Elementary Number Theory
Lecture Notes

Michael Francis

Spring 2023

Contents

Chapter 1

Introduction

These notes were written to accompany a short four-week course in elementary number theory which I gave at the University of Western Ontario in Spring 2023. A number of references were helpful in putting these notes together, especially as sources of exercises and examples. The main references used were *Number Theory* by G. E. Andrews; a set of unpublished lecture notes on elementary number theory by C. M. Mynhardt; *Discrete Mathematics: Number Theory, Modular Arithmetic, and Graph Theory*, by S. A. Rankin & I. J. W. Robinson; *Beginning Number Theory* by N. Robbins; and *Elementary Number Theory and Its Applications* by K. H. Rosen. It is also a pleasure to thank Xiangyuan Liang, Zirui Si and Sina Babaei Zadeh for numerous corrections which helped to improve the readability of these notes.

Number Theory, not surprisingly, refers to the study of various sorts of numbers. Of all the diverse things which we sometimes think of as numbers, the positive integers are in some sense the most basic and therefore the most important. Among the positive integers, the prime numbers $\{2, 3, 5, 7, 11, \ldots\}$ play a particularly important role. The *Fundamental Theorem of Arithmetic* shows that they are the basic building blocks out of which all positive integers can be built.

Number theory is perhaps the oldest branch of mathematics and its history stretches back millennia. Some problems in number theory were considered by ancient mathematicians more than 2000 years ago, but still remain open today.

For much of its history, number theory was also considered one of the "purest" branches of mathematics. *Pure Mathematics* refers to mathematics with no (or very few) applications; mathematics whose problems are motivated primarily by aesthetics and theoretical considerations. This paradigm completely changed, however, with the advent of computer technology. Number theory is now the foundation of modern cryptography on which our computer security protocols are based. Cryptography is just one of many applications of number theory which have emerged in the modern era.

The term *Elementary Number Theory* refers to the part of number theory which does not make heavy use of other mathematical topics. For example, *Analytic Number Theory* is a branch of number theory which utilizes the theory of complex variables and *Algebraic Number Theory* is a branch of number theory which makes heavy use of abstract algebra. By contrast,

problems in elementary number theory can be stated using only basic notions (integers, primes, divisibility, congruence, etc.) and can be solved without recourse to specialized tools. Note that elementary number theory does not refer to number theory that is easy! Much ingenuity may still be needed to devise a proof of a statement, even when no specialized tools are needed.

A rough overview of the topics covered in these notes is as follows: Chapter 2 covers basic properties of the integers including a review of induction, the relation of divisibility and the Euclidean algorithm. Chapter 3 focuses on prime numbers, covering Euler's proof that there are infinitely many primes, the unique factorization theorem, Mersenne primes, Fermat primes, and a brief discussion of the prime number theorem. Chapter 4 covers modular arithmetic, rings of integers modulo n, Fermat's little theorem (and Euler's generalization) and the Chinese remainder theorem.

Chapter 2

The Integers

Throughout this course we use the following notations:

- The integers: $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$
- The natural numbers: $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$
- The positive integers: $\mathbb{Z}^+ = \{1, 2, 3, 4, \ldots\}$
- The rational numbers: $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z} \text{ and } b \neq 0\}$
- The real numbers: $\mathbb{R} = (-\infty, \infty)$

2.1 The Principle of Mathematical Induction

Induction is an indispensable tool in our toolkit of proof techniques and we begin with a short review of it. As we advance through the material, we may become less formal when we write our induction arguments. However, at least in the early stages, we should aim to be precise.

First, we recall that the validity of induction as a proof technique is actually an axiom, rather than a theorem to derived from more basic principles.

Axiom 2.1.1 (Induction)**.** Suppose that $P(n)$ is a mathematical statement for every positive integer n. If $P(1)$ is true and the implication $P(k) \Rightarrow P(k+1)$ holds for every positive integer k, then $P(n)$ is true for every positive integer n.

Example 2.1.2. We use the principal of induction to prove that $1+2+3+\ldots+n = \frac{n(n+1)}{2}$ for every positive integer n.

Proof. Base case: If $n = 1$, the left hand side of the given equation equals 1 and the right hand side equals $\frac{1(1+1)}{2} = 1$, so the statement true.

Inductive step: Assume that the desired statement is true when $n = k$, where k is some positive integer. That is, assume $1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2}$. We must deduce from this assumption the truth of the statement when $n = k + 1$. Indeed,

$$\begin{aligned} 1 + 2 + \ldots + (k+1) &= 1 + \ldots + k + (k+1) \\ &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} \\ &= \frac{(k+1)((k+1)+1)}{2}, \end{aligned}$$

so the desired equality is satisfied for $n = k + 1$.

Conclusion: By the principle of mathematical equation, the desired statement is true for all positive integers n. □

The principle of induction can be modified into several forms which look a bit different from the axiom stated above, but which are nonetheless equivalent:

- In the so-called *strong principle of induction*, the inductive step instead consists of assuming the truth of $P(1), \ldots, P(k)$ for some positive integer k, and deducing the truth of $P(k + 1)$.
- An induction may start at places other than $n = 1$. It may also sometimes be necessary to verify several small base cases "by hand", if we find we are unable to make the induction step work without imposing an additional assumption that k is larger than some specific number.

Another important consequence of the principle of induction is that it allows us to define sequences *recursively* by specifying sufficiently many "seed values" and giving a recipe for computing subsequent terms from preceding ones. For example, the **Fibonacci sequence** $F_1, F_2, F_3, F_4, \ldots$ is defined recursively by:

$$F_1 = 1, F_2 = 1 \qquad \text{and} \qquad F_n = F_{n-1} + F_{n-2} \text{ for every integer } n \geq 2.$$

Exercise 2.1.3. Prove that, for every positive integer n, $F_1 + F_2 + \ldots + F_n = F_{n+2} - 1$.

The principle of induction can also be shown to be equivalent to another standard axiom called the *well-ordering principle*. Generally, any proof by induction can be rephrased as a proof using the well-ordering principle, and vice versa. Doing so is a valuable exercise.

Axiom 2.1.4 (Well-Ordering Principle)**.** If S is a nonempty set of positive integers, S has a smallest element.

In general, S does not need to only contain positive integers for the conclusion to apply. It is enough for S to be a nonempty set of integers which is **bounded below** in the sense that there exists some $n \in \mathbb{Z}$ such that $n \leq m$ for all $m \in S$. On the other hand, if S is not bounded below, or if we try to work with numbers other than integers, things can go wrong; the well-ordering principle may or may not apply.

Exercise 2.1.5.

(a) Prove that any nonempty set of integers that is bounded above has a largest element.

(b) Give an example of a nonempty set of rational numbers which is bounded below, but doesn't have a smallest element.

(c) Show that every nonempty subset of $\{1 - \frac{1}{n} : n = 1, 2, 3, \ldots\} \cup \{2 - \frac{1}{n} : n = 1, 2, 3, \ldots\}$ has a smallest element (meaning a smallest element *belonging to the subset*).

Here are a couple more induction problems for practice.

Exercise 2.1.6. Fix a real number $x \neq 1$. Use the principle of induction to prove the validity of the geometric series formula

$$\sum_{i=0}^{n} x^i = \frac{1 - x^{n+1}}{1 - x}$$

for every positive integer n.

Exercise 2.1.7. Conjecture a formula for the sum of the first n **even** Fibonacci numbers. Use induction to prove your conjecture is correct. Do the same thing for the sum for the first n odd Fibonacci numbers.

2.2 Divisibility

The following definition is fundamental.

Definition 2.2.1. Let a and b be integers. If there exists an integer q such that $a = qb$, we say that **b divides a** or that **a is divisible by b**. We can also say that b is a **divisor** or a **factor** of a. We may also express this relationship in symbols by writing $b|a$.

You may be used to thinking of b being divisible by a as meaning "the fraction $\frac{b}{a}$ is an integer". That is often OK, but Definition 2.2.1 tends to be cleaner to work with. Also, 0 is divisible by 0 according to the definition above, but not according to the fraction definition! This is the only point of disagreement between these definitions, however.

Here are some basic exercises to practice using Definition 2.2.1.

Exercise 2.2.2. Prove the following assertions.

(a) Every integer divides 0.

(b) Every integer is divisible by 1 and itself.

(c) If $a|b$ and $b|a$, then $a = \pm b$.

(d) If a is a nonzero integer and b is a divisor of a, then b lies between a and $-a$. In particular, the set of factors of a is finite.

The following are basic properties of divisibility which we will use **all the time**. The proofs are not difficult and will make good exercises in applying Definition 2.2.1.

Theorem 2.2.3. *Let a, b, c be integers.*

1. *If $a|b$ and $b|c$, then $a|c$.*

2. *If $c|a$ and $c|b$, then $c|(sa + tb)$ for all integers s, t.*

Proof. Exercise. □

Property (1) says that divisibility is a **transitive** relation; it behaves similarly to human ancestry. If Alice is descendant of Bob, and Bob is a descendant of Carlos, then Alice is a descendant of Carlos.

An expression like $sa + tb$ where s and t are integers is called an **integral linear combination** of a and b. Property (2) says that, if a number divides a and b, it also divides all the integral linear combinations of a and b. For example, both quarters and dimes are divisible by nickels; property (2) tells us that any amount of change we can make using quarters and dimes could also be payed out using nickels.

We now give the definition of a prime number. These are, in many ways, the main protagonists of number theory. Note that every integer n is divisible by 1 and n; these are its **trivial divisors**.

Definition 2.2.4. A positive integer n that has a nontrivial positive divisor (i.e. a positive divisor other than 1 and n) is called a **composite** number. In contrast, a positive integer p not equal to 1 whose only positive divisors are 1 and p is called a **prime** number.

Note that 1 is neither prime nor composite. Instead, it is a **unit** and there are good reasons for excluding it from the list of prime numbers.

Prime numbers are central objects in number theory and mathematicians have have studied them for thousands of years. They are somewhat analogous to atoms, being objects that cannot be broken down into smaller pieces. The complete list of primes smaller than 100 is as follows:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

A **common divisor** of two integers a and b is an integer x such that $x|a$ and $x|b$. If a and b are not both zero, the set of common divisors of a and b is finite and contains 1 (see Exercise 2.2.2). Therefore, by the well-ordering principle, the set of common divisors of a and b has a greatest element, which is necessarily positive (since 1 is included).

Definition 2.2.5. Let a and b be integers that are not both zero. The **greatest common divisor** of a and b, denoted $\gcd(a, b)$, is the positive integer that is uniquely characterized as the largest integer dividing both a and b.

Exercise 2.2.6. Let a, b, c be integers, with $a, c \neq 0$. Prove the following formulas:

(a) $\gcd(a, b) = \gcd(|a|, |b|)$

(b) $\gcd(ca, cb) = c \cdot \gcd(a, b)$

(c) $\gcd(1, b) = 1$

(d) $\gcd(a, 0) = |a|$

Definition 2.2.7. Two integers a and b (not both zero) are said to be **relatively prime** if $\gcd(a, b) = 1$. In other words, a and b are relatively prime if the only positive integer dividing them both is 1.

Exercise 2.2.8. Prove each implication if it is true, or give a counterexample if it is false.

1. If $a|c$ and $b|d$, then $ab|cd$.
2. $a|c$ and $b|d$, then $(a + b)|(c + d)$.
3. If n is an odd number and $n|2a$, then $n|a$.

Exercise 2.2.9. Prove or give a counterexample: Let a and n be positive integers. If a is commmon divisor of n and $n + 4$, then $a \in \{1, 2, 4\}$.

Exercise 2.2.10. Prove that, if p is a prime and n is not divisible by p, then p and n are relatively prime. In particular, prove that, if p and q are distinct prime numbers, then p and q are relatively prime.

We conclude the section with some divisibility exercises with which to practice proof by induction.

Exercise 2.2.11. Use induction to prove $6|(n^3 - n)$ for every positive integer n.

Exercise 2.2.12. Use induction to prove $11|(15^n - 4^n)$ for every nonnegative integer n.

2.3 The Division Algorithm

The theorem below is known as the division algorithm because we could implement it algorithmically. To find the remainder of a divided by b, we subtract b from a repeatedly until we encounter a point where doing so again would give a negative result. The final number reached is the **remainder** and the number of subtractions is the **quotient**. Of course, in practice, there are more efficient strategies than repeated subtraction.

Theorem 2.3.1 (Division algorithm)**.** *Let a, b be integers with b positive. Then, there exist unique integers q, r such that $0 \leq r < b$ and $a = qb + r$.*

Proof. For simplicity, we assume $a \geq 0$ (this typically being the case when the result is applied). The case $a < 0$ proceeds similarly and is left as an exercise.

First, let us prove existence. Let S be the set of all integers q such that $a - qb \geq 0$. Observe S is nonempty, as $0 \in S$. Furthermore, S is bounded above because $q \in S$ implies $q \leq a/b$. By the well-ordering principle (see Exercise 2.1.5), there exists a largest element q_0 in S. Set $r = a - q_0 b$. By the definitions of q_0 and r, we have $0 \leq r$ and $a = q_0 b + r$. If $r \geq b$ occurred, we would have $r - b = a - (q_0 + 1)b \geq 0$ so that $q_0 + 1 \in S$, contradicting the definition of q_0 as the largest element of S. Thus, $r < b$ as required.

Next, let us prove uniqueness in the case $a = 0$. Clearly $q = r = 0$ does the job. Could there exist another expression $0 = qb + r$ with $0 \leq r < b$? Then, $-qb = r$ which, since $r < b$, is only possible if $q = 0$, whence $r = 0$ as well.

Finally, let us prove uniqueness general. Suppose $a = q_1 b + r_1 = q_2 b + r_2$, with both representations fulfilling the brief. Without loss of generality, $r_1 \geq r_2$. Subtraction then yields $0 = (q_1 - q_2)b + (r_1 - r_2)$ where $0 \leq r_1 - r_2 \leq r_1 < b$ so, by the uniqueness result of the preceding paragraph, $q_1 = q_2$ and $r_1 = r_2$. □

Actually, the division algorithm works with real numbers as well. If $a, b > 0$, it still makes sense to ask "how many times does b go into a, and what is the remainder"? To get a useful definition, we still insist the quotient q is an integer, but the remainder can be a real number r.

Exercise 2.3.2. Prove that, if $a, b \in \mathbb{R}$ and $b > 0$, there exist unique $q \in \mathbb{Z}$ and $r \in [0, b)$ such that $a = bq + r$.

In particular (the case of no remainder), we can extend the concept of divisibility to the real line: we say that a **divides** b for $a, b \in \mathbb{R}$ if $b = qa$ for some $q \in \mathbb{Z}$ (the quotient is still required to be an integer). Extending the discussion to real numbers gets us into the topic of how ancient Greeks thought of two quantities as being commensurate. Saying that b divides a means that we can measure out the length a using a rope of length b. But, even if neither of a or b divides the other one, they may still have a greatest common divisor. For example $\frac{1}{6}$ is the greatest common divisor of $\frac{1}{2}$ and $\frac{1}{3}$. Not all pairs of real numbers will have a greatest common divisor, however. This was a philosophical stumbling point for the ancient Greeks as it means that some lengths are not commensurate with each other, i.e. not common multiples of some other (perhaps very small) unit of length. As the following exercise shows, the possible nonexistence of a greatest common divisor for two real numbers is very much related to the discovery of irrational numbers, which caused ancient mathematicians much consternation.

Exercise 2.3.3. Let a be a positive, irrational number. Show that a and 1 are not commensurate in the sense that there does not exist any positive number $d > 0$ such that d divides both a and 1.

2.4 The Euclidean Algorithm

How would you compute the greatest common divisor of two integers? In elementary school, you may have calculated the greatest common divisor by one or both of the following (quite closely related) methods:

- **Method 1:** Write out all the divisors, extract the common divisors and choose the biggest one. For example, ignoring signs, 20 is divisible by $\{1, 2, 4, 5, 10, 20\}$ and 30 is divisible by $\{1, 2, 3, 5, 6, 10, 15, 30\}$. The common divisors are $\{1, 2, 5, 10\}$, and the greatest common divisor is 10.
- **Method 2:** Factor the numbers into primes and identify the common factors. For example, to find $\gcd(12, 100)$, we might write $12 = 2^2 \cdot 3$ and $100 = 2^2 \cdot 5^2$ and conclude that their greatest common divisor is $2^2 = 4$.

It may be a surprise to learn that those familiar methods are actually the **hard way** of finding the greatest common divisor in the sense that it would be very difficult to use those methods on large numbers. Indeed, the fact that it is very computationally expensive to find prime factors of large integers is the basis of modern cryptography.

The Euclidean algorithm, which we study at the end of this section, is the **easy way** (i.e. computationally efficient way) to find the greatest common divisor and bypasses the issue of factoring the inputs. On first exposure, the Euclidean algorithm may seem more complicated than the methods outlined above, but this is only an illusion stemming from the fact we are creatures of limited patience and most of us don't have experience trying to find the greatest common divisor of two very large digits where the advantages of the Euclidean algorithm would shine through.

The Euclidean algorithm has an ancient Greek name[1] and is also based on an ancient Greek idea, relating again to the idea of commensurate quantities. Suppose you have two ropes of length a and b. What lengths can you measure out using the ropes in combination? For example, if $a = 5$ and $b = 7$, we can measure a length of 1 by measuring out a length of 15 using rope a and then subtract away a measurement of 14 using rope b.

Exercise 2.4.1. Building on the discussion above, argue that a rope of length 5 and a rope of length 7 can be used in tandem to measure out any integer length.

In general, given a rope of length a and rope of length b, the distances you can measure are exactly the integral linear combinations of a and b, that is the numbers of the form $sa + tb$ where s and t are integers. Out of all the lengths that can be constructed out of a and b, there is a smallest positive one (because of the well-ordering principal). This smallest positive length is equal to the greatest common divisor, giving us a second characterization.

Theorem 2.4.2 (Bézout identity)**.** *Let a and b be integers which are not both zero. Then, $\gcd(a, b)$ is the smallest positive element of the set $\{sa + tb : s, t \in \mathbb{Z}\}$. In particular, it is possible to write $\gcd(a, b) = sa + tb$ for some $s, t \in \mathbb{Z}$.*

[1]The Euclidean algorithm was discovered and used independently by Chinese and Indian mathematicians as well. Aryabhata called it by the much more exciting name, translating to "pulverizer".

Proof. Let S denote the set of positive elements of $\{sa + tb : s, t \in \mathbb{Z}\}$. Note S is not empty (for example, $a^2 + b^2$ is an element of S). According to the well-ordering principle, S has a smallest element, which we denote by d. We claim that d divides a. To see this, use the division algorithm to write $a = qd + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < d$. Now, if $r > 0$, then $r \in S$ (*Exercise: Prove this claim*), contradicting the definition of d as the smallest element of S. Therefore, $r = 0$ which gives that d divides a. A similar argument shows that d divides b, so d is a common divisor of a and b. On the other hand, any common divisor of a, b must divide any integral linear combination of a and b (Exercise 2.2.3). In particular, $\gcd(a, b)$ divides d and therefore $\gcd(a, b) \leq d$. Since $\gcd(a, b)$ is supposed to be the biggest common divisor of a and b, we must have $\gcd(a, b) = d$. □

The above theorem is an example of a "min-max principle"; the maximum element of one set (common divisors of a and b) is actually equal to the minimum element of another set (integral linear combinations of a and b which are positive). Draw a diagram of two blobs, one above the other, meeting in a point. Situations like this one occur frequently in mathematics.

Exercise 2.4.3. Let a and b be integers, not both zero. Prove that, not only is $\gcd(a, b)$ the largest out of all the common divisors of a and b, it is in fact *divisible* by all the common divisors of a and b.

Exercise 2.4.4. Prove that, if p and q are any distinct primes, there exist $s, t \in \mathbb{Z}$ such that $sp + tq = 1$.

Exercise 2.4.5. Given $a, b \in \mathbb{Z}$ not both zero, show that $\gcd(a, b) \leq \gcd(a + b, a - b)$.

Theorem 2.4.2 says that $\gcd(a, b)$ is the smallest positive element of $\{sa + tb : s, t \in \mathbb{Z}\}$. Put concretely, $\gcd(a, b)$ is the smallest positive distance we can measure using, in tandem, a rope of length a and a rope of length b. The Euclidean algorithm works by using the division algorithm to produce smaller and smaller distances that can be constructed out of a and b until no smaller distance can be found.

The following lemma is the heart of the Euclidean algorithm.

Lemma 2.4.6. *If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.*

Proof. Since a is an integral linear combination of b and r and, conversely, r can be written as an integral linear combination of a and b, it follows (*Exercise: check this*) that the set of the integral linear combinations of a and b is equal to the set of integral linear combinations of b and r. In symbols: $\{sa + tb : s, t \in \mathbb{Z}\} = \{sb + tr : s, t \in \mathbb{Z}\}$. Thus, $\gcd(a, b) = \gcd(b, r)$ by Theorem 2.4.2. □

Theorem 2.4.7 (Euclidean Algorithm)**.** *Let a and b be positive integers with $a > b$. Generate sequences $a = r_0, b = r_1, r_2, r_3, \ldots$ and $q_1, q_2, \ldots$ by repeatedly applying the division algorithm*

as shown below:

$$\begin{array}{rll} a = q_1 b + r_2 & 0 \leq r_2 < b & \text{Line 1} \\ b = q_2 r_2 + r_3 & 0 \leq r_3 < r_2 & \text{Line 2} \\ r_2 = q_3 r_3 + r_4 & 0 \leq r_4 < r_3 & \text{Line 3} \\ \vdots & \vdots & \vdots \\ r_{n-1} = q_n r_n + 0 & r_{n+1} = 0 & \text{Line } n \end{array}$$

Terminate the procedure on the first line n with $r_{n+1} = 0$. Then, $\gcd(a, b) = r_n$.

Proof. Since $a > b > r_2 > r_3 > \ldots$, a smallest n with $r_{n+1} = 0$ exists by the well-ordering principle. By Lemma 2.4.6, we have

$$\gcd(a, b) = \gcd(b, r_2) = \gcd(r_2, r_3) = \ldots = \gcd(r_n, 0) = r_n$$

as desired. □

In summary, the Euclidean algorithm proceeds as follows:

- Input: two positive numbers.
- Recursive step: replace the larger number with its remainder on division by the smaller number.
- Repeat the recursive step until a remainder of 0 occurs.
- The penultimate remainder, i.e. the last nonzero remainder, is the gcd of the inputs.

Example 2.4.8. Determine $\gcd(986, 391)$.

$$\begin{array}{ll} 986 = 2 \cdot 391 + 204 & \text{Line 1} \\ 391 = 1 \cdot 204 + 187 & \text{Line 2} \\ 204 = 1 \cdot 187 + 17 & \text{Line 3} \\ 187 = 11 \cdot 17 & \text{Line 4} \end{array}$$

Therefore, $\gcd(986, 391) = \gcd(391, 204) = \gcd(204, 187) = \gcd(187, 17) = \gcd(17, 0) = 17$.

With a bit more work, we can furthermore use the Euclidean algorithm to express $\gcd(a, b)$ as an integral linear combination of a and b. In other words, the Euclidean algorithm gives us a way to concretely realize the Bézout identity (Theorem 2.4.2). Perhaps the most direct way to achieve this is by performing "back substitution" on the equations:

Example 2.4.9. In the preceding example, rewrite all the lines so the smallest remainder is on the left, omitting the last line. Boxes are drawn around the remainders to remind us not to multiply them out; it is their coefficients we are trying to calculate.

$$\begin{aligned} \boxed{204} &= \boxed{986} - 2 \cdot \boxed{391} && \text{Line 1} \\ \boxed{187} &= \boxed{391} - \boxed{204} && \text{Line 2} \\ \boxed{17} &= \boxed{204} - \boxed{187} && \text{Line 3} \end{aligned}$$

Next, working in reverse order, substitute each line into the one below:

$$\begin{aligned} \boxed{17} &= \boxed{204} - \boxed{187} && \text{Line 3} \\ &= \boxed{204} - \left(\boxed{391} - \boxed{204}\right) && \text{Substitute Line 2} \\ &= 2\,\boxed{204} - \boxed{391} && \text{Collect coefficients} \\ &= 2\left(\boxed{986} - 2\,\boxed{391}\right) - \boxed{391} && \text{Substitute Line 1} \\ &= 2\,\boxed{986} - 5\,\boxed{391} && \text{Collect coefficients} \end{aligned}$$

So, in the end, we obtain the Bézout identity:

$$\gcd(986, 391) = (2)(986) + (-5)(391) = 17.$$

Exercise 2.4.10. Use the Euclidean algorithm to show that $\gcd(1127, 391) = 23$. Then, use back substitution to obtain the Bézout identity $23 = (8)(1127) + (-23)(391)$.

Exercise 2.4.11. Use the Euclidean algorithm to show that $\gcd(23121, 8074) = 367$. Then, use back substitution to obtain the Bézout identity $367 = (7)(23121) + (-20)(8074)$.

The following special case of the Bézout identity is of particular importance.

Proposition 2.4.12. *If a and b are relatively prime, then $sa + tb = 1$ for some $s, t \in \mathbb{Z}$.*

Proof. Follows from Theorem 2.4.2. □

It turns out being able to write $sa + tb = 1$ is extremely useful; we will this expression again and again. One important application is given below.

Proposition 2.4.13. *If a and b are relatively prime and $a|bc$, then $a|c$.*

Proof. Using Proposition 2.4.12, write $sa + tb = 1$. Then, $c = sac + tbc$. Because a divides itself and bc, and because we have expressed c as an integral linear combination a and bc, it follows that $a|c$. □

Note that the above proposition is fairly obvious if we already know that every positive integer has a unique prime factorization. However, we have not yet proved this is the case and, as a matter of fact, the idea of the above proposition will play a key role in our proof of the unique factorization theorem!

2.5 The Extended Euclidean algorithm

In the preceding section, we showed how to use the Euclidean algorithm to produce a solution to the Bézout equation by the method of "back substitution". This solution is known as the *Euclidean solution*. In this section, we show that the Euclidean solution is, in a sense, the smallest possible solution to Bézout's equation. In order give a precise definition of the Euclidean solution, we revisit the problem of obtaining a Bézout identity from the Euclidean algorithm more formally using the language of recurrence relations. This is sometimes known as the *extended Euclidean algorithm*.

Note that the Euclidean solution is never the unique solution to $sa + tb = \gcd(a, b)$, as the following exercise explores.

Exercise 2.5.1. Let a and b be integers, not both zero. Prove there are infinitely many integer solutions (s, t) to the equation $sa + tb = \gcd(a, b)$.

The following proposition gives the complete answer to the uniqueness question.

Proposition 2.5.2. *Let a and b be integers, not both zero, and set $d = \gcd(a, b)$. Suppose (s_0, t_0) is one solution to Bézout's equation: $sa + tb = d$. Then, the full set of solutions consists of all pairs (s, t) where $s = s_0 - \frac{mb}{d}$ and $t = t_0 + \frac{ma}{d}$ for some $m \in \mathbb{Z}$.*

Proof. We assume a and b are nonzero, leaving the case where one of them is zero to the reader. We furthermore assume, without loss of generality, that a and b are relatively prime, so that $d = 1$ (*Exercise: justify these reductions*). Let $x = s - s_0$ and $y = t - t_0$ so that $xa + yb = 0$, i.e. $xa = -yb$. Since a divides yb from the latter equation, and a and b are relatively prime, it follows from Proposition 2.4.13 that a divides y and we write $y = ma$ where $m \in \mathbb{Z}$. Similarly, $b|x$ and we write $x = nb$ where $n \in \mathbb{Z}$. Thus, $nab = -mab$ and, because a and b are nonzero, $n = -m$. Summing up, $s = s_0 + x = s_0 - mb$ and $t = t_0 + y = t_0 + ma$ as desired. □

Given input integers $a > b > 0$, recall the Euclidean algorithm produces a sequence of remainders (r_i) and quotients (q_i) according to the following procedure:

$$\begin{aligned} a &= q_1 b + r_2 & 0 \le r_2 < b \\ b &= q_2 r_2 + r_3 & 0 \le r_3 < r_2 \\ r_2 &= q_3 r_3 + r_4 & 0 \le r_4 < r_3 \\ &\vdots & \vdots \\ r_{n-1} &= q_n r_n + 0 & r_{n+1} = 0. \end{aligned}$$

We have $\gcd(a, b) = r_n$, where r_n is the last nonzero remainder.

Note that, if we treat the sequence (q_i) as given, we may think of (r_i) as solving the following recurrence relation:

$$\begin{aligned} r_0 &= a \\ r_1 &= b \\ r_{i+1} &= r_{i-1} - q_i r_i & 1 \le i \le n \end{aligned} \tag{2.1}$$

In the extended Euclidean algorithm, we introduce two additional sequences (s_i) and (t_i) which satisfy the same recurrence relation (2.1), but have different intitial conditions.

Definition 2.5.3. Given integers $a > b > 0$, the **extended Euclidean algorithm** produces, as well as the usual sequences (q_i) and (r_i) of quotients and remainders, two sequences (s_i) and (t_i) defined by the following recurrence relations:

$$\begin{aligned} s_0 &= 1 & t_0 &= 0 \\ s_1 &= 0 & t_1 &= 1 \\ s_{i+1} &= s_{i-1} - q_i s_i & t_{i+1} &= t_{i-1} - q_i t_i \qquad 1 \leq i \leq n \end{aligned} \tag{2.2}$$

Here n is the stopping time; the time such that $r_n = \gcd(a, b)$ and $r_{n+1} = 0$.

The relevance of the extended Euclidean algorithm to the Bézout identity is assured by the following theorem.

Theorem 2.5.4. *Let a, b be integers with $a > b > 0$ and let (q_i), (r_i), (s_i), (t_i) be the sequences produced by the extended Euclidean algorithm. Then,*

$$s_i a + t_i b = r_i \qquad 0 \leq i \leq n+1.$$

In particular, we have $s_n a + t_n b = r_n = \gcd(a, b)$, where r_n is the last nonzero remainder.

Proof. Since $s_0 a + t_0 b = a = r_0$ and $s_1 a + t_1 b = b = r_1$, the theorem is valid for $i = 0, 1$. Suppose the theorem is true for $i = k - 1$ and $i = k$ for some positive integer k. Then, $s_{k+1} a + t_{k+1} b = (s_{k-1} a + t_{k-1} b) - q_k (s_k a + t_k b) = r_{k-1} - q_k r_k = r_{k+1}$ so, by the principle of induction, the theorem is proved. □

Definition 2.5.5. Let a, b be integers with $a > b > 0$. The **Euclidean solution** to Bézout's equation $sa + tb = \gcd(a, b)$ is the solution given by the extended Euclidean algorithm.

Remark 2.5.6. The back substitution method in the last section gives the same solution to Bézout's equation as the extended Euclidean algorithm, as you are welcome to contemplate.

Example 2.5.7. Starting with $a = r_0 = 1053$ and $b = r_1 = 481$, applying the extended Euclidean algorithm generates the following table:

i	q_i	r_i	s_i	t_i
0		1053	1	0
1	2	481	0	1
2	5	91	1	-2
3	3	26	-5	11
4	2	13	16	-35
5		0	-37	81

We have $\gcd(1053, 481) = 13$. One may check that $s_i(1053) + t_i(481) = r_i$ indeed holds for $0 \leq i \leq 5$. In particular, when $i = 4$ we obtain $(16)(1053) + (-35)(481) = 13$, the Euclidean solution to the Bézout equation.

Exercise 2.5.8. Apply the extended Euclidean algorithm to $a = 1533$ and $b = 477$, generating a table like the one in Example 2.5.7. Verify that $s_i a + t_i b = r_i$ for all i.

The following theorem makes precise the sense in which the Euclidean solution is minimal.

Theorem 2.5.9. *Let a and b be integers with $a > b > 0$. Set $d = \gcd(a, b)$. Suppose that $s_0 a + t_0 b = d$ is the Euclidean solution to the Bézout equation and $sa + tb = d$ is some other solution. Then, the following hold:*

1. *$|s_0| \leq \frac{b}{2d}$ and $|t_0| \leq \frac{a}{2d}$.*
2. *$|s| \geq |s_0|$ and $|t| \geq |t_0|$.*
3. *If $|s| \leq \frac{b}{2d}$ and $|t| \leq \frac{a}{2d}$, then $s = s_0$ and $t = t_0$.*

The first of the three statements is the most substantial one and we defer its proof to a bit later on. For now, we assume it holds and deduce the other two statements.

Proof of Statements 2 and 3. Without loss of generality, we assume that a and b are relatively prime (*Exercise: justify this reduction*). Thus, $d = 1$ and the bounds of Statement 1 amount to $|s_0| \leq b/2$, $|t_0| \leq a/2$. By Proposition 2.5.2, we may write $s = s_0 - mb$ and $t = t_0 + ma$ for some $m \in \mathbb{Z}$. We assume $m \neq 0$, or else $(s, t) = (s_0, t_0)$ and there is nothing to prove.

For Statement 2, we have $|s| + |s_0| \geq |s - s_0| = |mb| \geq b \geq 2|s_0|$, whence $|s| \geq |s_0|$, as desired. The proof that $|t| \geq |t_0|$ is similar.

For Statement 3, we assume $|s| \leq b/2$ and $|t| \leq a/2$ both hold and derive a contradiction. Observe the only distinct numbers in $[-b/2, b/2]$ which are a nonzero integer multiple of b apart are $\pm b/2$, so we must have $\{s_0, s\} = \{-b/2, b/2\}$ and. Similarly, $\{t_0, t\} = \{-a/2, a/2\}$. Since both of a pair of Bézout coefficients clearly can't be negative, the only possibility is that one of (s, t) and (s_0, t_0) equals $(-b/a, a/2)$ and the other equals $(b/2, -a/2)$. This, however, leads to the absurd conclusion that $d = -d$. □

As an alternative to the recurrence relation approach of (2.2), we can instead generate (s_i) and (t_i) using repeated matrix multiplication. This is an instance of a general principle connecting linear recurrence relations to matrices and is taken up in the following exercise.

Exercise 2.5.10. Let a, b be integers with $a > b > 0$. Let (q_i), (r_i), (s_i), (t_i) be the sequences produced by the extended Euclidean algorithm. Define

$$E_i = \begin{bmatrix} 0 & 1 \\ 1 & -q_i \end{bmatrix} \qquad\qquad 1 \leq i \leq n,$$

where n is the stopping time. Prove by induction that

$$E_i \cdots E_1 \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} r_i \\ r_{i+1} \end{bmatrix} \qquad \text{and} \qquad E_i \cdots E_1 = \begin{bmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{bmatrix} \qquad 1 \leq i \leq n.$$

We use the matrix formalism of the above exercise to run an inductive argument, completing the proof of Theorem 2.5.9. If you don't like the matrices, another inductive proof could be given instead relying on an understanding of the following sentence: "the solution to a linear recurrence relation is linear in the initial conditions"

Proof of Theorem 2.5.9, Statement 1. Without loss of generality, a and b are relatively prime so that $d = 1$ (*Exercise: justify this reduction*). We proceed by induction on n, the number of steps needed to execute the Euclidean algorithm on a and b. If $n = 1$, then $b = 1$ and $a \geq 2$. The Euclidean solution is $(0)a + (1)b = 1$ and, indeed, $0 \leq b/2$ and $1 \leq a/2$.

Next, suppose the number of steps needed to execute the Euclidean algorithm for a and b is $n \geq 2$, and that the theorem holds for all pairs of relatively prime integers requiring fewer than $n-1$ steps. Let (q_i) and (r_i) be the sequences of quotients and remainders arising from the Euclidean algorithm applied to a and b. In particular, $a = q_1 b + r_2$. By the nature of the Euclidean algorithm, applying the Euclidean algorithm to b and r_2 yields the same sequence of quotients, except q_1 is omitted. Thus, according to Exercise 2.5.10,

$$E_n \cdots E_1 = \begin{bmatrix} s & t \\ * & * \end{bmatrix} \qquad\qquad E_n \cdots E_2 = \begin{bmatrix} x & y \\ * & * \end{bmatrix}$$

where $sa + tb = 1$ is the Euclidean solution for a and b and $xb + yr_2 = 1$ is the Euclidean solution for b and r_2. Irrelevant entries are omitted. Right-multiplying the second matrix equation above by $E_1 = \left[\begin{smallmatrix} 0 & 1 \\ 1 & -q_1 \end{smallmatrix}\right]$, we see $s = y$ and $t = x - q_1 y$. By the inductive hypothesis, $|x| \leq r_2/2$ and $|y| \leq b/2$. Thus, $|s| = |y| < b/2$ and $|t| = |x - q_1 y| \leq |x| + q_1|y| \leq r_2/2 + q_1 b/2 = a/2$ as desired. □

We conclude with an instructive exercise involving the Fibonacci numbers. Recall we define these by the recurrence $F_1 = 1$, $F_2 = 1$ and $F_k = F_{k-1} + F_{k-2}$ for $k \geq 3$.

Exercise 2.5.11. Apply the extended Euclidean algorithm to two consecutive Fibonacci numbers $a = F_{k+1}$ and $b = F_k$, where $k \geq 2$. What is their greatest common divisor? What is the Euclidean solution to the Bézout equation? How many steps before the Euclidean algorithm terminates? Can you find formulas for the terms of the sequences (q_i), (r_i), (s_i), (t_i)? Illustrate your findings with a medium-sized example, say $a = 89$ and $b = 55$.

Chapter 3

Prime Numbers

3.1 The infinitude of primes

Recall that a positive integer p is *prime* if $p \geq 2$ and the only positive integer divisors of p are the trivial divisors 1 and p (Definition 2.2.4). Prime numbers are some of the most studied mathematical entities in human history. Mathematicians have thought about prime numbers for thousands of years, yet many important questions about them are still unanswered. We will encounter several such open problems as we go along. Prime numbers play a key role in modern crytography which underpins information security. It is commonly suggested the mathematicians of an alien civilization should also appreciate the importance of prime numbers.

You are probably aware of the fundamental theorem of arithmetic: every positive integer can be broken down uniquely as a product of primes. We will prove this in the next section. For now, the following proposition is a modest step in that direction.

Proposition 3.1.1. *Every positive integer $n \geq 2$ has a prime factor.*

Proof. Let S be the set of positive divisors of n which are ≥ 2. Note that S is not empty because $n \in S$. By the well-ordering principle, there is a smallest element $p \in S$. If p has a nontrivial positive divisor, i.e. a divisor d with $1 < d < p$, then, by transitivity, d is a divisor of n which is smaller than p, contradicting the definition of p. Thus, the only divisors of p are 1 and p itself, so p is prime. □

It is sometimes useful to have the following sharper version of the above theorem.

Proposition 3.1.2. *A number $n \geq 2$ is composite if and only if it has a prime factor p satisfying $p \leq \sqrt{n}$.*

Proof. Exercise for the reader. □

Example 3.1.3. According to the above proposition, to determine whether a given positive integer smaller than 100 is prime or not, you only need to test for divisibility by the primes smaller than $\sqrt{100} = 10$, which are $2, 3, 5, 7$. For example, the fact that 97 is not divisible

by any of $2, 3, 5, 7$ proves that it is prime. On the other hand, 91 is divisible by 7 and is composite.

The complete set of primes smaller than 100 is as follows:

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}$$

It is not possible to write down a complete list of all prime numbers because there are infinitely many of them! This was proven in Euclid's *Elements* in 300 BC.

Theorem 3.1.4 (Euclid)**.** *The set of prime numbers is infinite.*

Proof. We shall prove that, given any finite list of primes $p_1, p_2, \ldots, p_n$, there exists a prime number p which is not on the list. Define $m = p_1 p_2 \cdots p_n$. Observe that all of $p_1, \ldots, p_n$ divide m. Therefore, none of $p_1, \ldots, p_n$ divide $m+1$, or else they would also divide $1 = (m+1) - m$. By Proposition 3.1.1, there exists a prime p dividing $m + 1$. This prime p is a prime not appearing on our list. □

Exercise 3.1.5. Suppose n is positive integer and $p_1 < p_2 < \ldots < p_n$ are the first n prime numbers.

1. Give three examples where $p_1 \cdots p_n + 1$ prime.
2. Give an example where $p_1 \cdots p_n + 1$ is composite. Does this present a problem for Euclid's proof for the infinitude of primes?

Open Problem 3.1.6 (Primorial primes)**.** Are there infinitely many positive integers n such that $p_1 \cdots p_n + 1$ is prime, where $p_1, \ldots, p_n$ are the first n primes?

Exercise 3.1.7. Prove that, for every positive integer n, it is possible to find at set of n consecutive composite numbers. For example, $\{24, 25, 26, 27, 28\}$ is a set of 5 consecutive composite numbers. *Hint: the factorial is your friend!*

The above exercise shows that the gaps between prime numbers can be arbitrarily large. One can also ask how small gaps between prime numbers can get. The must extremem case is a pair of prime numbers which are 2 part from one another. Such primes are referred to as **twin primes**. For example, $\{11, 13\}$ and $\{29, 31\}$ are twin primes.

Open Problem 3.1.8 (Twin prime conjecture)**.** Do there exist infinitely many twin primes?

The *twin prime conjecture* asks whether there exist infinitely many *twin primes*; pairs of primes which are 2 apart from each other. For a long time, it was not even known whether there exists a fixed number M (maybe very large) such that there exist infinitely many pairs of primes within distance M of each other. Eventually, this weaker statement was proven to be true by Yitang Zhang in 2014 for $M = 7 \times 10^7$. The important thing is that this number is finite! Since then, a massive collaborative project called *Polymath* has refined Zhang's bound down to $M = 246$, but the twin prime conjecture itself remains open.

3.2 The unique factorization theorem

In this section, we prove that every positive integer has a unique expression as a product of primes. This is sometimes called the *fundamental theorem of arithmetic*. First, let us show that every positive integer has at least one expression as a product of primes[1].

Proposition 3.2.1. *Every integer $n \geq 2$ can be expressed as a finite product of primes. That is, there is a list of primes $p_1, \ldots, p_r$ such that $n = p_1 \cdots p_r$.*

Proof. We prove this by strong induction on n. If $n = 2$, then n is prime and the proposition is clearly true. Next, suppose that $k \geq 3$ and that the proposition is true for all n with $2 \leq n < k$. If k is prime, then the proposition obviously holds for $n = k$. On the other hand, if k is not prime, then it has a prime factor p by Proposition 3.1.1 and we may write $k = pm$ where $1 < m < k$ (if $m = 1$, then $k = p$ is prime, contrary to supposition; if $m = k$, then $p = 1$, which is not a prime). By inductive hypothesis, the theorem holds for $n = m$ and there exists a list of primes such that $m = p_1 \cdots p_r$. Adding p to the list, we have $p_1 \cdots p_r \cdot p = mp = k$, so the proposition is also valid for $n = k$. By induction, the proposition is valid all $n \geq 2$. □

Note that if an integer n divides even one of a pair of integers a and b, then it also divides the product ab . Primes are special in that the converse statement is also true. This simple property is surprisingly important. Indeed, this property is sometimes used to define the "prime elements" of number systems other than $\mathbb{Z}$.

Theorem 3.2.2. *Suppose a and b are integers and p is prime. If $p|ab$, then $p|a$ or $p|b$.*

Proof. If $p|a$, we are done, so suppose p does not divide a. Since the only positive divisors of p are 1 and p, we therefore have $\gcd(a, p) = 1$. Therefore, there exist integers s and t such that $sa + tp = 1$ (Bézout's identity). Using this, we have $b = s(ab) + (tb)p$. Since both ab and p are divisible by p, so is any integral linear combination of them, whence b is divisible by p. □

Example 3.2.3. The number 4 divides $6 \cdot 14$, but 4 does not divide either 6 or 14. That can happen for composite numbers! On the other hand, 7 divides $6 \cdot 14$, and 7 divides 14. Because 7 is prime, it was necessarily the case that 7 divides one 6 and 14.

Using induction, we can improve the above result to work for products with more terms.

Theorem 3.2.4. *Suppose $a_1, \ldots, a_n$ are integers and p is prime. If $p|a_1 \cdots a_n$, then $p|a_i$ for some $i \in \{1, \ldots, n\}$.*

Proof. Exercise for the reader. □

[1]You might complain about the positive integer 1. The usual response is that 1 is represented as an "empty" product of primes. Just as the most agreeable answer to the question "what is the sum of no numbers?" is "zero", the most agreeable answer to the question "what is the product of no numbers?" is "one". The point is that 0 is the additive identity and 1 is the multiplicative identity; 0 is to addition as 1 is to multiplication. We will usually simply dodge around this issue by considering integers 2 or larger.

We now come to the theorem on uniqueness of prime factorizations. We know that every integer $n \geq 2$ can be expressed as the product of some finite list of primes (repeats are OK)

$$n = p_1 \cdots p_r.$$

Since multiplication is commutative, we could rearrange the factors on the right in any way and still get the result n. In the theorem below, when we say that every positive integer $n \geq 2$ has a unique prime factorization, this uniqueness is understood to hold up to the operation of rearranging factors.

Theorem 3.2.5. *Every positive integer $n \geq 2$ has a unique factorization into primes.*

Proof. We prove this by induction on n. It is easy to see that there is only one way to factor $n = 2$ as a product of primes. Suppose $k \geq 3$ and the theorem is true for every $n < k$. Consider two (allegedly equal) prime factorizations of k:

$$k = p_1 \cdots p_r \qquad\qquad k = q_1 \cdots q_s.$$

Let $p = p_1$. Since $p|k$ and $k = q_1 \cdots q_s$, Theorem 3.2.4 implies the existence of a $t \in \{1, \ldots, s\}$ for which $p|q_t$. Since the only positive divisors of q_t are 1 and q_t, and $p \neq 1$, we must conclude that $p = q_t$. Thus, we have

$$\frac{k}{p} = p_2 \cdots p_r = q_1 \cdots q_{t-1} q_{t+1} \cdots q_s$$

By inductive hypothesis, the theorem is valid for $n = k/p < k$, and we may conclude that the lists $p_2, \ldots, p_r$ and $q_1, \ldots, q_{t-1}, q_{t+1}, \ldots, q_s$ are rearrangements of one another. Therefore, the same is true if we add back the prime $p = p_1 = q_t$ to both lists, so the theorem is valid for $n = k$ and hence, by induction, for all $n \geq 2$. □

The fundamental theorem of arithmetic is very often absorbed at a young age as a "fact". Because it is so familiar, it may be hard to shake the impression that the fundamental theorem of arithmetic is "obviously true" and does not need a proof. The following (somewhat naïve) example may help you to feel more like the fundamental theorem of arithmetic needs a proof.

Exercise 3.2.6. Let E be the set of all positive even numbers. Note that E is closed under addition and multiplication; we can think of it as a number system unto itself. Define an element of E to be an *even prime* if it cannot be factored as the product of two elements of E. Prove that some elements of E do not have a unique representation as a product of even primes.

Remark 3.2.7. If you delve further into number theory or abstract algebra, you will encounter more convincing examples of number systems where the concept of a "prime number" is still meaningful, but uniqueness of prime factorization does not hold. Here is a standard example. Add the imaginary number $a = i\sqrt{5}$ to the integers and consider the larger number system $\{m + na : m, n \in \mathbb{Z}\}$. It turns out that 6 has more than one prime factorization in this system. Namely, $6 = 2 \cdot 3$ as well as $6 = (1 + a)(1 - a)$. Additional background is needed to make this example precise, however.

Next, we consider some standard ways to display the prime factorization of a number.

1. If we sort the primes occurring in the prime factorization of $n \geq 2$ in increasing order, and group together the equal ones using exponents, we get that every integer $n \geq 2$ has a unique expression of the form

$$n = p_1^{\epsilon_1} \cdots p_k^{\epsilon_k},$$

where $p_1, \ldots, p_k$ are distinct primes, listed in increasing order, and $\epsilon_1, \ldots, \epsilon_k$ are positive integers. For example,

$$4400 = 2^4 \cdot 5^2 \cdot 11^1.$$

2. At least one other formalism is sometimes useful. First, write *all* the primes in increasing order, i.e. $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, \ldots$. In this notation, we get that every positive integer n has a unique expression of the form

$$n = p_1^{\epsilon_1} \cdots p_k^{\epsilon_k},$$

where k is a (sufficiently large) positive integer and $\epsilon_1, \ldots, \epsilon_k$ are nonnegative integers. An exponent $\epsilon_i = 0$ corresponds to a prime which does not occur in a given factorization of p into primes. For example,

$$4400 = 2^4 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^2.$$

The following proposition is an example of a situation where allowing nonnegative exponents is desirable.

Definition 3.2.8. Let a and b be nonzero integers. The **least common multiple** of a and b is the smallest positive integer $\text{lcm}(a, b)$ which is both a multiple of a and a multiple of b.

Proposition 3.2.9. *Suppose that $p_1, \ldots, p_k$ are distinct primes and*

$$a = p_1^{s_1} \cdots p_k^{s_k} \qquad\qquad b = p_1^{t_1} \cdots p_k^{t_k}$$

where $s_1, \ldots, s_k, t_1, \ldots, t_k$ are nonnegative integers. Then,

1. $\gcd(a, b) = p_1^{\epsilon_1} \cdots p_k^{\epsilon_k}$, *where* $\epsilon_i = \min(s_i, t_i)$ *for* $i = 1, \ldots, k$.
2. $\text{lcm}(a, b) = p_1^{\epsilon_1} \cdots p_k^{\epsilon_k}$, *where* $\epsilon_i = \max(s_i, t_i)$ *for* $i = 1, \ldots, k$.
3. $ab = p_1^{\epsilon_1} \cdots p_k^{\epsilon_k}$, *where* $\epsilon_i = s_i + t_i$ *for* $i = 1, \ldots, k$.

Proof. Exercise for the reader. □

We conclude this section with some miscellaneous exercises involving prime factorization.

Exercise 3.2.10. Let $m = 7^{13} \cdot 11^{10} \cdot 19^4$ and $n = 7^4 \cdot 11^{12} \cdot 13^5$. Find the prime factorizations of $\gcd(m, n)$ and $\text{lcm}(m, n)$.

Exercise 3.2.11. Prove that every positive integer can be uniquely expressed as a power of 2 times an odd number.

Exercise 3.2.12. Determine the prime factorization of 9999.

Exercise 3.2.13. Show that a positive integer is the square of another positive integer if and only if all of the exponents appearing in its prime factorization are even.

Exercise 3.2.14. Let a and b be positive integers. Prove that, if $a^3|b^2$, then $a|b$.

Exercise 3.2.15. Let $n = p_1^{\epsilon_1} \cdots p_k^{\epsilon_k}$, where $p_1, \ldots, p_k$ are distinct primes and $\epsilon_1, \ldots, \epsilon_k$ are positive integers.

(a) If d is a positive integer dividing n, what must the prime factorization of d look like?

(b) Come up with a formula for the number of positive integers dividing n.

Exercise 3.2.16. Let $n = 2^6 \cdot 3 \cdot 5^5$. How positive divisors does n have? How many positive divisors does n have that are relatively prime to 14? How many positive divisors does n have that are divisible by 12? How many positive divisors does n have that are perfect squares?

3.3 Mersenne primes

In this and the following section, we study prime numbers that can be written in the form $2^n \pm 1$, i.e. primes which are one more or one less than a power of two. Both of these types of prime numbers are famous and have surprising connections to other mathematics.

Definition 3.3.1. A **Mersenne prime** is a prime number which can be expressed in the form $2^n - 1$, where n is a positive integer.

On Assignment 1, you proved the following.

Proposition 3.3.2. *If n is a positive composite number, then $2^n - 1$ is a composite number.*

Proof. Exercise for the reader. *Hint: use the geometric series formula.* □

Example 3.3.3. The numbers $4, 6$ and 9 are composite. Accordingly, $2^4 - 1 = 15$, $2^6 - 1 = 63$ and $2^9 - 1 = 511 = 7 \cdot 73$ are composite.

Proposition 3.3.2 immediately tells us something interesting about Mersenne primes.

Corollary 3.3.4. *Every Mersenne prime is of the form $2^p - 1$ where p is prime.*

How often is it the case that $2^p - 1$ is prime for a prime p? We can attempt to investigate some small cases by hand:

p	$2^p - 1$	Mersenne prime?
2	3	Yes
3	7	Yes
5	31	Yes
7	127	Yes
11	2,047	No! Equals $23 \cdot 89$

So, $2^p - 1$ is prime for the first four primes, but the streak breaks down at the fifth prime.

Clearly it will be very difficult to make further progress working by hand; computer assistance is required. Shown below is a list of all the primes less than 100 with a box drawn around each prime p for which $2^p - 1$ is a Mersenne prime.

$$\boxed{2}, \boxed{3}, \boxed{5}, \boxed{7}, 11, \boxed{13}, \boxed{17}, \boxed{19}, 23, 29, \boxed{31}, 37, 41, 43, 47, 53, 59, \boxed{61}, 67, 71, 73, 79, 83, \boxed{89}, 97$$

Thus, it appears that prime exponents leading to Mersenne primes become less common as p increases.

prime p	Mersenne prime $2^p - 1$
2	3
3	7
5	31
7	127
13	8,191
17	131,371
19	524,287
31	2,147,483,647
61	2,305,843,009,213,693,951
89	618,970,019,642,690,137,449,562,111

Table 3.1: The 10 smallest Mersenne primes.

Mersenne primes grow very quickly and play a significant role in the search for extremely large prime numbers. Many of the largest numbers proven to be prime are Mersenne primes. Currently, the largest known prime number is the Mersenne prime

$$2^{82,589,933} - 1,$$

which has $24,862,048$ digits when written out in base ten.

Both of the following questions are open at time of writing, though many mathematicians believe the answer to both of them is probably "yes".

Open Problem 3.3.5. Are there infinitely many primes p such that $2^p - 1$ is prime? In other words, are there infinitely many Mersenne primes?

Open Problem 3.3.6. Are there infinitely many primes p such that $2^p - 1$ is composite?

Mersenne primes have a surprising connection to the study of *perfect numbers*, positive integers that are equal to the sum of their positive, proper divisors. The ancient Greeks studied perfect numbers, but were only aware of the four smallest examples: $6, 28, 496, 8128$. The following definition/notation will make it more convenient for us to talk about perfect numbers.

Definition 3.3.7. Given a positive integer n, we write $\sigma(n)$ for the sum of all the positive divisors of n. We call σ the **divisor sum function**.

Example 3.3.8. $\sigma(100) = 1 + 2 + 4 + 5 + 10 + 20 + 25 + 50 + 100 = 192$.

Exercise 3.3.9. Give a formula for $\sigma(p^k)$ where p is prime and k is positive integer. Prove that $\sigma(p^k q^\ell) = \sigma(p^k)\sigma(q^\ell)$ if p and q are distinct primes and k and ℓ are positive integers. Use what you have learned to efficiently calculate $\sigma(6000)$.

Exercise 3.3.10. Prove that $\sigma(mn) = \sigma(m)\sigma(n)$ when m and n are relatively prime positive integers. Give examples to show this formula doesn't always hold. *Note: this exercise says that σ is an example of "multiplicative arithmetic" function.*

Exercise 3.3.11. Prove that a positive number p is prime if and only if $\sigma(p) = p + 1$.

We can think of $\sigma(n)$ as a sort of measure of how "divisible" the number n is, which explains the choice of terminology below.

Definition 3.3.12. Let n be a positive integer.

- If $\sigma(n) = 2n$, we say n is a **perfect number**. This is the same as saying that n equals the sum of its *proper* positive divisors.
- If $\sigma(n) < 2n$, we say n is a **deficient number**
- If $\sigma(n) > 2n$, we say n is an **abundant number**

Example 3.3.13.

(a) $\sigma(14) = 1+2+7+14 = 24 < 2 \cdot 14$, so 28 is a deficient number. It is "not very divisible".

(b) $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28 > 2 \cdot 12$, so 12 is an abundant number. It is "highly divisible".

(c) $\sigma(6) = 1 + 2 + 3 + 6 = 2 \cdot 6$, so 6 is a perfect number. It is right in the middle in terms of divisibility.

Exercise 3.3.14.

(a) Prove that every prime number is deficient. More generally, prove that p^k is deficient whenever p is prime and k is a postive integer.

(b) Prove that, if a is an abundant number, then ma is an abundant number for every positive integer m.

Mersenne primes have an intriguing connection to perfect numbers which was established in Euclid's *Elements*.

Theorem 3.3.15 (Euclid)**.** *Let p be a prime for which $2^p - 1$ is a Mersenne prime. Then $n = 2^{p-1}(2^p - 1)$ is a perfect number.*

Proof. Let $q = 2^p - 1$ for brevity. Because $n = 2^{p-1}q$ is the prime factorization of n, we can see that the positive divisors of n are exactly the integers $2^i q^j$ where $i \in \{0, 1, \ldots, p-1\}$ and $j \in \{0, 1\}$. Thus,

$$\sigma(n) = \sum_{i=0}^{p-1} \sum_{j=0}^{1} 2^i q^j = \sum_{i=0}^{p-1} \left(2^i + 2^i q\right) = \sum_{i=0}^{p-1} (1+q)2^i = (1+q)\frac{2^p - 1}{2 - 1} = 2^p(2^p - 1) = 2n.$$

□

Exercise 3.3.16. Reprove Euclid's theorem using your findings from Exercise 3.3.9 and/or Exercise 3.3.10.

Euclid's theorem shows that every Mersenne prime determines a perfect number. To be more precise, every Mersenne prime determines an *even perfect number*, because of the appearance of 2^{p-1} in the formula. There is no known example of an odd perfect number and it is a long-standing open question whether any exist at all.

Open Problem 3.3.17. Does there exist an odd perfect number?

Even perfect numbers were also studied by Hasan Ibn al-Haytham who conjectured that the converse of Euclid's theorem is true. In other words, he conjectured that even perfect numbers and Mersenne primes are in one-to-one correspondence with each other. This conjecture was eventually proven correct by Euler.

Theorem 3.3.18 (Euler)**.** *If n is an even perfect number, then $n = 2^{p-1}(2^p - 1)$ where $2^p - 1$ is a Mersenne prime. That is, p and $2^p - 1$ are both prime.*

Proof. Write $n = 2^k m$, where $k \geq 0$ and m is odd (see Exercise 3.2.11). Actually, because n is even, we have $k \geq 1$. We have $2n = \sigma(n)$, which means

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

using Exercise 3.3.14. The equation above shows $2^{k+1} - 1$ divides $2^{k+1}m$ and so, because it is relatively prime to 2^{k+1}, Proposition 2.4.13 implies that $2^{k+1} - 1$ divides m. We may therefore write $m = s(2^{k+1} - 1)$ for some positive integer s and arrive at:

$$2^{k+1}s = \sigma(m).$$

Now, s and m itself are two distinct (*why?*) divisors of $m = s(2^{k+1} - 1)$, so we have

$$2^{k+1}s = \sigma(m) \geq s + m = 2^{k+1}s.$$

Therefore, the inequality above is an equality and we obtain

$$\sigma(m) = s + m$$

This implies $s = 1$, or else $1, s, m$ are 3 distinct divisors of m and $\sigma(m) \geq 1+s+m$. Therefore, $m = 2^{k+1} - 1$ and, from $\sigma(m) = m + 1$, we have that $m = 2^{k+1} - 1$ is a Mersenne prime (see Exercise 3.3.11). Relabelling $p = k + 1$, we have $n = 2^k m = 2^k(2^{k+1} - 1) = 2^{p-1}(2^p - 1)$, where $2^p - 1$ is a Mersenne prime. □

Exercise 3.3.19. Define a positive integer n to be **superperfect** if $\sigma(\sigma(n)) = 2n$. Prove that n is an even superperfect number if and only if $n = 2^{p-1}$, where $2^p - 1$ is a Mersenne prime.

3.4 Fermat primes

Whereas as the last section was about primes one less than a power of two, this section is about primes one *greater* than a power of two. For example:

$2^1 + 1 = 3$	prime
$2^2 + 1 = 5$	prime
$2^3 + 1 = 9$	not prime
$2^4 + 1 = 17$	prime
$2^5 + 1 = 33$	not prime

The first thing we want to do is narrow down the list of exponents n that can possibly lead to primes $2^n + 1$.

Proposition 3.4.1. *Let $b \geq 2$ be an integer. Then $b^m + 1$ is composite for every odd number $m \geq 3$.*

Proof. Because m is odd, we have the factorization $b^m + 1 = (b+1)(1 - b + b^2 - \ldots + b^{m-1})$ (*Exercise: check this*). Because $b > 1$ and $m \geq 2$, we have $1 < b + 1 < b^m + 1$, so $b^m + 1$ is composite. □

Corollary 3.4.2. *If n is a positive integer such that $2^n + 1$ is a prime number, then $n = 2^k$ for some nonnegative integer k.*

Proof. Write $n = 2^k m$ where k is a nonnegative integer and m is odd (Exercise 3.2.11). Define $b = 2^{2^k} \geq 2$ so that $2^n + 1 = b^m + 1$. If $m \geq 3$, then $b^m + 1$ is composite by the preceding proposition. Therefore, $m = 1$ and we are finished. □

Definition 3.4.3. The numbers $2^{2^k}+1$, where k is a nonnegative integer, are called **Fermat numbers**. A Fermat number which is also prime is known as a **Fermat prime**.

How often does a Fermat number turn out to be a Fermat prime? We can attempt to investigate some small cases by hand, but computer assistance quickly becomes necessary. Table 3.2 shows the smallest 7 Fermat numbers and indicates which are prime.

k	2^k	Fermat number $2^{2^k}+1$	Fermat prime?
0	1	3	Yes
1	2	5	Yes
2	4	17	Yes
3	8	257	Yes
4	16	65,537	Yes
5	32	4,294,967,297	No
6	64	18,446,744,073,709,551,617	No

Table 3.2: The 7 smallest Fermat numbers.

So, $2^{2^k}+1$ is prime for $k = 0, 1, 2, 3, 4$, but the streak breaks down at $k = 5$. This refutes a conjecture of Fermat that all of the numbers $2^{2^k}+1$ are prime. Actually, $2^{2^k}+1$ is known to be composite for $5 \leq k \leq 32$ and heuristics suggest that $2^{2^k}+1$ is composite for all $k \geq 5$. In other words, researchers expect that $\{3, 5, 17, 257, 65537\}$ is the complete set of all Fermat primes. However, very little about Fermat primes is known for certain. Both of the following questions are unanswered at the time of writing.

Open Problem 3.4.4. Are there infinitely many Fermat primes?

Open Problem 3.4.5. Are there infinitely many composite Fermat numbers?

Exercise 3.4.6. Observe that, if n is a positive integer, then the polynomial $p(x) = x^n - 1$ has a root $x = 1$. Observe that, if m is an odd positive integer, then the polynomial $p(x) = x^m + 1$ has a root $x = -1$. Connect these observations to the following statements which we used in our study of Mersenne primes and Fermat primes.

(a) $b^n - 1$ is composite if $b \geq 3$ and $n \geq 2$.

(b) $b^n + 1$ is composite if $b \geq 2$ and $m \geq 3$ is odd.

Exercise 3.4.7. Let b and n be integers with $b \geq 2$ and $n \geq 1$. Prove that, if $b^n + 1$ is prime, then b is even and $n = 2^k$ for some nonnegative integer k. Investigate the primality of $6^{2^k}+1$ and $10^{2^k}+1$ for small values of k.

Exercise 3.4.8. Denote the Fermat number $2^{2^k}+1$. Show that:

$$f_k = f_0 f_1 \cdots f_{k-1} + 2$$

for every positive integer k.

We can use the recurrence relation for Fermat numbers obtained in the preceding exercise to prove an interesting result.

Proposition 3.4.9. *Any two distinct Fermat numbers are relatively prime to one another.*

Proof. Consider two distinct Fermat numbers $f_k = 2^{2^k} + 1$ and $f_\ell = 2^{2^\ell} + 1$, where $0 \leq k < \ell$. Suppose that d is a positive integer dividing both f_k and f_ℓ. From Exercise 3.4.8, we may write $f_\ell = f_0 f_1 \cdots f_{\ell-1} + 2$. Note that d divides $f_0 f_1 \cdots f_{\ell-1}$, because $k < \ell$ so f_k appears among $f_0, f_1, \ldots, f_{\ell-1}$. Thus, from the equation

$$2 = f_\ell - f_0 f_1 \cdots f_{\ell-1},$$

we conclude that d divides 2. Therefore either $d = 1$ or $d = 2$. However, it is not possible that $d = 2$ because every Fermat number is odd, and therefore not divisible by 2. Thus, the ony positive integer dividing f_k and f_ℓ is 1, i.e. f_k and f_ℓ are relatively prime. □

The above proposition is somewhat of a vindication for Fermat's wrong conjecture that all Fermat numbers are prime. Even though it seems that most f_k are *not* prime, it is still the case that the prime factors of a given Fermat number are "brand new primes" which do not appear as prime factors of any previous Fermat number.

Exercise 3.4.10. Use Proposition 3.4.9 to give yet another proof that the set of prime numbers is infinite.

The remainder of this section will not appear on the assignments or tests.

Fermat primes have an unexpected connection to *compass and straightedge constructions*. This is a classical topic in geometry studied by the ancient Greeks. The ancient Greeks knew how to construct an equilateral triangle, a square and a regular[2] pentagon by compass and straightedge. They also knew how to double the number of sides of a given regular polygon by compass and straightedge. For about 2000 years, no further constructions of regular polygons by compass and straightedge were discovered until a young Gauss showed it is possible to construct a regular 17-sided polygon with compass and straightedge. In fact, Gauss showed that, if m is any number that is a product of distinct Fermat primes, then it is possible to construct a regular m-sided polygon by compass and straightedge. Gauss also asserted (without proof) that no more compass and straightedge constructions of regular polygons are possible. Eventually, this was proven to be correct by Wantzel. So, for example, we know it is not possible to construct a 7-sided regular polygon by compass and straightedge. A proof of any of these results is far outside the scope of this course.

Theorem 3.4.11 (Gauss, Wantzel)**.** *It is possible to construct a regular polygon with n sides if and only if $n = 2^k$ for $k \geq 2$ or $n = 2^k m$ where $k \geq 0$ and m is the product of one or more distinct Fermat primes.*

Exercise 3.4.12. Is it possible to construct a regular polygon with 306 sides by compass and straightedge? What about a regular polygon with 170 sides?

[2]Meaning all sides and and angles are equal

3.5 The prime number theorem

This section will not appear on the assignments or tests.

In this section we discuss how the primes are distributed amongst the positive integers. An early result in this area, conjectured by Bertrand and proved correct by Chebyshev, is the following:

Theorem 3.5.1 (Bertrand's postulate)**.** *For every integer $n \geq 2$, there exists a prime number p satisfying $n < p < 2n$.*

This result gives some modest predictive power over how long one needs to wait to see the "next prime". The next prime following n must occur before we get to $2n$. Although we state the above result without proof, a reasonably elementary proof was given by Erdös. An enthusiastic reader may wish to look this proof up.

The following definition will help us talk about the distribution of primes more precisely.

Definition 3.5.2. Given a positive number x, we write $\pi(x)$ for the number of primes less than or equal to x. The function π is called the **prime counting function**.

Exercise 3.5.3. Use Bertrand's postulate to prove $\pi(2^n) \geq n$ for every positive integer n.

Bertrand's postulate, it turns out, is actually a rather blunt instrument. For large n, there are many more primes between n and $2n$ than the 1 prime guaranteed by Bertrand's postulate.

Example 3.5.4.

- There are 25 prime numbers smaller than 100, meaning $\pi(100) = 25$. The proportion of integers in the interval $[1, 100]$ which are prime is about 0.25.
- There are 1229 prime numbers smaller than 10000, meaning $\pi(10^4) = 1229$. The proportion of integers in the interval $[1, 10^4]$ which are prime is about 0.12.
- There are 5761455 prime numbers smaller than 10^8, meaning $\pi(10^8) = 5761455$. The proportion of integers in $[1, 10^4]$ which are prime is about 0.06.

Note that, every time we square x (which roughly doubles the number of digits), we find that the proportion of primes in the interval $[1, x^2]$ seems to be about half of the proportion of primes in the interval $[1, x]$. In particular, prime numbers seem to become less and less frequent the farther out we look. The *prime number theorem* gives the precise asymptotics of the prime counting function. Conventional proofs of the prime number theorem use the methods of complex analysis and belong to a subject called *analytic number theory*.

Theorem 3.5.5 (Prime number theorem)**.** $\pi(x) \approx \dfrac{x}{\log x}$*, in the sense that* $\displaystyle\lim_{x\to\infty} \frac{\pi(x)}{\left(\frac{x}{\log x}\right)} = 1.$

Exercise 3.5.6. Argue that the prime theorem can be intepreted as saying "the proportion of integers in the interval $[1, x]$ which are prime is approximately $\frac{1}{\log(x)}$". Use this interpretation, and the properties of logarithms, to explain why the number of primes in $[1, x]$ is roughly half the number of primes in $[1, x^2]$.

Exercise 3.5.7. Using Bertrand's postulate (see Exercise 3.5.3), there are at least 100 primes smaller than 2^{100}. How does this compare to the number of primes smaller than 2^{100} predicted by the prime number theorem.

Chapter 4

Modular Arithmetic

4.1 Informal discussion

Modular arithmetic is a framework for doing calculations with divisibility relations. The modern approach was developed by Gauss in his *Disquisitiones Arithmeticae*. At first, it may look as though we are just introducing new words and notations for old concepts that we have already been studying, but it will hopefully soon become clear that the language of modular arithmetic is both useful and powerful.

Let's start with an informal discussion. "Working modulo 14" more or less means regarding two numbers which differ by a multiple of 14 as being "equal". We are allowed to "cast out 14s" whenever we like. For example:

$$30 = 16 = 2 = -12 \qquad\qquad 14 = 0 = -14$$

As a consequence, we only really need to work with the numbers $\{0, 2, 3, \ldots, 13\}$ because all another integers are equivalent to one of these. More specifically, every integer is equivalent to its remainder on division by 14. Doing arithmetic (addition, subtraction and multiplication) may take us outside of this set, but we can always reduce our results by multiples of 14 to get back. For example:

$$10 + 9 = 19 = 5 \qquad\qquad 10 \cdot 3 = 30 = 2$$

It is all well and good to declare $14 = 0$ and explore the implications, but what really makes this useful mathematics is the following principle:

Principle 4.1.1. Working modulo a positive integer is "consistent" with the operations of arithmetic.

What is meant by that? Well suppose we want to calculate the remainder of $20 \cdot 30$ modulo 14. One approach would be to multiply then reduce.

$$20 \cdot 30 = 600 = 12 \qquad\qquad \text{because } 600 = 42 \cdot 14 + 12.$$

Note multiplying first left us with the large number 600 to deal with. Another idea would be to reduce and then multiply. Let's try that too:

$$20 = 6 \qquad 30 = 2 \qquad 20 \cdot 30 = 6 \cdot 2 = 12.$$

Both approaches led us to the same conclusion: $20 \cdot 30 = 12$ modulo 14. This is what is meant when we say that working modulo 14 is consistent with the operations of arithmetic. Some or all of the numbers in an arithmetical expression can be replaced with equivalent numbers modulo 14 without affecting the overall result modulo 14.

Let's do one more example, this time working modulo 9. Let's exploit the nature of our base-10 system for representing numbers and the fact that $10 = 1$, working modulo 9, to try to work out whether 7245 is divisible by 9. We have

$$7245 = 7000 + 200 + 40 + 5 = 7(10)^3 + 2(10)^2 + 4(10) + 5.$$

However, because we are working modulo 9, we can replace all the 10s above with 1s, which gives

$$7245 = 7 + 2 + 4 + 5 = 18 = 0.$$

This suggests that 7245 and 0 differ by a multiple of 9 which exactly means that 9 divides 7245. This reasoning is actually legitimate! We have $7245/9 = 805$.

4.2 Definitions

Now it is time to make the informal discussion of the preceding section into rigorous mathematics. Here is the fundamental definition.

Definition 4.2.1. Let n be a positive integer. We say **x is congruent to y modulo n** and write $x \equiv y \pmod{n}$ if $x = y + kn$ for some $k \in \mathbb{Z}$. Writing $x \underset{n}{\equiv} y$ is an acceptable alternative notation.

More informally put, $x \equiv y \pmod{n}$ means that "x and y differ by a multiple of n".

Example 4.2.2.

- x is divisible by n if and only if $x \equiv 0 \pmod{n}$.
- x is *even* if and only if $x \equiv 0 \pmod{2}$
- x is *odd* if and only if $x \equiv 1 \pmod{2}$
- x and y have the same *parity* if and only if $x \equiv y \pmod{2}$

The following proposition gives a couple of slightly different, but equivalent, ways to think about congruence modulo n.

Proposition 4.2.3. *Let n be a positive integer.*

1. *Show that* $x \equiv y \pmod{n}$ *if and only if* n *divides* $x - y$.

2. *Show that every* $x \in \mathbb{Z}$ *is congruent to exactly one element of* $\{0, 1, \ldots, n-1\}$*, namely the remainder of* x *upon division by* n*. Show that* $x \equiv y \pmod{n}$ *if and only if* x *and* y *have the same remainder upon division by* n*.*

Proof. Exercise for the reader. □

Congruence modulo n is an example of an *equivalence relation*, the definition of which we now recall:

Definition 4.2.4. Let $\sim$ be a relation on a set X. We say that $\sim$ is an **equivalence relation** if all of the following conditions are satisfied:

1. **Reflexivity:** $x \sim x$ for all $x \in X$.

2. **Symmetry:** If $x, y \in X$ are such that $x \sim y$, then $y \sim x$.

3. **Transitivity:** If $x, y, z \in X$ are such that $x \sim y$ and $y \sim z$, then $x \sim z$.

Given $x \in X$, we write $[x] = \{y \in X : x \sim y\}$ and call $[x]$ the **equivalence class** of x.

Equivalence relations are closely related to partitions, as the following standard properties indicate:

- The equivalence classes form a partition of X.

- Given $x, y \in X$, we have $x \sim y$ if and only if $[x] = [y]$.

Proposition 4.2.5. *For any positive integer* n*, the relation* $\equiv_n$ *of congruence modulo* n *is an equivalence relation on* $\mathbb{Z}$*.*

Proof.

- *Reflexivity:* Suppose $x \in \mathbb{Z}$. Then, $x = x + 0n$, where $0 \in \mathbb{Z}$, so $x \equiv x \pmod{n}$.

- *Symmetry:* Suppose $x, y \in \mathbb{Z}$ and $x \equiv y \pmod{n}$. By definition, $x = y + kn$ for some $k \in \mathbb{Z}$. Then, $y = x + (-k)n$, where $-k \in \mathbb{Z}$, so $y \equiv x \pmod{n}$.

- *Transitivity:* Suppose $x, y, z \in \mathbb{Z}$ and that $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n}$. That is, $x = y+kn$ and $y = z+\ell n$ for some $k, \ell \in \mathbb{Z}$. Then, $x = y+kn = z+\ell n+kn = z+(k+\ell)n$ where $k + \ell \in \mathbb{Z}$, so $x \equiv z \pmod{n}$.

□

Definition 4.2.6. The equivalence class of an integer x is denote with respect to $\equiv_n$ is referred to as a **congruence class** and is denoted $[x]_n$.

Example 4.2.7.

$$[1]_7 = \{1 + 7k : k \in \mathbb{Z}\} = \{\ldots, -6, 1, 8, 15, 22, \ldots\}$$
$$[4]_3 = \{4 + 3k : k \in \mathbb{Z}\} = \{\ldots, -2, 1, 4, 7, 10, \ldots\}$$
$$[99]_{10} = \{99 + 100k : k \in \mathbb{Z}\} = \{-1, 9, 19, 29, \ldots, 99, 109, \ldots\}$$

In contexts when only one modulus n is being considered and confusion seems unlikely, we may choose to drop the n and simply write $[x]$. Actually, one sometimes dispenses with the brackets altogether and simply writes "x" for the congruence class of x, but we will try to avoid doing that at this introductory level.

The following proposition shows that the operations of addition and multiplication are consistent with the relation of congruence modulo n. It is a precise version of the vague idea espoused in Principle 4.1.1 from the preceding section.

Proposition 4.2.8. *Let n be a positive integer. Suppose $x \equiv x' \pmod{n}$ and $y \equiv y' \pmod{n}$. Then,*

1. $x + y \equiv x' + y' \pmod{n}$
2. $xy \equiv x'y' \pmod{n}$

Proof. Write $x' = x + kn$ and $y' = y + \ell n$ where $k, \ell \in \mathbb{Z}$. Then,

$$x' + y' = (x + y) + (k + \ell)n,$$

where $k + \ell \in \mathbb{Z}$, so $x' + y' \equiv x + y \pmod{n}$. Also,

$$x'y' = (x + kn)(y + \ell n) = xy + (ky + \ell x + k\ell n)n,$$

where $ky + \ell x + k\ell n \in \mathbb{Z}$, so $x'y' \equiv xy \pmod{n}$. □

Exercise 4.2.9. Determine (with proof or counterexample) which of the following statements is true for all positive integers m, n, x, y.

(a) If $x \equiv y \pmod{n}$, then $n \equiv -y \pmod{x}$.

(b) If $x \equiv y \pmod{n}$ and $m|n$, then $x \equiv y \pmod{m}$.

(c) If $x \equiv y \pmod{n}$ and $n|m$, then $x \equiv y \pmod{m}$.

(d) If $x \equiv y \pmod{n}$, then $mx \equiv my \pmod{n}$.

(e) If $x \equiv y \pmod{n}$ and x and y are divisible by m, then $\frac{x}{m} \equiv \frac{y}{m} \pmod{n}$.

(f) If $x \equiv y \pmod{n}$ and x, y, n are all are divisible by m, then $\frac{x}{m} \equiv \frac{y}{m} \pmod{\frac{n}{m}}$.

Exercise 4.2.10. Let n be a positive integer. Use modular arithmetic to work out all the possible remainders of n^2 upon division by 3. *Hint: start your argument like this: "we examine* 3 *cases:* $n \equiv 0 \pmod 3$, $n \equiv 1 \pmod 3$ *and* $n \equiv 2 \pmod 3$*".* Similarly, work out all the possible remainders of n^2 upon division by 6.

Exercise 4.2.11. Use arithmetic modulo 8 to prove that, if $x \equiv 7 \pmod 8$, then it is impossible to express x as the sum of three nonzero squares.

Exercise 4.2.12. Suppose m and n are positive integers such that $2^m + 3 = 7^n$. Use arithmetic modulo 8 to prove that $m = 2$ and $n = 1$.

Exercise 4.2.13. Use modular arithmetic to prove, with very little computation that 39 divides $53^{103} + 103^{53}$. *Hint: to show* $39|n$*, it suffices to show* $3|n$ *and* $13|n$ *(why?).*

Exercise 4.2.14. Prove that a positive integer n is divisible by 3 if and only if the sum of the digits of its base 10 decimal representation is divisible by 3.

Exercise 4.2.15. Prove that a positive integer is divisible by 11 if and only if the *alternating* sum of the digits of its base 10 decimal representation is divisible by 11. For example, if $n = 18,272,639$, then the alternating digit sum of n is

$$9 - 3 + 6 - 2 + 7 - 2 + 8 - 1 = 22,$$

so we may conclude that n is divisible by 11.

Example 4.2.16. Let's find the remainder of 4444^{4444} upon division by 9. In the language of modular arithmetic, we are trying to find the unique $r \equiv 4444^{4444} \pmod 9$ with $0 \leq r < 9$. Firstly, using the fact that $10 \equiv 1 \pmod 9$ and that congruence modulo 9 is compatible with addition and multiplication, we have

$$4444 = 4(10)^3 + 4(10)^2 + 4(10) + 4 \underset{9}{\equiv} 4 + 4 + 4 + 4 = 16 \underset{9}{\equiv} 7 \underset{9}{\equiv} -2$$

and so $4444^{4444} \equiv (-2)^{4444} \pmod 9$.

Next, rather than raise -2 to such a high power, let's first see if some smaller power of -2 is equal to ± 1 or 0 (those are the only integers it is easy to take powers of!). We quickly see that:

$$(-2)^3 = -8 \underset{9}{\equiv} 1.$$

Writing $4444 = 1481 \cdot 3 + 1$, we therefore have

$$(-2)^{4444} = \left((-2)^3\right)^{1481} \cdot (-2)^1 \underset{9}{\equiv} (1)(-2) \underset{9}{\equiv} 7.$$

Thus, $4444^{4444} \equiv 7 \pmod 9$, i.e. the remainder of 4444^{4444} on division by 9 is 7.

Note we did not even really need to find the quotient 1481 when 4444 was divided by 3. It was enough to know the remainder was 1. We could have used modular arithmetic to compute $4444 \equiv 1 \pmod 3$ and got by with even less calculation.

4.3 Fermat's little theorem and Euler's generalization

In this section we state two theorems whose proofs will be returned to at a later point.

Theorem 4.3.1 (Fermat's little theorem)**.** *Let p be a prime number. Let a be an integer which is relatively prime to p. Then, $a^{p-1} \equiv 1 \pmod{p}$.*

Note that, since p is prime, saying an integer a is relatively prime to p is the same thing as saying p does not divide a.

A complete proof of Fermat's little theorem will be given later. For now, let us note that only a finite amount of calculation is needed to check the theorem is true for any specific prime number p.

Example 4.3.2. If $p = 5$, the claim is that $a^4 \equiv 1 \pmod{5}$ for every integer a that is not divisible by 5. Since every integer not divisible by 5 is congruent to exactly one element of the set $\{1, 2, 3, 4\}$, we can prove the theorem in this specific case by checking it holds for each of these numbers.

$$\begin{aligned} a &= 1 & 1^4 &= 1 \\ a &= 2 & 2^4 &= 16 \underset{5}{\equiv} 1 \\ a &= 3 & 3^4 &= 81 \underset{5}{\equiv} 1 \\ a &= 4 & 4^4 &\underset{5}{\equiv} (-1)^4 = 1 \end{aligned}$$

Exercise 4.3.3. Prove Fermat's little theorem for the specific prime $p = 7$ using the brute force approach of Example 4.3.2.

Exercise 4.3.4. State in simple terms what Fermat's little theorem says about the prime 2.

Exercise 4.3.5. Use Fermat's little theorem to calculate the remainder of 42^{12345} on division by 47.

Exercise 4.3.6. Prove that n and n^5 have the same last digit in base 10 for every positive integer n. *Be careful! Fermat's little theorem helps with some cases, but not all.*

Exercise 4.3.7. Check that $4^{14} \equiv 1 \pmod{15}$ and $7^{14} \not\equiv 1 \pmod{15}$. This demonstrates the fact that, if a is relatively prime to n but n is not prime, it may or may not be the case that $a^{n-1} \equiv a \pmod{n}$.

Note that "Fermat's little theorem" is not the same as the more famous "Fermat's last theorem" which states that, for every integer $n \geq 3$, the equation $x^n + y^n = z^n$ has no positive integer solutions. The latter was a notorious open problem for hundreds of years. Fermat claimed to have a short proof which the "margin was too narrow to contain", but it is virtually certain he was mistaken on this point. Fermat's last theorem was finally proved by Andrew Wiles in the 1990s. Somewhat entertainingly, Wiles proof led to a "continuity

error" in *Star Trek: The Next Generation* as Captain Jean-Luc Picard stated the problem was still open in the 24th century.

Although Fermat's little theorem does not get as much publicity as its more famous cousin Fermat's last theorem, there is a sense in which Fermat's little theorem is actually the more important of the two results because it is the first step towards a circle of results called *primality tests*. In the field of cryptography, it is important to be able to generate very large prime numbers. In practice, the way this is done is to pick large numbers at random and use primality tests to check whether they are primes (or at least "industry-grade primes", i.e. numbers that are "probably prime" with extremely high confidence). The following exercise is intended to give you some flavour of how Fermat's little theorem could be of some use for computationally efficient primality testing.

Exercise 4.3.8. The number $n = 281487861809153$ is *not* prime. Because of Fermat's little theorem, we could prove n is not prime by demonstrating that $2^{n-1} \not\equiv 1 \pmod{n}$. But, is it feasible for a computer to calculate 2^{n-1} modulo n? Find a way to do it with only 52 multiplications and reductions modulo n. *Hint 1: repeated squaring can be used to compute* 2^{2^k} *with only* k *multiplications. Hint 2: Write the exponent* $n-1$ *as a sum of powers of* 2 *(in other words, write it in binary).*

The following exercise gives some indication of the shortcomings of Fermat's last theorem as a test for primality. For yet more disheartening information, one can read about *Carmichael numbers*.

Exercise 4.3.9. Let p be prime and set $n = 2^p - 1$. According to Fermat's little theorem, a necessary condition for n to be a Mersenne prime is $2^{n-1} \equiv 1 \pmod{n}$. Prove that, actually, $2^{n-1} \equiv 1 \pmod{n}$ regardless of whether or not n is a Mersenne prime, so this "test" is completely useless here.

Euler proved a generalization of Fermat's little theorem which doesn't require p to be prime. To state Euler's theorem, we first need a definition.

Definition 4.3.10. Given a positive integer n, we write $\varphi(n)$ for the number of integers k such that $1 \leq k \leq n$ and k is relatively prime to n. The function φ is called the **Euler totient**.

Example 4.3.11.

- Among $\{1, 2, 3, 4, 5, 6\}$, only 1 and 5 are relatively prime to 6, so $\varphi(6) = 2$.
- From the list of positive integers up to 15, we remove the multiples of 3 and 5.

  $$1 \quad 2 \quad \not{3} \quad 4 \quad \not{5} \quad \not{6} \quad 7 \quad 8 \quad \not{9} \quad \not{10} \quad 11 \quad \not{12} \quad 13 \quad 14 \quad \not{15}$$

  Then, $\varphi(15) = 8$ because the 8 remaining numbers are relatively prime to 15.
- If p is prime, then $\varphi(p) = p - 1$ because each of $1, 2, \ldots, p-1$ is relatively prime to p.

The following proposition shows that $\varphi(n)$ can be calculated very easily from the prime factorization of n. This is nice for small examples, but not very helpful in general because factoring large integers is very computationally expensive (that's the basis of public key encryption!).

Proposition 4.3.12.

1. *If p is a prime and k is a positive integer, then $\varphi(p^k) = p^k - p^{k-1}$.*
2. *If m and n are relatively prime positive integers, then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Proof (first part only). Let p be a prime and k a positive integer. The numbers among $\{1, 2, 3, \ldots, p^k\}$ that are *not* relatively prime to p^k are exactly those numbers that are divisible by p. That is, the numbers mp where $m = 1, 2, 3, \ldots, p^{k-1}$. We are removing p^{k-1} elements from set with p^k elements and the remaining count is $\varphi(p^k) = p^k - p^{k-1}$, as desired. We omit the proof of the second statement (perhaps we will return to it later). □

This is not the first time we have encountered a function satisfying the property in the second part of Proposition 4.3.12. Recall that the divisor sum function σ (Definition 3.3.7) had the same property (Exercise 3.3.10). Both φ and σ are examples of what are sometimes called *multiplicative functions* or *arithmetic functions*. Number theory is full of such functions.

Example 4.3.13. We apply Proposition 4.3.12 to calculate $\varphi(100)$.

$$\varphi(100) = \varphi(2^2 5^2) = \varphi(2^2)\varphi(5^2) = (2^2 - 2)(5^2 - 5) = (2)(20) = 40$$

Thus, exactly 40 of the positive integers up to 100 are relatively prime to 100.

Exercise 4.3.14. Suppose $n = p_1^{\epsilon_1} \cdots p_k^{\epsilon_k}$ is the prime factorization of a positive integer n. Give a formula for $\varphi(n)$.

Now we state Euler's result

Theorem 4.3.15 (Euler's generalization of Fermat's little theorem)**.** *Let n be a positive integer. Let a be an integer which is relatively prime to n. Then, $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Note this really is a generalization of Theorem 4.3.1 because $\varphi(p) = p - 1$ when p is prime.

Example 4.3.16. We checked $\varphi(15) = 8$ in Example 4.3.11. Since 2 is relatively prime to 15, Euler's theorem predicts that $2^8 \equiv 1 \pmod{15}$. Indeed:

$$2^8 = (2^4)(2^4) = (16)(16) \underset{15}{\equiv} (1)(1) = 1.$$

Exercise 4.3.17. Use Euler's theorem to efficiently calculate the remainder of 3^{555555} upon division by 35.

Exercise 4.3.18. Use Euler's theorem to efficiently calculate the last two digits of 3^{444444}.

4.4 The ring of integers modulo n

Recall Proposition 4.2.8 which, roughly speaking, says that addition and multiplication are compatible with congruence. Because of this, it makes sense to do arithmetic *on congruence classes*. Proposition 4.2.8 exactly means that adding/multiplying two congruence classes by adding/multiplying arbitrarily chosen representatives yields well-defined operations.

Definition 4.4.1. Let n be a positive integer. We denote by $\mathbb{Z}/n$ the set of all congruence classes of integers modulo n. In other words (see Proposition 4.2.3 (b)), we have:

$$\mathbb{Z}/n = \{[0], [1], [2], \ldots, [n-1]\}.$$

We define addition and multiplication operations on $\mathbb{Z}/n$ by

$$[x] + [y] = [x + y] \qquad [x][y] = [xy] \qquad \text{for all } x, y \in \mathbb{Z}.$$

The **ring of integers modulo n** refers to $\mathbb{Z}/n$ together with these two operations.

The operations above make $\mathbb{Z}/n$ into a number system in its own right with similar properties to other familiar numbers systems such as the integers $\mathbb{Z}$, the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$. All of these are examples of a general concept from abstract algebra known as a *commutative ring*.

Definition 4.4.2. Let R be a set on which operations called **addition** and **multiplication** have been defined; any two elements $x, y \in R$ have a sum $x + y$ and a product xy. If all of the following axioms hold, we call R, together with its operations, a **commutative ring**.

- **Closure:** If $x, y \in R$, then $x + y \in R$ and $xy \in R$.
- **Associativity:** If $x, y, z \in R$, then $(x+y)+z = x+(y+z)$. Since rebracketing doesn't change the sum, it makes sense to write $x + y + z$, omitting the brackets. The same discussion applies to multiplication: $(xy)z = x(yz)$ and we may simply write xyz.
- **Commutativity:** If $x, y \in R$, then $x + y = y + x$ and $xy = yx$.
- **Distributive property:** If $x, y, z \in R$, then $x(y + z) = xy + xz$.
- **Additive and multiplicative identities:** There are elements 0 and 1 in R with the property that $x + 0 = x$ and $1x = x$ for all $x \in R$.
- **Additive inverses:** For every $x \in R$, there is an element $-x \in R$ with the property that $x + (-x) = 0$.

Proposition 4.4.3. *For any positive integer n, the ring $\mathbb{Z}/n$ of integers modulo n is a commutative ring.*

Proof. Exercise for a patient reader. □

Proposition 4.4.3 shows that $\mathbb{Z}/n$ is similar in many ways to other familiar number systems like $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$. There are also some important differences however:

- $\mathbb{Z}/n$ only has finitely many elements, namely n.
- We cannot always "cancel" a nonzero element from an equation in $\mathbb{Z}/n$. For example, working in $\mathbb{Z}/15$, we have $[3][4] = [3][9]$ where $[3] \neq [0]$, but we cannot cancel $[3]$ because $[4] \neq [9]$.
- It is sometimes possible for two nonzero quantities to multiply to zero in $\mathbb{Z}/n$. For example, working in $\mathbb{Z}/15$ again, we have $[3][5] = [0]$ even though $[3], [5] \neq [0]$.

The following definition will help us make sense of the issues raised above.

Definition 4.4.4. Let R be a commutative ring and let $a \in R$. We say $a \in R$ is a **unit** if there exists $b \in R$ such that $ab = 1$. We say a is a **zero divisor** if there exists a *nonzero* $b \in R$ such that $ab = 0$.

Remark 4.4.5. The reader is warned that, in some mathematical contexts, the word "unit" refers specifically to the identity element 1. This clashes with the way we use the word above, to refer to all the elements that are invertible with respect to multiplication.

Example 4.4.6. Working in the integers $\mathbb{Z}$, the only units are 1 and -1 and the only zero divisor is 0 itself. Working in the rational numbers $\mathbb{Q}$, every nonzero rational number is a unit, and the only zero divisor is 0 itself.

Here are some important properties of units:

Proposition 4.4.7 (Properties of units)**.** *In any commutative ring R, the following hold:*

1. ***Cancellation:*** *If $a, r_1, r_2 \in R$ and a is a unit, then $ar_1 = ar_2$ implies $r_1 = r_2$.*
2. ***Uniqueness of multiplicative inverses:*** *if a is a unit of R, then there is exactly one element of R, usually denoted a^{-1}, with the property that $aa^{-1} = 1$.*
3. ***Closure under multiplication:*** *If $a, b \in R$ are units, then ab is a unit.*

Proof. For the first statement, a is a unit, so $ba = 1$ for some $b \in R$. Therefore,

$$ar_1 = ar_2 \qquad \Longrightarrow \qquad bar_1 = bar_2 \qquad \Longrightarrow \qquad 1r_1 = 1r_2 \qquad \Longrightarrow \qquad r_1 = r_2.$$

For the second statement, suppose a is a unit and $b_1, b_2 \in R$ both satisfy $ab_1 = ab_2 = 1$. Then, by the first statement, we can cancel a from the equation $ab_1 = ab_2$ to obtain $b_1 = b_2$.

For the third statement, suppose $a, b \in R$ are units. By definition, they have multiplicative inverses a^{-1} and b^{-1}. Then,

$$(ab)(a^{-1}b^{-1}) = (aa^{-1})(bb^{-1}) = (1)(1) = 1,$$

which shows ab is a unit whose multiplicative inverse is $a^{-1}b^{-1}$. □

Exercise 4.4.8. Prove that an element of a commutative ring cannot be both a unit and a zero divisor.

Exercise 4.4.9. Generalize Part 1 of Proposition 4.4.7 by proving that, if $a, r_1, r_2 \in R$ and a is not a zero divisor, then $ar_1 = ar_2$ implies $r_1 = r_2$.

Here is an example looking at the units and zero divisors in a specific ring $\mathbb{Z}/n$.

Example 4.4.10. Consider $\mathbb{Z}/12$. Then, $[1], [5], [7], [11]$ are units. Actually, each of these is its own multiplicative inverse (it won't always work this way):

$$[1][1] = [1] \qquad [5][5] = [25] = [1] \qquad [7][7] = [49] = [1] \qquad [11][11] = [-1][-1] = [1].$$

The remaining elements $[0], [2], [3], [4], [6], [8], [9], [10]$ are all zero divisors, as the equations below demonstrate:

$$\begin{array}{lll} [0][1] = [0] & [2][6] = [12] = [0] & [3][4] = [12] = [0] \\ [8][3] = [24] = [0] & [9][4] = [36] = [0] & [10][6] = [60] = [0] \end{array}$$

We comment briefly on where these equations are coming from. Consider $[10]$. What should we multiply it by to make it divisible by 12 so that we get $[0]$? Well, the prime factorization of 10 has one 2 and one 5. The prime factorization of 12 has two 2s and one 3. So, we need to introduce one more 2 and a 3 to make 10 divisible by 12. This is the reason we multiplied it by $6 = 2 \cdot 3$ above.

In the preceding example, we saw that every element of $\mathbb{Z}/12$ was either a unit or a zero divisor, with no overlap between these two categories (actually, Exercise 4.4.8 shows overlap is impossible). The following proposition shows there is always a dichotomy like this in the ring $\mathbb{Z}/n$. Every element is either a unit or a zero divisor, with no overlap. Moreover, there is a simple way to to tell which elements are which.

Proposition 4.4.11. *Let n be a positive integer and let $a \in \mathbb{Z}$.*

1. *If a is relatively prime to n, then $[a]$ is a unit in $\mathbb{Z}/n$.*
2. *If a is not relatively prime to n, then $[a]$ is a zero divisor in $\mathbb{Z}/n$.*

Proof. If a is relatively prime to n, then there exists $s, t \in \mathbb{Z}$ such that $sa + tn = 1$ (Bézout), whence $sa \equiv 1 \pmod{n}$ and $[s][a] = [sa] = [1]$. This means $[a]$ is a unit. If, on the other hand, a and n are not relatively prime then $d = \gcd(a, n)$ satisfies $d > 1$. Therefore, $\frac{n}{d} < n$ which implies $[\frac{n}{d}] \neq [0]$. Furthermore, $[a][\frac{n}{d}] = [\frac{an}{d}] = [\frac{a}{d}][n] = [0]$, so $[a]$ is a zero divisor. $\square$

Exercise 4.4.12. Sort out which elements of $\mathbb{Z}/20$ are units and which are zero divisors. Give equations to check your claims (for example $[2]$ is a zero divisor because $[2][10] = [0]$).

The appearance of the Bézout equation in Part 1 of the above proposition suggests how we should go about finding the multiplicative inverse of a given unit in $\mathbb{Z}/n$. Namely, we should use the Euclidean algorithm! We demonstrate this idea in the following example.

Example 4.4.13. Since 41 is relatively prime to $n = 150$, we know that $[41]$ is a unit in $\mathbb{Z}/150$. How should we go about finding $[41]^{-1}$, the multiplicative inverse of $[41]$? The naïve approach would be to calculate $[41][b]$ for $b = 1, 2, 3, \ldots, 150$ until we find a number satisfying $[41][b] = [1]$. However, the vastly more efficient approach is to use the Euclidean algorithm to find a solution to the Bézout equation.

$$\begin{aligned} 150 &= 3 \cdot 41 + 27 && \text{(Running the Euclidean algorithm)} \\ 41 &= 27 + 14 \\ 27 &= 14 + 13 \\ 14 &= 13 + 1 \end{aligned}$$

$$\begin{aligned} 1 &= 14 - 13 && \text{(Performing back substitution)} \\ &= 14 - (27 - 14) \\ &= 2 \cdot 14 - 27 \\ &= 2 \cdot (41 - 27) - 27 \\ &= 2 \cdot 41 - 3 \cdot 27 \\ &= 2 \cdot 41 - 3(150 - 3 \cdot 41) \\ &= 11 \cdot 41 - 3 \cdot 150 \end{aligned}$$

We obtain the equation $1 = 11 \cdot 41 - 3 \cdot 150$ which shows that $11 \cdot 41 \equiv 1 \pmod{150}$. In other words, $[11][41] = [1]$, or $[41]^{-1} = [11]$.

Exercise 4.4.14. Using the result of the preceding example, find an integer x such that $41x \equiv 6 \pmod{150}$.

Exercise 4.4.15. For each given a and n find the multiplicative inverse of $[a]$ in $\mathbb{Z}/n$ or explain why this can't be done.

(a) $a = 17$, $n = 104$

(b) $a = 54$, $n = 105$

(c) $a = 118$, $n = 303$

Exercise 4.4.16. Prove or give a counterexample to each assertion below.

(a) If $2x \equiv 2y \pmod{100}$, then $x \equiv y \pmod{100}$.

(b) If $2x \equiv 2y \pmod{101}$, then $x \equiv y \pmod{101}$.

(c) If $2x \equiv 2y \pmod{100}$, then $x \equiv y \pmod{50}$.

4.5 The multiplicative group of units modulo n and the proof of Euler's theorem

Because the units of $\mathbb{Z}/n$ are closed under multiplication (Proposition 4.4.7), it makes sense to restrict the multiplication operation to the units. This leads us to the following definition.

Definition 4.5.1. Let n be a positive integer. We call the set of units in $\mathbb{Z}/n$ under multiplication the **multiplicative group of units** in $\mathbb{Z}/n$ and denote it by $(\mathbb{Z}/n)^\times$.

The reader with some background in abstract algebra will see that the $(\mathbb{Z}/n)^\times$ is an example of an abelian group.

Exercise 4.5.2. Are the units of $\mathbb{Z}/n$ closed under addition? Are the zero divisors of $\mathbb{Z}/n$ closed under addition? Are the zero divisors of $\mathbb{Z}/n$ closed under multiplication?

Example 4.5.3. Here are a couple examples of multiplicative groups of units mod n

- If $n = 12$, then $(\mathbb{Z}/12)^\times = \{[1], [5], [7], [11]\}$.
- If p is prime, then every integer is either divisible by p or relatively prime by p. Thus, every nonzero congruence class in $\mathbb{Z}/p$ is a unit and $(\mathbb{Z}/p)^\times = \{[1], [2], \ldots, [p-1]\}$.

Specializing to $p = 5$ and working out all the products in the preceding two examples results in the multiplications tables below.

$\times$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

Table 4.1: Multiplication table for $(\mathbb{Z}/12)^\times = \{[1], [5], [7], [11]\}$.

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Table 4.2: Multiplication table for $(\mathbb{Z}/5)^\times = \{[1], [2], [3], [4]\}$.

Exercise 4.5.4. Work out the multiplication table for $(\mathbb{Z}/14)^\times$, the multiplicative group of units modulo 14.

Recall (Definition 4.3.10) that $\varphi(n)$ denotes the number of integers a relatively prime to n with $1 \leq a \leq n$. According to Proposition 4.4.11, such a exactly correspond to the units in $\mathbb{Z}/n$, leading to the following proposition as a corollary. The proof is an exercise in unwinding the definitions.

Proposition 4.5.5. *Let n be a positive integer. Then, the number of elements of $(\mathbb{Z}/n)^\times$, in other words the number of units in $\mathbb{Z}/n$, is equal to the Euler totient $\varphi(n)$.*

We now return to give the proof of Theorem 4.3.15, Euler's generalization of Fermat's little theorem, repeated here for convenience:

Theorem. *Let n be a positive integer. Let a be an integer which is relatively prime to n. Then, $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

First, we point out that, if you know a bit of group theory, Euler's theorem is trivial.

Proof by group theory. By a corollary of Lagrange's theorem, if G is any finite group and $g \in G$, we have $g^{|G|} = 1$. Since $(\mathbb{Z}/n)^\times$ is a group and $\varphi(n)$ is its number of elements, we have $[a]^{\varphi(n)} = [1]$ for every $[a] \in (\mathbb{Z}/n)^\times$. □

Since we don't have time to set up the basics of group theory, we give another proof. Historically, this second proof came before the proof of Lagrange's theorem. I call the following proof a "dirty trick" because it makes essential use of the commutativity of multiplication in $(\mathbb{Z}/n)^\times$. This could potentially give the reader the impression that this property is needed when in fact it is not.

Proof by dirty trick. For brevity, define $k = \varphi(n)$ and $g = [a] \in (\mathbb{Z}/n)^\times$. There are k elements in $(\mathbb{Z}/n)^\times$ and we list them in some arbitrary way:

$$h_1, h_2, \ldots, h_k.$$

By the closure property of Proposition 4.4.7, $h \mapsto gh$ defines a function $(\mathbb{Z}/n)^\times \to (\mathbb{Z}/n)^\times$. Moreover, this function is a bijection because it has an inverse function given by $h \mapsto g^{-1}h$. Thus,

$$gh_1, gh_2, \ldots, gh_k$$

is also a list of all the elements of $(\mathbb{Z}/n)^\times$, possibly permuted in some way. Because the order of multiplication does not matter in $(\mathbb{Z}/n)^\times$, both of these lists have the same product:

$$(gh_1)(gh_2)\cdots(gh_k) = h_1h_2\cdots h_n.$$

Collecting all the occurrences of g on the left hand side and inserting the identity $[1]$ on the right hand side, we have

$$g^k \cdot (h_1h_2\cdots h_k) = [1] \cdot (h_1h_2\cdots h_k).$$

By Proposition 4.4.7, we can cancel $h_1 \cdot h_k$ from both sides of the above equation, which gives $[1] = g^k = [a]^{\varphi(n)}$. This exactly means that $a^{\varphi(n)} \equiv 1 \pmod{n}$, as was required. □

Observe that Euler's formula yields a formula of sorts for the multiplicative inverse of a unit in $\mathbb{Z}/n$.

Corollary 4.5.6. *Suppose that n is a positive integer and a is relatively prime to n. Then, $[a]^{-1}$, the multiplicative inverse of $[a]$ in $(\mathbb{Z}/n)^\times$, is equal to $[a]^{\varphi(n)-1}$.*

Proof. We have $[a][a]^{\varphi(n)-1} = [a]^{\varphi(n)} = [1]$, by Euler's theorem. □

It should be noted that the above formula for $[a]^{-1}$ is impractical from a computational standpoint. A much faster way to find the multiplicative inverse of $[a]$ is to use the Euclidean algorithm, as we illustrated in Example 4.4.13.

Next we discuss the concept of the *order* of an element of $(\mathbb{Z}/n)^\times$. Although Euler's theorem shows that every element of $(\mathbb{Z}/n)^\times$ can be raised to the power $\varphi(n)$ to get 1, it is often the case that a smaller power suffices to achieve this.

Example 4.5.7. Consider $n = 50$. Since $\varphi(50) = \varphi(2)\varphi(5^2) = (1)(5^2 - 5^1) = 20$, Euler's theorem implies that every unit in $\mathbb{Z}/50$, raised to the power 20, gives 1. The following table shows the powers of 7 and 11 modulo 50 up to the exponent $\varphi(50) = 20$.

k	$7^k \mod 50$	$11^k \mod 50$
1	7	11
2	49	21
3	43	31
4	1	41
5	7	1
6	49	11
7	43	21
8	1	31
9	7	41
10	49	1
11	43	11
12	1	21
13	7	31
14	49	41
15	43	1
16	1	11
17	7	21
18	49	31
19	43	41
20	1	1

Table 4.3: Powers of 7 and 11 modulo 50.

We can see that, while 7^{20} and 11^{20} are indeed both 1 modulo 50, smaller exponents also give 1. More specifically, we can see that $7^k \equiv 1 \pmod{50}$ whenever k is a multiple of 4 and, in fact, the sequence of powers of 7 modulo 50 is periodic with period 4. Similarly, $11^k \equiv 1 \pmod{50}$ whenever k is a multiple of 5 and the sequence of powers is periodic with period 5. Note as well that these minimal exponents 4 and 5 are divisors of $\varphi(50) = 20$.

The following proposition turns our observations from the last example into general principles.

Proposition 4.5.8. *Let n be a positive integer and let a be relatively prime to n. Then the following statements hold.*

1. *There exists a smallest positive integer k with the property that $a^k \equiv 1 \pmod{n}$.*
2. *For any nonnegative integer m, we have $a^m \equiv 1 \pmod{n}$ if and only if $k|m$.*
3. *For any nonnegative integers m_1 and m_2, we have $a^{m_1} \equiv a^{m_2} \pmod{n}$ if and only if $m_1 \equiv m_2 \pmod{k}$.*

Proof. Towards the first statement note that, as long as the set of positive integers m such that $a^m \equiv 1 \pmod{n}$ is nonempty, the well-ordering principle will guarantee the existence of a smallest element k. One way to see this set is nonempty is to note that $\varphi(n)$ belongs to the set by Euler's theorem. Let us give a different argument, however, as it illustrates a useful idea. Note that there are infinitely many positive integers, but only finitely many possible remainders modulo n. Therefore, there must exist two positive integers $m_1 < m_2$ such that $a^{m_1} \equiv a^{m_2} \pmod{n}$ (this is a sort of infinite pigeonhole principle). Then, by the cancellation property (Proposition 4.4.7), we have $a^m \equiv 1 \pmod{n}$ where $m = m_2 - m_1 > 0$.

The "if" part of the second statement is clear if we write $a^m = (a^k)^{m/k}$. For the "only if" part, suppose that m is a nonnegative integer for which $a^m \equiv 1 \pmod{n}$ and write $m = qk + r$ where $q \geq 0$ and $0 \leq r < k$. Then

$$1 \underset{n}{\equiv} a^m = a^{qk+r} = \left(a^k\right)^q a^r \underset{n}{\equiv} a^r.$$

If $r > 0$, we have contradicted the definition of k, so $r = 0$ and $k|m$ as desired.

For the third statement, assume without loss of generality that $m_1 \leq m_2$. Then, using the cancellation property and the second statement, we see

$$[a]^{m_1} = [a]^{m_2} \quad \Leftrightarrow \quad [1][a]^{m_1} = [a]^{m_2 - m_1}[a]^{m_2} \quad \Leftrightarrow \quad [1] = [a]^{m_2 - m_1} \quad \Leftrightarrow \quad k|(m_2 - m_1).$$

This exactly says that $a^{m_1} \equiv a^{m_2} \pmod{n}$ if and only if $m_1 \equiv m_2 \pmod{k}$. □

Definition 4.5.9. Given a positive integer n and a relatively prime to n, we call the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$ the **order** of a modulo n. We denote the order by $\text{ord}_n(b)$, or simply $\text{ord}(b)$ if the modulus n is understood from the context.

Example 4.5.10. From Table 4.3, we can see that $\text{ord}_{50}(7) = 4$ and $\text{ord}_{50}(11) = 5$.

Exercise 4.5.11. Calculate the orders of 2 and 3 modulo 7. Calculate the orders of 3 and 7 modulo 10.

Exercise 4.5.12. Let n be a positive integer and let a be relatively prime to n. Prove that $\text{ord}_n(a)$ divides $\varphi(n)$.

Exercise 4.5.13. Calculate the order of 2 modulo 17. *Suggestion: Since $\varphi(17) = 16$, the preceding exercise implies that $\text{ord}_{17}(2)$ must divide 16. This should cut down on the amount of computation you need to do.*

Exercise 4.5.14. Let n be a positive integer. Prove that if $[a]$ and $[b]$ are multiplicative inverses in $(\mathbb{Z}/n)^\times$, them $\text{ord}_n(a) = \text{ord}_n(b)$.

Exercise 4.5.15. Let p be prime. Prove that, if $\text{ord}_p(a) = 2$, then $a \equiv -1 \pmod{p}$.

Exercise 4.5.16. Suppose n is positive integer an a is relatively prime to n. If $\text{ord}_n(a) = \varphi(n)$ we say that a is a **primitive root** modulo n. It is known every prime number has a primitive root. Give examples of primitive roots for $p = 5, 7, 11, 13$. Find the smallest positive number n which does *not* have a primitive root.

4.6 Congruence equations and the Chinese remainder theorem

In this section we study techniques for solving individual congruence equations as well as systems of congruence equations (the Chinese remainder theorem). This section will be less rigorous than preceding sections with various details left to the reader to fill in. On your assessments, the primary expectation is that you should be able to solve congruence equations, and systems of congruence equations. There will not be much in the way of proof-based questions drawing from this section.

Definition 4.6.1. A **linear congruence equation** is an equation of the form

$$ax \equiv b \pmod{n}$$

where $a, b, n \in \mathbb{Z}$ with $n > 0$ are given, and $x \in \mathbb{Z}$ is the variable to be solved for.

One basic observation we can make about linear congruence equations is that, if they have any solutions at all, then they have infinitely many solutions; if x_0 is one solution to $ax \equiv b \pmod{n}$, then $x_0 + kn$ is also a solution for any $k \in \mathbb{Z}$. Note however that the spacing between solutions can be smaller than the modulus n. For example, $5x \equiv 0 \pmod{5}$ is true for all $x \in \mathbb{Z}$.

The following example showcases our main technique for solving congruence equations.

Example 4.6.2. Let's solve the linear congruence

$$2x \equiv 5 \pmod{29}.$$

The analogous equation in the world of nonmodular arithmetic is $2x = 5$ and we find the solution $x = 5/2$ by dividing through by 2. What should it mean to "divide by 2" when we are working modulo 29? The natural thing is to use the multiplicative inverse of $[2]$, which exists in $\mathbb{Z}/29$ because 2 is relatively prime to 29 (see Proposition 4.4.11). Observe $[2][15] = [30] = [1]$, so $[2]^{-1} = [15]$. When we multiply our congruence equation by 15, the left hand side becomes congruent to x and the right hand side becomes congruent to $15 \cdot 5 = 75 \equiv 17 \pmod{29}$ and we arrive at

$$x \equiv 17 \pmod{29}.$$

This congruence is equivalent to the original one and its solutions are simply:

$$x = 17 + 29k, \text{ where } k \in \mathbb{Z}.$$

It is important to note that multiplying a congruence equation modulo n through by a number which is a unit modulo n is a *reversible process*. To get back to the original congruence, we would just multiply by the unit's inverse. In other words, the solution set remains unchanged when we multiply by a unit. We formalize this as a lemma:

Lemma 4.6.3. *If u is a unit modulo n, then the following two congruence equations have the exact same solutions $x \in \mathbb{Z}$.*

$$ax \equiv b \pmod{n} \qquad\qquad uax \equiv ub \pmod{n}$$

Proof. Exercise for the reader. □

Let's look at a different kind of example:

Example 4.6.4. We want to solve the linear congruence

$$4x \equiv 8 \pmod{36}.$$

This time, 4 is not a unit modulo 36, i.e. $[4]_{36}^{-1}$ does not exist. We cannot "divide by 4" to solve for x, at least not if we are only working modulo 36. On the other hand, let's unpack what this congruence equation means:

$$4x = 8 + 36k, \text{ for some } k \in \mathbb{Z}.$$

All the numbers appearing in the above equation are divisible by 4. Dividing through by 4, we see this is equivalent to:

$$x = 2 + 9k, \text{ for some } k \in \mathbb{Z}.$$

That is our solution set! The solutions to the original congruence are all $x = 2 + 9k$, $k \in \mathbb{Z}$.

It is important to note that the step used in the example above (dividing the whole congruence equation including the modulus by some number) is also a reversible process. To get back to the original congruence, we just multiply by the same number. We formalize this as a lemma as well.

Lemma 4.6.5. *Suppose that d is a positive integer and a, b, n are all divisible by d. Then, the following congruence equations have the exact same solutions $x \in \mathbb{Z}$.*

$$ax \equiv b \pmod{n} \qquad\qquad \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$$

Proof. Exercise for the reader. □

Some congruence equations require us to use the two preceding lemmas in tandem to be solved. This is demonstrated in the following example.

Example 4.6.6. We want to solve the congruence equation:

$$36x \equiv 12 \pmod{60}.$$

Dividing both sides as well as the modulus by 12 gives:

$$3x \equiv 1 \pmod{5}.$$

According to Lemma 4.6.5, this congruence has the same solutions as the original one. Next, note $[2]_5[3]_5 = [6]_5 = [1]_5$, i.e. 2 is a multiplicative inverse modulo 5. We "divide by 3" modulo 5 by multiplying by 2. The resulting congruence is:

$$x \equiv 2 \pmod{5}.$$

According to Lemma 4.6.3, this congruence has the same solutions as the preceding one. The solutions to this congruence, and therefore to the original one as well, are:

$$x = 2 + 5k, \text{ where } k \in \mathbb{Z}.$$

Finally, let's look at an example of a congruence equation that does not have *any* solutions:

Example 4.6.7. Consider the congruence equation $2x \equiv 1 \pmod{4}$. This means $2x = 1+4k$ for some $k \in \mathbb{Z}$. However, this is impossible; the left hand side is even and the right hand side is odd.

The following theorem exactly captures the obstruction to solving a linear congruence equation.

Theorem 4.6.8. *Suppose $a, b, n \in \mathbb{Z}$ with n positive. Let $d = \gcd(a, n)$. Then, the congruence equation*

$$ax \equiv b \pmod{n}.$$

has a solution if and only if d divides b.

Proof. Suppose $x_0 \in \mathbb{Z}$ is a solution. Thus $ax_0 = b + kn$ for some $k \in \mathbb{Z}$. But then, b can be expressed as an integral linear combination of a and n, so any number dividing both a and n must divide b as well. In particular, $d|b$.

Conversely, suppose that $d|b$. Then, using Lemma 4.6.5, the original congruence has the same solutions as

$$a'x \equiv b' \pmod{n'},$$

where $a' = a/d$, $b' = b/d$ and $n' = n/d$. However, in this new congruence, a' and n' are relatively prime, so a' has a multiplicative inverse modulo n', and we can solve this new congruence by the method of Lemma 4.6.3. □

Exercise 4.6.9. Find the general solution to each of the following congruence equations, or explain why no solutions exist.

(a) $5x \equiv 3 \pmod{11}$

(b) $12x \equiv 16 \pmod{92}$

(c) $35x \equiv 63 \pmod{203}$

(d) $30x \equiv 5 \pmod{40}$

(e) $54x \equiv 81 \pmod{105}$

Exercise 4.6.10. Prove that, if $\gcd(a, n) = d$ and d divides b, then the number of solutions x to the congruence equation $ax \equiv b \pmod{n}$ which satisfy $0 \leq x < n$ is d.

Exercise 4.6.11. How many integers x with $0 \leq x < 70$ satisfy $49x \equiv 21 \pmod{70}$? Find them.

Exercise 4.6.12. A *linear diophantine equation* is an equation $ax + by = c$ where a, b, c are given integers and x, y are integers to be solved for. Assume $a, b \neq 0$. Explain why solving the linear diophantine equation $ax + by = c$ is equivalent to solving the congruence equation $ax \equiv c \pmod{b}$ and also equivalent to solving the congruence equation $by \equiv c \pmod{a}$.

Exercise 4.6.13. Find the general solution to the diophantine equation $24x + 36y = 500$. How many solutions are there with $x, y > 0$?

Now we move on to the more general problem of solving systems of linear congruences.

Example 4.6.14. For motivation, consider the following translated quotation taken from the *Sun-tzu Suan-ching* written in 3rd century China. Unfortunately, little seems to be known about the precise identity of this work's author.

> "There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?"

If we let x be the unknown number of things, then we can rephrase the above problem as looking for a number x which simultaneously solves the following system of congruences.

$$x \equiv 2 \pmod{3} \tag{4.1}$$
$$x \equiv 3 \pmod{5} \tag{4.2}$$
$$x \equiv 2 \pmod{7} \tag{4.3}$$

We use this example to illustrate a general approach for solving such systems.

- **Step 1:** The general solution to (4.1) alone is $x = 2 + 3r$, where $r \in \mathbb{Z}$.

- **Step 2:** Substitute the general solution to (4.1) into (4.2) to find the general solution to the pair of equations (4.1) and (4.2). We obtain

$$2 + 3r \equiv 3 \pmod 5$$

which is equivalent to

$$3r \equiv 1 \pmod 5.$$

Multiplying through by 2, which is a multiplicative inverse for 3 modulo 5, we obtain the equivalent congruence equation

$$r \equiv 2 \pmod 5$$

which means

$$r = 2 + 5s, \text{ for some } s \in \mathbb{Z}.$$

Substituting this into our expression for x, we get that

$$x = 2 + 3r = 2 + 3(2 + 5s) = 8 + 15s.$$

The general solution to (4.1) and (4.2) is $x = 8 + 15s$ where $s \in \mathbb{Z}$.

- **Step 3:** Substitute the general solution to (4.1) and (4.2) from Step 2 into (4.3) to find the general solution to the whole system. We obtain

$$8 + 15s \equiv 2 \pmod 7$$

which is equivalent to

$$15s \equiv s \equiv -6 \equiv 1 \pmod 7.$$

This means exactly that

$$s = 1 + 7t, \text{ for some } t \in \mathbb{Z}.$$

Substituting back into our equation for x gives

$$x = 8 + 15s = 8 + 15(1 + 7t) = 23 + 105t.$$

The general solution to the whole system of congruences is $x = 23 + 105t$, $t \in \mathbb{Z}$.

Indeed 23 has remainder 2 modulo 3, remainder 3 modulo 5, and remainder 2 modulo 7. Adding multiples of 105 to 23 does not affect the validity of any of our congruences because $105 = 3 \cdot 5 \cdot 7$ is divisible by all three of $3, 5, 7$.

We first state the Chinese remainder theorem for systems of two congruences and then extend to the general case using induction. The attentive reader will see that the induction step more or less emulates the procedure followed in the example above.

Theorem 4.6.15 (Chinese remainder theorem, case of two equations)**.** *Suppose n_1, n_2 are relatively prime positive integers and $b_1, b_2 \in \mathbb{Z}$. Then, there exists a simultaneous solution $x_0 \in \mathbb{Z}$ to the following system of congruence equations:*

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2}. \end{aligned}$$

Moreover, the general solution to the system is $x = x_0 + sm$, $s \in \mathbb{Z}$, where $m = n_1 n_2$.

Proof. Note that the general solution to the first congruence is $x = b_1 + rn_1$ where $r \in \mathbb{Z}$. Such an x is a solution to the second congruence too if and only if $b_1 + rn_1 \equiv b_2 \pmod{n_2}$, which we rearrange to $n_1 r \equiv b_2 - b_2 \pmod{n_2}$. Because n_1 is relatively prime to n_2, this last congruence is equivalent to one of the form $r \equiv r_0 \pmod{n_2}$, where r_0 is $b_2 - b_2$ times a multiplicative inverse for n_1 modulo n_2 and its general solution is $r = r_0 + sn_2$. Then, the general solution to the whole system of congruences is $x = b_1 + (r_0 + sn_2)n_1 = x_0 + sm$, where $x_0 = b_1 + r_0 n_1$ and $m = n_1 n_2$. □

Now we extend to an arbitrary number of equations. At its heart, the strategy for solving more than two equations is simply to solve two at a time.

Theorem 4.6.16 (Chinese remainder theorem, general case)**.** *Suppose that $n_1, \ldots, n_k$ are pairwise relatively prime positive integers and $b_1, \ldots, b_k \in \mathbb{Z}$. Then, there exists a simultaneous solution $x_0 \in \mathbb{Z}$ to the following system of congruence equations:*

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_k \pmod{n_k}. \end{aligned}$$

Moreover, the general solution to this system is $x = x_0 + sm$, $s \in \mathbb{Z}$, where $m = n_1 \cdots n_k$.

Proof. The case $k = 1$ is trivial. The case $k = 2$ holds by Theorem 4.6.15 above. Assume for induction that $k \geq 3$ and that the theorem holds when there are only $k - 1$ congruences. Then, there exists a simultaneous solution y_0 to the first $k-1$ congruence equations and the general solution to the first $k - 1$ congruences is $x = y_0 + rn_1 \cdots n_{k-1}$, $r \in \mathbb{Z}$. Restated, the solutions to the first $k-1$ congruences are the same as the solutions to the single congruence:

$$x \equiv y_0 \pmod{n_1 \cdots n_{k-1}}.$$

Thus, the full system has the same solutions as the following system of only two congruences:

$$\begin{aligned} x &\equiv y_0 \pmod{n_1 \cdots n_{k-1}} \\ x &\equiv b_k \pmod{n_k}. \end{aligned}$$

Since $n_1 \cdots n_{k-1}$ is relatively prime to n_k, Theorem 4.6.15 shows that this system of two congruences has a solution $x_0 \in \mathbb{Z}$ and its general solution is $x = x_0 + sn_1 \cdots n_k$, $s \in \mathbb{Z}$. By the principle of induction, we are finished. □

Exercise 4.6.17. Find the general solution to the following system of congruence equations:

$$\begin{aligned} x &\equiv 7 \pmod{9} \\ x &\equiv 5 \pmod{10} \\ x &\equiv 2 \pmod{11} \end{aligned}$$

Exercise 4.6.18. Find the general solution to the following system of congruence equations:

$$\begin{aligned} x &\equiv 6 \pmod{9} \\ x &\equiv 3 \pmod{11} \\ 3x &\equiv 4 \pmod{13} \end{aligned}$$

Exercise 4.6.19. Find the general solution to the following system of congruence equations:

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 2 \pmod{4} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

Exercise 4.6.20. Find the general solution to the following system of congruence equations:

$$\begin{aligned} x &\equiv 9 \pmod{12} \\ x &\equiv 3 \pmod{13} \\ x &\equiv 6 \pmod{25} \end{aligned}$$

Exercise 4.6.21. Let $n_1, n_2, \ldots, n_k$ be relatively prime positive integers. Note that n_1 is relatively prime to $n_2 \cdots n_k$, so there exist $s_1, t_1 \in \mathbb{Z}$ such that

$$s_1 n_1 + t_1 n_2 \cdots n_k = 1$$

Define $e_1 = t_1 n_2 \cdots n_k$.

(a) Prove that $e_1 \equiv 1 \pmod{n_1}$ and $e_1 \equiv 0 \pmod{n_i}$ for $i = 2, \ldots, k$.

(b) Continuing in this way, construct integers $e_1, \ldots, e_k$ such that $e_i \equiv 1 \pmod{n_i}$ and $e_i \equiv 0 \pmod{n_j}$ when $i \neq j$.

(c) Use the $e_1, \ldots, e_k$ from part (b) to give an alternative proof that, for any $b_1, \ldots, b_k \in \mathbb{Z}$, there exists an $x_0 \in \mathbb{Z}$ simultaneously solving the congruences:

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_k \pmod{n_k} \end{aligned}$$

Hint: build x_0 out of $e_1, \ldots, e_k$.