides x and z, contradicting $(x, z) = 1$; this proves (1). Finally, to prove (3), suppose both m, n are odd. Then,

$$z \equiv 1 + 1 \equiv 0 \pmod 2 \quad \text{and} \quad x \equiv 1 + 1 = 2 \equiv 0 \pmod 2,$$

a contradiction with $(x, z) = 1$. This shows m, n are not both odd and, since they are coprime by (1), they cannot be both even, proving (iii). ☕

Example 30.4. Using Theorem 47, we can easily produce non-trivial primitive Pythagorean triples. For example, taking $m = 5, n = 2$ gives

$$(x, y, z) = (21, 20, 29),$$

and taking $m = 6, n = 5$ gives

$$(x, y, z) = (11, 60, 61).$$

We can also take $m = 3^{10}$, $n = 2^{10}$ to obtain

$$(x, y, z) = (3485735825, 120932352, 3487832977).$$

Proposition 32. *Let $a, b, c \in \mathbb{Z}$ with $a, b > 0$, $(a, b) = 1$ and $ab = c^2$. Then a and b are squares. That is, there are positive integers m and n such that $a = m^2$ and $b = n^2$.*

Proof. Since $(-c)^2 = c^2$ we may assume $c > 0$. Consider the prime factorizations

$$a = p_1^{e_1} \cdots p_k^{e_k}, \qquad b = q_1^{s_1} \cdots q_m^{s_m}, \qquad c = \ell_1^{d_1} \cdots \ell_n^{d_n},$$

where p_i are distinct primes and similarly for q_i and ℓ_i. From $ab = c^2$, we have

$$(p_1^{e_1} \cdots p_k^{e_k})(q_1^{s_1} \cdots q_m^{s_m}) = \ell_1^{2d_1} \cdots \ell_n^{2d_n}.$$

Since $(a, b) = 1$ we have that $p_i \neq q_j$ for all i, j. By uniqueness of the prime factorization, we conclude that both sides of the equation are the unique prime factorization of c^2. It follows that $n = k + m$ and, for all $1 \leq i \leq k$ and $1 \leq j \leq m$, there are $1 \leq z_i, z_j \leq n$ such that

$$p_i^{e_i} = \ell_{z_i}^{2d_{z_i}} \qquad q_j^{s_j} = \ell_{z_j}^{2d_{z_j}}.$$

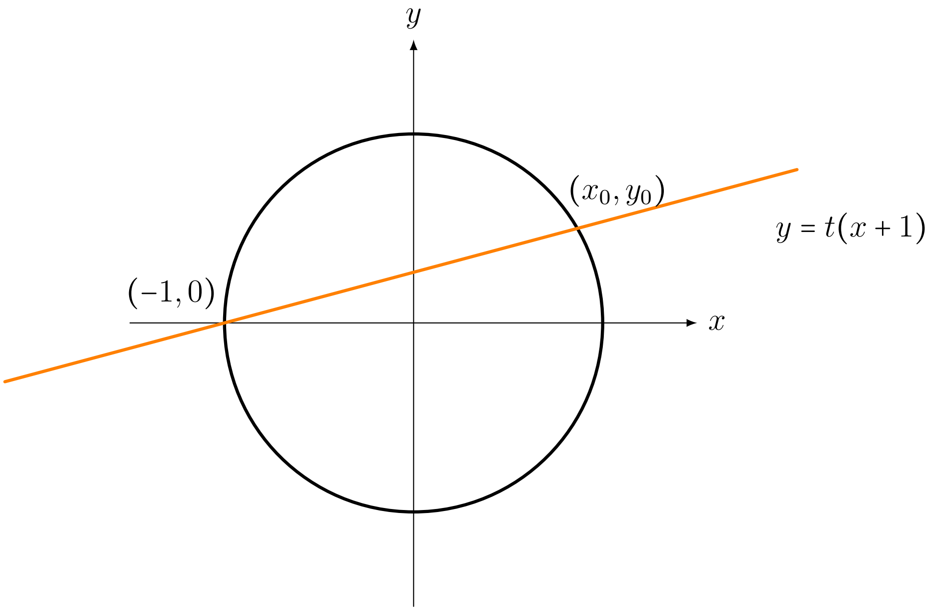
Therefore,

$$a = \ell_{z_1}^{2d_{z_1}} \cdots \ell_{z_k}^{2d_{z_k}} = (\ell_{z_1}^{d_{z_1}} \cdots \ell_{z_k}^{d_{z_k}})^2$$

hence a is a square. Similarly, b is a square. ☕

Remark 30.5. The hypothesis in Proposition 32 are necessary. Indeed, $(-4)(-9) = 6^2$ and $(-4, -9) = 1$ but neither -4 or -9 is a square. Moreover, $(3 \cdot 2^2) \cdot 3 = 6^2$ and both factors are positive, but neither $3 \cdot 2^2$ or 3 is a square. However, we also have $(2^2)(3^2) = 6^2$, where the factors are positive, coprime and squares, as predicted by the proposition.

30.2. **Geometric View of Pythagorean Triples.** In this section we will interpret Pythagorean triples in a geometric way as points of positive rational coordinates on the unit circle, which we recall is defined by the equation $x^2 + y^2 = 1$.



Suppose that $a, b, c > 0$ form a Pythagorean triple. Then, since $c \neq 0$, we have

$$a^2 + b^2 = c^2 \iff \left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1, \tag{30.6}$$

which shows that the point $(x_0, y_0) = \left(\frac{a}{c}, \frac{b}{c}\right)$ is on the unit circle. Conversely, if (x_0, y_0) is a point on the unit circle with rational coordinates x_0, y_0 then, for some choice of a common denominator c, we can write $x_0 = a/c$ and $y_0 = b/c$ and the equivalence (30.6) shows that a, b, c, when positive, form a Pythagorean triple.

Example 30.7. The triple $3^2 + 4^2 = 5^2$ gives rise to the point $\left(\frac{3}{5}, \frac{4}{5}\right)$ on the unit circle.

It follows from the previous discussion that we can describe Pythagorean triples by describing the points on the unit circle having rational coordinates. We will now obtain an explicit description of such points.

Consider the line $y = t(x+1)$, passing through the point $(-1, 0)$ and a point (x_0, y_0) on the unit circle. This line has slope $t = \frac{y_0}{x_0+1}$ which is a rational number if the coordinates x_0, y_0 are rational. In particular, when $(x_0, y_0) = \left(\frac{a}{c}, \frac{b}{c}\right)$ arises from a Pythagorean triple, the slope t is rational. Conversely, if we intersect the unit circle with the line $y = t(x+1)$ for a rational value of the slope t we obtain a point (x_0, y_0) with rational coordinates. Indeed, the intersection are points whose coordinates (x, y) satisfy both equations

$$x^2 + y^2 = 1 \qquad \text{and} \qquad y = t(x+1).$$

Substituting the equation for y into the first equation leads to

$$x^2 + (t(x+1))^2 = 1 \iff x^2 - 1 + t^2(x+1)^2 = 0 \iff (x-1)(x+1) + t^2(x+1)^2 = 0$$
$$\iff (x+1)((x-1) + t^2(x+1)) = 0,$$

hence

$$x + 1 = 0 \qquad \text{or} \qquad x - 1 + t^2(x+1) = 0.$$

Solving this for x gives

$$x = -1 \qquad \text{or} \qquad x = \frac{1-t^2}{1+t^2}.$$

Now, by replacing these values in the equation $y = t(x+1)$ we see that the corresponding y coordinates are

$$y = 0 \qquad \text{or} \qquad y = t\left(\frac{1-t^2}{1+t^2} + 1\right) = \frac{2t}{1+t^2}.$$

Therefore, the points of intersection of the line with the unit circle are

$$(-1, 0) \qquad \text{and} \qquad (x_0, y_0) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right).$$

The first point was expected due to our construction of the line, while the second has rational coordinates if the slope t is a rational number, as desired. Suppose now $t = m/n$ is rational with $m, n > 0$. Then,

$$(x_0, y_0) = \left(\frac{1-(m/n)^2}{1+(m/n)^2}, \frac{2(m/n)}{1+(m/n)^2}\right) = \left(\frac{m^2-n^2}{m^2+n^2}, \frac{2mn}{m^2+n^2}\right)$$

and by the argument in the beginning of this section, we obtain the Pythagorean triple

$$m^2 - n^2, \quad 2mn, \quad m^2 + n^2,$$

recovering the formulas in Theorem 47.

Exercises.

Exercise 30.8. Find formulas for the integers of all Pythagorean triples (x, y, z) with $z = y + 1$.

Exercise 30.9. Use the classification of primitive Pythagorean triples to show that if (x, y, z) is a PPT, then at least one of x, y, and z is divisible by 4.

31. Fermat's Last Theorem and Infinite Descent

We have fully described the solutions to the equation $x^2 + y^2 = z^2$, so now it is natural to consider

$$x^3 + y^3 = z^3, \quad x^4 + y^4 = z^4, \quad x^n + y^n = z^n,\ n \geq 3$$

and ask if it is possible to describe all solutions. To solve this problem, it has taken mathematicians around 350 years. A proof was completed by Andrew Wiles in 1995 and was one of the greatest mathematical achievements of the 20th century.

Theorem 48 (Fermat's Last Theorem)**.** *Let $a, b, c \in \mathbb{Z}$ satisfy the Fermat equation*

$$a^n + b^n = c^n$$

with $n \geq 3$. Then $abc = 0$.

To prove FLT, it is enough to consider the case $n = 4$ or $n = p$, for p an odd prime. Indeed, for a composite $n \geq 3$ we can write $n = ab$ where $b = 4$ or $b = p$ is an odd prime. Therefore, from a solution $x_0^n + y_0^n = z_0^n$ we get $(x_0^a)^b + (y_0^a)^b = (z_0^a)^b$. That is, a solution for exponent b. So, if we show that $x^b + y^b = z^b$ has no solutions in non-zero integers, then the original equation $x^n + y^n = z^n$ also cannot have solutions in non-zero integers.

We shall shortly prove Fermat's Last Theorem for $n = 4$ by combining Theorem 47 with a method called *infinite descent* due to Fermat.

Let us first sketch the main idea of infinite descent. Suppose x_0, y_0, z_0 is an integral solution to the equation $x^4 + y^4 = z^4$ such that $x_0y_0z_0 \neq 0$. Starting from this solution, we construct another solution to the same equation on non-zero integers x_1, y_1, z_1 with the property that $0 < z_1 < z_0$. Then, from x_1, y_1, z_1, we construct another solution on non-zero integers x_2, y_2, z_2 such that $0 < z_2 < z_1 < z_0$. Repeating this procedure, the values of z_i form a strictly decreasing infinite sequence of positive integers; this is clearly impossible, therefore the original solution x_0, y_0, z_0 cannot exist.

To illustrate infinite descent in a simpler situation, we will prove the following fact.

Theorem 49. *The number $\sqrt{2}$ is not rational.*

Proof. Suppose $\sqrt{2} \in \mathbb{Q}$. Then, there are coprime integers p and q such that $\sqrt{2} = \frac{p}{q}$. Thus, squaring both sides leads to

$$2 = \frac{p^2}{q^2} \iff 2q^2 = p^2 \implies 2 \mid p^2 \implies 2 \mid p,$$

so $p = 2r$ for some $r \in \mathbb{Z}_{>0}$. Then,

$$2q^2 = (2r)^2 = 4r^2 \iff q^2 = 2r^2,$$

hence, as above, $2 \mid q$, i.e. $q = 2s$ for some $s \in \mathbb{Z}_{>0}$. Therefore,

$$\frac{p}{q} = \frac{2r}{2s} = \frac{r}{s}, \quad \text{with } 0 < r < p,\ 0 < s < q$$

Now, starting from $2 = r/s$ and arguing as above, we get r', s' such that $2 = r'/s'$ with $0 < r' < r < p$ and $0 < s' < s < q$. Continuing this procedure generates a strictly decreasing infinite sequence of positive integers, which is a contradiction. ☕

Finally, we will prove the following theorem, which implies FLT for $n = 4$.

Theorem 50 (Fermat)**.** *The equation $x^4 + y^4 = z^2$ has no solutions in non-zero integers.*

Corollary 23. *FLT holds for exponent $n = 4$.*

Proof of Corollary. Suppose x_0, y_0, z_0 is a solution in non-zero integers to $x^4 + y^4 = z^4$. Then,

$$x_0^4 + y_0^4 = z_0^4 \iff x_0^4 + y_0^4 = (z_0^2)^2,$$

so that x_0, y_0, z_0^2 is a solution in non-zero integers to $x^4 + y^4 = z^2$, contradicting Theorem 50. ☕

Proof of Theorem 50. Suppose x_1, y_1, z_1 satisfy $x_1^4 + y_1^4 = z_1^2$ and $x_1 y_1 z_1 \neq 0$. Since the exponents are even we can assume $x_1, y_1, z_1 > 0$. Further, we can assume $(x_1, y_1) = 1$. Indeed, if $x_1 = dx_1'$, $y_1 = dy_1'$, then $(x_1', y_1') = 1$ and $x_1, y_1, z/d^2$ also satisfies the equation, because

$$d^4 x_1'^4 + d^4 y_1'^4 = z^2 \iff x_1'^4 + y_1'^4 = \left(\frac{z}{d^2}\right)^2.$$

We will show there is another solution $x_2, y_2, z_2 > 0$ such that $(x_2, y_2) = 1$ and $z_2 < z_1$.

Note that

$$x_1^4 + y_1^4 = (x_1^2)^2 + (y_1^2)^2 = z_1^2 \quad \text{and} \quad (x_1^2, y_1^2, z_1) = 1,$$

so that x_1^2, y_1^2, z_1 forms a primitive Pythagorean triple. Further, we know that, by swapping x_1^2 and y_1^2 if necessary, we can assume y_1^2 to be even, hence y_1 is even and x_1 odd. Then, from Theorem 47, there are coprime integers $m > n > 0$ with different parity such that

$$x_1^2 = m^2 - n^2, \quad y_1^2 = 2mn, \quad z_1 = m^2 + n^2.$$

In particular, $x_1^2 + n^2 = m^2$ so that x_1, n, m forms a primitive Pythagorean triple with n even. Again from Theorem 47, there are coprime integers $a > b > 0$ with different parity such that

$$x_1 = a^2 - b^2, \quad n = 2ab, \quad m = a^2 + b^2.$$

We claim that m, a and b are squares, that is, there are positive integers z_2, y_2, x_2 such that

$$m = z_2^2, \quad a = x_2^2, \quad b = y_2^2$$

with $(x_2, y_2) = 1$ since $(a, b) = 1$. Finally, from $m = a^2 + b^2$ and the claim, we obtain $x_2^4 + y_2^4 = z_2^2$, meaning that x_2, y_2, z_2 give a solution to the equation $x^4 + y^4 = z^2$ satisfying $(x_2, y_2) = 1$ and $x_2 y_2 z_2 \neq 0$. Furthermore,

$$0 < z_2 \leq z_2^2 = m \leq m^2 < m^2 + n^2 = z_1,$$

as desired. A contraction now follows by infinite descent as explained above.

We will now prove the claim. We have to show m, a, b are squares. Recall that

$$y_1^2 = 2mn = m(2n), \quad (m, 2n) = 1, \quad m > 0,\ 2n > 0,$$

hence m and $2n$ are squares by Proposition 32. Since $2n$ is a square, there is an integer $c > 0$ such that $2n = 4c^2$, hence $n = 2c^2$. Now

$$n = 2ab \iff 2c^2 = 2ab \implies ab = c^2$$

and, since a and b are positIve and coprime, by Proposition 32 they must be squares. ☕

Exercises.

Exercise 31.1. Prove that there is at most one square in any Pythagorean triple.

32. Fermat Factorization

Fermat factorization, named after Pierre de Fermat, is a factorization method based on the representation of an odd integer as the difference of two squares

$$n = a^2 - b^2 = (a-b)(a+b)$$

and, if neither factors $a-b$ or $a+b$ equals 1, this is a proper factorization of n.

Lemma 13. *Let $n \in \mathbb{Z}_{>0}$ be odd. Then there is a $1-1$ correspondence between factorizations of n into 2 positive odd numbers and differences of squares that equal n.*

Proof. Let $n = ab$, with a, b odd. We set

$$s = \frac{a+b}{2} \quad \text{and} \quad t = \frac{a-b}{2}.$$

Since a, b are both odd, we note that $s, t \in \mathbb{Z}$. It follows that $s^2 - t^2 = (s+t)(s-t)$ gives the desired factors of n. ☕

Based on this lemma, to apply Fermat factorization, one tries various values t, hoping that $t^2 - n$ is a square. More precisely, for $n > 0$ odd, we apply the following steps:

(i) Find the smallest integer $t \geq \sqrt{n}$

(ii) Consider the sequence of numbers

$$t^2 - n,\ (t+1)^2 - n,\ (t+2)^2 - n, \ldots$$

until a square $s_0^2 = (t+k)^2 - n$ is found.

(iii) Let $t_0 = t + k$. We have

$$n = t_0^2 - s_0^2 = (s_0 + t_0)(s_0 - t_0).$$

This procedure (ii) will terminate since

$$n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 \iff \left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2$$

and

$$\frac{n+1}{2} \geq \sqrt{n}.$$

Corollary 24. *Successive applications of Fermat's factorization will factor n completely. In particular, if $n = pq$ one application suffices.*

Example 32.1. Take $n = 6077$. The smallest integer t such that $t \geq \sqrt{n}$ is $t = 78$. We therefore compute the sequence of numbers $(t+k)^2 - n$ for $k \geq 0$ until a square is found.

$$t^2 - n = 78^2 - 6077 = 7$$

$$(t+1)^2 - n = 79^2 - 6077 = 164$$

$$(t+2)^2 - n = 80^2 - 6077 = 323$$

$$(t+3)^2 - n = 81^2 - 6077 = 484 = 22^2.$$

We conclude that

$$6077 = 81^2 - 22^2 = (81+22)(81-22) = 103 \cdot 59$$

Example 32.2. Fermat's factorization works best when n has factors which are close to each other. Let us consider the extreme case, where $n = pq$ with p, q being 'twin primes', that is, p and $q = p + 2$ are consecutive odd numbers.

We note first that $p < \sqrt{n} \leq p + 1$. Indeed, suppose for contradiction that $\sqrt{n} \leq p$. Then $n = \sqrt{n}\sqrt{n} \leq p^2$, which is impossible because $n = pq = p^2 + 2p$. Similarly, suppose $\sqrt{n} > p + 1$. It follows that $\sqrt{n} \geq p + 2 = q$ and $pq = \sqrt{n}\sqrt{n} \geq q^2$, a contradiction. So $t = p + 1$ is the smallest integer $\geq \sqrt{n}$. Next, we compute the numbers $(t + k)^2 - n$ for $k \geq 0$ until a square is found. Indeed, we see that

$$t^2 - n = (p + 1)^2 - p(p + 2) = p^2 + 2p + 1 - p^2 - 2p = 1 = 1^2$$

so we stop in one step. We conclude that

$$n = (p + 1)^2 - 1^2 = (p + 1 - 1)(p + 1 + 1) = pq.$$

Exercises.

Exercise 32.3. Using the Fermat factorization method, factor 8051.

33. The Pollard $p-1$ Factorization Method

We will now introduce a factorization method due to John Pollard. Let n be a large integer and compute $R_k \equiv 2^{k!} \pmod{n}$ recursively using fast modular exponentiation and the formula

$$R_k \equiv R_{k-1}^k \pmod{n}.$$

At each step, compute $(R_k - 1, n)$ with the Euclidean Algorithm. Since $0 \leq R_k \leq n-1$, we have $R_k - 1 < n$. Hence, if $(R_k - 1, n) > 1$, we have found a proper divisor of n.

Why does this work? Suppose p divides n and $p-1 \mid k!$ for some k. Note this is true at least for $k \geq p-1$. Hence, there exists $a \in \mathbb{Z}$ such that $k! = (p-1)a$, and we have

$$2^{k!} = 2^{(p-1)a} = \left(2^{p-1}\right)^a \equiv 1^a \equiv 1 \pmod{p}$$

by FLT. It follows that p divides $2^{k!} - 1$. Since $R_k \equiv 2^{k!} \pmod{n}$, we also have

$$R_k = 2^{k!} + bn$$

for some $b \in \mathbb{Z}$. Then $R_k - 1 = (2^{k!} - 1) + bn$, which implies $p \mid (R_k - 1)$ since $p \mid n$ and $p \mid (2^{k!} - 1)$. Therefore $p \mid (R_k - 1, n)$.

Example 33.1. Consider $n = 10403$. We compute

$R_k \pmod{n}$	$(n, R_k - 1)$
$R_2 \equiv 2^2 \equiv 4 \pmod{n}$	$(n, 3) = 1$
$R_3 \equiv 4^3 \equiv 64 \pmod{n}$	$(n, 63) = 1$
$R_4 \equiv 64^4 \equiv 7580 \pmod{n}$	$(n, 7579) = 1$
$R_5 \equiv 7580^5 \equiv 4438 \pmod{n}$	$(n, 4437) = 1$
$R_6 \equiv 4438^6 \equiv 6862 \pmod{n}$	$(n, 6861) = 1$
$R_7 \equiv 6862^7 \equiv 137 \pmod{n}$	$(n, 136) = 1$
$R_8 \equiv 137^8 \equiv 196 \pmod{n}$	$(n, 195) = 1$
$R_9 \equiv 196^9 \equiv 3619 \pmod{n}$	$(n, 3618) = 1$
$R_{10} \equiv 9798 \pmod{n}$	$(n, 9797) = 101.$

Since $(n, 9797) = 101 > 1$ we divide 10403 by 101 to get the factorization $10403 = 101 \cdot 103$.

Note that a large k always exists but is not practical. The Pollard $p-1$ factorization method is good if we can find small k such that $p-1 \mid k!$ for some $p \mid n$. This is likely to happen when $p-1$ has small prime factors.

Example 33.2. In the previous example, $n = 10403$ has the prime factor $p = 101$. We note that $p - 1 = 100 = 2^2 \cdot 5^2$ and $100 \mid k!$ for $k \geq 10$, finding a factor in 10 steps.

Of course, we can replace 2 by any other base $b \geq 2$. Lastly, we note that in practice, this is used after trial by division by small primes and before harder methods (which are not part of these notes!).

Exercises.

Exercise 33.3. Use the Pollard $p-1$ method to find a divisor of 689.

34. Cryptography

Suppose two friends, Alice and Bob, wish to communicate over an insecure channel in such a way that their opponent Eve cannot understand or change what is being said. To keep their conversation secure, Alice and Bob must consider the tools they are using to ensure that their messages are kept secret, as well as the possible attacks on these tools to find out their weaknesses.

The information that Alice wants to sent to Bob is called the *plaintext.* This is simply data that can be read and understood without any special measures. Using a key, Alice will *encrypt* the plaintext to obtain a *ciphertext.* To the unknowning observer, ciphertext appears as unreadable gibberish. However, Bob, who knows the key, can *decrypt* the ciphertext to obtain the original message from Alice. The following figure illustrates this process.

$$\begin{tikzcd}
\text{Plaintext} \arrow[r, "\text{Encryption}"] & \text{Ciphertext} \arrow[l, bend left, "\text{Decryption}"]
\end{tikzcd}$$

Definition 34.1. *Cryptography* is the design and implementation of secure systems. *Cryptanalysis* is the process of breaking secure systems. The science that encompasses both of these ideas is called *cryptology.*

The above process requires that both Alice and Bob have access to this key. However, this key needs to be kept secret otherwise third parties such as Eve can use the key to decrypt their messages. Encryption algorithms which have this property are called *symmetric cryptosystems* or *private key cryptosystems.* There is a form of cryptography which uses two different types of keys, one which is publicly available and used for encryption whilst the other is private and used for decryption. These latter types of cryptosystems are called *asymmetric cryptosystems* or *public key cryptosystems.* We will return to these types of cryptosystems later in this section.

In this section, we use the mathematical techniques that we have thus far learned to encrypt and decrypt messages that we wish to be kept secret. We will describe some historical encryption methods that were used in the pre-computer era to encrypt data, as well as the attacks on them.

Definition 34.2. A *cryptosystem* is made up of

- $\mathscr{P}$: the set of all plaintext messages,
- $\mathscr{C}$: the set of all ciphertext messages,
- K: the set of all keys,
  and a correspondence

$$k \mapsto (E_k, D_k), \quad \text{for some } k \in K$$

where

$$E_k : \mathscr{P} \to \mathscr{C}, \quad \text{the } \textit{Encryption function} \text{ and}$$
$$D_k : \mathscr{C} \to \mathscr{P}, \quad \text{the } \textit{Decryption function.}$$

These functions satisfy

$$D_k(E_k(x)) = x, \quad \forall x \in \mathscr{P}.$$

In the private key cryptosystem described above, Eve wants to know what information Bob and Alice are exchanging, and can attempt to decipher their messages and change the information being sent between the two. To keep their messages secret from Eve, Alice and Bob will first choose a random key $k \in K$. Then, to send a message to Bob over an insecure channel, Alice will encrypt her message using E_k. That is, if the message is a string

$$x = x_1 x_2 \cdots x_n,$$

for some integer $n > 0$, where each $x_i \in \mathscr{P}$, then she will encrypt each x_i as $y_i = E_k(x_i)$ and send the resulting ciphertext

$$y = y_1 y_2 \cdots y_n$$

to Bob. When Bob receives y, he deciphers it using D_k. Applying this protocol, their message should remain secret from Eve, provided that she is not able to determine the key k. In the following sections, we study classical cryptosystems based on congruences.

34.1. **The Shift Cipher.** When Julius Caesar sent messages to his generals, he did not trust his messengers. So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet. Only someone who knew the "shift by 3" rule could decipher his messages. This simple encryption algorithm is known as the *Caesar cipher*. Of course, one could shift the alphabet by any arbitrary number. Such a generalization of Caesar's cipher is called a *shift cipher*.

Before describing this encryption algorithm, we must first translate the letters of the English alphabet into numbers as follows.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Note that we could extend this list by including symbols and numbers. For now, however, we will just use the alphabet. In this case, $\mathscr{P} = \mathscr{C} = K = \mathbb{Z}/26\mathbb{Z}$. Let $b \in K$ so that $b \in \{0, 1, \ldots, 25\}$.

Definition 34.3. The *shift cipher* is described via the correspondence

$$b \longmapsto E_b(x) = x + b \pmod{26}, \quad D_b(x) = x - b \pmod{26}$$

where the key $b \in K$ is fixed and secret.

Example 34.4. Suppose Alice wants to send the message "MEET AT FOUR" to Bob using a shift cipher with the key $b = 3$. This plaintext may be represented numerically as

$$\text{MEET AT FOUR} \longrightarrow 12\ 04\ 04\ 19\ 00\ 19\ 05\ 14\ 20\ 17.$$

Applying the shift cipher $E_3(x) = x + 3 \pmod{26}$ to each of the above numbers yields the ciphertext

$$15\ 07\ 07\ 22\ 03\ 22\ 08\ 17\ 23\ 20 \longrightarrow \text{PHHWDWIRXU},$$

where "PHHWDWIRXU" is the corresponding alphabetic representation of the ciphertext. Hence, Alice sends the message "PHHWDWIRXU" to Bob.

Example 34.5. Using a shift cipher with the key $b = 19$, suppose Alice receives the message

BEHOXGBVDXEUTVDIEXTLXWHGMMXEETGRHGX

from Bob. Numerically, this corresponds to

01 04 07 14 23 06 01 21 03 23 04 20 19 21 03 08

04 23 19 11 23 22 07 06 12 12 23 04 04 19 06 17 07 06 23

To translate this back into plaintext, Alice uses the decryption function $D_3(x) = x - 19 \pmod{26}$ to obtain

08 11 14 21 04 13 08 02 10 04 11 01 00 02 10 15

11 04 00 18 04 03 14 13 19 19 04 11 11 00 13 24 14 13 04,

so that Alice deciphers the message as

I LOVE NICKELBACK PLEASE DONT TELL ANYONE.

The shift cipher is easy to break as soon as one understands the statistics of the underlying language, in our case English. The distribution of English letter frequencies is described in the table below.

Letter	Percentage	Letter	Percentage
A	8.2	N	6.7
B	1.5	O	7.5
C	2.8	P	1.9
D	4.2	Q	0.1
E	12.7	R	6.0
F	2.2	S	6.3
G	2.0	T	9.0
H	6.1	U	2.8
I	7.0	V	1.0
J	0.1	W	2.4
K	0.8	X	0.1
L	4.0	Y	2.0
M	2.4	Z	0.1

To break a shift cipher, we compute the frequencies of the letters in the ciphertext and compare them with the frequencies obtained from English.

For instance, suppose Eve intercepts the ciphertext

PTLKPAHALHASVUKVUKYBNZLCLYFTVYUPUN.

Suppose further that she knows $\mathscr{P}$, $\mathscr{C}$ and that an encryption function of the form

$$E_b = x + b \pmod{26}$$

was used. She wants to find b. To proceed, Eve begins by translating the ciphertext into its numerical equivalent as

15 19 11 10 15 00 07 00 11 07 00 18 21 20 10 21 20 10 24 01 13 25 11 02 11 24 05 19 21 24 20 15 20 13.

Looking at the frequency of each letter appearing in the ciphertext, we note that the letters L and U each occur four times. Since the most common letters in the English alphabet is 'E', it is reasonable to guess that L or U correspond to E. Indeed, suppose that E is encrypted as U. That is,

$$E_b(4) = 4 + b \equiv 20 \pmod{26} \implies b = 16.$$

Using this key, Eve decrypts the message as

25 03 21 20 25 10 17 10 21 17 10 02 05 04 20 05 04 20 08 11 23 09 21 12 21 08 15 03 05 08 04 25 04 23

which corresponds to

ZDVUZKRKVRKCFEUFEUILXJVMVIPDFIEZEX.

Of course, this is just nonsense so we suppose instead that E is encrypted as L. That is

$$E_b(4) = 4 + b \equiv 11 \pmod{26} \implies b = 7.$$

Using this key, Eve decrypts the message as

08 12 04 03 08 19 00 19 04 00 19 11 14 13 03 14 13 03 17 20 06 18 04 21 04 17 24 12 14 17 13 08 13 06.

This corresponds to

IMEDITATEATLONDONDRUGSEVERYMORNING

so that Eve deciphers the message as "I mediate at London Drugs every morning."

34.2. **The Affine Cipher.** A generalization of the shift cipher is the affine cipher. In this case, the key is (a, b, n) where a and n are coprime. We will denote the key simply by (a, b) when the value of n is clear from the context.

Definition 34.6. The corresponding encryption function for the *affine cipher* is

$$(a, b) \mapsto E_{a,b}(x) = ax + b \pmod{n}.$$

Of course, when $a = 1$, we recover the shift cipher.

We note that these ciphers can also be broken by frequency analysis, but unlike the shift cipher, we now need 2-bits of information. Indeed, we want to find

$$D_{a,b}(y) = cy + d$$

satisfying

$$D_{a,b}(E_{a,b}(x)) \equiv x \pmod{n} \quad \forall x \in \mathscr{P} \iff c(ax + b) + d = cax + cb + d \equiv x \pmod{n}.$$

Since this congruence must hold for all $x \in \mathscr{P}$, taking

$$\begin{aligned} x \equiv 0 \pmod{n} \quad &\text{yields} \quad cb + d \equiv 0 \pmod{n}, \quad \text{and} \\ x \equiv 1 \pmod{n} \quad &\text{yields} \quad ca + cb + d \equiv 0 \pmod{n}. \end{aligned}$$

Combining these, we obtain

$$c \equiv a^{-1} \pmod{n} \quad \text{and} \quad d \equiv -a^{-1}b \pmod{n},$$

where a^{-1} exists because a and n are coprime. However, since we do not have access to (a,b), we cannot determine $D_{a,b}$ and therefore need another way.

Example 34.7. Suppose we intercepted ciphertext

23 16 07 03 25 08 06 25 10 17 20 07 24 10 12 05 20 08 17 25 12

08 06 25 23 25 07 12 25 08 06 25 04 05 11 07 21 25 23 05 10 08

06 25 23 08 07 12 23 06 17 16 25 20 08 25 12 16 12 17 23 25.

This corresponds to

XQHDZIGZKRUHYKMFUIRZMIGZXZHMZIG

ZEFLHVZXFKIGZXIHMXGRQZUIZMQMRXZ

where the most common letters are Z and I. The most frequent letters in English are E and T, so we try

$$E \xrightarrow{E_{a,b}} Z \quad T \xrightarrow{E_{a,b}} I$$

$$4 \longrightarrow 25 \quad 19 \longrightarrow 8.$$

Therefore, $D_{a,b}(x) = cx + b$ must satisfy

$$\begin{cases} D_{a,b}(25) \equiv 4 \\ D_{a,b}(8) \equiv 19 \end{cases} \iff \begin{cases} 25c + d \equiv 4 \pmod{26} \\ 8c + d \equiv 19 \pmod{26}. \end{cases}$$

Subtracting both equations gives

$$17c \equiv -15 \equiv 11 \pmod{26}.$$

Since $17^{-1} \equiv 23 \pmod{26}$, we obtain

$$c \equiv 11 \cdot 23 \equiv 19 \pmod{26}$$

$$d \equiv 4 - 25 \cdot 19 \equiv 23 \pmod{26}$$

hence $D_{a,b}(y) = 19y + 23 \pmod{26}$. If decrypting the intercepted ciphertext message with this function leads to meaningful text, we conclude that

$$E \leftrightarrow Z \quad \text{and} \quad T \leftrightarrow I$$

was the correct guess. Indeed, using (19,23) as our decryption key, we obtain

18 15 00 02 04 19 07 04 05 08 13 00 11 05 17 14 13 19 08 04 17

19 07 04 18 04 00 17 04 19 07 04 21 14 24 00 06 04 18 14 05 19

07 04 18 19 00 17 18 07 08 15 04 13 19 04 17 15 17 08 18 04,

which corresponds to the plaintext

SPACE THE FINAL FRONTIER

THESE ARE THE VOYAGES OF THE STARSHIP ENTERPRISE.

Sometimes we may need more than 2-bits of information to break the affine cipher. Suppose we enlarge our alphabet to 28 symbols by adding

$$\begin{aligned} \text{blank space} &= 26 \\ ? &= 27 \end{aligned}$$

and we use the affine cipher

$$f(x) = ax + b \pmod{28}.$$

We want to find

$$g(y) = cy + d \pmod{28},$$

which is the decryption of f.

Example 34.8. Suppose we intercept the ciphertext

27 10 17 18 11 13 15 11 18 10 01 11 17 13 12 15 06 01 01 26 11 24 01 22 03 23

13 18 05 11 03 04 11 17 00 11 21 00 22 17 26 01 00 11 15 27 17 22 22 03 27 14

which corresponds to the message

?KRSLNPLSKBLRNMPGBB LYBWDXNSFLDELRALVAWR BALP?RWWD?O.

Suppose by frequency analysis, we know

$$\begin{array}{cccccc} \text{blank space} & \overset{g}{\to} & \text{D} & \text{O} & \overset{g}{\to} & ? \\ 26 & \longrightarrow & 3 & 14 & \longrightarrow & 27, \end{array}$$

That is,

$$\begin{cases} 26c + d \equiv 3 \pmod{28} \\ 14c + d \equiv 27 \pmod{28}. \end{cases}$$

Subtracting both gives

$$12c \equiv 4 \pmod{28}$$

so we get 3 solutions

$$\begin{cases} c \equiv 5 \\ d \equiv 13 \end{cases} \quad \text{or} \quad \begin{cases} c \equiv 12 \\ d \equiv 13 \end{cases} \quad \text{or} \quad \begin{cases} c \equiv 19 \\ d \equiv 13. \end{cases}$$

At this point we can

(1) Decipher the text with both and see if at least one makes sense;
(2) Continue with the next letter on the frequency analysis. Since L is the most frequent letter in the ciphertext, we suppose that

$$\begin{array}{ccc} \text{L} & \overset{g}{\to} & \text{blank space} \\ 11 & \longrightarrow & 26, \end{array}$$

$$g(11) \equiv 26 = 11c + d \pmod{28} \implies c = 15, d = 13.$$

and we decrypt the message to obtain the plaintext

22 07 00 19 26 08 18 26 19 07 04 26 00 08 17 18 15 04 04 03 26 21 04 11 14 02

08 19 24 26 14 05 26 00 13 26 20 13 11 00 03 04 13 26 18 22 00 11 11 14 22 27,

corresponding to

WHAT IS THE AIRSPEED VELOCITY OF AN UNLADEN SWALLOW?

34.3. **Exponential Ciphers.**

Definition 34.9. Let p be a prime. We encrypt $x \pmod p$ via the *exponential cipher*

$$f(x) = x^e \pmod p,$$

where the (p, e) is the encryption key with $e \in \mathbb{Z}$ such that $(e, p-1) = 1$. The decryption transformation is the exponential function

$$g(y) = y^d \pmod p$$

where $d \equiv e^{-1} \pmod{p-1}$.

Indeed, since $d \equiv e^{-1} \pmod{p-1}$, we have that $de \equiv 1 \pmod{p-1}$ and hence $de = 1 + k(p-1)$ for some integer k. It follows that

$$\begin{aligned} g(f(x)) &= g(x^e) \\ &\equiv (x^e)^d \pmod p \\ &\equiv x^{de} \pmod p \\ &\equiv x^{1+k(p-1)} \pmod p \\ &\equiv x^1 (x^{p-1})^k \pmod p \\ &\equiv x \pmod p \quad \text{by FLT since } x \not\equiv 0 \pmod p. \end{aligned}$$

Note that if $x \equiv 0 \pmod p$, then $g(f(x)) = g(0) = 0 \equiv 0 \pmod p$ also.

To use this cipher, both Bob and Alice must know the key (p, e), which is kept secret. We use the normal correspondence with an added zero (if necessary) to make all numbers have 2-digits. That is

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Example 34.10.

E	X	A	M	P	L	E
04	23	00	12	15	11	04

Next, we group the resulting numbers into blocks of $2m$ digits, where $2m$ is the largest positive integer such that all blocks are $< p$. We choose our blocks in this way so that the numerical value of each block does not get reduced modulo p. For instance, the word BB corresponds to 0101, and the word LJ corresponds to 1110. If we choose $p = 1009$ and $2m = 4$, then $0101 \equiv 1110 \pmod p$, so that BB is indistinguishable from LJ. In this case, for this value of p, the correct choice of block length is $2m = 2$. On the other hand, if $2525 < p < 252525$, then $m = 2$. Note that the largest value of a 2-letter word is ZZ, which corresponds to 2525.

Example 34.11. Take $p = 2633$ and $e = 29$ so that $(2632, 29) = 1$ and $m = 2$. In the example above, we group the blocks

$$0423\ 0012\ 1511\ 0425$$

where the last 25 is used to fill the last block so that every block has 4 digits. Using $f(x) = x^{29} \pmod{2633}$ yields the following ciphertext

$$2437\ 2425\ 1729\ 0687.$$

In order to decrypt an exponential cipher, one must compute d satisfying $ed \equiv 1 \pmod{p-1}$ and apply the function $g(x) = x^d \pmod{p}$ to each block. However, exponential ciphers resist frequency analysis, making them harder to break than affine ciphers.

Indeed, suppose Eve knows p and that the plaintext x corresponds to ciphertext y. Then she must solve for d in the equation

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

to obtain the decryption key d. By analogy with the real numbers, we call this the "discrete log problem" because

$$d = \log_y(x).$$

if we were working in $\mathbb{R}$. In general, no efficient classical algorithm is known for computing discrete logarithms. The simplest approach to compute d is to raise y to larger and larger powers k until $y^k \equiv x \pmod{p}$, however such an algorithm is practical only for small primes p.

More sophisticated algorithms exist, usually inspired by similar algorithms for integer factorization. These algorithms run faster than the naive algorithm, however none of them run in polynomial time. In other words, this problem is very hard computationally for large p; this is what makes exponential ciphers secure.

Example 34.12. Suppose that Eve intercepts the ciphertext

$$1207\ 2012\ 0214\ 1088\ 0034\ 1402\ 1795\ 1531\ 0155$$
$$0718\ 0931\ 2652\ 2186\ 2137\ 0186\ 1580\ 0884\ 2280.$$

Suppose that additionally, she knows that $p = 2707$ and that the plaintext 1802 corresponds to 1207. To decrypt this message, she must solve

$$1207^d \equiv 1802 \pmod{2707}.$$

Using the naive algorithm, Eve must compute 2570^k for $k \geq 1$ until $1207^k \equiv 1802 \pmod{2707}$. In doing so, she finds that this holds for any k in the set

$$\{217, 463, 709, 955, 1201, 1447, 1693, 1939, 2185, 2431, 2677\}.$$

In fact, by FLT, there are infinitely many values k for which $1207^k \equiv 1802 \pmod{2707}$. From here, Eve must test every one of these values as a potential decryption key d until a sensical plaintext is found. For instance, $d = 217$ yields

$$1802\ 2050\ 2253\ 1567\ 1763\ 1213\ 2649\ 1794\ 0508$$
$$0301\ 1200\ 1058\ 0124\ 1730\ 0134\ 0266\ 0406\ 1104,$$

which is nonsense since 2050 cannot correspond to any pair of letters. Similarly, $d = 463$ yields

$$1802\ 2616\ 1809\ 0668\ 2524\ 2274\ 0958\ 1193\ 0508$$
$$0532\ 1200\ 2544\ 0124\ 2617\ 0432\ 1668\ 2271\ 1104,$$

where again 2616 cannot correspond to any pair of letters. Finally, using $d = 709$, Eve computes

$$1802\ 1413\ 0418\ 0017\ 0409\ 2018\ 1912\ 2005\ 0508$$
$$1318\ 1200\ 0304\ 0124\ 1100\ 2524\ 1504\ 1415\ 1104,$$

which corresponds to the plaintext

SCONES ARE JUST MUFFINS MADE BY LAZY PEOPLE.

34.4. **The RSA Cryptosystem.** Up until now, we have looked at cryptosystems that required both communicating parties to have a copy of the same secret key. There is a form of cryptography which uses two different types of keys, one which is publicly available and used for encryption whilst the other is private and used for decryption. These latter types of cryptosystems are called *asymmetric cryptosystems* or *public key cryptosystems*. In this section, we will discuss the world's first public key cryptosystem, RSA.

RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1978. The RSA algorithm is based on the difficulty of finding prime factors of large integers. In such a system, any person can encrypt a message using the public key of the receiver, but such a message can be decrypted only with the receiver's private key. An analogy to this cryoptosystem is that of a locked mail box with a mail slot. The mail slot is exposed and accessible to the public - its location (the street address) is, in essence, the public key. Anyone knowing the street address can go to the door and drop a written message through the slot. However, only the person who possesses the key can open the mailbox and read the message.

Definition 34.13. To use an *RSA cipher*, each communicating party must choose two large primes p and q and an exponent e such that

$$1 < e < (p-1)(q-1) \quad \text{and} \quad (e, (p-1)(q-1)) = 1.$$

Let $n = pq$ so that $\phi(n) = (p-1)(q-1)$ and define $d = e^{-1} \pmod{\phi(n)}$. The (public) encryption key is (n, e) and the corresponding encryption function is

$$E_k(x) = x^e \pmod{n}.$$

The (private) decryption key is (n, d) with decryption function

$$D_k(x) = x^d \pmod{n}.$$

The following theorem verifies that D_k does indeed recover the original message.

Theorem 51. *We have $D_k(E_k(x)) \equiv x \pmod{n}$.*

Proof. We need to show $x^{ed} \equiv x \pmod{n}$. By CRT, it is enough to show that

$$x^{ed} \equiv x \pmod{p} \quad \text{and} \quad x^{ed} \equiv x \pmod{q}.$$

Suppose first that $x \equiv 0 \pmod{p}$. Then

$$x^{ed} \equiv 0 \equiv x \pmod{p},$$

and we are done. Suppose now that $x \not\equiv 0 \pmod{p}$. By construction, $d \equiv e^{-1} \pmod{\phi(n)}$ so

$$ed = 1 + \phi(n)k = 1 + (p-1)(q-1)k$$

hence

$$x^{ed} \equiv x^{1+(p-1)(q-1)k} \equiv x(x^{p-1})^{(q-1)k} \equiv x \pmod{p},$$

where the last equivalence follows by FLT since $(x,p) = 1$. The same argument holds for $x^{ed} \equiv x \pmod{q}$, which completes the proof. ☕

Example 34.14. Take $p = 11, q = 3$. Then $n = pq = 33$ so that $\phi(n) = (p-1)(q-1) = 20$. Choose $e = 3$ and note that this is a valid choice since $(e,(p-1)(q-1)) = (3,20) = 1$. In this case, we find that $d = e^{-1} \equiv 7 \pmod{\phi(n)}$. Hence, the public key is given by $(n,e) = (33,3)$ and the private key is $(n,d) = (33,7)$.

Suppose we want to use this system to encrypt the message "This is an example." Since $25 < n < 2525$, after changing each letter into its corresponding 2-digit number, we group the resulting numbers into blocks of $2m$ digits, where $m = 1$. This means that $2m = 2$ is the largest positive integer such that all blocks are $< n$. Hence, we have

19 07 08 18 08 18 00 13 04 23 00 12 15 11 04

Now, for each of these 2-digit numbers x, we compute $x^3 \pmod{33}$ to obtain the ciphertext integers

28 13 17 24 17 24 00 19 31 23 00 12 09 11 31.

Example 34.15. Consider the system $(n,e) = (3127,11)$ and suppose we want to encrypt the message "Number theory is my favourite class." Converting the plaintext into digits and separating these digits into blocks yields

1320 1201 0417 1907 0414 1724 0818 1224 0500 2114 2017 0819 0402 1100 1818.

Of course, here, since $n = 3127$ and $2525 < n < 252525$, we take $m = 2$ so that each block has $2m$ digits to ensure that each block is $< n$. Using our encryption key, we compute $x^e \pmod{n}$ for each block x. This gives the encrypted ciphertext

1464 2549 0702 1854 1122 2356 1196 2193 2150 0399 1611 1499 1988 0991 0100.

The reason why RSA is secure is that factoring large integers is very hard computationally. Indeed, suppose we factor $n = pq$, then we can compute $\phi(n) = (p-1)(q-1)$ and since (n,e) is public we can find $d \equiv e^{-1} \pmod{\phi(n)}$ via the Euclidean Algorithm. To break RSA we only need the value of d which can be computed from $\phi(n)$ and e and not necessarily the factorization of n. However, the following argument shows that computing the value of $\phi(n)$ is not simpler than factoring n. Indeed, suppose we know both n and $\phi(n)$. We have

(i) $\phi(n) = (p-1)(q-1) = pq - p - q + 1 \iff p + q = pq - \phi(n) + 1 = n - \phi(n) + 1$
(ii) $p - q = \sqrt{(p+q)^2 - 4n}$,

Therefore, with the value of n and $\phi(n)$ we compute $p + q$ using (i), then we use (ii) to compute $p - q$. Finally we can determine p and q, computing

$$\begin{cases} p = \frac{1}{2}((p+q) + (p-q)) \\ q = \frac{1}{2}((p+q) - (p-q)), \end{cases}$$

showing that from knowing $\phi(n)$ we can factor n. There have been however successful attacks on RSA but these issues were solved by being more careful when setting up an implementation. For example, the primes p and q should not be close because of Fermat factorization (see Example 32.2); moreover, we should choose p and q such that $p-1$, $q-1$ have large factors to avoid a successful factorisation of $n = pq$ with Pollard $p-1$ factorization method from Section 33.

Exercises.

Exercise 34.16. Consider an affine cipher with encryption key $(a, b, 26)$. We say that a letter with numerical value x is "fixed" if x is enciphered as x. Is it possible to choose a, b with $\gcd(a, 26) = 1$, so that there is

(a) exactly one fixed letter?
(b) exactly two fixed letters?
(c) exactly three fixed letters?
(d) exactly four fixed letters?
(e) exactly 13 fixed letters?

In each part, give a proof if the answer is "no," and an example if the answer is "yes".

Exercise 34.17.

(a) Consider the RSA encryption scheme with public encryption key $(2623, 11)$. Encipher the message PATIENCE IS A VIRTUE.
(b) Decipher the message 284 926 2489 445 662 2445 926 178 using the encryption key as in Part (a).

Exercise 34.18. Suppose a cryptanalyst discovers a message P that is not relatively prime to the enciphering modulus $n = pq$ used in an RSA cipher. (He can confirm this by running the Euclidean algorithm.) Show that the cryptanalyst can factor n.