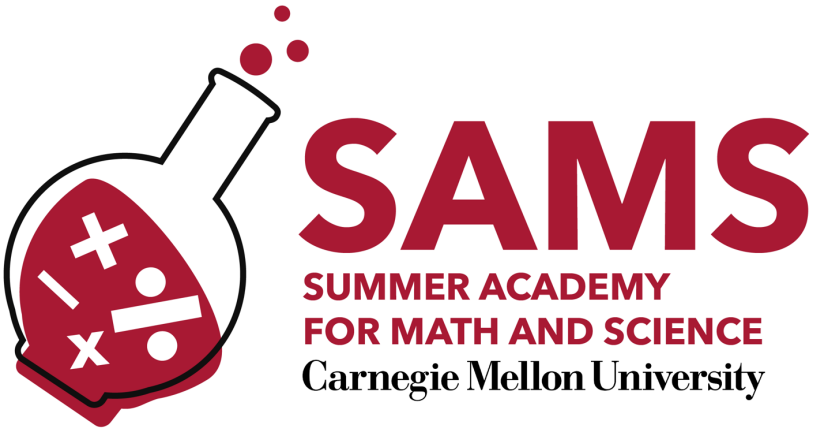
Number Theory
SAMS 2024 Workbook



Elisa Bellah

Contents

Preface

Broadly speaking, number theory studies the additive and multiplicative properties of the integers. It is one of the oldest areas of mathematics, and has many applications, especially in computer science. In this introductory course, we'll explore some of the fundamental topics of number theory. Topics will include:

- Divisibility and linear Diophantine equations, which will help us explore how addition and multiplication interact;
- Prime numbers and the fundamental theorem of arithmetic, where we'll explore the multiplicative "building blocks" of the integers;
- Modular arithmetic, where we'll see how the division algorithm can "fold up" the number line;

This course is appropriate for high school students at all levels, and is written with two goals: (1) for students to gain a conceptual understanding of some of the core topics from elementary number theory, and (2) to give students exposure to writing and reading mathematical proofs.

How to Use This Workbook

Mathematics is best learned by *doing*. Even the most talented musicians and athletes cannot play a piece of music or perform an athletic skill by just watching someone else do it – learning any skill requires *practice*. This workbook is designed to keep you active throughout the learning process, so that you can leave the course with a skillful understanding of the course material. Note that this workbook is yours to keep – feel free to write in it as you wish, and note that there are several pages for notes and scratch work in the back.

To best learn from this workbook, students should:

(1) Read through the exposition in each section, and complete the embedded Reading Exercises;
(2) Take time to *really understand* what the definitions and propositions are saying, don't just skim over them;
(3) Complete all or most of the Core Problems at the end of each chapter;
(4) Choose a few of the Additional Challenge Problems at the end of each chapter to dive into.

Course Logistics and Expectations

In general, we will meet Monday, Wednesday, and Friday 10:30am-12pm in Wean Hall (WEH) 4623. During our meeting times, I will answer questions and give a short exposition to motivate the day's material. For the rest of class, you will be working in small groups to progress through this workbook. I will be cycling through the room to answer your questions and to see how you're doing with material, and we will periodically stop as a class to discuss your progress.

Each week, you will also be given a short assignment, which will include some goal setting, personal reflection, and space to submit a completed problem that you are proud of. I will take attendance each day, and expect you to arrive in class on time and to work kindly and collaboratively with your group mates.

List of Notation

The following list of notation will appear throughout the text.

$\mathbb{Z}$	the set of integers
$\in$	is an element of
$a \mid b$	a divides b
$a \nmid b$	a does not divide b
$\gcd(a, b)$	greatest common divisor of a and b
$a \equiv b (\mathrm{mod}\, n)$	a is congruent to b modulo n

Chapter 1

Divisibility

1.1. The Set of Integers

In this course, we'll mainly be concerned with the INTEGERS. Recall that an integer is any whole number, zero, or any negative whole number. If we were to list the collection of integers, this would look like

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

Reading Exercise 1.1. *Write down five integers which are not listed above. Then, write down five numbers which are not integers.*

In math, it's often convenient to study a collection of objects by considering them as elements of a *set*.

Definition 1.1. A SET is any collection of objects. The objects a set contains are called its ELEMENTS. If a is an element of a set S, we write "$a \in S$".

Reading Exercise 1.2. *Consider the following set*

$$S = \{2, 3, \circ, -\pi, \triangle\}$$

List all of the elements of the set S. Give three examples of elements that are not contained in the set S.

Notation 1.2. The set of integers is denoted by $\mathbb{Z}$. That is,

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

Note that, since $\mathbb{Z}$ contains infinitely many elements, we cannot list them all like we did in Exercise 1.2. However, our use of ellipses in the notation above indicates to our reader that we'd continue on listing elements in the fashion we started.

Reading Exercise 1.3. *Using notation similar to above, write the set of all even integers.*

1.2. The Formal Definition of Divisibility

Reading Exercise 1.4. *Before you read on, think about the following questions. Don't worry about being right or wrong here, just explore these questions using your own intuitive understanding.*

(1) Does 3 divide 14? Explain why or why not.

(2) Does 3 divide 15? Explain why or why not.

(3) In general, how can you tell whether an integer is divisible by 3?

(4) Is 10 even or odd? Explain how you know this.

(5) In general, how you can you tell whether an integer is even or odd?

The following definitions are meant to give a method to precisely and formally answer the questions from Exercise 1.4.

Definition 1.3. Suppose that a and b are integers. We say that a DIVIDES b, or that b is DIVISIBLE BY a, if there exists an integer k so that $b = ak$. In this case, we write $a \mid b$. If a does not divde b, we write $a \nmid b$.

Reading Exercise 1.5. *Using the definition above, explain how we know that 3 divides 15.*

Definition 1.4. An integer a is EVEN if $2 \mid a$. Recall, this means there exists an integer k so that $a = 2k$.

One way to define odd integers is those integers that **are not** divisible by 2. However, it's generally a bit more tricky to show that a given integer **does not** divide another. We give a more convenient definition instead.

Definition 1.5. An integer b is ODD if there exists an integer k so that $b = 2k + 1$.

Reading Exercise 1.6. *Using the definitions above, explain why each integer listed below is either even or odd*

$$-17,\ 102,\ 0$$

We can understand Definition 1.5 intuitively: integers of the form $2k + 1$ are just one "after" an even integer, and so they should be the integers "in between" the evens. But we should always be cautious about intuition. Let's see if we can dig a bit deeper and understanding why this is in fact the definition we want for odd integers. Let's prove the following proposition.

Proposition 1.6. If an integer b is odd (as defined in Definition 1.5) then b is not even (as defined in Definition 1.4). Furthermore, if b is not even then it is odd.

Note that a "proposition" is a mathematical statement which is either true or false, and a "proof" is a mathematical argument which justifies why this statement is true. Read through the proof below, and fill in the missing steps as you follow along. Our goal is construct an irrefutable argument, using logic and sound mathematical reasoning, that proves the proposition above is always true.

Proof. Suppose first that b is an odd integer, as given in Definition 1.5. Then, there exists an integer k so that $b = 2k + 1$.

Reading Exercise 1.7. *Show that if b were divisible by 2, then $1/2$ would need to be an integer.*

So, it must be the case that b is not divisible by 2 (*does the logic of this make sense to you?*). Thus b is not even, as needed.

Next, suppose that b is not even.

Reading Exercise 1.8. *In your own words (or by using a few examples), explain why for any integer b we can write $b = 2q + r$ where $r = 0$ or 1 and q is an integer (think of quotients and remainders).*

But if $r = 0$ then we would have $b = 2q$ is even. Hence, we must have $r = 1$ and so $b = 2k + 1$ for an integer $k = q$, as needed. □

In Exercise 1.8 we used a special case of the following key theorem. *Note that "theorem" is just another for "proposition", and is usually used to indicate the importance of a proposition.*

Theorem 1.7 (The Division Algorithm.)**.** *Suppose that a and b are integers, and that $a > 0$. Then, there exists unique integers q and r so that*

$$b = qa + r$$

and $0 \leq r < a$. We call q the quotient and r the remainder when dividing b by a.

We won't give a proof of this fact, but hopefully the concept is familiar (observe that this is basically long division!).

Reading Exercise 1.9. *For the following pairs of integers, find the quotient and remainder when dividing b by a.*

(1) $b = 7$, $a = 2$

(2) $b = 23$, $a = -4$

(3) $b = 6$, $a = 8$

Reading Exercise 1.10. *Use the division algorithm to explain how we know that 3 does not divide 14.*

1.3. Greatest and Least Common Divisors

So far, we've related two integers by asking whether or not they divide each other. Sometimes it's the case that even though two integers don't divide each other, they still have some related divisors. We have the following definition.

Definition 1.8. Let a and b be integers. We say that an integer d is a COMMON DIVISOR of a and b if $d \mid a$ and $d \mid b$.

Reading Exercise 1.11. *Find all common divisors of the integers 15 and 10. Then, find all common divisors of the integers 15 and 14.*

Observe that ± 1 are common divisors of every pair of integers.

Definition 1.9. The GREATEST COMMON DIVISOR of integers a and b is the largest integer d so that d is a common divisor of a and b. In this case, we use the notation $d = \gcd(a, b)$.

Reading Exercise 1.12. *Find* $\gcd(15, 10)$ *and* $\gcd(15, 14)$.

Definition 1.10. If $\gcd(a, b) = 1$ we say that a and b are relatively prime.

So far, the only method we have to find the greatest common divisors of two integers is guess and check. That is, to find $\gcd(a, b)$, we generally need to list *all* divisors of a and *all* divisors of b and then search for the largest common integer in our list. This can get tedious quite quickly. For example, what if we wanted to find

$$gcd(109839, 2023)?$$

The following result will give us a much faster method.

Theorem 1.11. *Let a and b be integers with $a > 0$. Using the Division Algorithm, write*

$$b = aq + r$$

for $0 \leq r < a$. Then $\gcd(b, a) = \gcd(a, r)$.

Let's first understand *why* this theorem is true. Then, we'll look at how to apply it to our problem if finding gcds.

Proof. Let $d = \gcd(b, a)$. Then we have $d \mid b$ and $d \mid a$ so there exist integers k, ℓ so that

$$b = dk \text{ and } a = d\ell.$$

Now let's use the division algorithm to divide b by a. Recall that we can write

$$b = aq + r$$

for integers r and q with $0 \leq r < a$.

Reading Exercise 1.13. *Use the equalities above to show that* $r = d(k - \ell q)$.

So $d \mid r$. This tells us that d is a common divisor of a and r. To prove our claim, we need to show that d is the *greatest* common divisor of a and r. To do this, suppose that d' is any common divisor of a and r. Then there exist integers m, n so that

$$a = d'm \text{ and } r = d'n.$$

Recall that we have $b = aq + r$.

Reading Exercise 1.14. *Use the equalities above to show that* $b = d'(mq + n)$.

Hence, d' is a common divisor of both a and b. But recall that we assumed d was the greatest common divisor of a and b, and so we must have $d' \leq d$. Hence, d is larger than all other common divisors of a and r, and so $d = \gcd(a, r)$ as needed. □

Theorem 1.11 gives a way to reduce our gcd calculation. The method outlined in the following exercise is called the EUCLIDEN ALGORITHM. Carefully read through this example, and then use it to guide you through the subsequent reading exercise.

Example 1.12 (The Euclidean Algorithm)**.** Let's find

$$\gcd(128, 34).$$

First, we use the division algorithm to divide 34 into 128. We get

$$128 = 34(3) + 26.$$

So, by Theorem 1.11 we have

$$\gcd(128, 34) = \gcd(34, 26).$$

So now our problem is a bit simpler! We could go about our business as before (find all divisors of 34, all divisors of 26, and then compare) but there's no reason to stop here. We can use the division algorithm again to write

$$34 = 26(1) + 8$$

and so by Theorem 1.11 we have

$$\gcd(34, 26) = \gcd(26, 8).$$

Once again, we use the division algorithm to write

$$26 = 8(3) + 2$$

and by Theorem 1.11 we get

$$\gcd(26, 8) = \gcd(8, 2).$$

We could stop here since we know that $2 \mid 8$, but for the sake of generalizing this, we could use the division algorithm again to write

$$8 = 2(4) + 0.$$

So, by Theorem 1.11 we get

$$\gcd(8, 2) = \gcd(2, 0) = 2.$$

Since equality is transitive, this gives us $\boxed{\gcd(128, 34) = 2}$.

Reading Exercise 1.15. *Use the Euclidean Algorithm to find* $\gcd(150, 14)$.

The Euclidean Algorithm actually gives us something more. We'll show the following.

Proposition 1.13. There exist integers x and y so that

$$128x + 34y = 2. \tag{1.1}$$

Equation (1.1) is an example of a *linear Diophantine equation.*

Definition 1.14. A LINEAR DIOPHANTINE EQUATION is an equation of the form

$$ax + by = c,$$

for integers a, b and c.

Proof of Proposition 1.13. Let's rewrite the steps of the Euclidean Algorithm a bit more succinctly.

$$\begin{aligned} &\gcd(128, 34) && 128 = 34(3) + 26 \\ &\quad = \gcd(34, 26) && 34 = 26(1) + 8 \\ &\quad = \gcd(26, 8) && 26 = 8(3) + 2 \\ &\quad = \gcd(8, 2) = 2 && 8 = 2(2) + 0 \end{aligned}$$

Here's the clever observation: on the second to last step, our equation with the division algorithm is a linear equation involving the gcd. Let's exploit this fact. We have

$$26(1) + 8(-3) = 2$$

This gives a solution $x = 1, y = -3$ to the linear Diophantine equation

$$26x + 8y = 2.$$

The right-hand side of this looks good, but the coefficients on the left-hand side aren't quite what we want. But all isn't lost! Using the third to last line in our division algorithm step, we can write

$$8 = 34(1) + 26(-1).$$

Let's use this new version of 8 to get

$$\begin{aligned} &26(1) + 8(-3) = 2 \\ \Rightarrow\ &26(1) + (34(1) + 26(-1))(-3) = 2 \end{aligned}$$

which can be rewritten as

$$26(4) + 34(-3) = 2.$$

This gives the solution $x = 4, y = -3$ to the linear Diophantine equation

$$26x + 34y = 2.$$

This is a bit closer! The right-hand side still looks good, and on the left hand side at least one of our coefficients (34) is correct. What do we do with the pesky coefficient of 26? Well we had one more line in the Euclidean algorithm to exploit. Using the first line in our division algorithm step, we can write

$$26 = 128(1) + 34(-3).$$

Let's use this new version of 26 to get

$$26(4) + 34(-3) = 2$$
$$\Rightarrow (128(1) + 34(-3))(4) + 34(-3) = 2$$

which we can rewrite as

$$128(4) + 34(-15) = 2.$$

And we've won! We now have the solution $x = 4, y = -15$ to the Diophantine equation $128x + 34y = 2$.

□

Reading Exercise 1.16. *Using the method outlined in the previous proof, along with your work in Exercise 1.15, find a solution to the linear Diophantine equation*

$$150x + 14y = 2.$$

It turns out that this method generalizes. On the Core Exercises of this chapter, I hope you convince yourself of the following.

Theorem 1.15 (Extended Euclidean Algorithm)**.** *Let a, b be integers. Then, there exists an integer solution x, y to the Diophantine equation*

$$ax + by = d$$

if and only if $\gcd(a, b)$ *divides* d.

Core Problems

P1. Use the formal definition of divisibility (Definition 1.3) to show the following

$$3 \mid 99,\ 13 \mid 1001,\ -5 \mid 500,\ \text{ and }\ 22 \mid -1716.$$

P2. Find all integers (positive **and negative**) that divide 66.

P3. Explain how we know that $10 \nmid 5$.

P4. Suppose that for integers a and b we have $a > b$. Is it possible for $a \mid b$? Why or why not?

P5. Let's explore some properties of integers divisible by 6.
   (a) List five examples of integers divisible by 6. Use the notation $6 \mid a$ given in Definition 1.3 in each of your examples.
   (b) Look at your list of examples from above. Is there another integer which divides each of your examples besides 6?
   (c) Formulate a *conjecture* (that is, something you believe to be true) of the form: " if a is an integer divisible by 6, then a is divisible by (blank)".
   (d) Convince the members of your group that your conjecture from the previous part is true. Try using the formal definition of divisibility in your justification.

P6. Next, let a and b be any integers with $a \mid b$. Do you think the following statement is true: if d divides a then d divides b? Why or why not? Can you convince your group members of your answer?

P7. What integers divide 1? What integers divide 0? Justify your answers.

P8. Suppose that a and b are integers with $a \mid b$ and $b \mid a$. Is it always going to be the case that $a = b$? Why or why not?

P9. Let a, b, and c be integers. Use the formal definition of divisibility to justify each of the following properties.
   (a) If $a \mid b$ and $a \mid c$ then $a \mid (b + c)$
   (b) If $a \mid b$ and $a \mid c$ then $a \mid (b - c)$

P10. For the following pairs of integers, use the division algorithm to find the unique quotient and remainder when dividing b by a.
   (a) $b = 277$, $a = 4$
   (b) $b = 33$, $a = 11$
   (c) $b = -48$, $a = 13$

P11. Recall that we saw that if an integer b is **not** even, then we can write it in the form $b = 2k + 1$ for some integer k, which justified our formal definition of odd integers.
   (a) Choose five odd integers, and write them in the form $2k + 1$ for an integer k.
   (b) Write the integers from the previous part in the form $2\ell - 1$ for some integer ℓ.
   (c) Do you think that all odd integers can be written in the form $2\ell - 1$ for some integer ℓ? Why or why not?

P12. Use the formal definition of even and odd integers to explain why each of the following statements are always true.
(a) The sum of any two even numbers is even.
(b) The sum of any two odd numbers is odd.
(c) The sum of an even and an odd number is odd.

P13. Determine which of the following statements are true or false. A statement is true if it holds for **any choice** of integers. A statement is false if there is **at least one choice** of integers where the statement doesn't hold true.
(a) True or False? For all integers a, b and c, if $a \mid (b + c)$ then $a \mid b$ or $a \mid c$.
(b) True or False? For integers a, b and c, if $a \mid bc$ then $a \mid b$ or $a \mid c$.
(c) True or False? The sum of the squares of any two odd integers is even.

P14. Find the following greatest common divisors. Which pairs are relatively prime?
(a) $\gcd(18, 12)$
(b) $\gcd(66, 22)$
(c) $\gcd(0, 21)$
(d) $\gcd(0, a)$ for any positive integer a
(e) $\gcd(0, -a)$ for any positive integer a
(f) $\gcd(0, 0)$
(g) $\gcd(1, 14598)$
(h) $\gcd(-1, 14598)$
(i) $\gcd(1, a)$ for any integer a
(j) $\gcd(-1, a)$ for any integer a

P15. Suppose that a and d are positive integers with $d \mid a$. What is $\gcd(a, d)$?

P16. Redo the example from lecture where we showed $\gcd(128, 34) = 2$ with the Euclidean Algorithm. Talk to your group about this process. Do you believe the algorithm will always work? How do we know it must always terminate?

P17. Use the Euclidean Algorithm to find the following greatest common divisors.
(a) $\gcd(112, 92)$
(b) $\gcd(31, 162)$
(c) $\gcd(12, 256)$
(d) $\gcd(243, 9)$

P18. Redo the example from lecture where we reversed the Euclidean algorithm to find an integer solution to the linear Diophantine equation

$$128x + 34y = 2.$$

Make sure you understand every step before moving on!

P19. Use your work in P4 to find any one integer solution to the following linear Diophantine equations. If no solutions exist, state why not.
(a) $112x + 92y = 4$
(b) $112x + 92y = -12$
(c) $112x + 92y = 3$
(d) $31x + 162y = 1$
(e) $31x + 162y = -27$

P20. Suppose that a and b are relatively prime. Show that every linear Diophantine equation

$$ax + by = c$$

has a solution.

P21. Suppose that $\gcd(a, b) > 1$. For what values of c does the linear Diophantine equation

$$ax + by = c$$

have a solution? How do you know this?

P22. For integers a and b, what do you think would be a good definition for the LEAST COMMON MULTIPLE of a and b? Construct and compute a few examples.

Challenge Problems

C1. Show that the product of any three consecutive integers is divisible by 6.

C2. How many integers between 100 and 1000 are divisible by 7?

C3. How many integers between 100 and 1000 are divisible by 49?

C4. Find the number of positive integers less than 1000 that are not divisible by 2 or 5.

C5. Find the number of positive integers less than 1000 that are not divisible by 2, 5 or 7.

C6. The FIBONACCI SEQUENCE is the integer linear recurrence sequence given by

$$f_0 = 0, f_1 = 1$$

$$f_{n+2} = f_{n+1} + f_n.$$

Some terms of the Fibonacci sequence are listed below

n	0	1	2	3	4	5	6
f_n	0	1	1	2	3	5	8

(a) Show that f_n is even if and only if n is divisible by 3.
(b) Show that f_n is divisible by 3 if and only if n is divisible by 4.
(c) Show that f_n is divisible by 6 if and only if n is divisible by 6.

C7. Let a, b and c be integers. If $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$.

C8. Let a, b and n be integers. If $a \mid n$, $b \mid n$ and $\gcd(a, b) = 1$ then $ab \mid n$.

C9. Let a, b, and n be integers. If $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$ then $\gcd(ab, n) = 1$.

C10. If a and b are positive integers, show that

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab.$$

C11. If a and b are positive integers, show that

$$\operatorname{lcm}(a, b) = ab$$

if and only if a and b are relatively prime.

Chapter 2

Prime Numbers

2.1. The Fundamental Theorem of Arithmetic

Last chapter, we started exploring some of the divisibility properties of the integers. In this chapter, we'll see that there are special integers, called *prime numbers*, which turn out to be the "building blocks" of the integers. We have the following definition.

Definition 2.1. An integer $p > 1$ is PRIME if the only positive divisors of p are 1 and p. An integer that is not prime is called COMPOSITE.

Reading Exercise 2.1. *Find the first ten prime numbers.*

The following theorem tells us that every integer can be understood by the prime numbers dividing it.

Theorem 2.2 (The Fundamental Theorem of Arithmetic)**.** *Let n be a positive integer. Then, there exist unique prime numbers $p_1, p_2, \ldots, p_t$ and positive integers $k_1, \ldots, k_t$ so that*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t} \tag{2.1}$$

where the primes p_i are distinct and ordered so that $p_1 < p_2 < \cdots < p_t$. We call Equation (2.1) THE PRIME FACTORIZATION OF *n.*

This result can be a bit much to look at in its full generality. Let's look at a few examples to make sense of what's going on here.

Example 2.3. We have the following prime factorizations

(1) $42 = 2 \cdot 3 \cdot 7$
(2) $108 = 2^2 \cdot 3^3$
(3) $1485 = 3^3 \cdot 5 \cdot 11$
(4) $7663 = 79 \cdot 97$

Remark 2.4. To prove the Fundamental Theorem of Arithmetic, we'd need a proof method called *mathematical induction*. Since our time together is limited and this proof method is one of the trickier ones to grasp, we'll omit this proof, and use our intuition to understand why this is always possible through example.

Reading Exercise 2.2. *Find the prime factorization of* 1020.

We have the following useful result.

Proposition 2.5. Let p be prime and a, b be any nonzero integers. If $p \mid ab$ then $p \mid a$ or $p \mid b$.

Proof. There's a clever argument for this fact using the Euclidean Algorithm. Suppose that $p \mid ab$. If $p \mid a$ then we're done, so suppose that $p \nmid a$.

Reading Exercise 2.3. *Show that* $\gcd(a, p) = 1$.

So, by the Extended Euclidean Algorithm (Theorem 1.15) we know that there exists integers x, y so that

$$ax + py = 1.$$

Multiplying on both sides by b gives

$$abx + pby = b,$$

and since $p \mid ab$ we know there exists an integer z so that $pz = ab$.

Reading Exercise 2.4. *Use the equations above to show that* $p(zx + by) = b$. *Conclude that* p *divides* b.

Hence, we've shown that $p \mid a$ or $p \mid b$, as needed. □

Reading Exercise 2.5. *Observe that Proposition 2.5 may or may not work for composite integers. Give an example of a* ***composite*** *integer* n *and integers* $a, b \neq 1$ *so that:*

(1) $n \mid ab$ *but* $n \nmid a$ *or* $n \nmid b$

(2) $n \mid ab$ *and* $n \mid a$ *or* $n \mid b$

2.2. Applications of the Fundamental Theorem

The fundamental theorem is named for a good reason. If you want to study the divisibility properties of the integers, this theorem is often going to be useful.

Proposition 2.6. Suppose that a positive integer n has prime factorization

$$n = p_1^{k_1} \cdots p_t^{k_t}.$$

Then, the divisors of n are given by $n = p_1^{\ell_1} p_2^{\ell_2} \cdots p_t^{\ell_t}$ where $0 \leq \ell_i \leq k_i$ for all $i = 1, \ldots, t$.

Before we dive into the proof of this proposition, let's look at some examples to make sure we understand what's going on.

Example 2.7. Consider the integer $n = 12$, which has prime factorization $12 = 2^2 \cdot 3$. By Proposition 2.6 n has the following positive divisors:

$$\begin{aligned} 1 &= 2^0 3^0 \\ 2 &= 2^1 3^0 \\ 4 &= 2^2 3^0 \\ 3 &= 2^0 3^1 \\ 6 &= 2^1 3^1 \\ 12 &= 2^2 3^1 \end{aligned}$$

Reading Exercise 2.6. *Use Proposition 2.6 to find all positive divisors of $n = 18$. Try to decide on a method to organize your list so that you can be sure you've listed every divisor!*

Now, let's look at the proof of Proposition 2.6. Take your time with this one, and be sure to ask questions if you get stuck.

Proof. Let d be a divisor of n. First, note that if p is a prime dividing d then by P6 of the Chapter 1 Core Problems, we know that $p \mid n$. So we have $p \mid p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$.

Reading Exercise 2.7. *Explain how we can use Proposition 2.5 to show that $p = p_i$ for some i.*

Hence, the only primes dividing d are $p_1, \ldots, p_t$. Since the prime factorization of an integer is unique this gives

$$d = p_1^{\ell_1} p_2^{\ell_2} \cdots p_t^{\ell_t}$$

for integers $\ell_i \geq 0$. Finally, let's show that we must have $\ell_i \leq k_i$.

Reading Exercise 2.8. *Observe that 3 divides 135. Find an integer ℓ so that $135 = 3^\ell \cdot r$ where $3 \nmid r$.*

As in the example above, observe that we can write $d = p_i^{\ell_i} r$ where $p_i \nmid r$. Since $d \mid n$ there exists an integer k so that

$$n = dk.$$

Now, write $k = p_i^m s$ where $p_i \nmid s$ and $m \geq 0$ is an integer. Then we have

$$n = p_i^{\ell_i} rk = p_i^{\ell_i + m} rs$$
$$\Rightarrow n = p_i^{\ell_i + m} rs.$$

This means that in the prime factorization of n, we have *at least* a power of $\ell_i + m$ on p_i. But since our prime factorization are unique, this gives

$$\ell_i \leq \ell_i + m = k_i$$

and so $\ell_i \leq k_i$ as desired. □

As we saw in Example 2.7 and Exercise 2.6, it can be tricky to keep track of all of the possibilities for divisors of an integer. Below we give a method to count the number of divisors, which allows us to check that we haven't missed any. We have the following definition.

Definition 2.8. The DIVISOR FUNCTION σ is defined as follows. For each positive integer n, $\sigma(n)$ denotes the number of positive divisors of n.

Reading Exercise 2.9. *Using Example 2.7 and Exercise 2.6, find* $\sigma(12)$ *and* $\sigma(18)$.

We have the following lemma. *Note: "lemma" is another word for "proposition", and is typically used to indicate a proposition which helps us prove a larger result.*

Lemma 2.9. *The divisor function* σ *is multiplicative. That is, if* $\gcd(m, n) = 1$ *then* $\sigma(mn) = \sigma(m)\sigma(n)$.

We'll leave the proof of this lemma as a Core Exercise. We now have the following Corollary to Proposition 2.6. *Note that "corollary" is yet another word for "proposition", and is typically used to indicate a proposition which follows as a consequence of a previous result.*

Corollary 2.10. Let n be a positive integer with prime factorization

$$n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}.$$

Then, the number of primes dividing n is equal to

$$(k_1 + 1)(k_2 + 1) \cdots (k_t + 1).$$

Proof. Using Lemma 2.9 repeatedly, we get

$$\sigma(p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}) = \sigma(p_1^{k_1})\tau(p_2^{k_2}) \cdots \tau(p_t^{k_t}).$$

Reading Exercise 2.10. *For a prime* p, *show that the divisors of* p^k *are precisely*

$$1, p, \ldots, p^k.$$

Hence, we have $\sigma(p_i^{k_i}) = k_i + 1$, and so the result follows. □

2.3. Infinitude of the Primes

The prime numbers, while incredibly useful, are also very mysterious. Researchers are still trying to understand questions about the prime numbers (where are they located? how can you construct them? etc). One thing we can at least say is that there are infinitely many prime numbers. We have the following.

Theorem 2.11. *There are infinitely many prime numbers.*

Proof. The following short proof famously was first document in Euclid's *Elements*. Suppose that there were only finitely many primes, call them $\{p_1, p_2, \ldots, p_k\}$. Then consider the integer

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

Reading Exercise 2.11. *Show that $p_i \nmid Q$ for any $i = 1, 2, \ldots, k$.*

Now, either Q itself is prime, or it has a prime divisor p. In either case, we've created a new prime not in our previous list $\{p_1, \ldots, p_k\}$, and so this must not have been an exhaustive list! Since we can do this for any attempt at a finite list of prime, it must be the case that there are infinitely many primes. □

Core Problems

P1. Find all of the prime numbers between 1 and 30.

P2. Show that 2 is the only even prime number.

P3. Find the unique prime factorization of the following integers.
   (a) 126
   (b) 1617
   (c) 4554

P4. Use the Fundamental Theorem of Arithmetic to find all divisors of the integers from P3.

P5. Use the Fundamental Theorem of Arithmetic to find the greatest common divisors of the following pairs of integers.
   (a) $\gcd(126, 1617)$
   (b) $\gcd(1617, 4554)$
   (c) $\gcd(126, 4554)$

P6. Suppose that a and b are integers with prime factorizations

$$a = p_1^2 p_2^5 p_3$$

$$b = p_1 p_2^2 p_3^4 p_4.$$

   What is $\gcd(a, b)$?

P7. Prove Lemma 2.9. That is, show that if m and n are integers with $\gcd(m, n) = 1$ then $\sigma(mn) = \sigma(m)\sigma(n)$.

Challenge Problems

C1. Without using a calculator, determine the number of zeros at the end of 25!, where

$$25! = 25 \cdot 24 \cdots 3 \cdot 2 \cdot 1$$

is the FACTORIAL of 25. *(Hint: use the Fundamental Theorem of Arithmetic).*

C2. Show that there do not exist natural numbers m, n so that $7m^2 = n^2$.

C3. Show that there do not exist natural numbers m, n so that $24m^3 = n^3$

C4. Recall that a RATIONAL NUMBER is any number of the form $\frac{a}{b}$ where a and b are integers and $b \neq 0$. Use the Fundamental Theorem of Arithmetic to show that $\sqrt{2}$ is not rational.

Chapter 3

Modular Arithmetic

3.1. Clocks and Modular Congruences

Consider for a moment the minute hand of a clock. Each hour, it travels one complete rotation around the clock, corresponding to exactly 60 minutes. Once the minute hand travels back past its starting place, we restart at minute zero again. For example, if the minute hand starts at zero and then travels for 72 minutes, it will be at minute twelve on our clock. So in some ways, we've "identified" 12 with 72.

Mathematically, what we've done is noticed that when we divide 72 by 60, we have a remainder of 12. That is,

$$72 = 60(1) + 12.$$

What ends up getting identified with minute 12 then? Well, every integer so that when it's divided by 60, we get twelve back. That is we'll identify all integers of the form

$$60q + 12$$

for some integer q as being "the same" as 12, since these minutes all end at the same place on a clock. This concept will turn out to be useful in a more general setting, and in fact captures a main feature of our discussion on the division algorithm (Theorem 1.7) in Chapter 1. We have the following definition.

Definition 3.1 (Modular Congruence, preliminary)**.** Let n be a fixed positive integer. We say that a is CONGRUENT TO r MODULO n if the remainder of a when divided by n is equal to r. In this case, we write

$$a \equiv r (\mathrm{mod}\, n).$$

Recall that the division algorithm tells us r is an integer with $0 \leq r \leq n - 1$.

Reading Exercise 3.1. *Let $n = 10$. Use the definition above to explain why the following congruences are true:*

(1) $15 \equiv 5 (mod\, 10)$

(2) $-2 \equiv 8 (mod\, 10)$

(3) $1 \equiv 1 (mod\, 10)$

Next, let's derive a new way to understand the congruence, which will turn out to be easier to work with in many cases. We'd like to extend our definition so that congruence works like equality. In our clock example, we have that

$$72 \equiv 12 (\text{mod}\, 60)$$

But also

$$132 \equiv 12 (\text{mod}\, 60).$$

Since minute 72 and 132 will land at the same place on our clock (mathematically speaking, they have the same remainder when divided by 60), it would be reasonable for us to want to say that 72 and 132 are congruent modulo 60. This doesn't exactly work with our division algorithm definition of modular congruence above, but it isn't far off since we can write

$$132 = 72 + 60(1),$$

which looks division-algorithm-like. Equivalently,

$$132 - 72 = 60(1) \Leftrightarrow 60 \mid (132 - 72).$$

This motivates the following general definition.

Definition 3.2 (Modular Congruence, final version.)**.** Let n be a positive integer. We say that integers a and b are CONGRUENT MODULO n if

$$n \mid (a - b).$$

Equivalently, a is congruent to b modulo n if there exists an integer k so that

$$a = nk + b.$$

In this case, we write

$$a \equiv b (\text{mod}\, n).$$

Example 3.3. Let $n = 13$. Use the definition above to show that the following congruences are true:

(1) $15 \equiv 2 (\mathrm{mod}\, 13)$

(2) $13 \equiv 0 (\mathrm{mod}\, 13)$

(3) $40 \equiv 14 (\mathrm{mod}\, 13)$

(4) $40 \equiv 1 (\mathrm{mod}\, 13)$

This notation takes some time to get used to – the more you practice with it the more natural it will become. I'd suggest working through some of the Core Exercises to get comfortable with this new machinery before moving onto the next section.

3.2. Modular Multiplicative Inverses

The modular world carries many similar properties to the integer world. That is, we can add, subtract, and multiply without having to think too hard (we'll look at this more precisely in the Core Problems). However, one of our typical operations comes with a few difficulties: division.

Recall what division really means. To divide two numbers, say a/b, what we mean is to multiply a by the multiplicative inverse of b, $b^{-1} = 1/b$. This is the notion we'll generalize.

Definition 3.4. Let a be an integer. Then the MULTIPLICATIVE INVERSE OF a MODULO n, if it exists, is the integer a^{-1} so that

$$aa^{-1} \equiv 1 (\mathrm{mod}\, n).$$

Reading Exercise 3.2. *Show that 8 is the multiplicative inverse of 5 modulo 13.*

Reading Exercise 3.3. *Find the multiplicative inverse of* 3 *modulo* 13*.*

Observe that when a^{-1} exists, there exists an integer k so that

$$aa^{-1} = 1 + kn.$$

That is,

$$aa^{-1} - kn = 1.$$

So $x = a^{-1}$ and $y = -k$ is a solution to the linear Diophantine equation

$$ax + by = 1.$$

BUT remember that the Extended Euclidean Algorithm (Theorem 1.15) states that such a solution exists only when $\gcd(a, b) = 1$. This gives the following.

Proposition 3.5. An integer a has a multiplicative inverse modulo n if and only if $\gcd(a, n) = 1$.

Reading Exercise 3.4. *Let* $n = 14$*. Which of the following integers have a multiplicative inverse modulo 14?*

(1) $a = 5$

(2) $b = 12$

(3) $c = 7$

Example 3.6. In this example, we'll use the Extended Euclidean Algorithm to find a modular multiplicative inverse. Let $a = 7$ and $n = 25$. Note that $\gcd(a, n) = 1$ and so by the previous proposition, a has a multiplicative inverse modulo n. Let's first use the Euclidean Algorithm: we divide 7 into 25 to get

$$25 = 7(3) + 4 \Rightarrow \gcd(25, 7) = \gcd(7, 4)$$
$$7 = 4(1) + 3 \Rightarrow \gcd(7, 4) = \gcd(4, 3)$$
$$4 = 3(1) + 1 \Rightarrow \gcd(4, 3) = \gcd(3, 1) = 1.$$

Now, going backward we have

$$1 = 4 + 3(-1)$$
$$\Rightarrow 1 = 4 + (7 + 4(-1))(-1)$$
$$= 4(2) + 7(-1)$$
$$\Rightarrow 1 = (25 + 7(-3))(2) + 7(-1)$$
$$= 25(2) + 7(-7).$$

This gives

$$1 = 25(2) + 7(-7) \equiv 7(-7) (\mathrm{mod}\, 25)$$
$$\Rightarrow 7(-7) \equiv 1 (\mathrm{mod}\, 25).$$

So, $7^{-1} \equiv -7 (\mathrm{mod}\, 25)$. Typically, we'll write the inverse as a number between 0 and $n - 1$. Since $-7 \equiv 14 (\mathrm{mod}\, 25)$ let's instead say

$$\boxed{7^{-1} \equiv 14 (\mathrm{mod}\, 25)}.$$

Reading Exercise 3.5. *Use the Extended Euclidean Algorithm to find the inverse of 3 modulo 13. Was this faster or slower than what you did in Exercise 3.3?*

Core Problems

P1. Determine which of the following congruences are true.

(a) $14 \equiv 2 (\mathrm{mod}\, 12)$
(b) $74 \equiv -1 (\mathrm{mod}\, 5)$
(c) $74 \equiv -1 (\mathrm{mod}\, 7)$
(d) $544 \equiv 16 (\mathrm{mod}\, 13)$
(e) $-177 \equiv 3 (\mathrm{mod}\, 15)$
(f) $70 \equiv 45 (\mathrm{mod}\, 22)$

P2. Let a and b be integers with $a \equiv b (\mathrm{mod}\, n)$ and $c \equiv d (\mathrm{mod}\, n)$.
(a) Show that $a + c \equiv (b + d) (\mathrm{mod}\, n)$.
(b) Show that $ac \equiv bd (\mathrm{mod}\, n)$.

P3. Explain why $n \mid a$ implies that $a \equiv 0 (\mathrm{mod}\, n)$. Conversely, explain why $a \equiv 0 (\mathrm{mod}\, n)$ implies that $n \mid a$.

P4. Find the multiplicative inverse of the following integers for the given modulus, if it exists. If it doesn't exist, explain why not.
(a) $a = 3$ modulo $n = 7$
(b) $a = 2$ modulo $n = 6$
(c) $a = 2$ modulo $n = 21$
(d) $a = 1$ modulo n for any integer n
(e) $a = -1$ modulo n for any integer n
(f) $a = n$ modulo n for any integer n

Challenge Problems

C1. In this problem, we'll derive the following divisibility test: A positive integer n is divisible by 3 *if and only if* the sum of the digits of n is divisible by 3. That is, *if* a positive integer is divisible by 3, then the sum of the digits of n is also divisible by 3. *And conversely* if the sum of the digits of n is divisible by 3, then n is divisible by 3.
(a) Let's start by checking to see if Theorem 1 holds for several examples.
(i) Observe that the following integers are divisible by 3, and the sum of their digits is also divisible by 3

$$13452, 279, 1020.$$

(ii) Choose a few integers whose digits *do not* sum to an integer divisible by 3. Check that they are not divisible by 3.
(b) Next, let's use modular arithmetic to show that 13452 is divisible by 3 without using a calculator.
(i) Find integers a_0, a_1, a_2, a_3, a_4 so that

$$13452 = a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + a_3 10^3 + a_4 10^4.$$

(ii) Check that $10 \equiv 1 (\mathrm{mod}\, 3)$.
(iii) Using P2 (b), convince yourself that we also have

$$10^2 \equiv 1 (\mathrm{mod}\, 3) \text{ and } |10^3 \equiv 1 (\mathrm{mod}\, 3).$$

(iv) Use P2 and the previous part to show that

$$13452 \equiv (a_0 + a_1 + a_2 + a_3 + a_4) \bmod 3.$$

(v) Check that $a_0 + a_1 + a_2 + a_3 + a_4 \equiv 0 (\text{mod}\, 3)$. Conclude from the previous part that $13452 \equiv 0 (\text{mod}\, 3)$.

(vi) Using P3 to conclude that $3 \mid 13452$.

(c) Finally, let's show that Theorem 1 holds for any integer. Our proof will follow similarly to the example in the previous part. Throughout, let n be any fixed integer.

(i) Explain how we know that there are integers $a_0, a_1, \ldots, a_k$ so that

$$n = a_0 + a_1 10^1 + a_2 10^2 + \cdots + a_k 10^k.$$

(ii) Explain how we know that $10^k \equiv 1 (\text{mod}\, 3)$ for any integer k.

(iii) Using P2 and the previous part, observe that

$$n \equiv (a_0 + a_1 + \cdots + a_k) (\text{mod}\, 3).$$

(iv) Suppose that $3 \mid n$. Use the previous part to show that

$$n \equiv 0 (\text{mod}\, 3).$$

Conclude that $3 \mid n$.

(v) Conversely, suppose that $3 \mid (a_0 + a_1 + \cdots + a_k)$. Show that $3 \mid n$.

C2. Lookup some other divisibility tests. You should be able to find them for the following integers: 2, 3, 5, 7, 11 and 13. You don't need to prove any of these, but it might be satisfying to check them for a few examples.

Scratch Paper and Notes