

Newbie Number Theorist

ELEMENTARY NUMBER THEORY
FOR THE
ENTHUSIASTIC NOVICE

Billy Wehring

To my sister Emily,
for sparking my love of math...

*I'm with you til'
the end of the line*

And to Numbers,
because I can always count on you.

Outline of Awesomeness

Commencement	ix
0.1 What is Number Theory?	ix
0.2 Let's Get Warmed Up	xi
0.2.1 Powers of 2	xi
0.2.2 Fibonacci Sequence	xvi
0.2.3 Triangular Numbers	xix
0.3 Pascal's Triangle	xx
0.3.1 Powers of 2 (Again) For Twice as Much Fun!	xxii
0.3.2 The Hidden Triangular Numbers . . .	xxiii
0.3.3 The Hidden Fibonacci Sequence . . .	xxiv
0.4 Remember, Have Some Fun	xxv
 1 Tools for our Tool Kits	 1
1.1 Sets and the Natural Numbers	1
1.2 What Are Sets	2
1.3 The Empty Set, The Natural Numbers, and The Integers	2
1.4 What's In the Set?	3
1.5 Defining a Set With A Rule	4
1.6 A Union of Sets	5

1.7	An Intersection of Sets	5
1.8	Subsets of Sets	6
1.9	Implications are Important	8
1.9.1	Statements and Implications	8
1.9.2	Confusing Converses	10
1.9.3	If and only If (iff)	10
1.9.4	Come on, What's a Contrapositive?	11
1.10	That's a Wrap!	11
2	Incredible Induction	13
2.1	The Problem	14
2.2	Motivating the Induction	16
2.3	Proving the Problem	17
2.4	But Why Does Induction Work?	21
2.5	Interesting Inductions	21
2.6	STRONG Induction	25
2.7	Improper Induction	25
3	Contradiction	29
3.1	What is a Proof by Contradiction?	29
3.2	A Beautiful Theorem due to Euclid	33
3.3	Final Thoughts	38
4	The Division Algorithm	41
4.1	Why are the Natural Numbers <i>Well-Ordered</i> ?	42
4.2	The Division Algorithm (Intuition)	44
4.3	Why Was This Necessary?	50
4.4	List of Takeaways From Chapter 4	51
5	The Euclidean Algorithm	53
5.1	Some Notation	53
5.1.1	Divisors	53
5.1.2	The Greatest Common Divisor	54

5.2	The Euclidean Algorithm	58
5.3	Euclidean Algorithm “Proof”	62
5.4	A Motivating Mystery	65
6	$ax + by = 1$	67
6.1	The Resolution	69
6.2	Bézout’s Identity	71
6.2.1	Boo! No Proof!	77
6.3	Generalization of Bézout’s Identity	77
6.4	Zero or Infinite?	78
6.4.1	Euler’s Lemma	81
6.4.2	Back to The Proof of Zero or Infinite?	83
6.5	It’s the Final Countdown... danananahhh	85
7	Prime Numbers	87
7.1	Fundamental Theorem of Arithmetic	89
7.2	More More More Questions!	94
7.3	Tag, you’re it!	95
8	Modular Arithmetic	97
8.1	A Motivating Mystery	97
8.2	Modular Arithmetic	98
8.2.1	Fun Fundamentals	98
8.3	Tricks of the Trade (mod n)	102
8.3.1	Aggravating Addition	103
8.3.2	Problematic Products	105
8.4	Delicate Division	106
8.4.1	What does <i>division</i> mean?	106
8.4.2	Does Division work?	107
8.5	A Motivating Mystery (The Solution)	113
8.6	And that’s a wrap,	114
8.6.1	Some Practice	114
8.7	It’s Your Time!	115

9	Fermat's Fantastic Little Theorem	117
9.1	Fermat's Little Theorem	117
9.2	A Marvelous Second Proof	122
9.3	Some Practice, For You!	122
9.4	Little Chapter for Little Theorem	123
10	Euler's Totient function	125
10.1	Time For Practice!	134
11	The Chinese Remainder Theorem	137
11.1	Solving A Linear Congruence	138
11.2	Back to Linear Congruences	142
11.3	The Chinese Remainder Theorem	145
11.4	Example Time	148
11.5	Closing Remarks	150
12	Euler's Little Theorem	151
12.1	Let's Discover it Together!	151
12.2	Euler's Little Theorem	155
12.3	An example	160
12.4	Big Things Come in Little Packages	161
A	Induction and Well-Ordering	165
A.1	The Connection	165
A.2	Closing Remarks	171
B	Irrational Numbers	173
B.1	What are rational and irrational numbers????	173
B.1.1	A Quick Comment	178
B.2	Don't be Irrational	179
C	Some Solutions	181
C.1	From Chapter 2	181
C.2	From Chapter 6	183

C.3	From Chapter 8	185
C.4	From Chapter 9	187
C.5	From Chapter 10	189
C.6	From Chapter 12	191

Commencement

“Pure mathematics is, in its way, the poetry of logical ideas,”

– Albert Einstein¹.

0.1. What is Number Theory?

There’s a good chance that you already have a good idea what number theory is, since you’ve bought and are currently reading this book! However, let’s take a few paragraphs to discuss, in part, number theory.

As a first pass and at its most basic, number theory is the study of the *integers*—positive and negative counting numbers like 0, 1, 43, -20, 100, etc. Number theorists love to search for and find patterns and structure hidden within the integers. They tend to ask questions such as:

- What integers solve the equation $x^2 + y^2 = z^2$?
–(for example, $3^2 + 4^2 = 5^2$ and $2322^2 + 1120^2 = 2578^2$. Mathe-

¹Some of you might be curious why the opening quote to a math book is from the physicist Einstein and not a quote from a mathematician. If you are thinking this, then you are my type of people!

maticians have answered this question! For any integers p and q , we have a solution: $x = p^2 - q^2$, and $y = 2pq$, and $z = p^2 + q^2$.)

- Is there a rectangular box whose side lengths, face diagonal lengths, and body diagonal length are all integers?
-(this is an open question, meaning that no one on Earth knows the answer!)
- Observe that,

$$6 = 1 \times 6 = 2 \times 3 \quad \text{and} \quad 6 = 1 + 2 + 3.$$

How awesome is that?!? The same numbers that you multiply to get 6, also add to 6 (excluding 6 in the addition). We call numbers, like 6, *perfect numbers*. Another example is 28, since

$$28 = 1 \times 28 = 2 \times 14 = 4 \times 7$$

and

$$28 = 1 + 2 + 4 + 7 + 14$$

Can you find the next perfect number? *Hint: This is a very challenging question!*

Number Theorists are interested in the question: *Are any odd perfect numbers?*

- (This is also an open problem!)

People sometimes think number theory is the study of prime numbers. This is because number theorists also ask a lot of questions, like,

- Is there always a prime number between n and $2n$ for any integer n ?
-(for example, between 10 and 20 we have four prime numbers: 11, 13, 17, and 19. It turns out that the answer is **YES** and the result is known as Bertrand's theorem)

- How many prime numbers are there less than n ?
-(an approximate answer to this question is called the prime number theorem)
- As we'll see, and you might already know, counting numbers can be expressed as a product of primes. For example, $12 = 2^2 \times 3$ and $30 = 2 \times 3 \times 5$. What about with addition, *can every even number greater than 2 be expressed as the sum of two primes?*
- For example, $4 = 2+2$ or $100 = 3+97$. This is an open problem, one of the oldest open problems in fact.

The main goal of this book is to provide you with enjoyment while learning math. We will accomplish this (I hope) by looking for patterns and coming up with our own questions, and when we find unexpected patterns and connections, we, as mathematicians, will work to prove that these patterns and connections are real.

0.2. Let's Get Warmed Up

In this preliminary chapter, we have not yet learned mathematics together. But that is no reason not to start making discoveries! Furthermore, the hope is that you need very little mathematical prowess to pick up and enjoy this book. Since it's also my hope that you get a sense of what people who do math for fun feel like when they do it, let's begin with some fun number patterns.

0.2.1 Powers of 2

Recall that a prime number is any number that is divisible only by 1 and itself, and even though we have not defined what divisibility is yet, I hope to rely on some of your intuition and knowledge from school. The first ten prime numbers are: 2, 3, 5, 7, 11, 13, 17, 19, 23, and 29. Observe that 2 is the only *even prime number*, this makes 2 the strangest prime number.²

² Or, you might say that 2 is the *oddest prime number*!

The number 2 is also the basis for computer programming through the use of *binary numbers*.³ The gist of binary is to use only the digits 0 and 1 to express a number in terms of sums of powers of 2:

$$\begin{array}{lll} 2^0 = 1, & 2^1 = 2, & 2^2 = 4, \\ 2^3 = 8, & 2^4 = 16, & 2^5 = 32, \\ 2^6 = 64, & 2^7 = 128 & 2^8 = 256. \end{array}$$

Which, in binary become:

$$\begin{array}{l} 1_2 = 2^0 = 1, \\ 10_2 = 2^1 = 2, \\ 100_2 = 2^2 = 4, \\ 1000_2 = 2^3 = 8, \\ 10000_2 = 2^4 = 16, \\ 100000_2 = 2^5 = 32, \\ 1000000_2 = 2^6 = 64, \\ 10000000_2 = 2^7 = 128 \\ 100000000_2 = 2^8 = 256. \end{array}$$

Where the tiny subscript ₂ on the left-hand side's numbers is meant to indicate that we are using binary.

Upon first glance, this is a novel and somewhat confusing notion. How would you think of doing this? Why would you think of doing this? However, the idea isn't so strange when you consider the standard decimal system we are all used to from school. Let's see why.

Consider the number 23,456. Did you know that 23,456 is shorthand for the expression:

$$23,456 = 2 \times 10,000 + 3 \times 1,000 + 4 \times 100 + 5 \times 10 + 6 \times 1$$

³ There are 10 kinds of people in the world: those who understand binary math, and those who don't.

$$= 2 \times 10^4 + 3 \times 10^3 + 4 \times 10^2 + 5 \times 10^1 + 6 \times 10^0$$

When we write 23,456, we are really writing, in shorthand, the above sum of powers of 10. This is so ingrained into the way we think of numbers that it can be difficult to think of this as a property of the way we are choosing to represent them and not a property of the number itself.

When we move to binary, we write numbers using only the digits 0's and 1's—instead of the digits 0, 1, 2, $\dots$, 9—and each place value will be a power of 2 and not a power of 10. For example, consider the binary number 110101. This is shorthand for the following sum of powers of 2:

$$\begin{aligned} \mathbf{110101} &= \mathbf{1} \times \mathbf{2^5} + \mathbf{1} \times \mathbf{2^4} + \mathbf{0} \times \mathbf{2^3} + \mathbf{1} \times \mathbf{2^2} + \mathbf{0} \times \mathbf{2^1} + \mathbf{1} \times \mathbf{2^0} \\ &= \mathbf{1} \times \mathbf{32} + \mathbf{1} \times \mathbf{16} + \mathbf{0} \times \mathbf{8} + \mathbf{1} \times \mathbf{4} + \mathbf{0} \times \mathbf{2} + \mathbf{1} \times \mathbf{1} \\ &= \mathbf{32} + \mathbf{16} + \mathbf{4} + \mathbf{1} \\ &= 53 \end{aligned}$$

So that $110101_2 = 53_{10}$ where the tiny subscripts $_2$ and $_{10}$ indicate that 110101 is in binary (base 2) and 53 is in decimal (base 10). For the most part, when we are working in standard base 10, we won't bother with the subscript 10—because I'm lazy.

We've just seen how to go from binary 110101_2 to decimal 53_{10} , but what if we started with 53 and wanted to find its binary form? How might you go about this? Let's convert 76 to binary, so that we don't know the answer beforehand!

- (i) First, we need to find the largest power of 2 that is smaller than or equal to 76. After taking a look at our list, we see that 2^6 is what we want,

$$2^6 = 64 \leq 76 < 128 = 2^7.$$

- (ii) Next, we subtract off this power of 2, from 76.

$$76 - 2^6 = 76 - 64 = 12.$$

$$\text{Thus, } 76 = 1 \cdot 2^6 + 12.$$

- (iii) Now we repeat step (i), replacing 76 with 12. That is, we want to find the largest power of 2 that is less than or equal 12. In this case, it's 2^3 :

$$2^3 = 8 \leq 12 < 16 = 2^4.$$

- (iv) Repeat step (ii) using 12 and 8 to get:

$$12 - 8 = 4.$$

$$\text{Thus, } 76 = 1 \cdot 2^6 + 12 = 1 \cdot 2^6 + 1 \cdot 2^3 + 4.$$

- (v) You guessed it, find the largest power 2 that is less than or equal to 4. But wait, $4 = 2^2$ so that 2^2 does the job:

$$2^2 = 4 \leq 4 < 2^3 = 8.$$

- (vi) And again, we subtract

$$4 - 2^2 = 0.$$

$$\text{Thus, } 76 = 1 \cdot 2^6 + 2^3 + 4 = 1 \cdot 2^6 + 1 \cdot 2^3 + 1 \cdot 2^2.$$

- (vii) Since we ended up with 0 in step (vi) we're done! All that is left is to put our final answer into binary form. We've found that,

$$\begin{aligned} 76 &= (1 \cdot 2^6) + (1 \cdot 2^3) + (1 \cdot 2^2) \\ &= (1 \cdot 2^6) + (0 \cdot 2^5) + (0 \cdot 2^4) + (1 \cdot 2^3) + (1 \cdot 2^2) \\ &\quad + (0 \cdot 2^1) + (0 \cdot 2^0). \end{aligned}$$

Now we put a 1 in the place values 2^6 , 2^3 , and 2^2 and zero everywhere else:

2^6	2^5	2^4	2^3	2^2	2^1	2^0
1	0	0	1	1	0	0

Thus, $76 = 1001100_2$.

Working in binary takes time to get the hang of, time that we won't spend here! So if you didn't like binary, then you'll be happy because we're done with it! But, since binary requires us to sum powers of two, let's take a look at summing consecutive powers of two:

$$2^0 = \boxed{1}$$

$$2^0 + 2^1 = 1 + 2 = \boxed{3}$$

$$2^0 + 2^1 + 2^2 = 1 + 2 + 4 = \boxed{7}$$

$$2^0 + 2^1 + 2^2 + 2^3 = 1 + 2 + 4 + 8 = \boxed{15}$$

$$2^0 + 2^1 + 2^2 + 2^3 + 2^4 = 1 + 2 + 4 + 8 + 16 = \boxed{31}$$

Do you happen to notice any patterns appearing? If not, let's condense what we wrote and rephrase our sums to be more... suggestive of a pattern,

$$2^0 = \boxed{2 - 1} = 2^1 - 1$$

$$2^0 + 2^1 = \boxed{4 - 1} = 2^2 - 1$$

$$2^0 + 2^1 + 2^2 = \boxed{8 - 1} = 2^3 - 1$$

$$2^0 + 2^1 + 2^2 + 2^3 = \boxed{16 - 1} = 2^4 - 1$$

$$2^0 + 2^1 + 2^2 + 2^3 + 2^4 = \boxed{32 - 1} = 2^5 - 1$$

When we add consecutive powers of 2, we get back the next power of 2 (minus 1)! More precisely, when we add the powers of two, 2^n , with $n = 0, 1, 2, 3, 4, 5, 6$, we will get back $2^7 - 1$. How cute is that?

$$2^0 + 2^1 + 2^2 + \cdots + 2^6 = 2^{6+1} - 1 = 2^7 - 1$$

This begs the question: Does this always happen? If we add $2^0 + 2^1 + 2^2 + \cdots + 2^{100}$ do we get $2^{101} - 1$? Do you think we will get back $2^{101} - 1$?

It turns out that $2^0 + 2^1 + 2^2 + \cdots + 2^{100} = 2^{101} - 1$. Why do you think this pattern is holding? This is where we pull out our creativity and problem-solving hats and become mathematicians!

Consider the sum $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5$, which would be the next sum if we continue our list. Since we already know the previous sum is $2^0 + 2^1 + 2^2 + 2^3 + 2^4 = 2^5 - 1$, when we add 2^5 to both sides we get:

$$\begin{aligned} 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 &= (2^5 - 1) + 2^5 \\ &= 2 \cdot (2^5) - 1 \\ &= 2^6 - 1. \end{aligned}$$

We used what we already knew to calculate the next sum! And, since we can keep doing this for larger exponents, our pattern continues to hold!

$$2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1.$$

Neat!

0.2.2 Fibonacci Sequence

No book on number theory would be complete without the Fibonacci numbers simply because everyone **loves** them! It's said that Fibonacci numbers show up everywhere: in nature, art, music, etc, without explanation! Of course, there is a logical explanation for these occurrences when they happen! But never mind that! We want to do some math!

The Fibonacci numbers, or Fibonacci sequence, is a list of numbers that follow a particular rule in their construction. This rule is: *add the previous two numbers*, and by starting with 0 and 1 we get the list,

$$F_n : 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 84, \cdots \quad (\P)$$

We will denote the n^{th} Fibonacci number by F_n . For example, the 9^{th} number on the list is $F_9 = 21$, as you can check.

Not only do we want to learn some awesome math throughout this book, but we also want to become more comfortable with fancy math jargon and notation. Here's a good place to add some in. We formally define the Fibonacci numbers as follows:

Definition 0.1: Fibonacci Numbers (Formal)

We define the n^{th} Fibonacci number F_n as follows:

- (i) Define $F_0 := 0$ and $F_1 := 1$, and
- (ii) $F_{n+2} := F_{n+1} + F_n$.^a

^a Note that $:=$ means 'defined to be' so that $F_0 := 0$ means F_0 is defined to equal 0.

This is called a *recursive* definition for the Fibonacci numbers. Recursive means: to find the next Fibonacci number, you must use the previous Fibonacci numbers.

Can you see how this definition yields the sequence (🐱)?

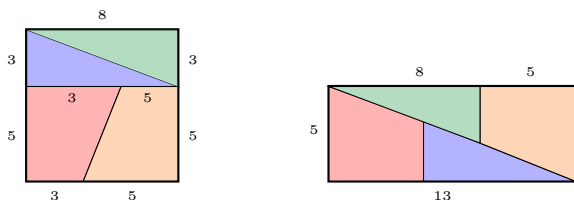
Have you ever seen the GIF where someone takes a chocolate bar, cuts it into pieces, removes a single piece, and then proceeds to do the seemingly impossible and construct a new chocolate bar with the remaining pieces? If not, you should search 'infinite chocolate' bar or scan the QR code; it's quite astonishing.⁴



⁴Or if you don't trust me and the QR code (I respect your skepticism), you can search: https://www.youtube.com/post/UgkxTktV1CjcJ6p6VeqUc15FGMDNzu30U_LM

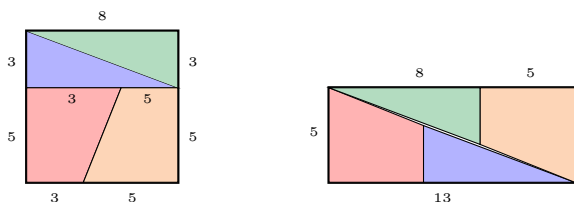
Let's illustrate what is happening with the chocolate bar using a square.

Consider an 8×8 square. First, this square has an area equal to $8^2 = 64$. We will cut it into four pieces and rearrange them to make the 5×13 rectangle on the right.



Wait just a moment, the area of the rectangle is $5 \times 13 = 65$, not 64! How wild is that? What just happened? Where did this extra area come from? *Take a few moments to sit in the bewilderment!*

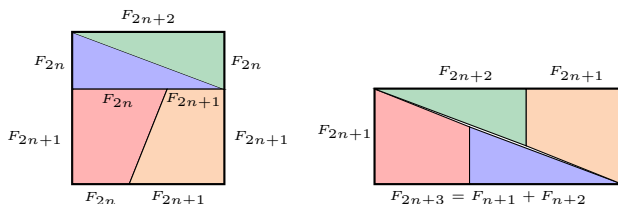
What happened is that the pictures lied to you! A 5×13 rectangle will indeed have an area of 65, but that's not what we have here! What we really have is the following, more accurate diagram:



Do you see that small white space in the center of the rectangle? That is where the extra 1 unit of area lives. The same is true for the chocolate; there is a hidden area.

What's amazing is that you can make your own squares and rectangles using the Fibonacci numbers! Did you notice that 3, 5, 8

are consecutive Fibonacci numbers? If you take the three consecutive Fibonacci numbers $F_{2n}, F_{2n+1}, F_{2n+2}$, then you can make the following diagram:



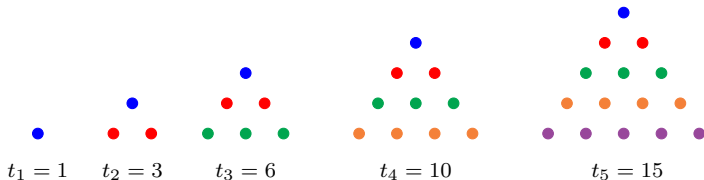
Note in the previous diagram we have: $F_{2(2)} = F_4 = 3$, $F_{2(2)+1} = F_5 = 5$, and $F_{2(2)+2} = F_6 = 8$.

We will show how to justify this geometric construction later on, once we learn about *induction* in a later chapter. For now, the reason we can do this is because the Fibonacci numbers satisfy the following relation:

$$(F_{2n+2})^2 = F_{2n+1}F_{2n+3} - 1.$$

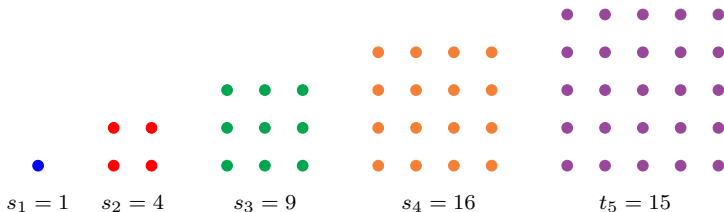
0.2.3 Triangular Numbers

Triangular numbers are numbers that you get when you draw, guess what, a triangle! Take a look at the following picture, t_n denotes the n^{th} triangular number:



In general, to go from t_n to t_{n+1} you add $n + 1$ more dots to the picture. How many patterns can you find?

One really interesting property that triangular numbers have relates them to *square numbers*. A square number is a number of the form n^2 . These, as the name implies, are the numbers that you get when you draw squares:



I know, I know, $t_1 = s_1$ are dots, not triangles or squares. It's close enough!

It turns out that the sum of any two consecutive triangular numbers equals a square number! Give it a try!

$$t_1 + t_2 = 4 = s_2$$

$$t_2 + t_3 = 9 = s_3$$

$$t_3 + t_4 = 16 = s_4$$

$$t_4 + t_5 = 25 = s_5$$

I challenge you to try to justify this using the pictures! Draw out some triangular numbers and see if you can rearrange them to make a square number!

Again, we will learn how to prove this using induction later!

0.3. Pascal's Triangle

Did you learn about *Pascal's Triangle* in school? If you didn't learn and have not heard of Pascal's triangle, then you are about to have a treat! For those who have, let's have a brief refresher.

Here's the idea: Start with a triangle with ones on the corners:

$$\begin{array}{c} 1 \\ 1 \quad 1 \end{array}$$

Then, take the 1 1 in the second row and add them to get 2 and place the 2 below both of the 1's as follows,

$$\begin{array}{c}
 1 \\
 \swarrow \quad \searrow \\
 1 \quad 1 \\
 \searrow \quad \swarrow \\
 2
 \end{array}$$

Fill in the rest of the third row with 1's so that there are three numbers in the third row,

$$\begin{array}{c}
 1 \\
 \swarrow \quad \searrow \quad \swarrow \quad \searrow \\
 1 \quad 1 \quad 1 \quad 1 \\
 \searrow \quad \swarrow \quad \searrow \quad \swarrow \\
 1 \quad 2 \quad 1
 \end{array}$$

Now take the first 1 and 2 in the third row and add them to get 3, place this 3 under the 1 and 2, likewise with the last 2 and 1:

$$\begin{array}{cccc}
 & & 1 & & \\
 & & 1 & & 1 \\
 & 1 & & 2 & & 1 \\
 1 & & 3 & & 3 & & 1
 \end{array}$$

Continue adding the consecutive pairs and placing the sums under the pairs

$$\begin{array}{cccccccccc}
 & & & & 1 & & & & \\
 & & & & 1 & & 1 & & \\
 & & & 1 & & 2 & & 1 & \\
 & & 1 & & 3 & & 3 & & 1 \\
 & & 1 & & 4 & & 6 & & 4 & & 1 \\
 & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
 & & 1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 \\
 1 & & 8 & & 28 & & 54 & & 70 & & 54 & & 28 & & 8 & & 1
 \end{array}$$

If you've seen Pascal's triangle, it was probably introduced as a tool to foil out products such as $(a+b)^7$ quickly. The way you'd do this is by taking the numbers in the seventh row of the triangle and using them as coefficients in the product. The variables that go with those coefficients will be of the form $a^n b^m$ where $n+m=7$. The way that the $a^n b^m$ fill in is by starting with $a^7 b^0 = a^7$ and decreasing the exponent of a while increasing the exponent of b as follows,

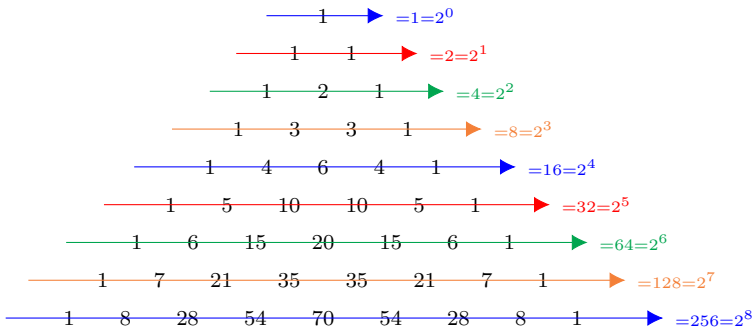
$$(a+b)^7 = 1a^7 + 7a^6b^1 + 21a^5b^2 + 35a^4b^3 + 35a^3b^4 + 21a^2b^5 + 7a^1b^6 + 1b^7$$

This is very useful when you need to foil out a sum of two numbers. However, this is only the tip of the iceberg!

0.3.1 Powers of 2 (Again) For Twice as Much Fun!

Would you believe me if I said powers of two are hidden within Pascal's triangle? No? Will keep reading!

Each row sums to a power of two!!!



Can we explain why this happens?

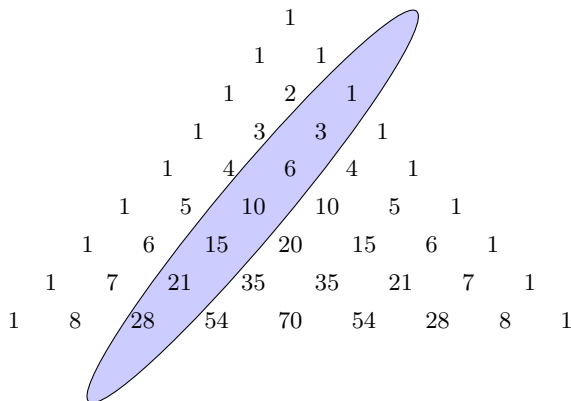
Yes, yes, we can!

If you take a look at the rule for constructing rows in Pascal's triangle, we can see that every number in the previous row is

added *twice*. For instance, to go from the row: 1 2 1, to the row: 1 3 3 1, we add each 2 twice and each 1 once. But, by dropping down the 1's on the outside, we double each 1's effect on the sum. Thus, we are doubling the previous row! This is why we get powers of 2.

0.3.2 The Hidden Triangular Numbers

Pascal's triangle does it again! The triangular numbers are hidden in plain sight!



How wonderful! Let's see if we can figure out why this happens.

If you go back to the pictures representing the triangular numbers, we can see that $t_{n+1} = t_n + (n + 1)$. For example, $t_5 = t_4 + 5 = 10 + 5 = 15$. Now, take a look at the number 15 in the blue oval above. You can see that we 15 there because we summed the previous row's 10 and 5. Or, by the triangular number $t_4 = 10$ and 5. This happens with each new triangular number t_{n+1} , which is formed by adding the previous triangular number t_n and the number $n + 1$.

0.4. Remember, Have Some Fun

*While you read this last bit of our Commencement, I recommend you listen to the music simultaneously. I hope that you enjoy it!*⁶



I want to end with two quotes, one from James Clear and another from Einstein. A lot of the time, particularly when learning math, we will often get stuck, confused, and become frustrated. It's okay, this is natural and happens to everyone; it's crucial you know that one reason mathematicians enjoy math is because it presents a **huge challenge**! So **never** feel defeated or that you are not up to snuff when you inevitably get confused. Assume it's because I didn't explain the material well enough, or maybe I made a typo, or maybe it's just a really challenging piece of mathematics and you'll have to push through and *go the*

⁶Again, if you don't trust me and the QR code, here's the link: https://youtu.be/go01_bXLYlw?si=qfPZmpYCELcYTJT7J

distance until you understand it. Whatever the reason(s) is/are, remember **never give up!** Take it from Einstein, intelligence comes from practice, hard work, and patience.

“It’s not that I’m so smart, it’s just that I stay with problems longer.”

– Albert Einstein.

And remember, math is supposed to be fun! So keep this last quote in mind, too.

“Whoever who has the most fun, wins.”

– James Clear.

Chapter 1

Tools for our Tool Kits

“The only way to learn mathematics is to do mathematics.”

— Paul R. Halmos, Hungarian-American mathematician

1.1. Sets and the Natural Numbers

Before we are ready to learn some number theory, we have some fundamentals that we need under our belt. Most of this will be notation, or mathematical shorthand, that we will be using throughout this book. More specifically, we will learn about *set notation* and to a lesser extent *set theory*.

As of now, we only need to know seven things about set notation/theory. First, we need to know what a set *is*. From there, we will discuss three very important examples of sets. Then we will learn two ways to describe what numbers are ‘contained in’ a set. Next, we will learn two ways to combine two sets: through a union and an intersection. Finally, we will learn when one set is

a *subset* of another set.

1.2. What Are Sets

A **set** is a collection of elements (in our case, ‘elements’ are usually numbers or other sets). We use curly brackets to ‘contain’ the set’s elements. For example, $\{1, 2, 3\}$ and $\{10, 209, 314, \dots\}$ are sets of numbers. And $\{\{1, 2\}, \{2, 3, 4, 5, 6\}\}$ is a set of sets. A non-example is the following: $(1, 2, 3)$ **is not a set**.

Furthermore, order does not matter, and we don’t care about repeated elements in a set. For example, the following are all the same sets,

$$\{1, 2, 3, 3, 3, 3, 3\} = \{2, 1, 3, 3, 3, 2, 2\} = \{1, 3, 2\} = \{1, 2, 3\}.$$

They all contain the numbers 1, 2, and 3.

1.3. The Empty Set, The Natural Numbers, and The Integers

The set that contains *nothing* is called the **empty set** and is denoted,

$$\emptyset := \{\},$$

note “ $:=$ ” means “defined as”.

The **natural numbers** are our counting numbers that we’ve known since kindergarten, but to be very professional, we will denote the *set of natural numbers* by this fancy-looking $\mathbb{N}$,

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

Lastly, we will sometimes need to use both positive and negative ‘natural numbers’, as well as the number 0. It’s therefore important to have a set that contains all these numbers. This is

where the **integers** come in. Standard notation is to use the fancy looking $\mathbb{Z}$ to denote the set of integers,¹

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

1.4. What's In the Set?

Sometimes we want to say that a certain element *is in a set*. But, since we are lazy, we don't want to have to keep writing: 1 is in the set $\{1, 2, 3\}$. Henceforth, we will use the symbol $\in$ to mean 'is an element of' or 'is in the set'. For example, $1 \in \{1, 2, 3\}$ translates to 1 *is in the set* $\{1, 2, 3\}$. Similarly, $2 \in \{1, 2, 3\}$ and $10 \in \mathbb{N}$.

It's just as useful to be able to have a shorthand to say, an element *is not in a set*. In this situation, we use $\notin$ to mean 'is not an element of'. For example, 5 isn't in the set $\{1, 2, 3\}$, so we write $5 \notin \{1, 2, 3\}$ which translates to 5 *is not in the set* $\{1, 2, 3\}$. Similarly, $0.5 \notin \mathbb{N}$ and $\frac{2}{3} \notin \mathbb{Z}$.

Lastly, sometimes we want to be able to quantify how many elements are in a set. To do so, we will write,

$$|S| = \text{number of elements in } S$$

Even though it looks like an absolute value, it's not!!!! We're determining the size of a set. For example, $|\{1, 2, 3\}| = 3$. Likewise, we have

$$\left| \{2, 5, 23, 5345, 2343, 100000\} \right| = 6.$$

However, we have to be careful with situations with sets of sets like

$$\{\{1, 2\}, \{2, 3, 4, 5, 6\}\}.$$

In this instance we have

$$\left| \left\{ \{1, 2\}, \{2, 3, 4, 5, 6\} \right\} \right| = 2,$$

¹ Apparently, we use the letter $\mathbb{Z}$ because of the German word *Zahlen* which means *numbers* [5]. Who knew!

since our set contains two elements that are sets.

1.5. Defining a Set With A Rule

A lot of the time, the elements of a set follow some *rule* or *pattern*. For example, the set of all even natural numbers could be written as $\{2, 4, 6, \dots\}$, which is fine, but there is an easier way to express the set of even natural numbers. We write the set of even numbers in the following way,

$$\begin{aligned}\{2, 4, 6, \dots\} &= \{n \in \mathbb{N} \mid n = 2k \text{ and } k \in \mathbb{N}\} \\ \text{or } &= \{n \in \mathbb{N} : n = 2k \text{ and } k \in \mathbb{N}\}.\end{aligned}$$

We would read the sets $\{n \in \mathbb{N} \mid n = 2k \text{ and } k \in \mathbb{N}\}$ and $\{n \in \mathbb{N} : n = 2k \text{ and } k \in \mathbb{N}\}$ as: the set of *natural numbers* n **such that** $n = 2k$ *where* k *is in the set* $\mathbb{N}$. More often than not, you can read the colon $:$ or the vertical line $\mid$ in the set as the words “such that”.

For another example, consider the set,

$$S = \{2n + 1 \in \mathbb{Z} \mid n \in \mathbb{Z} \text{ and } n > 10\}.$$

These symbols translate to: S is the set of all numbers of the form $2n + 1$ **such that** n is an integer greater than 10. Using this rule, we can calculate some of S 's elements:

$$\begin{aligned}\{2n + 1 \mid n \in \mathbb{N} \text{ and } n > 10\} &= \{2(11) + 1, 2(12) + 1, \dots\} \\ &= \{23, 25, 27, 29, \dots\}.\end{aligned}$$

For one last example, we could write the set of natural numbers as,

$$\mathbb{N} = \{n \in \mathbb{Z} : n \geq 1\}.$$

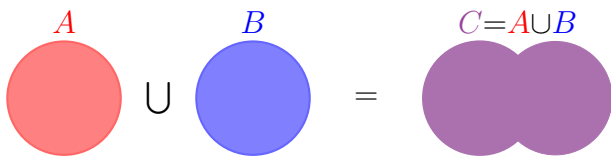
Which translates to: $\mathbb{N}$ is the set of integers n **such that** $n \geq 1$. Can you see why this is the set of natural numbers?

1.6. A Union of Sets

There are two ways to combine two sets. The first is called a *union* of two sets. A union between the sets A and B is a fancy way of saying, take everything from A and B and put them in a new set C . It's standard to denote a union with a large U :²

$$\text{Union : } A \cup B := \{c : c \in A \text{ or } c \in B\} \quad (\P)$$

Pictorially, we can represent the union of two sets using circles. Let A be the red circle and B be the blue circle below. The union of A and B gives the purple set, C .



An example of a union, let's take the sets $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{2, 4, 10, 11, 12, 26\}$. The union of A and B is the set

$$A \cup B = \{1, 2, 3, 4, 5, 6, 10, 11, 12, 26\}.$$

Note how the union contains everything that was in A and/or B .

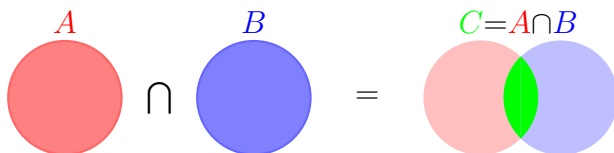
1.7. An Intersection of Sets

The second way to combine two sets is to take their *intersection*. An intersection of sets A and B is kind of what it sounds like: take every element that is in both A **and** B ,

$$\text{Intersection : } A \cap B := \{c : c \in A \text{ and } c \in B\} \quad (\&)$$

We use the symbol $\cap$ to denote intersection. The way I remember this is because it looks like the n in **inter**section and in **and**. Pictorially, we have

²We read $A \cup B = \{c : c \in A \text{ or } c \in B\}$ as, $A \cup B$ is the set of elements c such that c is either in the set A , or c is the set B . Note, *or* is the *inclusive or*. *Inclusive or* is synonymous with and/or.



Where the intersection of sets A and B is the green.

For an example of an intersection, let's again take the sets $A = \{1, 2, 3, 4, 5, 6\}$ and $B = \{2, 4, 10, 11, 12, 26\}$. The intersection of A and B is the set

$$A \cap B = \{2, 4\}.$$

since $2 \in A$ and $2 \in B$ likewise $4 \in A$ and $4 \in B$, and no other element is in both sets.

1.8. Subsets of Sets

We say that A is a **subset** of B if every element in A is also in B . That is, if a is in A , then a is also in B . In symbols: if $a \in A$, then $a \in B$. When this happens, we write $A \subset B$ or $A \subseteq B$. For example, $\mathbb{N} \subseteq \mathbb{Z}$ since every natural number $n \in \mathbb{N}$ is also an integer $n \in \mathbb{Z}$. Also, it's always the case that the set A is a subset of itself: $A \subseteq A$, since $a \in A$ implies $a \in A$.

Some more examples are,

$$\{2, 4\} \subseteq \{1, 2, 3, 4, 5, 6\}$$

and

$$\{2, 4\} \subseteq \{2, 4, 10, 11, 12, 26\}.$$

Or, using our definitions of A and B earlier,

$$A \cap B \subseteq A \quad \text{and} \quad A \cap B \subseteq B$$

we also have

$$A \subseteq A \cup B \quad \text{and} \quad B \subseteq A \cup B.$$

These turn out to be general properties of unions and intersections. This is going to be our first proven result!

Proposition 1.1: Intersection and Union Examples

Let A and B be sets. Then the following statements always hold,

- (i) $A \cap B \subseteq A$,
- (ii) $A \cap B \subseteq B$,
- (iii) $A \subseteq A \cup B$, and
- (iv) $B \subseteq A \cup B$.

This might be evident from the pictures, but it might also be helpful to see how we write a proof using set notation. Also, let's be excited that WE'RE ABOUT TO WRITE OUR FIRST PROOF TOGETHER!

Proof. Let A and B be sets. We first aim to prove (i) $A \cap B \subseteq A$. We will achieve this using the definition of a subset, that is, if $c \in A \cap B$, then $c \in A$.

With this goal in mind, let $c \in A \cap B$. By the definition of an intersection, $c \in A$ and $c \in B$. We're done! Since we've just concluded that $c \in A$. And we've also shown that $c \in B$ too and hence $A \cap B \subseteq B$ as well!

Now we aim to prove (iii) $A \subseteq A \cup B$. To this end, let $a \in A$. Then, by the definition of a union, we conclude that $a \in A \cup B$ since a is in A and hence $a \in A$ or $a \in B$. Therefore $A \subseteq A \cup B$.

Mimic the proof of part (iii) to prove part (iv).



Note: We'll use the symbol  to denote the end of a proof. When you see this symbol, it means that the proof is done and we are

about to move on to something else. The standard symbol to denote the end of a proof is $\square$, but I wanted a custom symbol so that every time we see it, we can remember: HAVE FUN and WOW, I'M AWESOME AND I JUST FINISHED ANOTHER PROOF!

1.9. Implications are Important

1.9.1 Statements and Implications

A **statement**, in mathematics, is a claim that is true or false—not both. For example, “ $2 + 2 = 4$ ” is a true statement. Likewise, “*Captain America is my favorite superhero*”, is a true statement. However, “*I can bench press 500lbs*”, is a false statement because “*I can only bench press 400lbs*”—which is also a false statement.

We can also construct new, longer statements from other statements. For instance, the statement: “ $2 + 2 = 4$ and *Captain America is my favorite superhero*” is a true statement which is made from two smaller, true statements. However, the statement: “ $2 + 2 = 4$ and *I can bench press 500lbs*” is a false statement made from one true statement and one false statement. The statement “ $2 + 2 = 4$ and *I can bench press 500lbs*” is false because I still cannot bench press 500lbs.

Formally, let A and B represent statements.³ It follows from the last example that the statement: “ A and B ”, is only true if both A and B are simultaneously true. If either A or B is false, then the whole statement “ A and B ” is false. See table 1.1.⁴

There are other ways we can combine smaller statements to form longer, more complex statements. We can create the statement: A or B . However, this ‘or’ is a special type of ‘or’ called *inclusive or*. Inclusive or is more like the phrase ‘and/or’. The

³For example, A could be “ $2 + 2 = 4$ ” and B could be “*Captain America is my favorite superhero*”.

⁴The statement, A and B , is called the conjunction of A and B and in logic it’s denoted: $A \wedge B$.

A	B	$A \text{ and } B$	$A \text{ or } B$	$A \implies B$
True	True	True	True	True
True	False	False	*True*	False
False	True	False	True	True
False	False	False	False	True

Table 1.1: This is called a *truth table*. It’s a compact way to show whether the statements $(A \text{ and } B)$, $(A \text{ or } B)$, and $(A \implies B)$ are true based on whether A and B are true or false. For example, take a look at the second row under $A \text{ or } B$, which says *True*. This denotes that the statement $A \text{ or } B$ is true when A is true and B is false.

combined statement “ $A \text{ or } B$ ” is true if A is true, B is true, or both A and B are true. Note that “ $A \text{ or } B$ ” is true even if A and B are both true. For example, “ $2+2=4$ ” or “*Captain America is my favorite superhero*” is a true statement. Likewise, “ $2+2=4$ ” or “*I can bench press 500lbs*” is also true since “ $2+2=4$ ” is true. Once you establish that the statement $A(B)$ is true, it doesn’t matter whether or not $B(A)$ is true/false—the statement $A \text{ or } B$ is already true. See table 1.1.⁵

There is one statement that uses A and B that we are most interested in here. It’s called an **implication**. An implication is a statement of the form: *if A , then B* . Which means: *if A is true, then B is true*. Many of the statements we will prove take this form. For example, we already proved proposition 1.1, which can be written (in part) as the following implication,

***If** A and B are sets,
then the intersection of A and B is a subset of both A and B .*

As with most things in math, people have developed shorthand

⁵When we say ‘or’ will always mean *inclusive or*. In formal logic, inclusive or statements are called disjunctions and they are denoted $A \vee B$.

symbols to represent implication. The statement *if A, then B* becomes $A \implies B$. So, we could have written our proposition as:

$$A \text{ and } B \text{ are sets} \implies A \cap B \subseteq A \text{ and } A \cap B \subseteq B.$$

1.9.2 Confusing Converses

Let the statement $A \implies B$ be our main focus. Then we call the statement $B \implies A$ the **converse** statement.

$$\textbf{Main Statement: } A \implies B$$

$$\textbf{Converse: } B \implies A$$

It's crucial to understand that the main statement and its converse are distinct statements. Just because one of them is true does not imply anything about the other! For example, take the true statement:

True: If you are Harry Potter, then you're a wizard.

The converse is false:

False: If you're a wizard, then you are Harry Potter.

You could be Hermione or Ron or some other character that's a wizard! Most statements don't have true converses.

1.9.3 If and only If (iff)

Some implications are so special that **both** $A \implies B$ and $B \implies A$ are true. When this happens, we use the symbol $\iff$, which translates to *if and only if*—sometimes abbreviated iff. Thus, we read the statement, $A \iff B$ as *A if and only if B*.

In logic, we say that statements A and B are (logically) equivalent to one another—this is because $A \iff B$ means that *A is only true if B is true, and B is only true if A is true*.

When we encounter an iff statement that we want to prove in the wild, we have to prove two statements. We need to write a proof for the statement $A \implies B$ and then write a second, different proof for $B \implies A$.

1.9.4 Come on, What's a Contrapositive?

Let $A \implies B$ be our main statement again. The statement: $\text{not } B \implies \text{not } A$ is called the **contrapositive**.

Main Statement: $A \implies B$

Contrapositive: $\text{not } B \implies \text{not } A$.

Unlike the converse, the contrapositive is logically equivalent to the main statement.

For example, take the statement from earlier regarding Harry Potter and being a wizard. That statement is logically equivalent to its contrapositive

True: If you are Harry Potter, then you're a wizard.

True: If you're NOT a wizard, then you are NOT Harry Potter.

Sometimes, it's too difficult to prove the statement $A \implies B$. When this happens, we can try to prove the contrapositive $\text{not } B \implies \text{not } A$ instead. Not always, but often, it's easier to prove the contrapositive.

1.10. That's a Wrap!

We've covered all the fundamentals to be ready to get started. Our goal for the following two chapters is to develop two extremely useful methods to prove theorems in number theory: induction and proof by contradiction.

Chapter 2

Incredible Induction

“To infinity, and beyond!”

— Buzz Lightyear, in Toy Story

Introduction

As stated at the end of the last chapter, our first task is to develop methods and tactics, along with tools for our mathematical toolkit, to aid us on our journey. Our first is a proof technique called *induction*. Induction is an incredibly useful technique used to prove an infinite number of statements. We will use it constantly throughout this book.

However, induction isn't the perfect proof technique. For instance, in order to use induction, you must know precisely what you are trying to prove before you can use induction to prove it. Induction gives you no clues on what statements need proving. For this reason, to give you a genuine induction experience, we will start with a problem, develop a conjecture, and then use induction to prove our conjecture.

2.1. The Problem

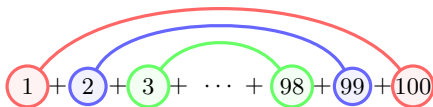
This is a classic problem in mathematics. What is the sum of every natural number from 1 to 100?

$$1 + 2 + 3 + \cdots + 99 + 100 = ???$$

We will call 1 our *starting number* and 100 our *ending number*.

As with a lot of math problems, there is more than one way to get to the answer. We'll be lazy and do it in a short (and clever) way.

The short way begins with some sitting and thinking—we're very lazy indeed—and after a while, we might notice that we can pair off numbers in our sum,



Do you see why this particular pairing is helpful? Take a moment to look again if you're not sure!

Seriously, go back and look again! It's so clever, and once you see the answer, you lose the chance to discover it yourself!

When you sum the paired numbers, each pair totals 101:

$$1 + 100 = 2 + 99 = 3 + 98 = \cdots = 50 + 51 = 101.$$

Instead of adding every number together, we now have a repeated addition, aka multiplication, problem. All we need to determine is how many pairs of 101 we form. See if you can figure out how many pairs there are.

Pause for another moment and take a guess!

There are fifty pairs of 101 in our sum. This is because we start with one hundred numbers to be added, and then each one is

paired with another number; cutting one hundred in half is fifty. Therefore, our sum equals,

$$1 + 2 + 3 + \cdots + 99 + 100 = \overbrace{101 + 101 + \cdots + 101}^{100 \div 2 = 50 \text{ pairs}}$$

Which begs to be simplified using some algebra,

$$\begin{aligned} 1 + 2 + 3 + \cdots + 99 + 100 &= 101 + 101 + \cdots + 101 \\ &= 50(101) \\ &= 5,050 \end{aligned}$$

But to be more suggestive, let's express 50 as $100/2$, since 100 is our ending number,

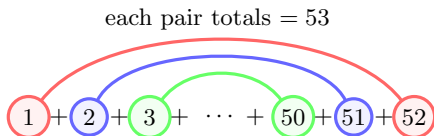
$$50(101) = \frac{100}{2} \cdot 101 = \frac{100(101)}{2}$$

Our conclusion is the following:

$$1 + 2 + 3 + \cdots + 100 = \frac{100(100 + 1)}{2} = 5,050$$

How clever is that? How long would it have taken you to add every number from 1 to 100 together? Even with a calculator, it would have taken a few minutes! Isn't math wonderful?¹

There was nothing special about the ending number 100; we can do the same trick when we add: $1 + 2 + 3 + \cdots + 52$. However, when we pair off the numbers this time, each pair totals 53 and we have $52/2 = 26$ pairs,



¹ By the way, the punctuation mark ‘?’ is called an *interrobang* and is used to punctuate question sentences that are said in an exclamatory manner.

This time, we can rewrite our sum as,

$$\begin{aligned}1 + 2 + 3 + \cdots + 51 + 52 &= \overbrace{53 + 53 + \cdots + 53}^{26 \text{ pairs}} \\&= 26(53) \\&= 1,378.\end{aligned}$$

Or, better yet, we can express our sum in much the same way as the boxed equation at the top of this page,

$$1 + 2 + 3 + \cdots + 52 = \frac{52(52 + 1)}{2} = 1,378.$$

Our takeaway is that this trick, pairing the first and last numbers, then the second and penultimate numbers, etc., always *seems* to work. We say ‘seems’ to work because we have yet to prove that it *always* works. But the pattern is compelling, so much so, that we might conjecture the following:

Conjecture 1. *For any natural number $n \in \mathbb{N}$ the formula below always holds,*

$$1 + 2 + \cdots + (n - 1) + n = \frac{n(n + 1)}{2}.$$

Now that we have a conjecture, as mathematicians, we want to prove it! This is where induction comes in.

2.2. Motivating the Induction

Before we learn induction, let’s take a moment to motivate *why* induction works.

Since we already know that $1 + 2 + \cdots + 100 = 5,050$, we can add the numbers 1 to 101 easily:

$$\begin{aligned}1 + 2 + \cdots + 100 + 101 &= (1 + 2 + \cdots + 100) + 101 \\&= 5,050 + 101\end{aligned}$$

$$= 5, 151.$$

By using our result for the sum $1 + \cdots + 100$, we made our life easy determining the new sum $1 + 2 + \cdots + 100 + 101$. Induction is like a more formal and general proof technique that's based on the same idea.

2.3. Proving the Problem

To set our intentions from the get-go, we want to prove the following formula,

$$1 + 2 + \cdots + (n - 1) + n = \frac{n(n + 1)}{2} \quad (\text{⚡})$$

works for any natural number n using induction. We are now ready to state the principle of mathematical induction:

The Principle of Mathematical Induction:

Let $n \in \mathbb{N}$, and let $P(n)$ be a statement that is either true or false. If

(i.) $P(1)$ is true; and

(ii.) " $P(n)$ is true" implies " $P(n + 1)$ is true",

then $P(n)$ is true for all natural numbers $\mathbb{N}$.

When we demonstrate step (i), we call it our **base case**. When we are aiming to prove the statement in step (ii), we will first assume $P(n)$ is true (this is called the **induction hypothesis**), and then the proof that $P(n)$ implies $P(n + 1)$ is called the **inductive step**. Here is the general framework for a proof using induction:

Proof. We will do a proof by induction on n .² Then, determine

²You could also start your proof by writing, We proceed by induction

what $P(n)$ is for the particular problem at hand, and then state what $P(n)$ is if you choose.

Base Case: Set $n = 1$ and demonstrate that $P(1)$ is true, (sometimes we might have a base case that starts at $n = 0$).

Induction Hypothesis: Assume that $P(n)$ is true for some $n \in \mathbb{N}$.

Inductive Step: We prove that $P(n)$ implies $P(n + 1)$ is true.

Conclusion: By induction, we have shown that $P(n)$ is true for all $n \in \mathbb{N}$.



It's possible to formally prove that induction works (and we do this in appendix A), but let's get an intuitive feel for why it works by proving our conjecture (⚡).

on n . Whatever you say, you must warn your reader that you are going to use induction and what you are inducting on, i.e., n .

Proof of Our Conjecture. We will do a proof by induction on n . Our statement $P(n)$ is the following:

$P(n)$ is the statement: $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$.

Base Case: Let $n = 1$ in our conjectured formula (⚡) and check to see if $P(1)$ is true:

$$1 \stackrel{\checkmark}{=} \frac{1(1+1)}{2} = \frac{1(2)}{2},$$

Since the formula holds, $P(1)$ is true.

Induction Hypothesis: Assume that $P(n)$ is true, that is, it's true that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ for some $n \in \mathbb{N}$.

Inductive Step: We must prove $P(n+1)$ is true, that is, our formula holds for $n+1$:

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &\stackrel{\text{want to show}}{=} \frac{(n+1)((n+1)+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

To do this, we will be assuming that $P(n)$ is true (which is our inductive hypothesis).

With this goal in mind, observe that the first n -terms in our sum total $\frac{n(n+1)}{2}$, by our *induction hypothesis*. Therefore,

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &= \left(1 + 2 + \cdots + n\right) + (n+1) \\ &= \left(\frac{n(n+1)}{2}\right) + (n+1). \end{aligned}$$

Which we can rewrite using some algebra tricks,

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

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

Hence,

$$1 + 2 + \cdots + (n+1) = \frac{(n+1)(n+2)}{2},$$

which is (⚡) with $n+1$ substituted for n .

We have shown that $P(1)$ is true as well as the fact that $P(n)$ implies $P(n+1)$, and by induction, we have proven our conjecture.



Woot! Our conjecture is now a full-blown proven theorem.

Theorem 2.1: Our First Theorem

For any natural number $n \in \mathbb{N}$ we have,

$$1 + 2 + \cdots + (n-1) + n = \frac{n(n+1)}{2}. \quad (\text{⚡})$$

Nice work! Now, when someone asks you to add every number from 1 to, say 1,000,000 you know that the sum is equal to,

$$\begin{aligned}
 1 + 2 + \cdots + 1\,000\,000 &= \frac{1\,000\,000(1\,000\,000 + 1)}{2} = \frac{1\,000\,001\,000\,000}{2} \\
 &= 500\,000\,500\,000.
 \end{aligned}$$

And you'll impress everyone with your mathematical prowess.

Hey, by the way! Remember triangle numbers from section 0.2.3 on page xix? Well, if you go back, you might notice that each triangular number $t_n = 1 + 2 + \cdots + n$. Thus, equation (⚡) is an equation for triangular numbers too! So we also have the following corollary!

Corollary 2.1: Triangular Numbers

t_n is the n^{th} triangular number if and only if

$$t_n = \frac{n(n+1)}{2}.$$

2.4. But Why Does Induction Work?

Let's run through our proof of our first theorem 2.1. In step (i), we showed in our base case that $P(1)$ was true. Then in step (ii), we showed that $P(n)$ implies $P(n+1)$. Thus, by applying (ii) to (i), we have that $P(1)$ implies $P(1+1) = P(2)$. And by (ii) again $P(2)$ implies $P(2+1) = P(3)$. Which then implies $P(3+1) = P(4)$ and so on... to infinity and beyond!

So how do we know that $P(1,000,000)$ is true? Well, because $P(999,999)$ is true since $P(999,998)$ is true because $P(999,997)$ is true since ... is true since $P(2)$ is true since $P(1)$ was shown to be true in our base case.

It's common for people to make an analogy between induction and a stack of dominoes. In this analogy, step (ii) is making sure that all the dominoes are set up close enough so that they knock each other over. Step (i) is like knocking over the first domino.

2.5. Interesting Inductions

Like with many things in math, in order to truly understand a concept, you must practice it by doing a bunch of examples/problems. This is what we will do now.

Proposition 2.1: The Sum of Consecutive Odd Numbers Equals a Square Number

The sum of consecutive odd numbers equals a square number, more precisely,

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

Remark: A square number is an integer of the form n^2 . For example, the integers: 4, 25, 49, and 100 are all square numbers since, $4 = 2^2$, $25 = 5^2$, $49 = 7^2$, and $100 = 10^2$. However, 8 is not a square number.³

I love this fact! Mainly because there is a great geometric way to think about this, and I encourage you to see if you can come up with a geometric proof! But, for the sake of practicing induction, we won't do the geometric proof here.

³Where do math lovers go on vacation? Times Square!

Proof. We proceed by induction on n . Our statement $P(n)$ is:
 $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.

Base Case: Let $n = 1$. Then $2(1) - 1 = 1$ and we conclude $1 = 1^2$.
 Done!

Induction Hypothesis: Assume that $1 + 3 + \cdots + (2n - 1) = n^2$
 holds for some $n \in \mathbb{N}$.

Inductive Step: We will prove that $P(n + 1)$ is true:

$$GOAL : 1 + 3 + \cdots + (2n - 1) + (2(n + 1) - 1) = (n + 1)^2.$$

Using the inductive hypothesis.

First note $(2(n + 1) - 1) = (2n + 1)$ and now consider the sum
 $1 + 3 + \cdots + (2n + 1)$, which using some algebra and our inductive
 hypothesis becomes,

$$\begin{aligned} 1 + 3 + \cdots + (2n - 1) + (2n + 1) &= \left(1 + 3 + \cdots + (2n - 1)\right) \\ &\quad + (2n + 1) \\ &= n^2 + (2n + 1), \quad \text{by inductive hypothesis} \\ &= n^2 + 2n + 1 \\ &= (n + 1)^2. \end{aligned}$$

Which completes the induction step, and by induction, we are
 done!



Recall in section 0.2.3 on page xix we said that the sum of
 two triangular numbers was a square number? We said that we'd
 come back to this fact when we had the tools to prove it, which
 is now because we have the tools to prove it!

*We will write the following proof like professional mathematicians
 do, which is more 'casual'. By casual, we don't mean that we're go-
 ing to be less rigorous; what we mean is that we won't state explic-
 itly "Base Case", "Induction Hypothesis", and "Induction Step"*

as we have been doing. We will still complete the required steps to fulfill the induction, but we will condense the steps into a single paragraph rather than outlining them as we have been. This allows you to read the proof more like a story.

Proposition 2.2: The Sum of Two Triangular Numbers is A Square Number

The sum of any two consecutive triangular numbers equals a square number. More precisely, let t_n and s_n denote the n^{th} triangular number and square number, respectively. Then

$$t_n + t_{n+1} = s_{n+1}$$

Proof. We proceed by induction on n . Our base case was already shown in section 0.2.3,

$$t_1 + t_2 = 4 = s_2$$

Now assume that $t_n + t_{n+1} = s_{n+1}$ and we will show $t_{n+1} + t_{n+2} = s_{n+2}$.

Recall that $t_{n+1} = t_n + (n + 1)$, we will be using this fact. Observe the following series of steps,

$$\begin{aligned} t_{n+1} + t_{n+2} &= t_n + (n + 1) + t_{n+1} + (n + 1) \\ &= (t_n + t_{n+1}) + (n + 1) + (n + 1) \\ &= s_{n+1} + 2n + 3, && \text{by inductive hypothesis} \\ &= (n + 1)^2 + 2n + 3, && \text{by definition of } s_{n+1} \\ &= n^2 + 2n + 1 + 2n + 3 \\ &= n^2 + 4n + 4 \\ &= (n + 2)^2 \\ &= s_{n+2}, && \text{by definition of } s_{n+2} \end{aligned}$$

Completing the inductive step and the proof!



2.6. STRONG Induction

Sometimes when we are trying to prove something, our usual induction hypothesis: “Assume $P(n)$ is true for some $n \in \mathbb{N}$ ” is not good enough. We need to make the *stronger* induction hypothesis “Assume $P(n)$ is true for all natural numbers less than or equal to $n \in \mathbb{N}$ ”. Note the difference:

Standard: “Assume $P(n)$ is true **for some** $n \in \mathbb{N}$ ”

Strong: “Assume $P(n)$ is true **for all** natural numbers less than or equal to $n \in \mathbb{N}$ ”

When we do this, we are using what is called *strong induction*.

Strong induction is *logically equivalent* to standard induction, and the steps are the same. The only difference is in our induction hypothesis. We will not go through any examples here, and we will usually need only standard induction throughout this book. There is only one exception. In chapter 7, we will need strong induction to prove the Fundamental Theorem of Arithmetic. But we can wait a little while for that!

2.7. Improper Induction

No discussion about induction would be finished without mentioning some pitfalls and mistakes that happen when using induction. There are three main ways that people tend to mess up their induction.

First, no one checks if the base case is correct! There are situations when you can show that $P(n)$ implies $P(n+1)$, where $P(n)$ is never true in the first place! This is like setting up our dominoes and never knocking any of them over!

Second, sometimes you need to check more than one base case. Or, you check the wrong base case. For instance, sometimes we will want to prove that $P(n)$ is true for all $n \geq 10$. In this situation, we let our base case be $n = 10$.

Lastly, sometimes the induction hypothesis is not used or is used incorrectly. For example, notice how we didn't start with n and then modify $P(n)$ to get $P(n+1)$. We started with $P(n+1)$ and then found a way to use $P(n)$. It's a subtle and important difference.

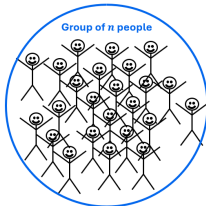
There are many, many great resources out there that show false inductions. Some great examples are found at Brilliant.org if you're interested. To get a taste, here's a variation on one classic:

Everyone is the Same Height!

We will 'prove' that everyone is just as tall as everyone else. More precisely, we will prove the statement $P(n)$: for any group of n people, everyone has the same height.

Base Case:  *Everyone in a group of 1 is the same height!*

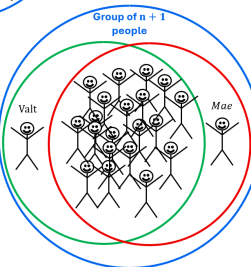
Inductive Hypothesis:



Assume that for any group of n people, everyone that group has the same height.

Inductive Step:

The green circle group has n people. By the inductive hypothesis, everyone in in the green circle group has the same height.



The red circle group has n people. By the inductive hypothesis, everyone in in the red circle group has the same height.

Conclusion: Therefore, everyone in the blue group of $n+1$ people have the same height, completing the induction step!

Base Case: For any group of 1 person, everyone in the group has the same height.⁴

Induction Hypothesis: Assume that for any group of n people, they are all the same height.

Inductive Step: We will use the Inductive Hypothesis to show that any group of $n + 1$ people are all the same height.

Indeed, since for any group of $n + 1$ people, we can take one person out, call that person Valt. Now we have a group of n people, and by our Inductive Hypothesis, everyone in that group has the same height.

Now, let Valt back into the group and take out another person named Mae. We again have a group of n people, and it follows from our Inductive Hypothesis that everyone has the same height.

Bring everyone back together to form our original group of $n + 1$ people. Since everyone had the same height in those two subsets of people, by induction, everyone in the whole group has the same height!

Clearly, this ‘proof’ is false. But why?

Take a moment to look back at the ‘proof’ and the following figure and see if you can find the flaw.

You got it!

The problem is in the inductive step; our reasoning fails when we have $n + 1 = 2$. To see why, consider a group with two people, call them Valt and Mae. When we can take Valt out, then it is true that everyone left in this group of $n = 1$ people (only Mae) has the same height. Now bring Valt back and take out Mae. The same thing happens. Everyone in this group of $n = 1$ (only Valt) has the same height. Here’s the issue: when we bring them together, we have no reason why Valt and Mae should have the same height! It’s very possible that Valt and Mae are not the same height. And since our base case only demonstrated that any group of $n = 1$ people will have the same height, not any group of $n = 2$ people. If, however, our base case concluded that any

⁴ We say statements like that are *vacuously true*.

group of two people has the same height, then it would be true that everyone would have the same height. But it didn't, and therefore, people can have different heights.

Time for a Problem and then a Break!

Induction is an incredible tool; however, to use it, you must be careful, as we have seen. It's very easy to make a subtle mistake; this is one reason why we have peer review in STEM fields!

Let me give you a thought-provoking problem to ponder for practicing your proficiency and prowess with induction.

 **Prove** that you can tile any $2^n \times 2^n$ checkerboard with one square removed using an L-shaped tile: .

I know, I know, this isn't a number theory-esque question, however, I couldn't help myself! This problem is too much fun! You can find the solution on page 181.

Since we began with a Toy Story quote, let's end with one too,

"So long, partner."

- Woody, in Toy Story 3.

Chapter 3

Contradiction

“Success is 1% inspiration, 98% perspiration, and 2% attention to detail.”

– Phil Dunphy on Modern Family (Season 4, Episode 2) 2012.

Introduction

We are continuing to acquire tools for our mathematical tool kits. In this chapter, we learn one of the most useful proof techniques there is: proofs by contradiction.

3.1. What is a Proof by Contradiction?

The basic idea is the following: When writing proofs, we have the following logical reasoning:

When Writing a Proof:

If your starting assumptions are true and your logic is sound, then your conclusion must be correct.

If, on the other hand, you assumed that some information was true and it was, in fact, false, (even if you thought it was true), then your conclusion could be right or could be wrong. It's like Schrödinger's proof! Next, say you did all the research and have a firm foundation of truth to start building your proof upon, but your logic is flawed in the proof—maybe you make some logical leaps—you end up in the same place: your conclusion could be right or wrong.

This probably makes intuitive sense. There doesn't seem to be any way around this statement when writing valid mathematical proofs.

The idea behind using a proof by contradiction is to exploit what we have just discussed.

Say you want to prove some statement using the method of proof by contradiction. First, assume that what you are trying to prove is false (this aligns with our “**assumptions are true**” concept, which we previously discussed). Next, you use all your mathematical know-how to deduce what your assumption implies (this goes into our “**logic is sound**” part of what we already discussed). Finally, if you can prove something you know to be incorrect, then something is amiss. As we already said, **assumptions true + logic sound = correct conclusion**. So if you know that your conclusion is false, then either your assumption was false, or your logic was flawed. But, since we made sure that our logic was airtight, the only option is that our assumption that what we are trying to prove is false is false. I.e., the statement we want to prove is not false, and hence true.

Let's take this for a test drive:¹

¹Forewarning, we will be taking some liberty with the assumptions

Theorem 3.1: There are an infinite number of Integers

There are infinitely many positive integers. Equivalently, there are an infinite number of natural numbers.

Scratch Work. I know what you're thinking! You cannot get more obvious than saying there are infinitely many counting numbers! True, but the point was not to learn some new theorem; it's to show you how to write a proof by contradiction.

Our recipe requires us to start by assuming that what we want to show is false. So, we will assume:

FALSE: There are infinitely many positive integers.

which means we're assuming that the following is true,

TRUE: There are a finite number of positive integers.

Now that we have our starting point, we want to use airtight logic to prove something incorrect—our contradiction. What might this be, and how do we know where to start? This is where your creativity can shine! Math is a **creative endeavor**, and this makes it challenging for everyone, and it is also what makes it fun!

When you're trying to find a contradiction, you will usually find that you need to try a lot of different things before you find a contradiction. And this is great! It's like a good video game level that you need to play a few times to win.

Okay, back to the proof at hand. Our starting point is that there are only a finite number of positive integers. If that's true, what else must be true? Here are some things that I came up with regarding the positive integers:

that we will make regarding the integers. This proof isn't, strictly speaking, a fully rigorous proof of this fact. However, even though this proof is flawed, it still illustrates the steps and *spirit* of a proof by contradiction.

- All the integers are spaced one apart.
- To go from one integer to the next, you only need to add 1 to it.
- The positive integers have a smallest number in them, and it's 1 (this is called the principle of well-ordering, and we will see it come into play later!)
- If there are only finitely many positive integers, then there is also a largest number.

Could you think of anything else? Can you use what we wrote to find a contradiction? Let's walk through it together. Have you ever been in a situation where you, or a classmate, got into the argument:

kid #1: "I'm a million times better at this game than you!"

kid #2 "No I'm 1,000,001 times better than you!"

kid #1: "I'm 1,000,002 times better at this game than you!"

kid #2 "No I'm 1,000,003 times better than you!"

kid #1: "No, I'm infinity times better than you are!"

kid #2: "Oh yeah! Well, I'm infinity plus 1 times better than you!"

etc.

Little did you know that you both were on the verge of using a proof by contradiction to demonstrate that the counting numbers go on forever!

I want you to have a little fun, so see if you can use the idea behind the argument to come up with a contradiction before you read on. Remember, it does NOT matter if you are able to write the proof on your own. What matters is that you tried and had fun!

It's customary, like with proofs using induction, to warn your reader that you are going to do a proof by contradiction. So we will almost always start by writing something like: *Let's assume for the hope of a contradiction.* As you will see, this is the beginning of our proof.

Proof. Let's assume for the hope of a contradiction that there are only a finite number of positive integers. It follows that there must be a largest integer, which we denote by N . Observe that $N + 1$ is also a positive integer and that $N + 1 > N$. This contradicts that we said N was the largest integer! We have reached a contradiction since both of the following cannot be true:

Contradiction: N is the largest integer,
and $N + 1$ is an integer larger than N .

We conclude that there are an infinite number of positive integers.



Beautiful!

This last proof illustrated the key ideas that we will use every time we write a proof using contradictions. Assume what we want to prove is false and find a contradiction. But I bet you want to prove something profound in mathematics, not something as obvious as the existence of an infinite number of counting numbers. What's great is that a lot of beautiful mathematics can be proved using this technique. This is where the next theorem comes in.

3.2. A Beautiful Theorem due to Euclid

Theorem 3.2: An Infinity of Primes

There are infinitely many prime numbers.

This theorem was ranked 3rd on the list of most beautiful math theorems,² and we now have some of the tools needed to prove it as Euclid did back in 300 BC. His proof is considered to be one of the most beautiful in all of mathematics. But, since we haven't learned any number theory yet, we will be relying on

²According to a polling of mathematicians, <https://planetmath.org/thetop10mostbeautifultheorems>.

your intuition regarding prime numbers. But don't worry, we will be covering this proof again in Chapter 7 when we cover prime numbers in detail.

First, recall that a prime number p is an integer whose factors are only 1 and itself p . So 2 and 3 are prime numbers, but 10 is not prime since $10 = 2 \times 5$, i.e., 10 has factors 2 and 5.

Now, how might we prove that there are an infinite number of primes? As you might guess, we will be *assuming that there is only a finite number of primes* and then try to deduce a contradiction. Let's see if we can do something similar to what we did earlier when proving that there are an infinite number of counting numbers.

Try to think about this on your own for a few moments, it's always more fun to try to do it on your own. Even if you are unable to solve the problem.

Recall what helped us find a contradiction when we proved there was an infinite number of positive integers. From our assumption that there was only a finite number of positive integers, we deduced the existence of a largest integer, N . Subsequently, we found an integer, $N + 1$, that's larger than N , reaching our contradiction.

Another way we can think about what we did is as follows: by assuming that there is only a finite number of integers, we can make a complete list of integers (a list that contains every integer): $1, 2, 3, \dots, N$. But then we found a way to make a *new integer* ($N + 1$) that was not on the so-called *complete list*. The contradiction was that we found a positive integer not on the list that was supposed to contain every positive integer. Maybe if we can discover a way to generate primes from primes, we can reach a similar contradiction!

Game plan: We are going to assume that there is only a finite number of primes. From that assumption, we will create a complete list of them. The key is that this list is finite. Our hope is to demonstrate that the list is somehow incomplete and therefore

reach a contradiction. Let's consider some examples to help us discover what to do.

Imagine if the only prime numbers we knew were:

'Complete' List of primes = 2, 3, 5, 7, and 11.

Can we use this list of primes to find a new prime not on our list? Let's run through some of my initial thoughts for what we could do.

We could add all the primes together, and maybe this new number will be a prime too. Unfortunately, $2+3+5+7+11 = 28$, and $28 = 4 \times 7$ is not a prime number. Scratch this idea.

New idea: Primes are connected to multiplication. Recall that a prime number is defined in terms of what its factors are: 1 and itself. Can we somehow use the primes on our list to make a new integer that doesn't have the primes on our list as a factor? Consider what we'd get by multiplying all the primes on our list together.

$$2 \times 3 \times 5 \times 7 \times 11 = 2,310$$

We know that 2,310 is not prime since it has the prime factors 2, 3, 5, 7, and 11 (actually, 2,310 has 32 factors in all when you take into account all the pairs of prime factors you can make).³ What happens if we shift 2,310 by 1, making 2,311?

What are 2,311's factors?

³Whenever you see a power of 2, such as 32, it's fun to see if you can justify why you'd get a power of 2. In this case, it's because 2,310 has five prime factors. Any of 2,310's factors must be of the form: $2^a \times 3^b \times 5^c \times 7^d \times 11^e$ where a, b, c, d, e are 0 or 1. (we will learn why this is true later) Then, by considering all possible choices for a, b, c, d, e , we get $2^5 = 32$ possible factors. For instance $a, b, c, d, e = 1, 0, 0, 0, 0$ or $a, b, c, d, e = 1, 1, 0, 0, 0$ or $a, b, c, d, e = 1, 1, 1, 0, 0$. By listing these, we get 32 possibilities. Haha, a rhyme.

First, can it be possible for 2, 3, 5, 7, or 11 to be a factor of 2,311? No! You can check this, and we will prove a more general statement later (can you guess what that statement is?). As it happens, 2,311 is a prime number! Thus, we have demonstrated that 2, 3, 5, 7, and 11 were an incomplete list and found our contradiction.

Are we done? Did we just find a way to generate new prime numbers?!?

Not so fast, we got lucky in this situation. Suppose we “knew” that 13 was also a prime number back at the beginning. Then our complete list would have been:

‘Complete’ List of primes = 2, 3, 5, 7, 11, and 13.

Considering the product of all of these, we now get,

$$2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30,030.$$

Adding 1 to the product gives 30,031. Unfortunately, 30,031 is not prime since primes 59 and 509 are its factors,

$$30,031 = 59 \times 509.$$

Gosh darn it! We thought we had a way to generate new primes, but now it seems like we will also generate composite (non-prime) numbers. Back to the drawing board? Before we scrap our work, how did we know that 50 and 509 are prime numbers? We shouldn’t because they aren’t on our list of primes: 2, 3, 5, 7, 11, and 13. So, we did in fact find new prime numbers, they just didn’t end up being the product (30,031), they ended up as factors of the product!

To write out our proof, we will show that one of two things can happen: either our product plus one is a prime not on our list, or it’s divisible by a new prime number not on our list. In either case, we have found a new prime not on the list, therefore reaching the contradiction:

Our list was a complete list of prime numbers,
and we found a prime number not on our list.

Proof of Theorem. Assume for the hope of a contradiction that there are only a finite number of prime numbers. Let's list all of them,

$$p_1, p_2, p_3, \dots, p_n.$$

Note that this list is assumed to be complete. Now consider the product of all these primes plus 1,

$$N = (p_1 \times p_2 \times \dots \times p_n) + 1$$

First, **we claim that no primes in our list are a factor of N .** To see this, we will use another proof by contradiction (wow, our proof is like a proof by contradiction fractal).

Assume for the hope of a contradiction that some prime p_i on our list was a factor of N . Since p_i is a factor of N we it must be that p_i divides N , or N is equal to p_i times some other number k ,

$$N = p_i \times k$$

This is the definition of what we mean when we say a number is a factor of another number. For example, 7 is a factor of 14 because we can write $14 = 7 \times 2$.

Let's equate the two product forms of N ,

$$N = p_i \times k = (p_1 \times p_2 \times \dots \times p_i \times \dots \times p_n) + 1.$$

Since the order of multiplication doesn't matter, let's move p_i to the front,

$$\begin{aligned} N = p_i \times k &= (p_1 \times p_2 \times \dots \times p_i \times \dots \times p_n) + 1 \\ &= p_i \times (p_1 \times p_2 \times \dots \times p_{i-1} \times p_{i+1} \times p_n) + 1. \end{aligned}$$

Let's subtract $p_i \times (p_1 \times p_2 \times \dots \times p_n)$ from both sides and then group all of the terms with p_i together,

$$p_i \left(k - (p_1 \times p_2 \times \dots \times p_n) \right) = 1$$

But this makes no sense! Since the product on the left is between two positive integers, it cannot equal 1, unless both of the integers are equal to one. This isn't the case since p_i is prime and hence is at least 2. Thus, it must be the case that none of our primes is a factor of N .

Almost done

Now that we've established that none of the numbers on our list are factors of N , there are two cases to consider: either N is prime or N is not prime! When N is prime, we're done, since N is not on our list, contradicting that our list was supposed to be a complete list of all the primes! (This was like when $N = 2, 311$.)

For the second case, suppose that N is not prime. Then by definition, N must have a prime factor (since N has to have factors other than 1 and N). But, as we've already shown, no primes on our list can be N 's factors. Thus, our list is incomplete because it's missing N 's prime factors. (This was like when $N = 30, 031$.)

In either case, we have shown that our list is incomplete and therefore reached a contradiction. Thus, our original assumption was false, and hence there are infinitely many primes.



3.3. Final Thoughts

Proofs using contradiction are essential, incredibly useful, and a lot of fun. Whenever we have a statement such as: *for all blank blah blah blah*, it's usually a good idea to try a proof by contradiction to start. This is because the assumption gives you a starting point. For example, in our proof of the infinitude of primes, assuming there was only a finite number gave us the ability to make a 'complete' list of them.

To convey how important this proof technique is, consider this quote from the great mathematician G. H. Hardy (yes, the same Hardy who worked alongside Srinivasa Ramanujan), because he said it best:

“[A proof by contradiction] is a far finer gambit than any chess gambit”

- G. H. Hardy

However, just like with induction, we need to end on a word of warning. Sometimes it's so tempting to try to use a proof by contradiction when you aren't sure where to start that you can end up in a situation where you didn't end up using the assumption that the statement you want to prove was false. This would mean that you didn't actually use a proof by contradiction, even though you wanted to. This is totally fine; there is no reason why you need to use one proof method over another (unless you're in a proof class and your professor told you to use one method over another). So, when you write a proof using a contradiction, double-check to see if you used all your assumptions; if not, then rewrite your proof without the unused assumptions. As Ernest Hemingway almost said, *the only kind of proof writing is proof rewriting*. Well, he actually said, "The only kind of writing is rewriting".

Chapter 4

The Division Algorithm

“There is nothing more deceptive than an obvious fact.”

- Sherlock Holmes

Introduction

Today’s a very special day! We’re about to start our discussion of number theory! We’re done with building our tool kit!

However, to begin, we must begin at the beginning!¹ So in this chapter, we will be covering some stuff that is not the *most interesting* math in the world, but it’s math that is needed in order to get to more fun math! For this reason, I want to make it clear that:

you can skip the proofs in this chapter!

The definitions, theorems, principles, etc., are the most important information to take from this chapter. The proofs were left in so

¹ To quote Lewis Carroll, “Begin at the beginning and go on till you come to the end; then stop.” [4]

that you can practice reading/understanding proofs. If you are interested, feel free to pursue them; if not, you can always come back later—that’s perfectly fine! This is truly a self-guided lesson plan! For those who are planning on skipping the proofs, there will be a list of results on page 51.

Our first goal is to learn about the *division algorithm*, which basically says that *you can take any two integers and divide them* (BUT DON’T DIVIDE BY ZERO) and your answer will be in the form of a (Quotient) and (Remainder). This is probably obvious to you because you’ve done this since you were in the 4th grade, and this is why you can skip the proof.

In order to prove the division algorithm, we look to what is called *well-ordering* for help. If you have already read Appendix A: Induction and Well-Ordering, then you are familiar with well-ordering. If not, go read the appendix first! Jk jk, it’s in the appendix and not the main book for a reason. Let’s discuss the well-ordering principle.

4.1. Why are the Natural Numbers *Well-Ordered*?

Let’s begin with a question: what observations can you make regarding *non-empty subsets* of the natural numbers? For example, what do the following sets have in common:

$$\mathbb{E} = \{2, 4, 6, 8, \dots\}$$

$$S = \{5, 120, 200\}$$

and

$$T = \{10\}.$$

Did you notice that the subsets $\mathbb{E}$, S , and T all have a *smallest number*, or *least element* in them? The number $2 \in \mathbb{E}$ is the smallest even number, $5 \in S$ is the smallest number in $S = \{5, 120, 200\}$, and $10 \in T$ is the smallest number in $T = \{10\}$.

Challenge: *Can you think of a non-empty subset of $\mathbb{N}$ that does NOT have a smallest number?*

Take a moment to ponder this and then turn the page.

I hope you weren't able to find a subset without a smallest number, since the well-ordering principle says it's impossible!

The Well-Ordering Principle: Every non-empty subset of natural number(s) contains a smallest number, or *least element*. Simple.

It's worth mentioning that some people consider 0 to be a natural number. We won't consider 0 to be a natural number, but we do want to have a set that contains the natural numbers and 0. So, we denote this set of numbers $\mathbb{W} = \{0, 1, 2, 3, \dots\}$ and call them the *whole numbers*.² Since $\mathbb{W}$ is basically the same as $\mathbb{N}$ (with zero put into, or unioned into, the set), well-ordering still applies to $\mathbb{W}$.³

The Well-Ordering Principle (Whole Number Version): Every non-empty subset of whole number(s) contains a least element. Simple, again!

An example of a set that we've seen that is not well-ordered is the set of integers $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$. It doesn't matter what number you choose from $\mathbb{Z}$, there is always a number smaller than it in $\mathbb{Z}$. Furthermore, the subset of even integers: $\{\dots, -4, -2, 0, 2, 4, \dots\}$ has no least element either.

4.2. The Division Algorithm (Intuition)

Do you remember wayyyy back when you learned how to divide two numbers, how your teacher wanted you to write your answer with a remainder? It's probably been a while since you've done this, so let's do two examples to jog your memory.

²Note how $\mathbb{W} = \mathbb{N} \cup \{0\}$.

³To the person who invented the number 0, thanks for nothing!

If we divide 43 by 10 we should get,

$$43 \div 10 = 4 \text{ R}3.$$

This is equivalent to,

$$43 = (4 \times 10) + 3.$$

Where we call 4 the **quotient** and 3 the **remainder**. Now consider what we get when we divide 201 by 26,

$$201 \div 26 = 7 \text{ R}19 \qquad \text{or} \qquad 201 = (7 \times 26) + 19.$$

Basically, choose any two natural numbers n and m , and you can divide them in such a way that you can always find a quotient q and a remainder r pair such that $0 \leq r < m$ (if you are doing $n \div m$). Furthermore, the quotient and remainder are unique (i.e., division problems have only one answer)!

Okay, the last paragraph was a lot to take in, so let's illustrate with our example setting $n = 43$ and $m = 10$.

$$\text{Dividend} = (\text{Quotient}) \times (\text{Divisor}) + \text{Remainder}$$

$$43 = (4 \times 10) + 3$$

$$43 - \text{Dividend} = n$$

$$10 - \text{Divisor} = m$$

$$4 - \text{Quotient} = q$$

$$3 - \text{Remainder} = r$$

Observe how the remainder 3 satisfies the inequality $0 \leq 3 < m = 10$. Also note that the only possible quotient q equals 4 and the only possible remainder r such that $0 \leq r < m = 10$ equals 3.

Similarly, for $n = 201$ and $m = 26$, we already found

$$\underbrace{201}_n = \left(\underbrace{7}_q \times \underbrace{26}_m \right) + \underbrace{19}_r.$$

Note $0 \leq 19 < 26$, and there are no other quotients/remainders other than $7R19$ that will be correct.

This is the main point of the division algorithm for natural numbers, that there exists a quotient and a remainder, q and r , such that $n = mq + r$ with $0 \leq r < m$.

The division algorithm also works with negative integers! For example, consider $n = -100$ and $m = 12$. Then, because

$$-100 = (-9 \times 12) + 8$$

we say that $-100 \div 12 = -9R8$. It's important that you notice that our remainder is still positive, $r = 8$, and that $0 \leq 8 < m$. If it were the case that m was negative, then we'd have to rewrite the inequality to be $0 \leq r < |m|$. As in the example,

$$\underbrace{123}_n = \underbrace{(-12 \times -10)}_q + \underbrace{3}_r.$$

so that $0 \leq 3 < |-10|$.

If we can prove that we can divide two positive integers, it makes sense that we could generalize to all integers. For this reason, we aim to prove the division algorithm for positive integers. Spoiler Alert: the proof relies on the well-ordering principle.

Theorem 4.1: The Division Algorithm

Let n and $m \neq 0$ be integers, then you can always find integers q and r , called the quotient and remainder respectively, such that

$$n = (m \times q) + r, \quad \text{where } 0 \leq r < |m|.$$

Furthermore, the integers q and r are unique.

Scratch Work. How do we prove this? Well, the only tool mentioned in this chapter is the well-ordering principle. So it makes

sense that we might want to restrict our focus to subsets of natural numbers, and since our goal is, in part, to find a positive remainder $r \geq 0$ it might make sense to solve $n = mq + r$ for r . For this reason, we will consider the set of whole numbers of the form $r = mq - n$ where we will be varying q —as to not confuse q with what will be our quotient, we use the label t ,

$$S = \left\{ (n - mt) \mid n - mt \geq 0 \text{ and } t \in \mathbb{W} \right\}.$$

Since we are considering only when $n - mt \geq 0$, all the numbers in S are in $\mathbb{W}$. Therefore, S is a subset of $\mathbb{W}$.

For example, let's still use $n = 43$ and $m = 10$. Our set S is,

$$\begin{aligned} S &= \left\{ \underbrace{43 - 10(0)}_{t=0}, \underbrace{43 - 10(1)}_{t=1}, \underbrace{43 - 10(2)}_{t=2}, \underbrace{43 - 10(3)}_{t=3}, \right. \\ &\quad \left. \underbrace{43 - 10(4)}_{t=4} \right\} \\ &= \{43, 33, 23, 13, 3\} \\ &= \{3, 13, 23, 33, 43\}. \end{aligned}$$

Notice how the smallest number in our set S is equal to 3. Hmm... where else did the number 3 show up? Recall $43 = (4 \times 10) + 3$, so it turns out the smallest number in S is equal to 3, which is also the remainder we get from the division algorithm with $n = 43$ and $m = 10$: Maybe this always happens? Indeed it does! This is the key idea, and it's our aim of attack! By well-ordering (second version), we can guarantee that there is a smallest number in S , and it just so happens that this number is the remainder r we want!

Proof of the Division Algorithm. Let n and m be natural numbers. We will break up our proof into two parts: (1) showing q and r exist with the desired properties, and (2) showing q and r are indeed unique. Forewarning, most of our work will be in step (1).

Part (1). Existence of q and r

Consider the set,

$$S = \left\{ (n - mt) \mid n - mt \geq 0 \text{ and } t \in \mathbb{W} \right\}.$$

We want to use well-ordering (whole number version) to conclude that there is a smallest element.

Recall, in order to use well-ordering, our set S must be non-empty and a subset of $\mathbb{W}$. Since we already know that S is a subset of $\mathbb{W}$, all we need to show S is always non-empty. We will accomplish this by showing that there is always at least one number in S .

To this end, consider when $t = 0$. Then $n - m(0) = n > 0$ since $n \in \mathbb{N}$. Therefore, we now know $n \in S$ always, and hence the set S is not empty.

We can now use the well-ordering principle (whole numbers version) to conclude that there is a smallest number in S . Let's denote this minimum element by something memorable... how about the letter r .

$$r := \min \{S\}.$$

For some choice of t we have $n - mt = r \in S$, and because we are already labeling the minimum number in S by the letter r , let's also label the choice of t that gives r by the letter q . That is, there is some $q \in \mathbb{W}$ such that,

$$n - mq = r = \min \{S\}.$$

We're almost there; we only need to show that $0 \leq r < m$, as stated in the division algorithm.

With this goal in mind, let's assume for the hope of a contradiction that $r \geq m$. We will show that this implies that there is an $r' \in S$ that is smaller than r . Indeed, let $r' = r - m$ and note that $r' \geq 0$ since we are assuming $r \geq m$. Now consider what

happens when we change q to $q + 1$ in the expression $n - mq = r$.

$$n - m(q + 1) = \underbrace{n - mq}_{=r} - m = r - m = r' > 0.$$

Therefore $n - m(q + 1) = r' \in S$ since $n - m(q + 1) > 0$. But wait, it cannot be that $r' \in S$ and $r' < r = \min\{S\}$. Thus, we found our contradiction! Hence, it must be that $0 \leq r < m$ as desired.

Step (2). Uniqueness of q and r

To demonstrate uniqueness, our game plan is to act like there are two different quotient and remainder pairs, q, r and q', r' , and then show that they are actually the same, $q = q'$ and $r = r'$.

To this end, assume there are numbers q, r, q', r' such that,

$$n = mq + r = mq' + r'$$

where $0 \leq r < m$ and $0 \leq r' < m$. Since we are thinking of r, r' as different numbers, let's choose to label them so that $r \leq r'$. With some rearranging, we see,

$$m(q - q') = r' - r.$$

Since $0 \leq r \leq r' < m$, it follows that $0 \leq r' - r < m$. Furthermore, $q - q' \geq 1$ since if it were not the case, then we'd have⁴ $q - q' \leq 0$ which implies $r \geq r'$, a contradiction. Altogether, we have shown,

$$m = m(1) \leq m(q - q') = r' - r < m.$$

Which is the statement $m < m$, which is a contradiction! Thus, $q = q'$ and $r = r'$. Concluding the proof.



⁴This is because it's not true that $q - q' \geq 1$. It follows that it is true that $q - q' < 1$. And the first integer less than 1 is 0, hence $q - q' \leq 0$.

And just like that, we can divide any two natural numbers n and m to get a unique quotient and remainder.

Take a moment to think back to how vital the well-ordering principle was in the proof. Remember, it was used to show that there was a smallest number in our set S which was the remainder we wanted. Well-Ordering, thank you again for coming in clutch!

4.3. Why Was This Necessary?

I know that many of you who decided to read the proofs given in this chapter are thinking, “*Why did we have to go through so much work to prove something so obvious?*” To that I say, I agree! This seems to be a lot of work for very little payoff.

But there is a reason.

At some point, we may start to ask questions that end up being answered more easily by using functions such as polynomials or complex numbers, instead of using integers (just take my word for the moment). When we get to this point, we will be confronted with the question: Is there an analogous division algorithm for polynomials? What about a division algorithm for complex numbers? If you remember polynomial or synthetic division, you can say “Yes, there is a division algorithm for polynomials.” But what about complex numbers: $n = a + ib$ and $m = c + id$ where a, b, c, d are integers and $i = \sqrt{-1}$. Can you divide n and m to find some q and r ? The answer is a little less obvious huh? If I gave you two specific complex numbers, you might find a way to divide them, but could you guarantee that no matter which two complex numbers I gave you, you’d be able to find a way?

I’ll let you ponder if there is a division algorithm for complex numbers. I’ve left enough breadcrumbs that with some time (okay, a lot of time), you might be able to convince yourself of the answer. However, you might find it hard to prove your answer.

Anywho, let me get back on my soapbox.

The crux of the matter is this: by proving the obvious, we

can develop tools and intuition for the less obvious. The tools we use and the intuition we gain are what we care about here, not necessarily the result, since you probably knew how to divide before you picked up this book anyway.

Lastly, division algorithms appear in various forms and contexts that may not resemble traditional division. One of these forms is called modular arithmetic. Don't worry if you are unfamiliar with modular arithmetic, we will cover it soon in chapter 8, but for those who already know a little about modular arithmetic, saying 23 is congruent to 2 (mod 3) is the same thing as saying that 23 has a remainder of 2 when divided by 3.

Remainders are important, huh!

4.4. List of Takeaways From Chapter 4

The Well-Ordering Principle: Every non-empty subset of natural number(s) contains a smallest number, or *least element*. Simple.

The Well-Ordering Principle (Whole Number Version): Every non-empty subset of whole number(s) contains a least element. Simple, again!

Theorem 4.2: The Division Algorithm

Let n and $m \neq 0$ be integers, then you can always find integers q and r , called the quotient and remainder respectively, such that

$$n = (m \times q) + r, \quad \text{where } 0 \leq r < |m|.$$

Furthermore, the integers q and r are unique.

Chapter 5

The Euclidean Algorithm

“[The Euclidean algorithm is] the granddaddy of all algorithms, because it is the oldest nontrivial algorithm that has survived to the present day.”

– Donald Knuth.

In this chapter, we talk about everything Euclidean, well, except for Euclidean geometry! We’re going to learn about another algorithm, which is a very useful tool to find common divisors of two integers. More than that, it can be used to find all combinations of those integers! But I’m getting ahead of myself. We’ll start at the beginning and discuss the Euclidean Algorithm and the greatest common divisor.

5.1. Some Notation

5.1.1 Divisors

Like any branch of mathematics, there are certain notational conventions that have become standard, and number theory is no

different. We want a shorthand for when a number is a *divisor* of another number.

For example, 5 is a divisor of 15. Likewise, 24 is a divisor of 96. Another way to say these two facts is: 5 divides 15 and 24 divides 96. The way we write this shorthand is the following:

Definition 5.1: Divisor $d \mid n$.

Let n and d be integers. If $n = dk$ for some integer k , then we say d divides n , or that d is a *divisor* of n , and we write $d \mid n$. Hence, the following two are equivalent statements:

$$d \mid n \iff n = dk.$$

We also say that n is a *multiple* of d .

With the numbers we were using, we can now write:

$$5 \mid 15 \quad \text{since} \quad 15 = 5(3)$$

and

$$24 \mid 96 \quad \text{since} \quad 96 = 24(4).$$

5.1.2 The Greatest Common Divisor

When I was in elementary school, I would always confuse *the greatest common divisor* and *the least common multiple*. Both are important (and related to one another), but we will focus on the greatest common divisor today.¹

If you remember from school, the greatest common divisor of integers n and m is the largest integer that divides both n and m .

¹Okay, I couldn't help myself. Let a and b be positive integers, then the connection between the greatest common divisor and least common multiple is $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$ where $\text{lcm}(a, b)$ is the least common multiple of a and b .

For example, the greatest common divisor of 30 and 42 is equal to 6, since (i) both 30 and 42 are divisible by 6 and (ii) no number larger than 6 divides 30 and 42.

In elementary school, the way I found the greatest common divisors was by listing the divisors of each number and finding the integers common to both lists. Let's continue using 30 and 42, I would have listed out the following:

$$\begin{aligned} 30 &: \boxed{1}, \boxed{2}, \boxed{3}, 5, \boxed{6}, 10, 15, 30 \\ 42 &: \boxed{1}, \boxed{2}, \boxed{3}, \boxed{6}, 7, 14, 21, 42 \end{aligned}$$

Where the boxed numbers are the ones that are common between the two lists, then I'd search for the greatest common number on the lists. In this case, 6 is the greatest common number. Thus, the greatest common divisor of 30 and 42 is equal to 6. Not bad...

This method of listing out factors is surefire; however, it's not always the best approach. For example, suppose that I asked you to find the greatest common divisor of the two large numbers, like 1,231,872,638,162 and 9,287,391,721,397. How would you write out the factor lists? You'd need to know the prime factorization of both numbers to even start. Not good.

This is where the Euclidean Algorithm comes into play. It's a series of steps that allow us to find the greatest common divisor of two numbers **without needing to do any factorization**. Yup, you read that correctly, NO FACTORIZING. However, its downside is that it can require a lot of steps. Sometimes, it's easier just to factor the numbers, so the Euclidean algorithm is not perfect. For instance, if all I needed was the greatest common divisor of 30 and 42, I would not use the Euclidean Algorithm, because factoring 30 and 42 is easy. But for numbers like 1,231,872,638,162 and 9,287,391,721,397, I would use the Euclidean Algorithm because factoring these numbers is much harder to do.

The Euclidean Algorithm also has some other advantages. But let's leave this for the section Mysterious Motivation and the next chapter.

Before we move on, let's write out the definition of the greatest common divisor.

Definition 5.2: The greatest common divisor

The greatest common divisor $d \in \mathbb{N}$ of two integers, a and b is the natural number that satisfies the two conditions:

- (i) d is a divisor of both a and b , i.e. $d \mid a$ and $d \mid b$, and
- (ii) For any other common divisor d' of a and b ($d' \mid a$ and $d' \mid b$), it must be $d' \leq d$.

If d satisfies both criteria, then we write $\gcd(a, b) = d$.

Previously, we said 6 was the greatest common divisor of 30 and 42. This is because (i) $6 \mid 30$ and $6 \mid 42$, and (ii) all the common factors of 30 and 42, (which are 1, 2, 3, 6), are less than 6, i.e., 6 is the largest common divisor. Thus, we have $\gcd(30, 42) = 6$.

Example 1. Consider $a = 100$ and $b = 75$. Then

$$\begin{aligned} 100 &: \boxed{1}, 2, 4, \boxed{5}, 10, 20, \boxed{25}, 50, 100 \\ 75 &: \boxed{1}, 3, \boxed{5}, 15, \boxed{25}, 75 \end{aligned}$$

Note that $\gcd(100, 75) = 25$ since $25 \mid 100$ and $25 \mid 75$, as well as the fact that $1 < 5 < 25$. ■

Note: The little black box ■ is used to denote the end of an example. Similar to how we use  to denote the end of a proof. We will be using this symbol often!

Let's consider what would happen when b divides a , that is $b \mid a$. For example, let $a = 15$ and $b = 5$. We have $5 \mid 15$. Now let's determine $\gcd(15, 5)$. The factors of 5 are 1 and 5, and the

factors of 15 are 1, 3, 5, and 15. The largest among the shared factors is 5, which is b itself! Thus $\gcd(15, 5) = 5$.

Similarly, $\gcd(36, 12) = 12$ since $12 \mid 36$ and $\gcd(150, 30) = 30$ because $30 \mid 150$.

As it happens, this happens every time $b \mid a$, in fact, this will be our first lemma!

Lemma 5.1: Our First Lemma! $b \mid a \implies \gcd(a, b) = b$

Let a and b be positive integers. If $b \mid a$, then $\gcd(a, b) = b$.

Proof. Let $b \mid a$. By definition 5.1 a is a multiple of b , hence there is some integer $k \in \mathbb{Z}$ such that $a = bk$. We aim to prove that $\gcd(a, b) = b$ using definition 5.2. To accomplish this, we must show (i) b divides both a and b and (ii) for any other divisor of a and b , b is the largest.

(i) By assumption $b \mid a$. Furthermore, since $b = b \times 1$ it's also the case that $b \mid b$. Hence b divides both a and b .

(ii) Let d' be another common divisor of both a and b , that is $d' \mid a$ and $d' \mid b$. We need to show that $d' \leq b$. Indeed, since $d' \mid b$ implies that $d' \leq b$.²

We have shown both parts of definition 5.2, therefore we conclude that $\gcd(a, b) = b$.



² This is because $d' \mid b$ implies $d' = bt$ for $t \in \mathbb{Z}$ (using the definition of a divisor). If $d' < 0$, then we clearly have $d' < 0 < d = b$. On the other hand, when $d' > 0$, it must be that $t > 0$ too. It follows that $t \geq 1$ and hence, $b = d't \geq d' \cdot 1 = d'$.

5.2. The Euclidean Algorithm

The Euclidean Algorithm is confusing notationally in its explanation; however, once you get the hang of it, actually carrying out the steps isn't so bad. Here's the idea: we have integers a and b with $a > b$, and our goal is to find the greatest common divisor of a and b , that is $\gcd(a, b)$. First, we use the division algorithm to conclude that there are $q_0 \in \mathbb{Z}$ and $r_0 \in \mathbb{Z}$ such that,

$$a = q_0 b + r_0 \quad \text{where } 0 \leq r_0 < b.$$

Next, we turn our attention to the remainder r_0 . Two things can happen: either $r_0 = 0$ or $r_0 \neq 0$. When $r_0 = 0$, we are done, since this implies $a = q_0 b$ and hence a is a multiple of b and hence $\gcd(a, b) = b$ by Our First Lemma 5.1. When $r_0 \neq 0$ we have some more work to do. So, let's assume $r_0 \neq 0$.

★ Here's the key claim: If $r_0 \neq 0$, then $\gcd(a, b) = \gcd(b, r_0)$. ★

If this observation is true, then we can shift our attention to finding $\gcd(b, r_0)$, which is useful since $r_0 < b < a$ and we are better at factoring smaller numbers. However, sometimes we still cannot factor b and r_0 . But don't fret, since $r_0 \neq 0$ we can play the same game with the division algorithm:

$$b = q_1 r_0 + r_1 \quad \text{where } 0 \leq r_1 < r_0$$

Like earlier, if $r_1 = 0$ then $b = q_1 r_0$ and we would conclude $\gcd(a, b) = \gcd(b, r_0) = r_0$ and be done. If we're not so lucky and $r_1 \neq 0$, we claim a similar statement to what we claimed earlier:

★ If $r_0 \neq 0$, then $\gcd(a, b) = \gcd(b, r_0) = \gcd(r_0, r_1)$. ★

Like before, we have found smaller numbers ($a > b > r_0 > r_1$) to work with when finding $\gcd(a, b)$!

We might have gotten lucky enough to be able to factor r_0 and r_1 , but who cares! This is too much fun! If $r_1 \neq 0$, we use the division algorithm again, and if the next reminder $r_2 \neq 0$ we do the same thing again, and then again. . .

. . . and again, and again, and again, as long as the remainders are nonzero. In the process, let's not worry whether or not we can factor our new, smaller numbers at each step. Carrying this process out, we eventually end up with a remainder that equals zero,

$$\begin{array}{ll}
 a = q_0 b + r_0, & \text{where } 0 < r_0 < b \\
 b = q_1 r_0 + r_1, & \text{where } 0 < r_1 < r_0 \\
 r_0 = q_2 r_1 + r_2, & \text{where } 0 < r_2 < r_1 \\
 r_1 = q_3 r_2 + r_3, & \text{where } 0 < r_3 < r_2 \\
 r_2 = q_4 r_3 + r_4, & \text{where } 0 < r_4 < r_2 \\
 \vdots & \vdots \\
 r_{n-1} = q_{n+1} r_n + r_{n+1}, & \text{where } 0 < r_{n+1} < r_n \\
 r_n = q_{n+2} r_{n+1} + \overbrace{r_{n+2}}^{=0}, & \text{where } r_{n+2} = 0.
 \end{array}$$

Each remainder is nonzero until we reach a point where some remainder r_{n+2} equals zero. When this happens, we're finally done, since all the previous remainders are nonzero ($r_0, r_1, \dots, r_{n+1} \neq 0$) we claim that the sequence of greatest common divisors are such that:

$$\star \gcd(a, b) = \gcd(b, r_0) = \gcd(r_0, r_1) = \dots = \gcd(r_n, r_{n+1}). \star$$

where the integers are decreasing:

$$a > b > r_0 > r_1 > r_2 > \dots > r_{n+1} > r_{n+2} = 0.$$

Note that every claim that's marked with $\star$ is really the same claim, just applied at each step.

Furthermore, since $r_{n+2} = 0$, we notice that $r_n = q_{n+2} r_{n+1}$. It follows from Our First Lemma 5.1 that $\gcd(r_n, r_{n+1}) = r_{n+1}$. And, if each claim $\star$ is true, then,

$$\gcd(a, b) = \gcd(b, r_0) = \gcd(r_0, r_1) = \dots = \gcd(r_n, r_{n+1}) = r_{n+1}$$

And we're done! The greatest common divisor between a and b is equal to the last non-zero remainder r_{n+1} .

But did you notice that we made an assumption that was not marked with a ★? We implicitly assumed that at some point the steps would come to an end when a remainder would equal zero, in this case $r_{n+2} = 0$. We didn't justify this step; however, the process does come to an end. We can see this is the case since all of these remainders are sandwiched between zero and the previous remainder. That is, each remainder is positive (or zero) and strictly smaller than the previous; they form a set of decreasing integers:

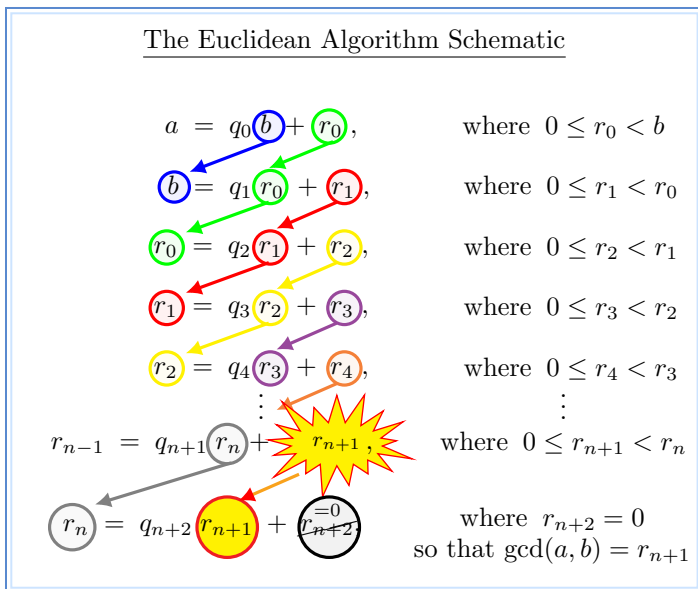
$$\overbrace{a > b > r_0 > r_1 > r_2 > \cdots > r_{n+1} > r_{n+2}}^{\text{All in } \mathbb{N}} \geq 0.$$

And since there are only finitely many integers less than a and greater than 0 (namely $0 < 1, 2, 3, \dots, a-1 < a$), the process must come to an end when some remainder reaches zero after at most a steps.³

Our biggest series of assumptions were the claims marked with the stars ★. Once we show that every claim made with the ★ above is true, then we're done! We have found The greatest common divisor, $\gcd(a, b) = r_{n+1}$ without factoring! This is the Euclidean algorithm, we progressively use the division algorithm in order to find smaller and smaller numbers to use to find the greatest common divisor, which ends up being the last nonzero remainder from the division algorithm.

Let's do an example, and then we'll go through the proof. But, to make the algorithm easier to follow, here is a schematic:

³For example, if $a = 10$, then the worst possible number of steps would lead to: $a = 10, b = 9, r_0 = 8, \dots, r_{6+2} = 0$.



Where we'd conclude $\gcd(a, b) = r_{n+1}$.

Example 2. Let's use the Euclidean algorithm to deduce the value of $\gcd(59, 301)$.

Remember, we progressively use the division algorithm, and the last nonzero remainder is the greatest common divisor.

$$\begin{aligned}
 301 &= 5(59) + 6, \\
 59 &= 9(6) + 5, \\
 6 &= 1(5) + 1, \\
 5 &= 5(1) + 0,
 \end{aligned}$$

or with color

$$\begin{aligned}
 301 &= 5(59) + 6, \\
 59 &= 9(6) + 5, \\
 6 &= 1(5) + 1, \\
 5 &= 5(1) + 0,
 \end{aligned}$$

Thus, $\gcd(59, 301) = 1$. ■

Example 3. Let's try another one. Let's determine $\gcd(142, 262)$.

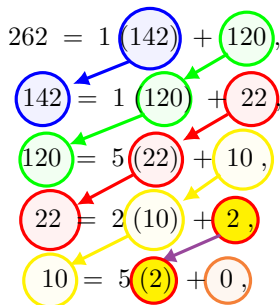
$$262 = 1(142) + 120,$$

$$142 = 1(120) + 22,$$

$$120 = 5(22) + 10,$$

$$22 = 2(10) + 2,$$

$$10 = 5(2) + 0, \quad \text{with color}$$



Thus $\gcd(142, 262) = 2$. ■

5.3. Euclidean Algorithm “Proof”

Lemma 5.2: Our Claims ★

Let a and b be positive integers with $a > b$. By the division algorithm, we have

$$a = q_0b + r_0 \text{ where } 0 \leq r_0 < b.$$

Then $\gcd(a, b) = \gcd(b, r_0)$.

Scratch Work. Let's denote $\gcd(a, b) = d_1$ and $\gcd(b, r_0) = d_2$. Our goal is to ultimately show that $d_1 = d_2$. How might we go about this? Well, since $r_0 = a - q_0b$, maybe we can show that any common divisors of a and b are also divisors of r_0 . Likewise, any common divisor of b and r_0 is a divisor of a . In other words,

*d is a common divisor of a and b
if and only if
d is a common divisor of b and r_0 .⁴*

This iff statement will imply our lemma because of part (ii) in definition 5.2. That is, “ $d_1 \mid a$ and $d_1 \mid b$ ” implies “ $d_1 \mid b$ and $d_1 \mid r_0$ ” (by the above if and only if statement). Hence, $d_1 \leq d_2$ since $\gcd(b, r_0) = d_2$. Similarly, “ $d_2 \mid b$ and $d_2 \mid r_0$ ” implies “ $d_2 \mid a$ and $d_2 \mid b$ ” (again, by the above if and only if statement), hence $d_2 \leq \gcd(a, b) = d_1$. Thus, we have shown both $d_1 \leq d_2$ and $d_2 \leq d_1$, which together imply $d_1 = d_2$.

There was a lot of algebraic gymnastics in that last paragraph, so feel free to reread it a few times as needed. Once you feel ready, you can move on to the proof!

Proof. Let a and b be positive integers with $a > b$ and let’s denote $\gcd(a, b) = d_1$ and $\gcd(b, r_0) = d_2$. We will show $d_1 = d_2$ by proving

*d is a common divisor of a and b
if and only if
d is a common divisor of b and r_0 .*

Forward: If d is a common divisor of a and b , then d is a common divisor of b and r_0 .

Consider some common divisor d of a and b . By the definition of a divisor, $d \mid a$ and $d \mid b$ are equivalent to the statements $a = dk$ and $b = dt$ for integers k and t . Keep this in mind.

Recall the division algorithm (on page 46) tells us there exist integers q_0 and r_0 such that:

$$a = q_0b + r_0 \quad \text{where } 0 \leq r_0 < b.$$

⁴This is one of special **if and only if** statements we mentioned in section 1.9 on page 8. This means that we have to prove two separate statements.

- (i) if d is a common divisor of a and b , then d is a divisor of b and r_0 , and
- (ii) if d is a common divisor of b and r_0 , then d is a divisor of a and b .

Solving for r_0 we get,

$$r_0 = a - q_0b.$$

Recall $a = dk$ and $b = dt$, which we can use to conclude,

$$r_0 = a - q_0b = dk - q_0dt = d \overbrace{(k - q_0t)}^{\text{integer}}.$$

Since $k - q_0t \in \mathbb{Z}$ it follows that d is a divisor of r_0 —since r_0 has the form: $d \cdot (\text{integer})$.

Backwards: If d is a common divisor of b and r_0 , then d is a common divisor of a and b .

The proof of the backward direction is the same as the forward direction, for the most part... So, I challenge you to finish this proof!

Here's the upshot, since d is a common divisor of a and b if and only if d is a divisor of b and r_0 , it must be that $\gcd(a, b) = \gcd(b, r_0)$ from the reasoning that we discussed in the scratch work earlier.



We now have enough to prove the next theorem!

Theorem 5.1: The Euclidean Algorithm really works

The Euclidean Algorithm really works...

Proof Idea. By repeatedly applying the division algorithm, we end up with a chain of remainders, where each new one is less than the previous one. Since each remainder is greater than or equal to 0 (by the division algorithm), this chain must come to an end when some remainder, say r_{n+2} , equals 0. This is because there are only finitely many integers less than a but greater than 0.

$$a > b > r_0 > r_1 > r_2 > \cdots > r_{n+1} > r_{n+2} = 0.$$

By applying our lemma 5.2 at each step of the division algorithm, the greatest common divisor is ‘carried along’ each application of the division algorithm, meaning:

$$\gcd(a, b) = \gcd(b, r_0) = \gcd(r_0, r_1) = \cdots = \gcd(r_n, r_{n+1}).$$

Furthermore, since $r_{n+2} = 0$ implies,

$$r_n = q_{n+2}r_{n+1} \iff r_{n+1} \mid r_n.$$

We have, $\gcd(r_n, r_{n+1}) = r_{n+1}$ and hence $\gcd(a, b) = r_{n+1}$ as stated.



5.4. A Motivating Mystery

Okay, so we have the Euclidean Algorithm now, and we know how to use it, but is it good for anything? Yes, yes it is. As we will see, we can use the Euclidean Algorithm to answer the following questions:

Let’s consider,

$$2x + 4y = 1.$$

Are there integer solutions? Meaning, are there integers x and y that satisfy this equation? (For example $x = 3$ and $y = -1$ don’t work since they give $2(3) + 4(-1) = 2 \neq 1$). Give it a try!

I’ll wait... Remember, math is more fun when you give it a go!

Did you find any? No? Does that mean you didn’t try enough, or are there no solutions?

Okay scratch that problem, try this one:

$$2x + 5y = 1.$$

It’s almost the same as the first, but with a $5y$. Give this one a go!

I’ll wait... this one is more fun than the last!

Did you find any solutions?

Maybe you found $x = -2$ and $y = 1$: since $2(-2) + 5(1) = -4 + 5 = 1$. Or, maybe you found $x = 3$ and $y = -1$ since $2(3) + 5(-1) = 6 - 5 = 1$. Or maybe you found another one that wasn't either of those two!

The first equation has no solutions, whereas the second one has infinitely many solutions. Which begs the questions: *What's the problem with the first equation? Why are there no solutions? And what's so nice about the second equation that allows for infinitely many solutions?*

TO BE CONTINUED...

Chapter 6

$$ax + by = 1$$

“The beauty of mathematics only shows itself to more patient followers.”

- Maryam Mirzakhani

*I was very tempted to begin this chapter with a play on: **Previously seen...** like what's done with TV shows that ended on a cliffhanger. However, I wanted to motivate our topic in a different way, but I couldn't get it to flow satisfactorily!*

Once Upon a Time...

. . . in your high school algebra class, you've probably seen equations like $5x + 3y = 10$ or $2x + 4y = 1$. Sometimes you were asked to find some points that are on the line, or to graph the line by hand (or calculator). One way that you can determine points on the line (or graph it) is to rearrange the equation $5x + 3y = 10$ to be in the form: $y = -\frac{5}{3}x + \frac{10}{3}$. From here, we could plug in values of x and 'easily' figure out what value of y corresponds to that x . For example, setting $x = \frac{6}{5}$ gives: $y = (-\frac{5}{3} \cdot \frac{6}{5}) + \frac{10}{3} = \frac{4}{3}$.

Hence, $(\frac{6}{5}, \frac{4}{3})$ is on the line. In other words, the pair of numbers $x = \frac{6}{5}$ and $y = \frac{4}{3}$ satisfy the equation $5x + 3y = 10$.

Now, let's ask a more difficult question.

Instead of plugging in any numbers x (or y) or graphing the equation $5x + 3y = 10$ —which gives all the real number solutions—can we find integer solutions to the equation $5x + 3y = 10$?

What makes finding integer solutions so challenging is that we can't start dividing by 3 or 5, like we did earlier, because then we get fractions. Not good. Also, there's no reason to assume that there are pair of integers (x, y) that satisfies $5x + 3y = 10$? And even if there is a solution, is there more than one solution? If so, how do we find them?

We will answer all these questions in this chapter!

NOTE: Throughout this chapter, when we say 'solution' we mean an integer solution.

Perviously Seen...¹

A Motivating Mystery

Okay, so we have the Euclidean Algorithm now, and we know how to use it, but is it good for anything? Yes, as we will see, we can use it to answer the following questions:

Let's consider,

$$2x + 4y = 1.$$

Are there integer solutions? Meaning, are there integers x and y that make this equation satisfy?

⋮

Okay, scratch that problem, try this one:

$$2x + 5y = 1.$$

It's almost the same as the first, but with a $5y$. Give this one a go!

¹ Okay, I tried to put it here!

⋮

The first equation has no solutions, whereas the second one has infinitely many solutions. Which begs the questions: *What's the problem with the first equation? Why are there no solutions? And what's so nice about the second equation that allows for infinitely many solutions?*

6.1. The Resolution

Were you able to justify to yourself why you couldn't find an integer solution to the equation: $2x + 4y = 1$? If not, maybe try to take a moment and plug in some numbers for x and y and see what *type of numbers* you get from $2x + 4y$. For example, $2(1) + 4(3) = 14$ and $2(3) + 4(5) = 26$.

x	y	$2x + 4y$
-1	2	6
0	2	8
1	2	10
3	-1	2
3	0	6
3	1	10

Take a look at the left-hand and right-hand sides:

$$\underbrace{2x + 4y}_{\text{even}} = \underbrace{1}_{\text{odd}}.$$

No matter what you choose for x and y , the left-hand side is always even. But since the right-hand side is 1, which is odd, there are no solutions. Because if there were a solution, we'd have the impossible (contradiction) statement: (Even Integer) = (Odd Integer), or that 1 is an even number. Moreover, notice this issue does not arise with the second equation we were interested in,

$2x + 5y = 1$, since the left-hand side can be odd or even depending on what we let x and y are.

x	y	$2x + 5y$
-1	2	8
0	2	10
1	2	12
3	-1	1
3	0	6
3	1	11

Using this example, we might conjecture: *if a or b is odd, then there is a solution to $ax + by = 1$.*² If this conjecture were correct, we should be able to find a solution to $15x + 21y = 1$, since $a = 15$ and $b = 21$ are odd.

There's a problem, because there is no integer solution to the equation $15x + 21y = 1$ even though both a and b are odd. So the issue is deeper than just having even or odd numbers.

The issue is not 15's and 21's even/odd-ness, but their divisibility by 3:

$$\underbrace{15x + 21y}_{\text{divisible by 3}} = \underbrace{1}_{\text{not divisible by 3}}.$$

It seems important to consider what numbers are divisors of both a and b in the equation $ax + by = 1$.

For another example, consider the situation when a and b share a common factor 5 (or, using our fancy notation: $5 \mid a$ and $5 \mid b$). We can therefore write: $a = 5k$ and $b = 5t$, where k and t are integers. Thus,

$$\underbrace{ax + by}_{\text{is a multiple of 5}} = 5 \underbrace{(k + t)}_{\text{integer}} = \underbrace{1}_{\text{is not a multiple of 5}}.$$

²Recall we use inclusive or, which means that “ a or b is odd” is true in any of the three situations: (i) a =odd and b =even, (ii) a =even and b =odd, (iii) a =odd and b =odd.

We can conclude that $ax + by = 1$ has no integer solutions. For if there was, then we'd conclude that $\frac{1}{5}$ is an integer since: integer = $k + t = \frac{1}{5}$.

We therefore focus on identifying common factors between a and b . But to make the following discussion easier to follow, here's some new language:

Definition 6.1: Relatively Prime or Coprime Integers

We say two integers a and b are **relatively prime** (or **coprime**) if they share no factors. Or, more simply, a and b are relatively prime when $\gcd(a, b) = 1$.

We now conjecture:

Conjecture 2. *If the equation: $ax + by = 1$ has a solution, then a and b are relatively prime.*

This conjecture is indeed true; actually, there is an even stronger statement than that which is true!

6.2. Bézout's Identity

Theorem 6.1: Bézout's Identity

Let a and b be integers. If $\gcd(a, b) = d$, then the equation $ax + by = d$ has an integer solution.

Scratch Work. We are going to rely heavily on the Euclidean Algorithm, here's the color-coded schematic from last time:

The Euclidean Algorithm Schematic

$$\begin{array}{ll}
 a = q_0 \overset{\text{blue}}{b} + \overset{\text{green}}{r_0}, & \text{where } 0 \leq r_0 < b \\
 \overset{\text{blue}}{b} = q_1 \overset{\text{green}}{r_0} + \overset{\text{red}}{r_1}, & \text{where } 0 \leq r_1 < r_0 \\
 \overset{\text{green}}{r_0} = q_2 \overset{\text{red}}{r_1} + \overset{\text{yellow}}{r_2}, & \text{where } 0 \leq r_2 < r_1 \\
 \overset{\text{red}}{r_1} = q_3 \overset{\text{yellow}}{r_2} + \overset{\text{purple}}{r_3}, & \text{where } 0 \leq r_3 < r_2 \\
 \overset{\text{yellow}}{r_2} = q_4 \overset{\text{purple}}{r_3} + \overset{\text{orange}}{r_4}, & \text{where } 0 \leq r_4 < r_3 \\
 \vdots & \vdots \\
 r_{n-1} = q_{n+1} r_n + \overset{\text{starburst}}{r_{n+1}}, & \text{where } 0 \leq r_{n+1} < r_n \\
 \overset{\text{grey}}{r_n} = q_{n+2} \overset{\text{red starburst}}{r_{n+1}} + \overset{\text{black starburst}}{r_{n+2} = 0}, & \text{where } r_{n+2} = 0 \\
 & \text{so that } \gcd(a, b) = r_{n+1}
 \end{array}$$

Since we want a solution to the equation $ax + by = \gcd(a, b)$, having an expression for $\gcd(a, b)$ seems like a good place to start. Observe that the remainder in the second-to-last equation in the schematic is the greatest common divisor $\gcd(a, b) = r_{n+1}$. This motivates us to rearrange the second-to-last equation to get the expression for $\gcd(a, b)$,

$$\gcd(a, b) = r_{n+1} = r_{n-1} - q_{n+1}r_n$$

We ultimately want a and b in our solution equation for $\gcd(a, b)$. Since they are in the first equation in the Euclidean Algorithm, let's see if we can move upward in the algorithm by solving for remainders and plugging in those expressions.

The line above the second-to-last equation isn't shown, but we can deduce that it would be $r_{n-2} = q_n r_{n-1} + r_n$. Again, let's

solve for the remainder r_n ,

$$r_n = r_{n-2} - q_n r_{n-1}.$$

We can plug this into our expression $\gcd(a, b) = r_{n-1} - q_{n+1}r_n$, bringing us closer to the first line in the algorithm that has a and b ,

$$\begin{aligned}\gcd(a, b) &= r_{n-1} - q_{n+1}r_n \\ &= r_{n-1} - q_{n+1}(r_{n-2} - q_n r_{n-1}) \\ &= (1 + q_n)r_{n-1} - q_{n-1}r_{n-2}\end{aligned}$$

Where we gathered all like terms.

Our game plan is to continue this process until we reach the top equation involving a and b . In other words, you just keep plugging in the expressions we find into the next remainder until you reach the top! Once you do, you'll end up with an expression of the form:

$$a(\text{stuff}) + b(\text{other stuff}) = d.$$

Where the *stuff* and *other stuff* are integer expressions full of remainders r_i 's and quotients q_i 's. But this doesn't really help us unless we do an example!

Example 4. Our aim to find integers x and y such that

$$59x + 301y = 1.$$

We already determined that $\gcd(59, 301) = 1$ in the previous chapter. If you'd like to see the color-coded schematic version, please go back to page 61. However, we will need the steps again, so here they are, uncolored:

$$\begin{aligned}301 &= 5(59) + 6, \\ 59 &= 9(6) + 5, \\ 6 &= 1(5) + \boxed{1}, \\ 5 &= 5(1) + 0.\end{aligned}$$

And since $\gcd(59, 301) = 1$ shows up in the third line, there will be three steps to find x and y .

Step 1: Solve the third line for $\gcd(59, 301) = 1$.

$$1 = 6 + (-1)(5).$$

Step 2: Solve the second line for its remainder, aka 5,

$$5 = 59 + (-9)(6)$$

Now plug this expression for 5 into step 1 and group the multiples of 6 and 59.

$$\begin{aligned} 1 &= 6 + (-1)(5) \\ &= 6 + (-1)(59 + (-9)(6)) \\ &= 10(6) + (-1)(59). \end{aligned}$$

Step 3: Solve the first line for its remainder aka 6,

$$6 = 301 + (-5)(59).$$

Plug this into the result of step 2.

$$\begin{aligned} 1 &= 10(6) + (-1)(59) \\ &= 10(301 + (-5)(59)) + (-1)(59) \\ &= (-51)(59) + (10)(301). \end{aligned}$$

And we're done. We've found a solution: $x = -51$ and $y = 10$.

$$\boxed{59(-51) + 301(10) = 1}.$$



Hey, I just want to jump in and say that it's okay if you are finding this challenging and a little hard to follow the steps that we are going through. This is just part of the process, and there is no way around it. I recommend pausing for a moment, taking a breath, and then reviewing the example. This will help you follow each step and understand where each number is going and why.

I would like to comment on the terms we are grouping in each step. For a concrete example to follow along with, go back to step 2 in the previous example. We solved for the remainder of the **second line** and got $5 = 59 + (-9)(6)$. Then, we plugged this expression for 5 into the result from step 1: $1 = 6 + (-1)(5) = 6 + (-1)(59 + (-9)(6))$. We then simplified the expression by grouping terms with 6 and 59 in them, and I would like to address why we grouped in terms of 6 and 59. We did this because we were going to use the first line in the next step (step 3), which has as its remainder: 6 and divisor 59. This is the general approach: simplify each expression by grouping in terms of the next line's remainder and divisor.

Example 5. We also found that $\gcd(142, 262) = 2$ using the following steps:

$$\begin{aligned} 262 &= 1(142) + 120, \\ 142 &= 1(120) + 22, \\ 120 &= 5(22) + 10, \\ 22 &= 2(10) + \boxed{2}, \\ 10 &= 5(2) + 0. \end{aligned}$$

Therefore, we ought to be able to find a solution to $142x + 262y = 2$. Let's go through the same steps:

Step 1: Solve the fourth line for $\gcd(142, 262) = 2$,

$$2 = 22 + (-2)(10).$$

Step 2: Solve the third line for its remainder, 10,

$$10 = 120 + (-5)(22).$$

Now plug this expression for 10 into the result of step 1 while grouping the multiples of 120 and 10,

$$\begin{aligned} 2 &= 22 + (-2)(10) \\ &= 22 + (-2)(120 + (-5)(22)) \\ &= 11(22) + (-2)(120). \end{aligned}$$

Step 3: Solve the second line for its remainder, 22,

$$22 = 142 + (-1)(120).$$

Now plug this expression for 22 into the result from step 2,

$$\begin{aligned} 2 &= 11(22) + (-2)(120) \\ &= 11(142 + (-1)(120)) + (-2)(120) \\ &= 11(142) + (-13)(120). \end{aligned}$$

Step 4: Finally, solve the first line for its remainder 120,

$$120 = 262 + (-1)(142).$$

Now plug this into the result from step 3,

$$\begin{aligned} 2 &= 11(142) + (-13)(120) \\ &= 11(142) + (-13)(262 + (-1)(142)) \\ &= 24(142) + (-13)(262). \end{aligned}$$

Step 5: Be happy that you're done and exult in our solution:

$$\boxed{142(24) + 262(-13) = 2}$$

which you can check with a calculator!



6.2.1 Boo! No Proof!

We won't give a detailed proof of Bézout's Identity, mostly because the proof relies on the Euclidean Algorithm's quotients and remainders to find the values of x and y . And, as we've seen in the examples, the algebra becomes messy. Not to mention how messy all the subscripts become! All we would do is formalize what we just did in the examples. However, we will give, and prove, a generalization of Bézout's Identity!

6.3. Generalization of Bézout's Identity

Bézout's Identity has a more general form. Let me ask you: What would happen if we tried to find a solution to the equation:

$$ax + by = 10d$$

Where we still identify $\gcd(a, b) = d$. Well, we know by Bézout's Identity that there is a solution to $ax + by = d$. Let's denote this guaranteed solution by x_0 and y_0 so that

$$ax_0 + by_0 = d.$$

But then multiplying every term by 10 gives:

$$a(10x_0) + b(10y_0) = 10d.$$

Thus, $10x_0$ and $10y_0$ solve our new equation.

The previous argument demonstrates that we can solve any equation $ax + by = md$ by taking our solution from $ax + by = d$ and multiplying it by m . This is our more general form is the following Corollary:

Corollary 6.1: Bézout's Identity Generalized

Let a and b be integers and $\gcd(a, b) = d$. Then the equation: $ax + by = n$ has an integer solution if and only if $d \mid n$.

The proof is the same as what we discussed preceding the corollary.

Proof. Let a and b be integers and $\gcd(a, b) = d$. Since we are proving an if and only if statement, we have two directions to prove.

Forward: If $ax + by = n$ has a solution, then $d \mid n$

Let $ax + by = n$ have a solution and denote this solution by x_0 and y_0 . Since $d \mid a$ and $d \mid b$, we know that $a = dk$ and $b = dt$ for $k, t \in \mathbb{Z}$. It follows that,

$$ax_0 + by_0 = d(kx_0 + ty_0) = n.$$

Hence, $d \mid n$.

Backward: If $d \mid n$, then $ax + by = n$ has a solution.

Using Bézout's Identity we know there is a solution x_0 and y_0 to the equation $ax + by = d$. Since $d \mid n$ we have $n = ds$ where s is an integer. Multiplying $ax_0 + by_0 = d$ through by s we get,

$$a(sx_0) + b(sy_0) = ds = n.$$

Thus, we have found a solution, ($x = sx_0$ and $y = sy_0$), and conclude our proof.



6.4. Zero or Infinite?

What's left to do? We claimed at the beginning that $2x + 4y = 1$ has zero solutions and $2x + 5y = 1$ has infinitely many. We've done enough work to conclude that $2x + 4y = 1$ has no solution—Bézout's Identity Generalized tells us there is no solution since $\gcd(2, 4) = 2$ and 2 does not divide 1. However, we have not done enough to demonstrate that there are infinitely many solutions to $2x + 5y = 1$.

As we'll soon see, there is either no solution or infinitely many solutions to $ax + by = n$, and nothing in between.

Theorem 6.2: Zero or Infinite

Let a and b be integers with $\gcd(a, b) = d$. If $d \mid n$, then the equation:

$$ax + by = n$$

has infinitely many integer solutions. If $d \nmid n$, then there is no solution.

Intuition: We already know why there is no solution when $d \nmid n$, so let's turn our attention to why there might be infinitely many solutions when $d \mid n$. Since we already know that there is at least one solution (x_0, y_0) when $d \mid n$, we will try to generate another solution using (x_0, y_0) .

Let's consider the examples we looked at in the beginning of this chapter,

$$2x + 4y = 1 \quad \text{and} \quad 2x + 5y = 1.$$

We aim to understand why there is no solution for the left equation, and infinitely many for the right. Let's graph these two equations and see what we notice, see Figure 6.1. Observe that every grid point hit by the green line (marked with a black $\times$) is an integer solution to the green line's equation $2x + 5y = 1$! This is the key idea and is what we are interested in exploiting.

Let's focus on the green line given by $2x + 5y = 1$, since it actually has some solutions.

Recall, we can rewrite $2x + 5y = 1$ in slope-intercept form: $y = -\frac{2}{5}x + \frac{1}{5}$. Now suppose that x_0 and y_0 is an integer solution to $2x + 5y = 1$. Since the slope of the line is $-\frac{2}{5}$, we deduce that $x_0 - 5k$ and $y_0 + 2k$ are also integer solutions, since

$$-\frac{2}{5}(x_0 - 5k) + \frac{1}{5} = \underbrace{\left(-\frac{2}{5}x_0 + \frac{1}{5}\right)}_{=y_0+2k} + 2k.$$

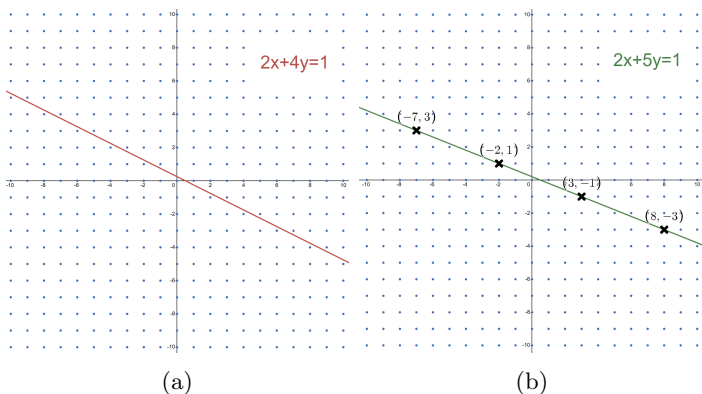


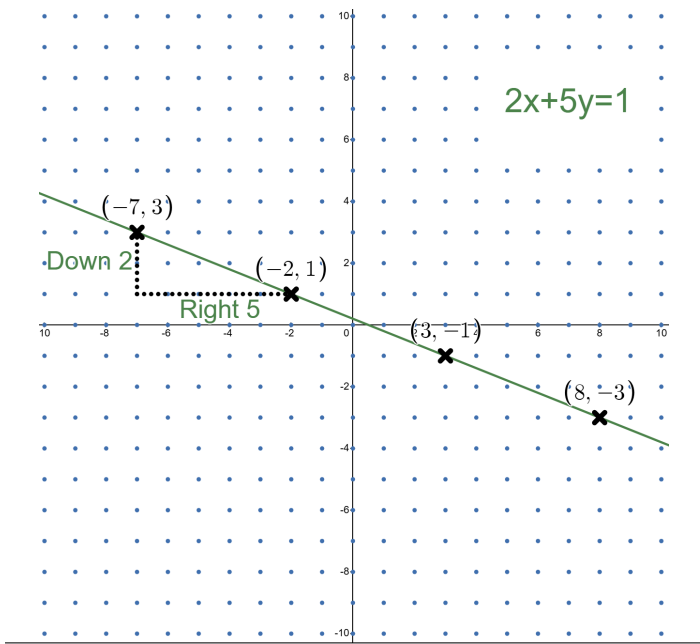
Figure 6.1

We chose to subtract $5k$ from x_0 on purpose, because the denominator of the slope is 5. Likewise, we added $2k$ to y_0 since the numerator of the slope is -2 and the 5 and the $5k$ will cancel the 5 in the denominator and give an integer.³ Thus, if we know one solution (x_0, y_0) we can construct an infinite number of solutions: $(x_0 - 5k, y_0 + 2k)$. One for each $k \in \mathbb{Z}$. We can see this graphically in the next figure.

There is ‘another’, algebraic, way to see how we find more solutions given (x_0, y_0) is a solution. It’s the same as the previous method, but we keep the equation as is, $2x + 5y = 1$, then add and subtract $2 \cdot 5k = 10k$ to $2x_0 + 5y_0 = 1$. From there, we will group terms together in order to find our new solutions,

$$\begin{aligned}
 2x_0 + 5y_0 &= 2x_0 - 10k + 5y_0 + 10k \\
 &= 2x_0 - 2(5k) + 5y_0 + 5(2k) \\
 &= 2(x_0 - 5k) + 5(y_0 + 2k) \\
 &= 1
 \end{aligned}$$

³Note we could have added $5k$ to x_0 and subtracted $2k$ from y_0 as well.



Again, see that $x_0 - 5k$ and $y_0 + 2k$ are solutions for any $k \in \mathbb{Z}$.

Before we prove Theorem 6.2, we will need a quick lemma.

6.4.1 Euler's Lemma

Here's the idea.

Take the numbers 7 and 490 and observe that $7 \mid 490$. We claim that any way we break down 490 into a product of its factors, we are guaranteed that 7 divides at least one of those factors. Let's check this when we write 490 as a product of two factors:

$$490 = 1 \cdot \underbrace{490}_{7 \mid 490} = 2 \cdot \underbrace{245}_{7 \mid 245} = 5 \cdot \underbrace{98}_{7 \mid 98} = \underbrace{7 \cdot 70}_{7 \mid 7 \text{ and } 7 \mid 70} = 10 \cdot \underbrace{49}_{7 \mid 49} = \underbrace{14 \cdot 35}_{7 \mid 14 \text{ and } 7 \mid 35}$$

Notice how 7 divides at least one of them!

Let's do another one. Consider again 490, but this time instead of 7 we use 10. We still have $10 \mid 490$, but every factor pair does not have at least one integer that is divisible by 10,

$$490 = 1 \cdot \underbrace{490}_{10 \mid 490} = \underbrace{2 \cdot 245}_{\text{None}} = \underbrace{5 \cdot 98}_{\text{None}} = 7 \cdot \underbrace{70}_{10 \mid 70} = \underbrace{10}_{10 \mid 10} \cdot 49 = \underbrace{14 \cdot 35}_{\text{None}}.$$

What's the difference?

Consider the situations where we fail to have one integer that is divisible by 10, such as the pair $490 = 14 \cdot 35$. Observe that the two factors that make up 10 (i.e., 2 and 5) are split between $14 = 2 \cdot 7$ and $35 = 5 \cdot 7$. This doesn't happen in situations where we succeeded in finding a factor divisible by 10, like $490 = 7 \cdot 70$, because 2 and 5 are both contained inside 70.

If we can somehow guarantee that none of the factors of 10 are split up, or that they are all in one factor, then it must be that ten divides that factor. We can do this by forcing one factor to be relatively prime to 10. That is, if $490 = a \cdot b$, and $\gcd(a, 10) = 1$, then $10 \mid b$. Just like with $490 = 7 \cdot 70$.

This is known as Euler's Lemma:

Lemma 6.1: Euler's Lemma

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

Proof. Let a , b , and c be integers such that $c \mid ab$ and $\gcd(a, c) = 1$. Since $\gcd(a, c) = 1$ we know there is a solution (in the integers) to the following equation by Bézout's Identity:

$$ax + cy = 1.$$

Multiplying through by b , we get,

$$(ab)x + bcy = b.$$

Recall that $c \mid ab$, so that $ab = ck$ for some integer k . Thus,

$$ckx + bcy = c(kx + by) = b.$$

Since c divides the left-hand side (and middle portion), c must also divide the right and side, aka b . Thus, we conclude $c \mid b$.



6.4.2 Back to The Proof of Zero or Infinite?

Proof of Zero or Infinite 6.2. We've already taken care of the second statement (when $d \nmid n$), so we focus on the first part of the theorem (when $d \mid n$). We will provide a constructive proof of this theorem by finding a formula that yields every solution.

Let a and b be integers, $\gcd(a, b) = d$, and $d \mid n$. We already know that there is at least one set of solutions to $ax + by = n$, since $d \mid n$. Denote this solution by x_0 and y_0 . We now employ a strategy that you might remember from high school algebra. We subtract the two equations,

$$\begin{array}{r} ax + by = n \\ -(ax_0 + by_0 = n) \\ \hline a(x - x_0) + b(y - y_0) = n - n = 0. \end{array}$$

Recall that $d \mid a$ and $d \mid b$, so that $a = dt$ and $b = ds$. We therefore can divide out by d ,

$$t(x - x_0) + s(y - y_0) = 0.$$

Leaving the integer coefficients $t = \frac{a}{d}$ and $s = \frac{b}{d}$.

Does it make sense that $\gcd(t, s) = 1$? Since $\gcd(a, b) = d$, the integers a and b shared at most a common factor of d . By getting rid of d through division, what's left will share no common factors other than 1. In symbols, $\gcd(\frac{a}{d}, \frac{b}{d}) = \gcd(t, s) = 1$ as we said.

Rearranging our equation above to be,

$$t(x - x_0) = -s(y - y_0),$$

helps us see that because the left-hand side is divisible by t , it must be that t divides the right-hand side too. So, we have

$$t \mid s(y - y_0) \quad \text{and} \quad \gcd(t, s) = 1.$$

Thus, by Euler's Lemma: $t \mid (y - y_0)$. Or,

$$y - y_0 = tk = \left(\frac{a}{d}\right)k$$

For some integer k . This is our solution set for y .

Plugging our solution set for y back into $t(x - x_0) + s(y - y_0) = 0$, we get our solution set for x ,

$$t(x - x_0) + s(tk) = 0,$$

canceling t we get,

$$(x - x_0) + sk = (x - x_0) + \left(\frac{b}{d}\right)k = 0.$$

Therefore, we have the two sets of solutions:

$$x = x_0 - \left(\frac{b}{d}\right)k \quad \text{and} \quad y = y_0 + \left(\frac{a}{d}\right)k \quad (\hat{\text{cap}})$$

Furthermore, since k is any integer, we have infinitely many integer solution pairs.



Let's do an example together!

Example 6. Let's continue with our running example, $2x + 5y = 1$. We already know that $x_0 = 3$ and $y_0 = -1$ is a solution. Plugging in these with $a = 2$, $b = 5$, $d = 1$ into the equation pair $(\hat{\text{cap}})$, we get: $x = 3 - \frac{5}{1}k$ and $y = -1 + \frac{2}{1}k$. Or, simply

$$x = 3 - 5k \quad \text{and} \quad y = -1 + 2k$$

Let's check different values of k .

If you check the graph from earlier on page 80, these points are the intersections there.



k	x	y
-1	8	-3
0	3	-1
1	-2	2
2	-7	3

6.5. It's the Final Countdown... danananahhh

I know you sang it in your head!

This chapter contains a lot more results, theorems, lemmas, corollaries, etc than usual. I hope you found it fun! Let's wrap this chapter up with one more vocabulary word (you're welcome). It's standard terminology when we are finding integer solutions to an equation to call the equation a **Diophantine equation**. There are many more Diophantine equations that we know how to solve. I recommend you check some out if you found this fun!

Your Own Problems

1. What are the integer solutions to $7x + 26y = 15$? This is the equation in the introduction.
2. We showed that our solution set is given by

$$x = x_0 - \left(\frac{b}{d}\right)k \text{ and } y = y_0 + \left(\frac{a}{d}\right)k.$$

Would

$$x = x_0 + \left(\frac{b}{d}\right)k \text{ and } y = y_0 - \left(\frac{a}{d}\right)k$$

work too?

3. If you restrict x and y to be greater than or equal to 0, that is $x, y \in \mathbb{N}$, what different numbers n can you get as a solution to: $ax + by = n$.

The solutions are given on page 183.

Chapter 7

Prime Numbers

*“Although the prime numbers are rigidly determined,
they somehow feel like experimental data.”*

– Timothy Gowers, Fields Medalist.

Prime Time

Wow, we are already seven chapters into this book, and we haven't really learned about prime numbers yet! Blasphemy! We have to fix this! Even though we've said what prime numbers are a few times in passing throughout this book, here's what it means for a number to be prime:

Definition 7.1: Prime Numbers

A positive integer $p \neq 1$ is called a **prime number** if the only positive divisors of p are 1 and itself. Or, to be more mathy:

We call p a prime number if

- (i) p is a positive integer,
- (ii) $p \neq 1$, and has the property
- (iii) if a positive integer d divides p , then $d = 1$ or $d = p$.

A number that is not 1 or prime is called composite.

Observation 1: You might be asking, “Why exclude 1 as a prime number?” If so, this is a great question! We will justify excluding 1 as a prime number using the Fundamental Theorem of Arithmetic. The Fundamental Theorem of Arithmetic states that **every nonzero integer has a unique prime factorization**, and if 1 were considered a prime, then this bold statement wouldn’t be true. We could factor 6 as,

$$6 = 1 \cdot 2 \cdot 3 = 1 \cdot 1 \cdot 2 \cdot 3 = 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 2 \cdot 3 = \text{etc.}$$

Basically, we want to exclude all the variation that the 1’s allow in the above factorizations. This is done most simply by excluding 1 as a prime number.

Observation 2: The integer 1 is neither prime nor composite; 1 is called the unit.

Observation 3: Composite numbers are numbers that have at least one factor other than 1 and itself. Or, n is composite if there exists a positive integer $d \neq 1$ or n such that $d \mid n$.

Some prime examples (haha pun intended) of prime numbers

are: 2, 3, 5, 7, 11, 101, etc. All these numbers have no divisors other than 1 and itself.

As you might guess, most numbers are composite. For example, 9, 15, 21, 25, 35, are composite, as well as *every even number besides 2*. Which leads us to our next theorem, before we get to the Fundamental Theorem of Arithmetic:

Theorem 7.1: Two is the oddest prime

The prime 2, is the oddest prime.

Proof. Since 2 is the only even prime number, it is the strangest prime number. A synonym of strange is odd. Therefore, 2 is the oddest prime.



7.1. Fundamental Theorem of Arithmetic

Back in school, you probably learned that every number can be factored into prime numbers. For example, $200 = 2^3 \cdot 5^2$, $49 = 7^2$, and $11 = 11^1$ since 11 is prime! This is probably so deeply ingrained into how you think of numbers that you think it forgoes the proof. In some aspect, you would be correct. However, if you read the chapter on the division algorithm, do you remember our discussion on page 50 regarding why it was important to prove the division algorithm? If you don't, or you did not read it, I would like to ask you to read section 4.3 on page 50 because the reason is the same.

When working with complex numbers, we end up needing to confront whether they factor into unique products. For example, 6 is a composite number that factors uniquely into,

$$6 = 2 \cdot 3$$

But by allowing complex numbers, we also have

$$6 = (1 + i) \cdot (1 - i) \cdot 3$$

since $(1 + i) \cdot (1 - i) = 1 + i - i - i^2 = 1 - i^2 = 1 - (-1) = 2$. So there is no longer unique factorization, if 2 is still considered a prime number in the complex numbers. But this is taking us too far afield. Suffice to say, we should try to prove the Fundamental Theorem of Arithmetic!

In the proof of the Fundamental Theorem of Arithmetic, we will utilize a corollary of Euler's Lemma (on page 82), known as Euclid's Lemma.

Lemma 7.1: Euclid's Lemma

Let p be a prime number and let a and b be integers. If $p \mid ab$ and $p \nmid a$, then $p \mid b$.

Proof. Since p is a prime number only 1 and p divide it. This means that either $\gcd(a, p) = 1$ or p . But, since $p \nmid a$, we know $\gcd(a, p) \neq p$ so it must be that $\gcd(a, p) = 1$. Now apply Euler's Lemma to arrive at Euclid's Lemma.



Since we will be considering numbers that may have multiple prime factors, we need a generalization of Euclid's lemma that applies to a product of prime numbers. The proof is left to you, you're welcome!

Corollary 7.1: Euclid's Lemma (COROLLARY)

Let p, p_1, p_2 , and p_n be prime numbers. If

$$p \mid p_1 p_2 \cdots p_n,$$

then there is some prime in the product such that $p \mid p_i$.
More precisely, $p = p_i$ for some i .

Now, the pièce de résistance:

Theorem 7.2: The Fundamental Theorem of Arithmetic

Every positive integer $n > 1$ can be expressed as a **unique** product of primes up to rearrangement. We call this product of primes, n 's **prime factorization**, or simply n 's factorization.

By *rearrangement*, we mean that we consider factorizations like, $6 = 2 \cdot 3 = 3 \cdot 2$ to be the same factorization.

Proof. We will break up this proof into two parts: (i) every integer larger than one has a prime factorization, and (ii) this prime factorization is unique up to rearrangement.

(i) Every positive integer $n > 1$ has a prime factorization

We will use *strong induction* on n .¹ Because this is our first time using strong induction, we will go back to writing out each step of the induction to keep everything clear.

¹Recall Strong induction on page 25. We mentioned that strong induction is, for the most part, the same as standard induction. The only difference is that our induction hypothesis assumes that our proposition $P(n)$ is true **for all** natural numbers less than or equal to n . Standard induction only assumed $P(n)$ was true for one n .

Base Case: Since our theorem concerns $n > 1$, our base case starts with $n = 2$. Furthermore, since 2 is prime, the prime factorization of n is simply $n = 2^1$.

Induction Hypothesis: Assume **every integer** that's greater than 1 and less than or equal to n has a unique prime factorization.

Inductive Step: Consider the natural number $n + 1$. Here's an obvious statement: Either $n + 1$ is prime or composite (not both). In the case that $n + 1$ is prime, we're done since its prime factorization is just $n + 1$.² On the other hand, if $n + 1$ is composite, then there are integers a and b (not necessarily distinct) whose product is $n + 1$, that is $n + 1 = ab$. Furthermore, a, b are greater than 1 and less than $n + 1$ (can you see why a and b are less than n ?). Since we don't know what a and b are, let's agree to label the smaller factor by a . Thus, $1 < a \leq b < n + 1$.³

Since $1 < a \leq b < n + 1$ we can use the induction hypothesis on a and b to deduce that a and b have a prime factorization. Let's denote a 's and b 's factorization,

$$a = p_1 \cdot p_2 \cdots p_m \quad \text{and} \quad b = q_1 \cdot q_2 \cdots q_\ell$$

Where the p 's and q 's are primes (not necessarily distinct from one another). It follows that $n + 1$ has the prime factorization,

$$n + 1 = p_1 \cdot p_2 \cdots p_m \cdot q_1 \cdot q_2 \cdots q_\ell.$$

Now all we have to do is show that this prime factorization is unique.

(ii) Uniqueness of the prime factorization

Note to the reader, we will be using the same letters, p and q , to represent primes. However, these aren't necessarily the same primes that were in a 's and b 's factorizations. There are not enough letters to use to represent primes!

²Just like the base case $n = 2$.

³Where $a = b$ in the case that n is a square number, $n = a^2$.

Assume that n has the prime factorizations,

$$n = p_1 \cdot p_2 \cdots p_m \quad \text{and} \quad n = q_1 \cdot q_2 \cdots q_\ell.$$

Where all the p 's and q 's are primes. NOTE: We are choosing not to group primes, so it can happen that $p_i = p_j$ with $i \neq j$. (For example, we'd express 24's prime factorization as, $24 = 2 \cdot 2 \cdot 2 \cdot 3$.)

Our goal is to show that these two factorizations are actually the same. We will do this by showing (i) there is an equal number of p 's and q 's, i.e., $m = \ell$, and (ii) each p_i equals some q_j .

Let's first consider the prime p_1 . Since $p_1 \mid n$ it follows that $p_1 \mid q_1 \cdot q_2 \cdots q_\ell$. Thus, by Euclid's Lemma (COROLLARY) 7.1, there is some $1 \leq A \leq \ell$ such that $p_1 = q_A$. We can cancel out this prime from both sides to conclude:

$$p_2 \cdot p_3 \cdots p_m = q_1 \cdot q_2 \cdots q_{A-1} \cdot q_{A+1} \cdots q_\ell.$$

Consider now the prime p_2 . We go through the same logic and similarly deduce that there is some q_B such that $p_2 = q_B$. Canceling this prime out from both sides again gives,

$$p_3 \cdot p_4 \cdots p_m = q_1 \cdot q_2 \cdots q_{A-1} \cdot q_{A+1} \cdots q_{B-1} \cdot q_{B+1} \cdots q_\ell.$$

Continue this same process for the prime p_3 , and then p_4 , etc.

We'll see that for each prime p_i we're considering, we'll find some prime q_j that equals p_i , which we can then cancel. If, for some reason, there were more p primes than q primes, then we'd end up with a contradiction concerning the leftover p primes:

$$p_a \cdot p_{a+1} \cdots p_m = 1,$$

which implies that $p_a, p_{a+1}, \dots, p_m = 1$. But by definition 1 is not a prime!

Likewise, if there were more q primes than p primes, then we'd find that the product of leftover q primes must equal 1 as well,

$$1 = q_a \cdot q_a \cdots q_\ell.$$

Thus, there must be an equal number of p 's and q 's where each p equals some q . From this, we conclude that both factorizations are rearrangements of one another and hence are the same.



7.2. More More More Questions!

There are so many more questions that we can ask regarding prime numbers! Once we start, it's not long before we reach the limits of modern mathematics! For example, one question that we already know the answer to is,

“How many primes are there?”

We answered this in chapter 3, and Euclid answered this question wayyyyy back in around 300BC! Since we know more number theory, let's go through our proof again. This time, we can justify each step with what we've learned!

**Theorem 7.3: There are Infinitely Many Primes
ala Euclid**

There are Infinitely Many Primes!

Proof. Assume for the hope of a contradiction that there were only finitely many primes. Let's say there are n primes, and let's list them out,

$$p_1, p_2, \dots, p_n.$$

Consider the integer N that is the product of all the primes (plus 1),

$$N = (p_1 \cdot p_2 \cdot \dots \cdot p_n) + 1.$$

Two things can happen: Either N is prime or N is composite.

(i) If N is prime, then we found a new prime number, contradicting that we had a complete list at the beginning.

(ii) Or, if N is composite, then there exists at least one prime that divides it. But N is not N divisible by any of the primes on our list, $p_1, p_2, \dots, p_n$. For if N was divisible by say, p_1 , then $N = p_1 k$ and it would follow that,

$$\begin{aligned} N - (p_1 \cdot p_2 \cdot \dots \cdot p_n) &= p_1 k - (p_1 \cdot p_2 \cdot \dots \cdot p_n) \\ &= p_1 (k - p_2 \cdot p_3 \cdot \dots \cdot p_n) \\ &= 1. \end{aligned}$$

Which implies that $p_1 \mid 1$, or that $p_1 = 1$, which is impossible! Hence, any prime that divides N is not on the list, contradicting that we had a complete list (again).



7.3. Tag, you're it!

There are many mysteries surrounding prime numbers. For example, we don't yet know if there are infinitely many twin primes (primes separated by two, like the pair 3 and 5 or the pair 101 and 103). We also don't know if there is always a prime between two square numbers. For example, we know that 11 is between 9 and 16, but it's unknown that this is true for any n^2 and $(n+1)^2$! We also don't have a formula to generate only prime numbers. And we don't have a fast way to check if a number is prime.

Maybe you will solve one of these problems and go down in mathematical history!

We do know some things; however, we know that there is a prime between n and $2n$. This is called Bertrand's Postulate, and the great mathematician Paul Erdős gave a stunning proof of this fact (you can Google it and find it on Wikipedia if you are interested). We also know that the number of prime numbers up to x is roughly equal to $x/\ln(x)$, this is known as the Prime Number Theorem. And we also know that there are infinitely many primes in the sequence $a+d, a+2d, a+3d, \dots$ if $\gcd(a, d) = 1$. This is known as Dirichlet's Theorem about Arithmetic Progressions.

Primes are an endless source of beautiful mathematics and fun problems.

To end this chapter, I figured I'd give you some of my favorite prime-related conjectures:

Conjecture 3. *UNNAMED Conjecture:* *Let q_n be the smallest prime that is larger than the product,*

$$P_n = p_1 \cdot p_2 \cdots p_n + 1.$$

Where $p_1, p_2, \dots, p_n$ are the first n primes. Here's the conjecture: the difference $q_n - P_n$ is a prime number. (Feel free to check this for a few n 's)

Conjecture 4. *Grimm's Conjecture:* *If $n+1, n+2, \dots, n+k$ are all composite, then there exists k -different prime numbers such that, $p_i \mid n+i$, with $1 \leq i \leq k$. (For example, 24, 25, 26, 27, 28 are composite, and the primes 2, 5, 13, 3, 7 divide them respectively.)*

Conjecture 5. *Legendre's conjecture:* *We already mentioned this one: For any integer n there is a prime in between n^2 and $(n+1)^2$.*

Chapter 8

Modular Arithmetic

“ $2+2 = 1$ ”

– Nobody.

8.1. A Motivating Mystery

Can you find an integer solution to the equation $x^2 + y^2 = 3$? Take a moment to try out some values for x and y and see what you get.

What about the equation $x^2 + y^2 = 307$? Can you find any solutions?

Did you find one? No? Is that because there are no solutions, similar to how there is no solution to $2x + 4y = 1$?

As it turns out, there are no solutions to the former equations. Furthermore, there are no solutions to $x^2 + y^2 = N$ when for any of the following values $N = 3, 19, 43, 103, 307$ either!

In this chapter, we’ll spend some time developing tools, called *modular arithmetic*, that might seem strange and potentially not very useful; however, you’ll be pleasantly surprised because many

problems' solutions become obvious when we use modular arithmetic. The above problem is an example of one of them!

8.2. Modular Arithmetic

8.2.1 Fun Fundamentals

Do you remember way back when you first learned how to divide two integers? We already talked about this when we discussed the division algorithm. Back then, you were supposed to answer your division problems with a quotient and a remainder. For example, when asked: What's 30 divided by 4? You were supposed to answer, 7 remainder 2.

$$30 \div 4 = 7 \text{ R}2$$

Just in case you skipped chapter 4, let's dust off those skills because we are going to need them again!

In chapter 4 on page 46, we learned that we can always find a quotient and a remainder as long as we aren't dividing by zero. But, for no other reason than because we can, we are going to focus on the remainders given in the division algorithm—we won't care about the quotient so much. And since the phrase “*# has a remainder of # when divided by #*” is very clunky and long—and remember, I'm lazy—we will adopt some new vocabulary: **congruence** and **mod**.

For example, instead of saying: 23 has a remainder 3 when divided by 10, we will now say: 23 is congruent to 3 (mod 10). Where congruent means “has a remainder” and mod means “when divided by”.

Definition 8.1: ‘Loose’ Definition of Congruence and Mod

If a divided by b is equal to c with a remainder d , then we will instead say that: a is congruent to $d \pmod{b}$.

Note that we don't bother finding the quotient c .

Example 7. Consider the following examples:

- 23 has a remainder of 3 when divided by 10 $\iff$ 23 is congruent to 3 (mod 10).
- 45 has a remainder of 5 when divided by 10 $\iff$ 45 is congruent to 5 (mod 10).
- 12 has a remainder of 0 when divided by 6 $\iff$ 12 is congruent to 0 (mod 6).
- 2000 has a remainder 43 when divided by 103 $\iff$ 2000 is congruent to 43 (mod 103).¹



Now that we have some new terminology, let's introduce some new symbols too. OOOoooo

Usually, when we want to express: 5 times 2 equals 10, we don't write out "times" and "equals" we use symbols like $\times$ and $=$. Introducing these symbols is a good idea because they enable our sentences to become concise expressions. Moreover, we can then manipulate the expressions, just as we do in algebra.

$$5 \text{ times } 2 \text{ equals } 10 \iff 5 \times 2 = 10.$$

But we aren't talking about equality; we are talking about congruency. As we will see, equality and congruency are similar to one another, and to highlight this similarity, we use similar symbols. When we say 23 is congruent to 3 (mod 10) we'll write: $23 \equiv 3 \pmod{10}$.

$$23 \text{ is congruent to } 3 \pmod{10} \iff 23 \equiv 3 \pmod{10}.$$

$$45 \text{ is congruent to } 5 \pmod{10} \iff 45 \equiv 5 \pmod{10}.$$

$$12 \text{ is congruent to } 0 \pmod{6} \iff 12 \equiv 0 \pmod{6}.$$

$$2000 \text{ is congruent to } 43 \pmod{103} \iff 2000 \equiv 43 \pmod{103}.$$

¹You can check this one on a calculator because I sure didn't do this one by hand!

I think the use of unfamiliar notation is a significant challenge people face when reading and learning math independently. Such as the three-lined “equal to” symbol $\equiv$ we are now using. When you see $\equiv$ along with $(\text{mod } \#)$, it’ll likely mean what we have outlined above: congruency $(\text{mod } \#)$.

The idea of thinking of congruency as short-hand for remainders is intuitive and quick (sometimes!). However, there is a more formal definition of congruency that captures this intuition and more. We will need this later, so let’s get it out now!

Definition 8.2: Formal Definition of Congruence and Mod

Two integers a and b are congruent $(\text{mod } n)$, if, $a - b$ is a multiple of n . Or if you prefer, when n divides $a - b$.

$$a \equiv b \pmod{n} \iff n \mid (a - b) \iff (a - b) = nk. \quad (\textcircled{1})$$

where $k \in \mathbb{Z}$.

Note that some people will say a and b are congruent modulo n instead of saying $\text{mod } n$.

Applying this definition to our running examples,

- $23 \equiv 3 \pmod{10} \iff 10 \mid (23 - 3) \iff (23 - 3) = 20 \times 1$
- $45 \equiv 5 \pmod{10} \iff 10 \mid (45 - 5) \iff (45 - 5) = 10 \times 4$
- $12 \equiv 0 \pmod{6} \iff 6 \mid (12 - 0) \iff (12 - 0) = 6 \times 2$
- $2000 \equiv 43 \pmod{103} \iff 103 \mid (2000 - 43) \iff (2000 - 43) = 103 \times 9$

The reason why definition 8.2 was chosen over the loose definition 8.1 is multifold. First, it has the advantage that we don’t

need to focus solely on remainders that come out of the division algorithm. Recall that the division algorithm requires the remainder to satisfy the inequality $0 \leq r < m$ when considering $n \div m$. Translating this to our loose modular language, we have $n \equiv r \pmod{m}$ only if $0 \leq r < m$. This turns out to be needlessly restrictive.

We can consider other numbers congruent to $23 \pmod{10}$, not just $3 \pmod{10}$. The formal definition of congruence and mod helps with this. For example, since $123 - 23 = 100$ and 10 divides 100 we also have, $23 \equiv 123 \pmod{10}$. Furthermore, we have all of the following,

$$3 \equiv 13 \equiv 23 \equiv \cdots \equiv 103 \equiv 113 \equiv 123 \equiv \cdots \pmod{10}.$$

And we don't need to stop before we get to negative numbers either:

$$\cdots \equiv -27 \equiv -17 \equiv -7 \equiv 3 \equiv 13 \equiv 23 \equiv \cdots \pmod{10}.$$

Since, $3 - (-27) = -30$ and $10 \mid (-30)$ since $-30 = 10(-3)$. Similarly, $10 \mid (3 - (-7))$ and $10 \mid ((-7) - (-27))$.

We will sometimes speak in terms of **reducing**. This is a similar concept to *simplification* with fractions. When we find what a number is congruent to mod n that is greater than or equal to 0 but less than the original number, we say that we *reduced* it. For example, since 103 is congruent to $23 \pmod{10}$, and $0 \leq 23 < 103$, we say that we reduced $103 \pmod{10}$ to $23 \pmod{10}$.

Another phrase that you might see is: **residue mod n** . Just like there is a simplest form of a fraction, there is a 'simplest form' of an integer $\pmod{n}$. We define residue to be the integer we get when we've reduced enough to be in the range 0 to $n - 1$ when reducing $\pmod{n}$. This is the integer that we'd get using the loose definition. For example, when working $\pmod{10}$, we say 3 is the residue of all of the following $-27, -17, -7, 3, 13, 23 \pmod{10}$ because 3 is the only integer that is in the range $0 \leq 3 < 10$.

You may also see the following phrase while reading about modular arithmetic **complete set of residues (mod n)**. This phrase applies to a list of integers, $a_1, a_2, \dots, a_{n-1}$. If we reduce each number on the list to its residue and we get back the list $1, 2, \dots, (n-1)$ (not necessarily in the same order) we say that the original list $a_1, \dots, a_{n-1}$ forms a complete set of residues (mod n). For example, the list 2, 4, 23, 51 forms a complete set of residues (mod 5) since: $2 \equiv 2 \pmod{5}$ and $4 \equiv 4 \pmod{5}$ and $23 \equiv 3 \pmod{5}$ and $51 \equiv 1 \pmod{5}$.² Thus, the reduced list is: 2, 4, 3, 1, which is a shuffled version of 1, 2, 3, 4.

Oh, and if you are wondering why modular arithmetic is sometimes called clock algebra, it's because you are doing modular arithmetic when you are reading an analogue clock (when it's past noon)! For example, 15 hours after midday is 3:00 pm, not 15:00, unless you are in the military (or Europe). Thus, in a way, 3:00 pm is the 'same as' 15:00. This is equivalent to the more mathematical statement, $15 \equiv 3 \pmod{12}$. So, the next time you are reading a clock, you can smile knowing that you are doing modular arithmetic mod 12.

8.3. Tricks of the Trade (mod n)

Now that we have some of the basics down, we might wonder if we can add, subtract, multiply, and divide congruences like we do with integers. For example, we already deduced that $23 \equiv 3 \pmod{10}$ and $45 \equiv 5 \pmod{10}$. Are any of the following true?

$$23 + 45 \stackrel{?}{\equiv} 3 + 5 \pmod{10}$$

or,

$$23 + 45 \stackrel{?}{=} 23 + 5 \stackrel{?}{\equiv} 3 + 45 \pmod{10}$$

²Yes, I know, I know, it's not grammatically correct to keep using *and* to list things out. But it's easier to read the math parts when you do this! So yes, I am a rebel.

or,

$$23 \times 45 \stackrel{?}{\equiv} 23 \times 5 \stackrel{?}{\equiv} 3 \times 45 \pmod{10}$$

Since it doesn't make sense to combine congruences that use a different mod number (or moduli), we won't ask any questions regarding changing $(\text{mod } 10)$ to some other $(\text{mod } n)$ mid calculation (this is akin to how you can't add fractions when the denominators are not the same). But when we stick to $(\text{mod } 10)$, we can try the addition situation.

First, $23+45=68$, and since 68 has a remainder of 8 when divided by 10, the residue of 68 $(\text{mod } 10)$ is 8 $(\text{mod } 10)$. Similarly, $3+5=8$, which also has a remainder of 8 when divided by 10. So,

$$23 + 45 \stackrel{\checkmark}{\equiv} 3 + 5 \pmod{10}.$$

Thus, it seems like *modular* addition works well. For the same reason, congruence works well with subtraction and multiplication (which is repeated addition). Division, however, that's... more tricky. We'll save that for later!

8.3.1 Aggravating Addition

What exactly are we aiming to show here?

We're aiming to demonstrate that reducing before or after adding doesn't affect the sum, up to congruence. Or,

Proposition 8.1: Modular Addition

If $a \equiv A \pmod{n}$ and $b \equiv B \pmod{n}$, then $a+b \equiv A+B \pmod{n}$. That is,

$$a \equiv A \pmod{n} \text{ and } b \equiv B \pmod{n} \implies a+b \equiv A+B \pmod{n}$$

How do we get a foothold for this proof? How do we compare remainders? This is why we went through the formal definition of congruence. We will be relying on it.

Proof. Let,

$$a \equiv A \pmod{n} \quad \text{and} \quad b \equiv B \pmod{n}.$$

Applying definition 8.2, we deduce:

$$a - A = nk_a \quad \text{and} \quad b - B = nk_b,$$

for some integers k_a and k_b .

Our goal is to demonstrate that $a + b \equiv A + B \pmod{n}$. We will accomplish this by showing that $(a + b) - (A + B) = nK$, for some integer K .

Add the expressions $a - A = nk_a$ and $b - B = nk_b$, and we see,

$$a - A + b - B = nk_a + nk_b.$$

With some rearranging and grouping,

$$(a + b) - (A + B) = nk_a + nk_b = n(k_a + k_b).$$

And since k_a and k_b are integers, their sum $(k_a + k_b)$ is an integer too!

We've found the integer K that we wanted, namely, $K = (k_a + k_b)$. We're done since $(a + b) - (A + B) = nK$ implies $a + b \equiv A + B \pmod{n}$.



By the way, we did not assume a, A, b, B were positive, so this same proof is valid for subtraction too!

Corollary 8.1: Modular Subtraction

If $a \equiv A \pmod{n}$ and $b \equiv B \pmod{n}$, then $a - b \equiv A - B \pmod{n}$.

8.3.2 Problematic Products

We now want to do the same thing we did with addition, but with multiplication:

Proposition 8.2: Modular Multiplication

If $a \equiv A \pmod{n}$ and $b \equiv B \pmod{n}$, then $ab \equiv AB \pmod{n}$. That is,

$$a \equiv A \pmod{n} \text{ and } b \equiv B \pmod{n} \implies a \cdot b \equiv A \cdot B \pmod{n}$$

Proof. We employ the same strategy! We know by definition,

$$a - A = nk_a \quad \text{and} \quad b - B = nk_b,$$

hence,

$$a = A + nk_a \quad \text{and} \quad b = B + nk_b.$$

Since we want to show $ab \equiv AB \pmod{n}$, let's multiply a and b and see what we get.

$$ab = (A + nk_a)(B + nk_b) = AB + Ank_b + Bnk_a + nk_a nk_b.$$

Do you see why we're finished? Take a look,

$$ab = AB + n \underbrace{(Ak_b + Bk_a + nk_a k_b)}_{\text{an integer}}.$$

By the definition of congruence and since we've just shown $ab - AB = n(\text{Integer})$, we conclude $ab \equiv AB \pmod{n}$.



What about division? Is there a division corollary?

8.4. Delicate Division

8.4.1 What does *division* mean?

Division is a tricky operation to manage. Since we are only concerned with whole numbers, what would $5 \div 2 \pmod{7}$ even mean? With normal division, $5 \div 2 = \frac{5}{2}$ because $2 \times \frac{5}{2} = 5$. So standard division is a way to undo standard multiplication. For this reason, we might be motivated to think in terms of undoing modular multiplication.

Let's work out this idea, but as it turns out, it's better to think of the fraction $\frac{1}{2}$ as the number that undoes multiplication by 2. For instance, let's think of the standard division problem $5 \div 2$ as the multiplication problem $5 \times \frac{1}{2}$. In doing so, we are thinking of $\frac{1}{2}$ as the number that gets you back to 1 when you multiply it by 2. Similarly, $24 \div 6 = 24 \times \frac{1}{6}$ where $\frac{1}{6}$ is the number such that $6 \times \frac{1}{6} = 1$.

In terms of modular division, let's interpret: the modular division problem $5 \div 2 \pmod{7}$ as the multiplication problem $5 \times \text{"}\frac{1}{2}\text{"} \pmod{7}$ where $\text{"}\frac{1}{2}\text{"} \pmod{7}$ is the number such that:

$$2 \times \text{"}\frac{1}{2}\text{"} \equiv 1 \pmod{7}.$$

Observe that, $2 \times 4 = 8 \equiv 1 \pmod{7}$. So it seems like $\text{"}\frac{1}{2}\text{"} \equiv 4 \pmod{7}$. Indeed! This is how we choose to define division: we define it in terms of undoing multiplication.

$$\begin{aligned} 2 \times \text{"}\frac{1}{2}\text{"} &\equiv 1 \pmod{7} \quad \text{and} \quad 2 \times 4 \equiv 1 \pmod{7} \\ \implies \text{"}\frac{1}{2}\text{"} &\equiv 4 \pmod{7}. \end{aligned}$$

Quick recap:

The modular division problem $5 \div 2 \pmod{7}$ becomes the modular multiplication problem $5 \times \text{"}\frac{1}{2}\text{"} \pmod{7}$. Furthermore, since $2 \times 4 = 8 \equiv 1 \pmod{7}$ we identify $\text{"}\frac{1}{2}\text{"} \equiv 4 \pmod{7}$. Thus, we are led to think of the division problem as follows:

$$5 \div 2 = 5 \times 4 = 20 \equiv 6 \pmod{7}.$$

One bit of notation before we move on. Since we only care about integers, writing “ $\frac{1}{2}$ ” (mod 7) is clunky and potentially confusing. So, we don’t write “ $\frac{1}{2}$ ”, instead we write 2^{-1} . More generally,

$$\frac{1}{k} \iff k^{-1}.$$

Definition 8.3: Inverse of b is equal to: “ $\frac{1}{b}$ ” = b^{-1}

Let b be an integer. We define the **multiplicative inverse** of b (mod n) to be the integer b^{-1} where $b \times b^{-1} \equiv 1$ (mod n).

We will sometimes (usually) call b^{-1} the integer b ’s **inverse** instead of multiplicative inverse.

Using the former definition, we can now formally define modular division.

Definition 8.4: Modular Division

We define the modular division problem $a \div b$ (mod n) to be equivalent to the modular multiplication problem

$$a \times b^{-1} \pmod{n}.$$

8.4.2 Does Division work?

Okay, so now we know what division means using mods. Is it always true that: if $a \equiv A$ (mod n) and $b \equiv B$ (mod n), then $a \div b \equiv A \div B$ (mod n)? Or, more accurately, $a(b^{-1}) \equiv A(B^{-1})$ (mod n). Let’s do a numerical experiment.

Example 8. Let’s work (mod 11). Consider the congruences

$$15 \equiv 4 \pmod{11} \text{ and } 24 \equiv 2 \pmod{11}.$$

Our goal is to check to see if it's true $15 \div 24 \equiv 4 \div 2 \pmod{11}$. Or, more accurately,

$$15(24^{-1}) \stackrel{?}{\equiv} 4(2^{-1}) \pmod{11}.$$

Step 1: Find $24^{-1} \pmod{11}$ and $2^{-1} \pmod{11}$.

Okay, so we need two integers a, b such that $24a \equiv 1 \pmod{11}$ and $2b \equiv 1 \pmod{11}$.³ Unfortunately, there's no easy way, in general, to find these numbers. Trial and error yield a possible solution:

$$24(17) \equiv 1 \pmod{11} \quad \text{and} \quad 2(6) \equiv 12 \equiv 1 \pmod{11},$$

Which I encourage you to check!

$$\text{Thus, } \boxed{24^{-1} = a = 17} \text{ and } \boxed{2^{-1} = b = 6}.$$

Step 2: “Divide”

Plugging $24^{-1} = a = 17$ and $2^{-1} = b = 6$ into our “division” problem we get:

$$15 \div 24 \equiv 15 \times 24^{-1} \equiv 15 \times 17 \equiv 255 \equiv 2 \pmod{11}$$

and

$$4 \div 2 \equiv 4 \times 2^{-1} \equiv 4 \times 6 \equiv 24 \equiv 2 \pmod{11}.$$

They match!⁴ Nice! ■

Let's try another one.

Example 9. Let's now work $\pmod{10}$ and consider a very similar problem to the one that we just worked through, but now $\pmod{10}$.

³ $2b$ or not $2b$, that is the question...

⁴Hey! Did you notice that $4 \div 2 = 2$ as we might have expected (and hoped)? Our definition of division turns out to be a good one, because it gives back answers that we would think division should give back. For example, $20 \div 5 \pmod{7}$ does equal $4 \pmod{7}$ since $20 \div 5 = 4$.

Observe the following congruences $15 \equiv 5 \pmod{10}$ and $24 \equiv 4 \pmod{10}$. Now let's try to compute,

$$15 \div 24 \pmod{10} \quad \text{and} \quad 5 \div 4 \pmod{10}.$$

Step 1: Find $24^{-1} \pmod{10}$ and $4^{-1} \pmod{10}$.

What number satisfies $24a \equiv 1 \pmod{10}$? *Hint:* If you guess and check some numbers, you might get disappointed. Let's instead ask a similar question that we know how to answer:

First, note that $24a \equiv 5 \pmod{10}$ is equivalent to $24a - 5 = 10k$. So, what number satisfies $24a - 1 = 10k$ equivalently, what integers a and k satisfy,

$$24a - 10k = 1?$$

Recall theorem 6.2 from chapter 6 on page 79 tells us how to find integer solutions to equations of the form: $ax + by = n$. There, we showed that there are **no integer solutions** to $ax + by = n$ if the greatest common divisor $\gcd(a, b)$ (in this case $\gcd(24, 10) = 2$) doesn't divide the right and side n , (in this case 1). It follows that there is no solution to the equation $24a - 1 = 10k$.

Cue the thought: What?!?!??? NO solution?

Yup, and as a consequence, no integer equals $24^{-1} \pmod{10}$. It follows that there is no way to divide by 24 $\pmod{10}$. **This means that some division problems don't make sense to ask.** ■

What failed $\pmod{10}$ and didn't fail $\pmod{11}$?

What failed $\pmod{10}$ was that 24 and 10 share a factor of 2. This then meant that $24x + 10y = 1$ had no integer solution, and as a consequence, there is no $24^{-1} \pmod{10}$, and no way to divide by 24. This wasn't a problem working $\pmod{11}$. Since 11 is prime, we know all non-multiples of 11 are relatively prime to 11, that is $\gcd(a, 11) = 1$ for all a where $11 \nmid a$. Therefore, dividing by 24 and 2 was fine to do $\pmod{11}$.

Remark: By the same logic, you cannot divide by any multiple of 11 (mod 11), such as 11, 22, 33, 44, 55, etc. This is equivalent to dividing by 0, since all these have a residue of 0 (mod 11).

Moral: In order to be able to divide a by b working (mod n) it must be that $\gcd(b, n) = 1$.

Now we can write a lemma and the division corollary.

Lemma 8.1: When $b^{-1} \pmod{n}$ Exists

Let b and n be integers. Then, there exists $b^{-1} \pmod{n}$ if and only if $\gcd(b, n) = 1$.

Proof Idea: We found a connection between the existence of an integer that equals $b^{-1} \pmod{n}$ and there being solutions to $bx + ny = 1$, (through theorem 6.2). I challenge you to fill in the details! You got this!

There is some blank space for you to write in your proof, for future reference!

Proof.



Using this lemma, we can prove the following:

Corollary 8.2: Modular Division

If $a \equiv A \pmod{n}$, $b \equiv B \pmod{n}$, and $\gcd(b, n) = 1$, then $a \div b \equiv A \div B \pmod{n}$ or, better yet,

$$ab^{-1} \equiv AB^{-1} \pmod{n}$$

Proof Idea: We know by the lemma 8.1 that it makes sense to convert division to multiplication (as defined in definition 8.4). Then, we can use modular multiplication, proposition 8.2 to finish out the proof.

There is some blank space for you to write in your proof, for future reference!

Proof.



Let's recap by bringing together all our propositions into one easy-to-reference theorem:

Theorem 8.1: Modular Arithmetic Rules

Let $a \equiv A \pmod{n}$ and $b \equiv B \pmod{n}$. Then the following are true,

$$(1) \quad a + b \equiv A + B \pmod{n}$$

$$(2) \quad a - b \equiv A - B \pmod{n}$$

$$(3) \quad a \cdot b \equiv A \cdot B \pmod{n}$$

If it's also true that $\gcd(b, n) = 1$, then $\gcd(B, n) = 1$ and both b^{-1} and B^{-1} exist so that,

$$(4) \quad a \div b \equiv A \div B \pmod{n}. \text{ Or more precisely, } a \cdot b^{-1} \equiv A \cdot B^{-1} \pmod{n}.$$

Corollary 8.3: Your Corollary: Modular Cancellation

Let $\gcd(b, n) = 1$. If $ab \equiv Ab \pmod{n}$, then $a \equiv A \pmod{n}$.

We're calling this *Your Corollary* because you are going to be the one to prove it! You have the tools and you have the know-how. If you want a hint, you might want to focus on rule (4).

I know there's a lot of stuff for you to prove on your own this chapter! I hope that you have fun with them! There is some blank space for you to write in your proof, for future reference!

Proof.



8.5. A Motivating Mystery (The Solution)

Recall our question from the beginning:

Can you see why you will never find an integer solution to $x^2 + y^2 = N$ with $N = 3, 19, 43, 103, 307$?

We now have the tools to tackle this problem!

Key Idea: If we had no tools at our disposal, we might guess and check different x and y to see what happens. When $N = 3$, it's not too bad to show that there is no integer solution by trial and error, but it becomes unreasonable when N gets large. However, our guess-and-check method has merit. All we need to do is *minimize* the set of numbers we need to guess and check for x and y .

Suppose that there was a solution to $x^2 + y^2 = N$. Then it's also true $x^2 + y^2 \equiv N \pmod{n}$ since we can reduce before or after we multiply and add, by theorem 8.1. Now we don't have so many numbers to check for x and y , we only have $(n - 1)$ integers to guess and check from. These are: $0, 1, 2, 3, \dots, n - 1 \pmod{n}$. This is much better!

The Solution:

With the hindsight of knowing the answer, let $n = 4$.⁵ This means that x and y will be congruent to 0, 1, 2, or 3 (mod 4). Consider the possible values for x^2 and y^2 (mod 4).

$$\begin{array}{ll} 0^2 \equiv 0 \pmod{4}, & 1^2 \equiv 1 \pmod{4}, \\ 2^2 \equiv 0 \pmod{4}, & 3^2 \equiv 1 \pmod{4}. \end{array}$$

Observe that x^2 and y^2 can only be congruent to 0 or 1 (mod 4). It follows that $x^2 + y^2 \equiv 0, 1, 2 \pmod{4}$ and not 3 (mod 4) since the only congruences we can have are: $0 + 0$ and $0 + 1$ and $1 + 0$, and $1 + 1$ and none of those equal 3.

Now take a look at $N \pmod{4}$ for $N = 3, 19, 43, 103, 307$. All these values of N are such that $N \equiv 3 \pmod{4}$, and we just showed that there is no way $x^2 + y^2 \equiv 3 \pmod{4}$! Thus, there is no way to solve the equation $x^2 + y^2 \equiv 3 \pmod{4}$. Hence, there is no solution! WOWWWW!

8.6. And that's a wrap,

Modular arithmetic is a very useful tool to have at your disposal. You'd be surprised to see how many times focusing on remainders simplifies life! (Life in general, not just math problems!) We will be relying on modular arithmetic for the rest of this book, and for this reason, here are some problems that you can try to work out!

8.6.1 Some Practice

The answers are given on 185.

- (1) If $3 \nmid c$, then $c^2 \equiv 1 \pmod{3}$.
- (2) What is the remainder when you divide $1! + 2! + 3! + \cdots + 100!$ by 5?⁶
- (3) Prove the following: If $a \equiv 1 \pmod{n}$, then $\gcd(a, n) = 1$.

⁵The other way to get at $n = 4$ is to try other n 's and realize 4 is the best!

⁶The exclamation point is called a *factorial* and is used as shorthand

8.7. It's Your Time!

We're finally ready to learn about *Fermat's Little Theorem!* It's a beautiful little theorem! We will cover it in the next chapter, but I want to give you a chance to discover it for yourself! So, consider the following problems:

See if you can see a pattern. If so, make a conjecture! Then try to prove it!

$$2^1 \pmod{5}, \quad 2^2 \pmod{5}, \quad 2^3 \pmod{5}, \quad 2^4 \pmod{5},$$

$$3^1 \pmod{5}, \quad 3^2 \pmod{5}, \quad 3^3 \pmod{5}, \quad 3^4 \pmod{5},$$

$$4^1 \pmod{5}, \quad 4^2 \pmod{5}, \quad 4^3 \pmod{5}, \quad 4^4 \pmod{5},$$

and

$$2^1 \pmod{7}, \quad 2^2 \pmod{7}, \quad 2^3 \pmod{7}, \quad 2^4 \pmod{7},$$

$$2^5 \pmod{7}, \quad 2^6 \pmod{7}, \quad 3^1 \pmod{7}, \quad 3^2 \pmod{7},$$

$$3^3 \pmod{7}, \quad 3^4 \pmod{7}, \quad 3^5 \pmod{7}, \quad 3^6 \pmod{7}.$$

If you need more data, try more exponents and more moduli. Feel free to use Wolfram Alpha!

If you want a more suggestive set of problems, try

$$1^{5-1} \pmod{5}, \quad 2^{5-1} \pmod{5}, \quad 3^{5-1} \pmod{5},$$

$$4^{5-1} \pmod{5}, \quad 1^{7-1} \pmod{7}, \quad 2^{7-1} \pmod{7},$$

$$3^{7-1} \pmod{7}, \quad 4^{7-1} \pmod{7}, \quad 5^{7-1} \pmod{7},$$

$$6^{7-1} \pmod{7}, \quad 1^{11-1} \pmod{11}, \quad 2^{11-1} \pmod{11},$$

$$3^{11-1} \pmod{11}, \quad 4^{11-1} \pmod{11}, \quad 5^{11-1} \pmod{11},$$

$$6^{11-1} \pmod{11}, \quad 7^{11-1} \pmod{11}, \quad 8^{11-1} \pmod{11},$$

$$9^{11-1} \pmod{11}, \quad 10^{11-1} \pmod{11}, \quad 11^{11-1} \pmod{11},$$

for: $n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (n-1) \cdot n$. For example, $5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$ and $10! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot 9 \cdot 10$.

Chapter 9

Fermat's Fantastic Little Theorem

“Sometimes when I consider what tremendous consequences come from little things, I am tempted to think there are no little things.”

– Bruce Barton.

Wow, we are already at chapter 9! This is going by fast—for me at least!

9.1. Fermat's Little Theorem

Did you happen to notice any pattern emerge in the data you found at the end of the last chapter? If you didn't try them all out because you thought it would be too much work, at least calculate these:

$$2^{5-1} \pmod{5},$$

$$3^{7-1} \pmod{7},$$

$$2^{11-1} \pmod{11},$$

$$3^{5-1} \pmod{5},$$

$$4^{7-1} \pmod{7},$$

$$5^{11-1} \pmod{11},$$

You might have noticed that every one of the exponentials with the exponent $p-1$ was congruent to 1. That is, $a^{p-1} \equiv 1 \pmod{p}$ for all of the a 's and p 's. In fact, this happens *for every prime* p and *every* integer a that is nonzero mod p . This observation is the content of Fermat's *Little Theorem*.¹

Even though this pattern is quite striking, it will take some work to prove it. So let's get started with a lemma.

Lemma 9.1: The integers $1a, 2a, 3a, \dots, (p-1)a$ are *incongruent* $\pmod{p}$

Let p be prime and let a be an integer where $a \not\equiv 0 \pmod{p}$. Then each of the integers

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

are *incongruent* $\pmod{p}$.

Remark: We will prove the following: Let $1 \leq m \leq n \leq p-1$. If the two integers on our list are congruent $na \equiv ma \pmod{p}$, then they are equal $na = ma$. The contrapositive of this statement is the statement in our Lemma: if $na \neq ma$, then $na \not\equiv ma \pmod{p}$

Proof. Suppose $na \equiv ma \pmod{p}$ where $1 \leq m \leq n \leq p-1$. First, subtract ma from both sides,

$$na - ma = (n - m)a \equiv 0 \pmod{p}.$$

It follows from definition 8.2 (Formal definition of congruence and mod)² that there is some integer k such that

$$(n - m)a = pk.$$

Hence, $p \mid (n - m)a$.

¹And yes, Fermat's Little Theorem is its real name!

²On page 100.

Recall Euclid's Lemma.³ It follows from Euclid's lemma that either $p \mid (n - m)$ or $p \mid a$. But since we assumed $a \not\equiv 0 \pmod{p}$, it cannot be that $p \nmid a$. Therefore, it must be that $p \mid (n - m)$.⁴ Let's label this conclusion,

$$p \mid (n - m). \quad (\square)$$

Recall $1 \leq m \leq n \leq p - 1$, which implies that the difference between n and m is such that $0 \leq (n - m) < p - 1$. Furthermore, since p is prime, no positive integer in this range is divisible by p . The only integer in this range that p divides is *zero*.⁵ Thus, using $(\square)$ we deduce $n - m = 0$ or $n = m$. Consequently, $na = ma$.

We have just shown that the only way we can have $na \equiv ma \pmod{p}$ is to have $na = ma$. The contrapositive of the former statement is what we wanted to prove: if $na \not\equiv ma$, then $na \not\equiv ma \pmod{p}$. Thus, the numbers in the list given in the statement of the lemma are incongruent to one another.



Example 10. Let's take $p = 7$ and $a = 3$. Our list of integers is then,

$$3, 6, 9, 12, 15, 18.$$

Which, when reduced $\pmod{7}$, give,

$$3, 6, 2, 5, 1, 4.$$

Note how all of these are different—as it should be because of our lemma! ■

³On page 90

⁴Can you see why $a \not\equiv 0 \pmod{p}$ implies $p \nmid a$? We can quickly deduce this is the case using the contrapositive: if $p \mid a$, then $a \equiv 0 \pmod{p}$. I'll leave the rest to you!

⁵You might be thinking, “You can't divide by zero!” And you're correct! But p can divide zero. By definition, $p \mid A$ when $A = pk$ for some $k \in \mathbb{Z}$. This condition is satisfied with $A = 0$ and $k = 0$:

$$p \mid 0 \text{ because } 0 = p \cdot 0.$$

However, strange, it's true. All integers divide zero!

A corollary of our lemma is that the list of integers in the lemma, $1a, 2a, 3a, \dots, (p-1)a$ form a complete set of residues (mod p) (see the discussion after definition 8.2 on page 102).

Take a look back at our example with $p = 7$ and $a = 3$. Observe how the second list contains every number $1, 2, 3, 4, 5, 6$ but in a shifted order.

Corollary 9.1: A Complete Set of Residues

Let p be prime and $a \not\equiv 0 \pmod{p}$. Then the list of integers,

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

forms a complete set of residues (mod p).

Proof. Using our previous lemma, we know that the list of integers

$$L = 1a \pmod{p}, 2a \pmod{p}, \dots, (p-1)a \pmod{p}$$

contains no repeats. Hence, the list contains $(p-1)$ integers. Furthermore, each integer in the list is in the range $1 \leq na \leq (p-1)a$. Therefore, the list L must contain every integer $1, 2, 3, \dots, (p-1)$. However, the order may be shuffled.



We're now ready, I'm so excited! Let's both take a deep breath... *inhale*. . . *exhale*. . .

Theorem 9.1: Fermat's Little Theorem

Let p be prime and let $a \not\equiv 0 \pmod{p}$, then

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

Equivalently, for any a ,

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

This proof is real snazzy!

Proof 1. Let p be a prime number and let a be an integer such that $a \not\equiv 0 \pmod{p}$. Consider the product of integers,

$$1a \cdot 2a \cdot 3a \cdots (p-1)a.$$

Recall our modular arithmetic rules on page 112. We know that we can either find the residue of each term in the product and then carry out the multiplication, or we could carry out the multiplication and then find the product's residue. We'll choose to reduce before multiplying.

By corollary 9.1, every term in the product when reduced is the same as the list $1, 2, 3, \dots, (p-1)$. Furthermore, since multiplication is commutative (the order doesn't matter, e.g. $2 \cdot 3 = 3 \cdot 2 = 6$) we deduce,

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

Using the *factorial* we get,

$$(p-1)! \cdot a \equiv (p-1)! \pmod{p} \quad (\clubsuit)$$

Note that every integer on the list $1, 2, 3, \dots, (p-1)$ is relatively prime to p , that is $\gcd(n, p) = 1$ for $n = 1, 2, 3, \dots, (p-1)$. This means that we can use Your Corollary on page 112 and cancel $(p-1)!$ from both sides of $(\clubsuit)$ and get

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

Which concludes our proof!⁶



⁶Note that we did not prove the second statement: for any a we have $a^p \equiv a \pmod{p}$. This version even holds for the case when $a \equiv 0 \pmod{p}$. I'll leave it for you to show!

Example 11. The previous proof was pretty challenging. For this, let's go through an example.

Let's continue using the prime $p = 7$ and integer $a = 3$. We already know that we have the list

$$1(3), 2(3), 3(3), 4(3), 5(3), 6(3) = 3, 6, 9, 12, 15, 18.$$

Next, take the product of all of these elements.

$$3^{7-1}6! = 3 \cdot 6 \cdot 9 \cdot 12 \cdot 15 \cdot 18 \equiv \overbrace{3 \cdot 6 \cdot 2 \cdot 5 \cdot 1 \cdot 4}^{=6!} \pmod{7}.$$

And, since we can cancel each of the integers 1, 2, 3, 4, 5, and 6 from both sides we have,

$$3^{7-1} \cancel{6!} \equiv \cancel{6!} \pmod{7}.$$

and thus, $3^{7-1} \equiv 1 \pmod{7}$. ■

9.2. A Marvelous Second Proof

Proof 2. I have a marvelous second proof of this theorem, but it's too long and I could not fit it here.⁷



9.3. Some Practice, For You!

There isn't much more to Fermat's Little Theorem, but it can be tricky to get used to! To help you on your journey, here are some problems! The solutions are on page 187.

(1) Compute $3^{24} \pmod{11}$ and $7^{115} \pmod{29}$.

⁷How many of you saw this joke coming?

(2) Find $1^{25} + 2^{25} + 3^{25} + \cdots + 100^{25} \pmod{7}$.

(3) A googol is 10^{100} . What day of the week will it be in a googol days? (from whatever day you are reading this on)

9.4. Little Chapter for Little Theorem

What a remarkable statement:

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

for all $a \not\equiv 0 \pmod{p}$ and primes p . You might be wondering if composite numbers can get in on the fun. Or, does this formula only work mod a prime? See if you can answer this question!

Give it a try! For instance, $3^{10-1} \stackrel{?}{\equiv} 1 \pmod{10}$?

You'll find that Fermat's Little Theorem doesn't work all the time for composite moduli. However, Euler did find a generalization. But that's a story for another day/chapter! See if you can work out what it might be!

See you next chapter!

Chapter 10

Euler's Totient function

“Read Euler, read Euler, he is the master of us all!”

– Pierre-Simon Laplace, French Scientist/Mathematician.

What's a *Totient* Function?

What is this strange-sounding function given in this chapter's title? (We know it must be important since it has Euler's name attached to it.)¹ Euler's *totient* function is simply *something* that, when given an integer n , spits out how many positive integers less than n are relatively prime to n .

At first, we might be wondering why we care about *how many positive integers less than n are relatively prime to n* . However, if you're patient, you'll see how incredibly useful this information will become.

¹For those who have not heard of Euler, or who have heard of him but don't know much about him, he's one of the greatest—if not the greatest—mathematician of all time! I recommend taking a look at any talk about Euler given by William Dunham. He's an outstanding communicator, and Euler is a wonderful person to learn about!

With all this said, let's get into it!

Definition 10.1: Euler's Totient Function

Let n be a positive integer. We define Euler's Totient Function, denoted ϕ , by,

$$\phi(n) = \left| \{m \in \mathbb{Z} : \gcd(n, m) = 1 \text{ and } 0 < m \leq n\} \right|. \quad (\text{👉})$$

Furthermore, we will define the set of all natural numbers that are both less than or equal to n and are relatively prime to n by $S_{\phi(n)}$,

$$S_{\phi(n)} = \{m \in \mathbb{Z} : \gcd(n, m) = 1 \text{ and } 0 < m \leq n\}. \quad (\text{👉})$$

Which means that $\phi(n) = |S_{\phi(n)}|$.

This definition needs an example, doesn't it?

Example 12. Let's let $n = 12$. We want to know how many integers between 1 and 12 are relatively prime to 12. First, let's list out all the integers between 1 and 12:

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$$

The even numbers, 2, 4, 6, 8, 10, and 12, all share 2 as a factor with 12. So let's get rid of those. This leaves the odd numbers,

$$1, 3, 5, 7, 9, 11$$

But 3 and 9 share a factor of 3 with 12, so we need to get rid of those, too. Getting rid of 3 and 9 leaves,

$$1, 5, 7, 11,$$

and you can check that all these numbers left share no factors with 12. Thus, $\phi(12) = 4$ and $S_{\phi(12)} = \{1, 5, 7, 11\}$. ■

Example 13. Likewise, you can check that $\phi(15) = 8$ by considering the following:

$$\begin{aligned} S_{\phi(15)} &= \{1, 2, \cancel{3}, 4, \cancel{5}, \cancel{6}, 7, 8, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, 14, \cancel{15}\} \\ &= \{1, 2, 4, 7, 8, 11, 13, 14\} \end{aligned}$$

■

Example 14. And one more for good measure. We can see that $\phi(19) = 18$ using,

$$\begin{aligned} S_{\phi(19)} &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, \cancel{19}\} \\ &= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18\}. \end{aligned}$$

Notice that 19 is prime and $\phi(19) = 19 - 1 = 18$? Do you think this happens in general? That is, is it true that $\phi(p) \stackrel{?}{=} p - 1$ for any prime p .

■

Example 15. Oh, note that $\phi(1) = 1$ since 1 is relatively prime to 1.

■

Euler's totient function has many wonderful and beautiful properties. Here are a few:

Proposition 10.1: Euler's Totient Function Properties

Let $\phi(n)$ be Euler's totient function. Then,

1. $\phi(p) = p - 1$ if and only if p is prime;
2. if p is prime and k is a positive integer, then

$$\phi(p^k) = p^{k-1}(p - 1);$$

3. if $\gcd(n, m) = 1$, then $\phi(nm) = \phi(n) \cdot \phi(m)$; and
4. if $n = p_a^{k_a} p_b^{k_b} \cdots p_m^{k_m}$, then

$$\phi(n) = n \left(1 - \frac{1}{p_a}\right) \left(1 - \frac{1}{p_b}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$

We want to try to prove these statements. Here we go!

See if you can work through some of the statements in the proposition! Even if you cannot prove them, try calculating some examples and see if you can make the statements intuitive.

★ *Proof of 1.* This is an if and only if statement, so we have to do each direction separately.

Forward: If $\phi(p) = p - 1$ then, p is prime.

We will do a proof by contradiction. Let $\phi(p) = p - 1$ and assume that p is not a prime number. Since p isn't a prime, there is a natural number a where $1 < a < p$ that divides p . Using Our First Lemma on page 57, it follows that $\gcd(a, p) = a \neq 1$. Thus $a \notin S_{\phi(p)}$, consequently $S_{\phi(p)}$ has at most $p - 2$ elements. Hence, $\phi(p) = |S_{\phi(p)}| \leq p - 2$ contradicting that $\phi(p) = p - 1$.

Backward: If p is prime then, $\phi(p) = p - 1$.

Let p be prime, then every number less than p (and greater than or equal to 1) is relatively prime to p . Thus, $S_{\phi(p)} = \{1, 2, 3, \dots, p-1\}$ consequently, $\phi(p) = p-1$.



★★ *Proof of 2.* Let p be prime and let $k \in \mathbb{Z}$ be positive. In order to determine $\phi(p^k)$, we will need to count the number of multiples of p that are less than or equal to p^k . From there, we subtract the number of multiples of p that are less than or equal to p^k from the total number of positive integers less than or equal to p^k . The result of these steps will be $\phi(p^k)$.

In the remainder of the proof, let the set S be equal to $S = \{1, 2, 3, \dots, p^k\}$.

Step 1: How many multiples of the prime p are in the set of integers S ?

The subset $T \subseteq S$ below,

$$T = \{1p, 2p, \dots, pp, \dots, p^2p, \dots, p^{k-1}p\}$$

contains all the multiples of p that we wanted to count. By inspection, there are p^{k-1} multiples.

Step 2: How many integers are in the set S ? Or, how many positive integers are less than or equal to p^k ?

There are p^k integers in the set S .

Step 3: Subtract step 2 from step 1 to determine how many elements the set $S_{\phi(p^k)}$ has.

There are $|S| - |T| = p^k - p^{k-1} = p^{k-1}(1 - p)$ elements in the set $S_{\phi(p^k)}$ as desired.



To clean up the proof for part 3, we will first prove a lemma. You know what they say, when life gives you lemmas, make lemmade.

Lemma 10.1: The Lemmanade lemma

If $\gcd(b, m) = 1$, then $\gcd(am + b, m) = 1$.

Proof of Lemma. Let $\gcd(b, m) = 1$. We will use corollary 6.1 on page 77, which states: there exists an integer solution to $ax + by = 1$ if and only if $\gcd(a, b) = 1$. So, we are going to find a solution to the equation: $(am + b)x + my = 1$ to prove $\gcd(am + b, m) = 1$.

Since $\gcd(b, m) = 1$, there is an integer solution to the equation $bx + my = 1$. Let's denote this solution by x_0 and y_0 ,

$$bx_0 + my_0 = 1.$$

Let's add and subtract ax_0 from y_0 ,

$$bx_0 + m(y_0 + ax_0 - ax_0) = 1.$$

We can move terms around to give,

$$(am + b)x_0 + m(y_0 - ax_0) = 1.$$

Which is the integer solution we wanted to find: $x = x_0$ and $y = y_0 - ax_0$! Thus, by corollary 6.1 $\gcd(am + b, m) = 1$.



There is, as always, another way to prove our lemonade lemma. It doesn't use the equation $ax + by = 1$. I'll let you try to discover it, but I will also leave it in this footnote!²

On to the proof of part 3. As a reminder, we want to prove:

If $\gcd(n, m) = 1$, then $\phi(nm) = \phi(n) \cdot \phi(m)$.

²I hope you gave it a go! Even if you couldn't find any other proof, it's great that you tried!

Our goal is to show: $\gcd(am + b, m) = \gcd(b, m)$ where we are assuming a, b are integers. We'll do this by first focusing on $d = \gcd(b, m)$. Since d divides both m we conclude $d \mid am$. Thus, $d \mid (am + b)$ since $d \mid b$. It follows that $d \mid \gcd(am + b, m)$. Therefore, $d \leq \gcd(am + b, m)$ (why?).

★★★ *Proof of 3.* Let $\gcd(n, m) = 1$. First, right off the bat, we know that there are $\phi(m)$ integers that are less than m and relatively prime to m by the definition of ϕ . Let's denote these integers by $b_1, b_2, \dots, b_{\phi(m)}$. That is,

$$S_{\phi(m)} = \{b_1, b_2, \dots, b_{\phi(m)}\}.$$

We will consider the numbers of the form: $am + b_i$ that are in the set of positive integers less than nm ,

$$am + b_i \in \{1, 2, 3, \dots, m, \dots, nm\}.$$

By our lemmnade lemma, we know $\gcd(am + b_i, m) = \gcd(b_i, m) = 1$. This fact motivates us to focus on subsets of $\{1, 2, \dots, nm\}$ that consist of elements of the form $am + b_i$, one for each of the different $b_1, b_2, \dots, b_{\phi(m)} \in S_{\phi(m)}$;

$$\begin{aligned} B_1 &:= \{m + b_1, 2m + b_1, 3m + b_1, \dots, (n-1)m + b_1\} \\ B_2 &:= \{m + b_2, 2m + b_2, 3m + b_2, \dots, (n-1)m + b_2\} \\ &\vdots \\ B_{\phi(m)} &:= \{m + b_{\phi(m)}, 2m + b_{\phi(m)}, \dots, (n-1)m + b_{\phi(m)}\} \end{aligned}$$

Note: every element in every one of the above sets is relatively prime to m by our lemonade lemma.

Recall that our goal is to find all the integers relatively prime to both m and n . So far, we have found the integers relatively prime to m . We will next count the number of integers in the sets B_i that are relatively prime to n .

Let's shift our attention to $D = \gcd(am + b, m)$, we know D divides m , am , and $am + b$. From these, we conclude $D \mid ((am + b) - am)$ or $D \mid b$. Thus, $D \leq d$. But, since $d \leq D$, it must be $d = D$, and in our lemma, $d = 1$.

To this end, consider one of the sets B_i ,

$$B_i = \{m + b_i, 2m + b_i, 3m + b_i, \dots, (n-1)m + b_i\}.$$

First, we claim that every one of the $n-1$ integers in B_i is different (mod n). To see this, suppose,

$$a_1m + b_i \equiv a_2m + b_i \pmod{n}.$$

Where $1 \leq a_1 \leq a_2 \leq n-1$ (so that $a_1m + b_i, a_2m + b_i \in B_i$). With some modular arithmetic, we deduce,

$$a_1m \equiv a_2m \pmod{n}.$$

Recall $\gcd(n, m) = 1$, so we know that we can safely cancel m from both sides (recall Your Corollary 8.3 on page 112) and get,

$$a_1 \equiv a_2 \pmod{n}.$$

Furthermore, since a_1 and a_2 are less than n it must be that $a_1 = a_2$, which is what we wanted to show.³

 **TAKEAWAY:** Every integer in B_i is different (mod n).

Using that every number in B_i is different (mod n) and that $|B_i| = (n-1)$, we deduce that each set B_i forms a complete set of residues (mod n).

 **TAKEAWAY:** Each set B_i forms a complete set of residues (mod n).

We will now show that there are $\phi(n)$ integers in B_i that are relatively prime to n .

We know that there are $\phi(n)$ positive integers less than n relatively prime to n . Let t be one of these integers. Since $1 \leq t \leq n-1$, there is some element $a_tm + b_i$ in the set B_i where

³This follows from the chain of logic: $a_1 \equiv a_2 \pmod{n} \implies a_2 - a_1 = nk$ for some integer k , and since $1 \leq a_1 \leq a_2 \leq (n-1)$, it must be that: $0 \leq a_2 - a_1 = nk < n$. Thus $k = 0$ and hence $a_1 = a_2$.

$a_tm + b_i \equiv t \pmod{n}$. This is because B_i forms a complete set of residues $\pmod{n}$ . We claim this implies $\gcd(a_tm + b, n) = 1$. *Note the similarities between what we need to prove and our lemmanade lemma.*

We aim to prove: if $a_tm + b \equiv t \pmod{p}$ and $\gcd(t, n) = 1$, then $\gcd(a_tm + b, n) = 1$. To see this, let $\gcd(a_tm + b, n) = d$. Since $a_tm + b \equiv t \pmod{n}$, we deduce by definition,

$$am_t + b - t = ns,$$

for some integer s . Solving t we see,

$$t = a_tm + b - ns,$$

which shows $d \mid t$ since we already know that $d \mid (a_tm + b)$ and $d \mid n$. But, $d \mid t$ and $d \mid n$ imply $d = 1$ since it was assumed that $\gcd(n, t) = 1$.

Therefore, there is $\phi(n)$ integers relatively prime to n for every set B_i . And since there are $\phi(m)$ such sets, there are $\phi(nm) = \phi(n)\phi(m)$ positive integers less than nm that are relatively prime to nm .



Vocabulary alert: When a function is defined for only integer inputs, like Euler's Totient function $\phi(n)$, we call the function **an integer function**. Furthermore, when the integer function has the property that $f(nm) = f(n)f(m)$ when $\gcd(n, m) = 1$, we call it **multiplicative**. So, we just showed that Euler's Totient function is a multiplicative integer function.

Whoa, that was a long and technical proof! Feel free to take a break and put the book down for a few!

Remark: This simply says that, given some prime factorization, we can compute $\phi(n)$ using the formula above. For example,

consider $\phi(20)$. After factoring 20 we find $20 = 2^2 \cdot 5^1$. Thus, by the formula given in proposition 10.1 part (iv):

$$\phi(20) = 20 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 8.$$

Which you can check!

★★★★ *Proof of 4.* I challenge you to finish this one! As a hint, use what we have shown so far. For example, for primes $p_a \neq p_b$ we have $\gcd(p_a^{k_a}, p_b^{k_b}) = 1$. Then, you can use part (iii) to conclude,

$$\phi(p_a^{k_a} p_b^{k_b}) = \phi(p_a^{k_a}) \phi(p_b^{k_b}).$$

Then, through an induction argument, you can show,

$$\phi(n) = \phi(p_a^{k_a}) \phi(p_b^{k_b}) \cdots \phi(p_m^{k_m}).$$

I believe in you! In fact, I believe in you so much that I'll leave some open space for you:



10.1. Time For Practice!

Euler's totient function is a wonderful and useful tool for much of number theory. We will see how we can use this tool to generalize Fermat's Little Theorem! It's so awesome! We will end with a few problems for you to try out:

-
- (1) What is $\phi(100)$?
 - (2) Prove that for every integer n greater than 2, $\phi(2)$ is even.
 - (3) Prove the two statements: (i) If n is odd, then $\phi(2n) = \phi(n)$, and (ii) If n is even, then $\phi(2n) = 2\phi(n)$.

The solutions are on page 189

Chapter 11

The Chinese Remainder Theorem

*“Different locks must be opened with different keys.
Every problem we face in life will require a different
set of skills to overcome.”*

– Chinese Proverb [7].

Way Back When...

Do you remember when you were asked to solve a system of equations back in algebra class? In the case that you don't, here's a brief reminder. The goal of these types of questions was to have you find a value of x and/or y that satisfied two equations at the same time. For example, $x = 2$ satisfies $5x + 2 = 12$ and $23x - 10 = 36$. Or, $x = 2$ and $y = 3$ satisfy $y = 5x + 2$ and $2y - 3x = 18$ simultaneously.

We are about to do something similar with what are called *modular congruences*. Modular congruence is the fancy (and mathy) way to say that we are going to find solutions (values of x) that satisfy congruences like $ax \equiv b \pmod{n}$.

Let's get started!

11.1. Solving A Linear Congruence

Let's begin with some examples. Let's try to solve the following congruences $5x \equiv 3 \pmod{7}$, $5x \equiv 3 \pmod{9}$, and $5x \equiv 3 \pmod{10}$.

Solving $5x \equiv 3 \pmod{7}$.

The good thing about solving congruences is that there isn't an infinite number of possible solutions. If our congruence is $\pmod{n}$, then there are only n possible values for x . In this case, there are 7 possible solutions: $x = 0, 1, 2, 3, 4, 5, 6$. Trial and error gives:

$$\begin{array}{ll} 5 \cdot 0 \equiv 0 \pmod{7} \\ 5 \cdot 1 \equiv 5 \pmod{7} \\ \star \quad 5 \cdot 2 = 10 \equiv 3 \pmod{7} & \star \\ 5 \cdot 3 = 15 \equiv 1 \pmod{7} \\ 5 \cdot 4 = 20 \equiv 6 \pmod{7} \\ 5 \cdot 5 = 25 \equiv 4 \pmod{7} \\ 5 \cdot 6 = 30 \equiv 2 \pmod{7} \end{array}$$

So that our solution is $x \equiv 2 \pmod{7}$. Note that our solution is any integer that is congruent to 2 $\pmod{7}$, for instance $5 \cdot 9 = 45 \equiv 3 \pmod{7}$. We can also express our solution as $x = 2 + 7k$ for $k \in \mathbb{Z}$. This form follows from the definition of congruence (equation ①) back on page 100

Solving $5x \equiv 3 \pmod{9}$.

Again, trial and error gives,

$$5 \cdot 0 \equiv 0 \pmod{9}$$

$$5 \cdot 1 \equiv 5 \pmod{9}$$

$$5 \cdot 2 = 10 \equiv 1 \pmod{9}$$

$$5 \cdot 3 = 15 \equiv 6 \pmod{9}$$

$$5 \cdot 4 = 20 \equiv 2 \pmod{9}$$

$$5 \cdot 5 = 25 \equiv 7 \pmod{9}$$

$$\star \quad 5 \cdot 6 = 30 \equiv 3 \pmod{9} \quad \star$$

$$5 \cdot 7 = 35 \equiv 8 \pmod{9}$$

$$5 \cdot 8 = 40 \equiv 4 \pmod{9}$$

Thus, we have $x \equiv 6 \pmod{9}$, or $x = 6 + 9k$ for $k \in \mathbb{Z}$.

Solving $5x \equiv 3 \pmod{10}$.

Try to give this one a go on your own, and then continue.

Yet again, some trial and error gives,

$$5 \cdot 0 \equiv 0 \pmod{10}$$

$$5 \cdot 1 \equiv 5 \pmod{10}$$

$$5 \cdot 2 = 10 \equiv 0 \pmod{10}$$

$$5 \cdot 3 = 15 \equiv 5 \pmod{10}$$

$$5 \cdot 4 = 20 \equiv 0 \pmod{10}$$

$$5 \cdot 5 = 25 \equiv 5 \pmod{10}$$

$$5 \cdot 6 = 30 \equiv 0 \pmod{10}$$

$$5 \cdot 7 = 35 \equiv 5 \pmod{10}$$

$$5 \cdot 8 = 40 \equiv 0 \pmod{10}$$

$$5 \cdot 9 = 45 \equiv 5 \pmod{10}$$

Wait, there isn't a solution! Is this surprising? Should we have seen this coming?

Why isn't there a solution to $5x \equiv 3 \pmod{10}$? It's because the equation $5x - 3 = 10y$ doesn't have a solution. We know this from our previous work in Chapter 6: $ax + by = 1$.

As we just discussed, one way we can interpret why there is no solution uses our work regarding Diophantine equations like $ax + by = 1$, however, there is another interpretation that uses our work on modular arithmetic.¹

How would we solve the equation $5x = 3$? We'd most likely divide both sides by 5, giving $x = \frac{3}{5}$. However, we've seen in chapter 8 on page 112 that we can safely divide both sides of $5x \equiv 3 \pmod{10}$ by 5 if and only if $\gcd(5, 10) = 1$. But $\gcd(5, 10) = 5 \neq 1$, therefore we cannot divide by 5. This is one way to see that we cannot find a solution.

However, we don't always need $\gcd(a, n) = 1$ in order to solve $ax \equiv b \pmod{n}$. For instance, there is a solution to $5x \equiv 5 \pmod{10}$. There are actually five solutions, $x = 1, 3, 5, 7, 9$. So there's a little more to this. As we will see, it's enough for $\gcd(a, n)$ to divide b in order to be able to solve $ax \equiv b \pmod{n}$. This is why $5x \equiv 5 \pmod{10}$ has a solutions, because $\gcd(5, 10) \mid 5$.

Let's record our work and then prove it for the general situation.

Theorem 11.1: Solvability of Linear Congruences

Let a , b , and n be integers and denote $d = \gcd(a, n)$. The linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$.

Proof. Let a , b , and n be integers and denote $d = \gcd(a, n)$. Let's do what we usually do and break up our "if and only if" proofs into two parts.

Forward: If there is a solution to $ax \equiv b \pmod{n}$, then $d \mid b$.²

¹Recall that Diophantine equations are equations that we want integer solutions to.

²This proof mimics proofs that we saw back in Chapter 6: $ax + by =$

Let x_0 be a solution to the linear congruence $ax \equiv b \pmod{n}$. By definition of congruence, we deduce,

$$ax_0 - b = nk,$$

for some integer k . Solving for b we get,

$$b = ax - nk.$$

Recall $d = \gcd(a, n)$, so that $d \mid (ax - nk)$, and therefore $d \mid b$.

Backward: If $d \mid b$ then, there is a solution to $ax \equiv b \pmod{n}$.

Let $d \mid b$ and hence $b = dt$ for some integer t . We aim to show that there is a solution to $ax \equiv b \pmod{n}$. Since $d = \gcd(a, n)$ we deduce, using Bézout's Identity Generalized on page 77, that there are integers x_0 and y_0 such that,

$$ax_0 - ny_0 = d.$$

Multiplying through by t gives,

$$a(x_0t) - n(y_0t) = dt = b.$$

Letting $x = x_0t$ we have found our desired solution, since the above equation is equivalent to: $a(x_0t) \equiv b \pmod{n}$.



Now that we know when there is a solution, we'd like to find a general form of the solution. For this, we'll need something that we've seen before, but cast in a new light.

Corollary 11.1: Solution Form

Let a , b , and n be integers and denote $d = \gcd(a, n)$. If $d \mid b$ then, the linear congruence $ax \equiv b \pmod{n}$ has a solution set:

$$x = x_0 + k \left(\frac{n}{d} \right).$$

Where x_0 is the solution guaranteed by Theorem 11.1 (Solvability of Linear Congruences) and k is an integer.

Proof. Observe that $ax \equiv b \pmod{n}$ is equivalent to $ax - ny = b$. Therefore, they have the same solution set. Take a look back at theorem 6.2, on page 79, and the proof given in subsection 6.4.2 *Back to The Proof of Zero or Infinite?* on page 83. There we showed that the equation $ax + by = n$ has a solution set given by equation ,

$$x = x_0 - \left(\frac{b}{d} \right) k \quad \text{and} \quad y = y_0 + \left(\frac{a}{d} \right) k \quad \left(\text{graduation cap icon} \right)$$

After making the appropriate substitutions, we arrive at our solution set for x .



11.2. Back to Linear Congruences

Not so bad, huh? Our new goal is to determine the number of solutions that the linear congruence $ax \equiv b \pmod{n}$ has. This might sound like a strange question since, if x is a solution, then for every integer k we also have $x + k \left(\frac{n}{d} \right)$ as a solution by the above corollary; and we've also seen this in our examples. For instance, we said that our solution to $5x \equiv 3 \pmod{7}$ was $x \equiv 2 \pmod{7}$ or, $x = 2 + 7k$ for $k \in \mathbb{Z}$

So we have infinitely many solutions, one for each integer k . So, we're done, right? There are infinitely many solutions.

Well, yes this is true, however, when we are working $(\text{mod } n)$, we don't think of x and $x + kn$ as different solutions since they are congruent, $x \equiv x + nk \pmod{n}$ for all integers k . What I should have asked is, *how many different solutions are there (mod n)?* In other words, if we only count solutions x_1 and x_2 that are distinct, by which we mean the solutions are incongruent $(\text{mod } n)$, i.e., $x_1 \not\equiv x_2 \pmod{n}$.

Theorem 11.2: Number of Solutions of Linear Congruences

Let a , b , and n be integers and denote $d = \gcd(a, n)$. If $d \mid b$, then there are d incongruent solutions $(\text{mod } n)$ to the linear congruence $ax \equiv b \pmod{n}$.

Proof. Let a , b , and n be integers and denote $d = \gcd(a, n)$. By our first theorem, we know that a solution exists. All we have to show is that there are d incongruent solutions $(\text{mod } n)$. To that end, let x_0 be such a solution. Then, Corollary (Solution Form), we know the form of the solution is

$$x = x_0 + k \left(\frac{n}{d} \right).$$

We therefore claim that the family of incongruent solutions $(\text{mod } n)$ is given by:

$$x_0, x_0 + \frac{n}{d}, x_0 + 2 \left(\frac{n}{d} \right), \dots, x_0 + (d-1) \left(\frac{n}{d} \right).$$

To prove this claim, we need to show three things; (i) every one of the integers above is a solution, (ii) all the claimed solutions are incongruent $(\text{mod } n)$, and (iii) any one of the infinitely many solutions to $ax \equiv b \pmod{n}$ is congruent to one of the solutions above $(\text{mod } n)$.

NOTE: Since we know there is a solution to $ax \equiv b \pmod{n}$, by theorem 11.1, we will let x_0 be a solution so that $ax_0 \equiv b \pmod{n}$.

(i) Every integer of the form $x_0 + k \left(\frac{n}{d} \right)$ is a solution to $ax \equiv b \pmod{n}$.

First, we show that any integer of the form $x_0 + k \left(\frac{n}{d} \right)$ is a solution to $ax \equiv b \pmod{n}$. To this end, observe the following,

$$\begin{aligned} a \left(x_0 + k \left(\frac{n}{d} \right) \right) &\equiv ax_0 + k \left(\frac{an}{d} \right) \pmod{n} \\ &\equiv b + nk \left(\frac{a}{d} \right) \pmod{n}, && \text{since } ax_0 \equiv b \pmod{n} \\ &\equiv b \pmod{n} \end{aligned}$$

Where we used that $d \mid a$ implies that $\frac{a}{d}$ is an integer. So, we see that every $x_0 + k \left(\frac{n}{d} \right)$ is a solution.

(ii) The list of solutions are all incongruent $\pmod{n}$.

We will prove the statement: if two solutions are congruent, then they are the same solution. With this goal in mind, let $x_0 + k \left(\frac{n}{d} \right)$ and $x_0 + t \left(\frac{n}{d} \right)$ be two solutions from our set such that $0 \leq k \leq t \leq d-1$ and

$$x_0 + k \left(\frac{n}{d} \right) \equiv x_0 + t \left(\frac{n}{d} \right) \pmod{n}.$$

With a little rearranging, we deduce the following,

$$t \left(\frac{n}{d} \right) \equiv k \left(\frac{n}{d} \right) \pmod{n}$$

or

$$t \left(\frac{n}{d} \right) - k \left(\frac{n}{d} \right) = ns.$$

Where $s \geq 0$ and is an integer. Canceling the n and moving the d over to the right we get,

$$t - k = ds.$$

Since we chose $0 \leq k \leq t \leq d-1$ it must be that $0 \leq t-k \leq d-1$. Or, that $0 \leq ds < d$. This implies that $s = 0$ and consequently, $t-k = ds = 0$, since $s \geq 0$ and is an integer. Therefore, $t = k$ and our two solutions were really the same solution.

(iii) Every solution (mod n) is in our family of solutions.

Let X be a solution to $ax \equiv b \pmod{n}$. By our Corollary (Solution Form), X is of the form:

$$X = x_0 + t \left(\frac{n}{d} \right).$$

If $0 \leq t \leq d-1$ then X is in our solution set, so let's assume that t is outside of this interval. By the division algorithm, we write $t = qd + r$ for $0 \leq r < d$. Thus,

$$\begin{aligned} X &= x_0 + (qd + r) \left(\frac{n}{d} \right) \\ &= x_0 + qn + r \left(\frac{n}{d} \right) \\ &\equiv x_0 + r \left(\frac{n}{d} \right) \pmod{n}. \end{aligned}$$

And since $0 \leq r < d$, we conclude that X is congruent to a solution already in our solution set.



We're ready for the pièce de résistance.

11.3. The Chinese Remainder Theorem

When your algebra class wanted to get really challenging, they would ask you to solve multiple equations at once! For instance, what values of x and y solve both $2x + 3y = 1$ and $4x - 10y = 3$? We are now about to do the same thing and ask for a solution to multiple congruences!

Theorem 11.3: The Chinese Remainder Theorem

Let $n_1, n_2, \dots, n_k$ be positive integers that are pairwise relatively prime (more precisely, $\gcd(n_i, n_j) = 1$ when $i \neq j$). Then the system of linear congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

has a unique solution $\pmod{N}$ where $N := n_1 n_2 \cdots n_k$ is the product of all the n_i 's.

Proof. We'll not only show that there is such a solution, we will also construct an expression for the solution!

First, let

$$N_t := \frac{n_1 n_2 \cdots n_k}{n_t} = \frac{N}{n_t} = n_1 n_2 \cdots n_{t-1} n_{t+1} \cdots n_k$$

for $1 \leq t \leq k$. Now, observe that $\gcd(N_t, n_t) = 1$ for all t . This is because $\gcd(n_i, n_j) = 1$ for all $i \neq j$.

By our first theorem, there is a solution to the linear congruence,

$$N_t x \equiv 1 \pmod{n_t} \quad (\text{🔑})$$

for $1 \leq t \leq k$, since $\gcd(N_t, n_t) = 1$. Denote this solution x_t . Thus, $N_t x_t \equiv 1 \pmod{n_t}$.

We claim that,

$$X = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_k N_k x_k \quad (\text{🔒})$$

is a solution to the system of congruences given in the theorem. To see this, observe that,

$$\begin{aligned} X &= a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots a_i N_i x_i \cdots a_k N_k x_k \\ &\equiv 0 + 0 + \cdots + \cdots + a_t N_t x_t + \cdots + 0 \pmod{n_t} \\ &\equiv a_t N_t x_t \pmod{n_t} \end{aligned}$$

Where we used that $N_i \equiv 0 \pmod{n_t}$ for $i \neq t$, since $n_t \mid N_i$ when $i \neq t$.

Recall we chose x_t so that $N_t x_t \equiv 1 \pmod{n_t}$. Thus,

$$X \equiv a_t N_t x_t \equiv a_t \pmod{n_t}$$

showing that X solves each congruence in the theorem as we claimed.

All we have left to do is show that X is a unique solution $\pmod{N}$. To this end, let $\overline{X}$ be another solution to the set of congruences. Then, for any i

$$X \equiv a_i \equiv \overline{X} \pmod{n_i}$$

Therefore, $X - \overline{X} = n_i m$ for all i . Recall that all the $n_1, n_2, \dots, n_k$ are pairwise relatively prime so that $\gcd(n_i, n_j) = 1$ when $i \neq j$. Consider when $i = 1$ and $j = 2$.

Using the previous paragraph, we have,

$$X \equiv a_1 \equiv \overline{X} \pmod{n_1} \quad (\text{6})$$

implying $X - \overline{X} = n_1 m_1$ for some $m_1 \in \mathbb{Z}$ and,

$$X \equiv a_2 \equiv \overline{X} \pmod{n_2} \quad (\text{7})$$

implying $X - \overline{X} = n_2 m_2$ for some $m_2 \in \mathbb{Z}$.

Equation (7) implies $n_2 \mid (X - \overline{X})$. Which, using (6)'s equivalent statement: $X - \overline{X} = n_1 m_1$ for some $m_1 \in \mathbb{Z}$ we deduce,

$$n_2 \mid n_1 m_1.$$

By Euler's Lemma (see footnote³) we conclude $n_2 \mid m_1$, since $\gcd(n_1, n_2) = 1$. Therefore, $m_1 = n_2 m_2$ and thus $X - \overline{X} = n_1 m_1 = n_1 n_2 m_2$.

We can apply the same series of steps as the previous paragraph using n_3 to conclude $n_3 \mid (X - \overline{X})$. Which, using our previous results, implies both $n_3 \mid n_1 n_2 m_2$ and $n_3 \mid m_2$ by Euler's Lemma. Hence, $m_2 = n_3 m_3$ and $X - \overline{X} = n_1 n_2 n_3 m_3$.

Continuing this same process for each of the for each n_i we get,

$$X - \overline{X} = n_1 n_2 n_3 \cdots n_k m_k = N m_k.$$

Hence,

$$X \equiv \overline{X} \pmod{N}$$

as we set out to show.



11.4. Example Time

Let's get our hands dirty with some calculations!

Example 16. Let's solve the system of congruences below:

$$5x \equiv 1 \pmod{3} \quad 2x \equiv 3 \pmod{5} \quad 2x \equiv 6 \pmod{11}$$

First, to use the Chinese Remainder Theorem, we must make sure that our moduli are pairwise relatively prime.

$$\gcd(3, 5) = 1 \quad \gcd(3, 11) = 1 \quad \gcd(5, 11) = 1$$

So we are all set! We can use the Chinese Remainder Theorem.

Next, we need to rewrite each of the congruences in our system in the form $x \equiv a \pmod{n}$. We do this by 'dividing' by each of the coefficients in our congruences,

$$x_1 \equiv 1 \cdot 5^{-1} \pmod{3} \quad x_2 \equiv 3 \cdot 2^{-1} \pmod{5} \quad x_3 \equiv 6 \cdot 2^{-1} \pmod{11}$$

³Recall, Euler's Lemma: Let a , b , and c be integers. If $c \mid ab$ and $\gcd(a, c) = 1$. Then, $c \mid b$.

We do this by trial and error, i.e., guessing! Guessing gives,

$$\begin{array}{lll} x \equiv 2 \pmod{3}, & x \equiv 4 \pmod{5}, & x \equiv 3 \pmod{11} \\ \implies a_1 = 2 & \implies a_2 = 4 & \implies a_3 = 3 \end{array}$$

Let's now determine the values of the N 's

$$\begin{aligned} N &= 3 \cdot 5 \cdot 11 = 165 \\ N_1 &= N/3 = 55 \\ N_2 &= N/5 = 33 \\ N_3 &= N/11 = 15 \end{aligned}$$

Now we need to solve the congruences (🔒) to determine the x_i in (🔒).

$$55x_1 \equiv 1 \pmod{3}, \quad 33x_2 \equiv 1 \pmod{5}, \quad 15x_3 \equiv 1 \pmod{11}$$

We can reduce each of the previous congruences to be,

$$1x_1 \equiv 1 \pmod{3}, \quad 3x_2 \equiv 1 \pmod{5}, \quad 4x_3 \equiv 1 \pmod{11}$$

This makes it easier to determine our solutions:

$$x_1 \equiv 1 \pmod{3}, \quad x_2 \equiv 2 \pmod{5}, \quad x_3 \equiv 3 \pmod{11}.$$

Plugging in all of our results gives,

$$\begin{aligned} X &= a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots a_k N_k x_k \\ &= 2 \cdot 55 \cdot 1 + 4 \cdot 33 \cdot 2 + 3 \cdot 15 \cdot 3 \\ &= 509 \end{aligned}$$

Most often, we will want the smallest solution $(\text{mod } N)$. In this case, after reducing $509 \pmod{165}$ we get our reduced solution, $X \equiv 14 \pmod{165}$. Which you can plug back into our original set of congruences to check. ■

11.5. Closing Remarks

The Chinese Remainder Theorem is a beautiful result that has been known for thousands of years! That is remarkable since modular arithmetic was only developed in 1801! There is a fascinating history behind the name, *The Chinese Remainder Theorem*. Since I'm not a historian, you should look up some of this history—and maybe email me if you find something that you think is particularly awesome. Along the way, you'll find some fun puzzles that you can now solve using the results from this chapter!

Chapter 12

Euler's Little Theorem

“Little by little, a little becomes a lot.”

– Tanzanian proverb.

As you might have guessed, we're going to learn about Euler's generalization of Fermat's Little Theorem, which I've dubbed: Euler's Little Theorem. Note, this is only what I call the theorem; unfortunately, no one else seems to call it this!¹ But, maybe if you start to refer to this result as Euler's Little Theorem then it'll catch on!

12.1. Let's Discover it Together!

Recall Fermat's Little Theorem,

Fermat's Little Theorem (Standard): Let p be prime and let $a \not\equiv 0 \pmod{p}$, then

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

¹The theorem is called *Euler's Totient Theorem*.

Let's take a moment and remember how the proof of Fermat's Little Theorem went. For all of the following steps, let $a \not\equiv 0 \pmod{p}$.

Sketch of the Proof for Fermat's Little Theorem

1. First, we proved corollary 9.1 on page 120 that stated: The list of integers $1a, 2a, 3a, \dots, (p-1)a$ form a complete set of residues.
2. We took the product of all the elements in the following list:

$$1a \cdot 2a \cdot 3a \cdots (p-1)a.$$

3. We reduced each term in the product using step 1 to conclude:

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

4. Since p is prime, all of the positive integers $1, 2, \dots, (p-1)$ are relatively prime to p . Equivalently,

$$S_{\phi(p)} = \{1, 2, 3, \dots, (p-1)\},$$

where $S_{\phi(p)}$ is the set defined on page 126.² Therefore, we can safely cancel each of the integers in $S_{\phi(p)}$ from both sides of the product:

$$a \cdot \cancel{2}a \cdot \cancel{3}a \cdots \cancel{(p-1)}a \equiv \cancel{2} \cdot \cancel{3} \cdots \cancel{(p-1)} \pmod{p}$$

to conclude,

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

²Recall the set $S_{\phi(p)}$ contains all the positive integers that are both relatively prime to p and less than p .

Not bad when it's written out like that, huh?

Let's focus on step 4.

The cancellation we did in step 4 was only possible because all of the integers in the products are in $S_{\phi(p)} = \{1, 2, \dots, (p-1)\}$ and hence relatively prime to p . Recall that you showed in Your Corollary 8.3 on page 112 that you can safely cancel terms from both sides of a congruence when they are relatively prime to the modulus. In this case, the modulus is the prime p , and hence, we can safely cancel each $n \in S_{\phi(p)}$ from both sides of the congruence as shown in step 4.

Suppose that we were, instead, working $(\text{mod } n)$ where n was **not** prime. This means that even if we were able to establish the following congruence

$$1a \cdot 2a \cdot 3a \cdots (n-1)a \stackrel{?}{\equiv} 1 \cdot 2 \cdot 3 \cdots (n-1) \pmod{n}$$

we couldn't cancel all the integers $1, 2, 3, \dots, (n-1)$ from both sides because not all of them will be relatively prime to n .³ We'd be stuck.

However, if we only worked with integers in $S_{\phi(n)}$, then we could cancel them! Let's say that $S_{\phi(n)} = \{m_1, m_2, \dots, m_{\phi(n)}\}$. If we were able to establish $m_1 a \cdot m_2 a \cdots m_{\phi(n)} a \equiv m_1 \cdot m_2 \cdots m_{\phi(n)}$, then we could cancel each m_i and deduce,

$$\begin{aligned} \overbrace{(m_1 \cdot m_2 \cdots m_{\phi(n)})} \cdot a^{\phi(n)} &\stackrel{?}{\equiv} \overbrace{(m_1 \cdot m_2 \cdots m_{\phi(n)})} \pmod{n} \\ \implies a^{\phi(n)} &\stackrel{?}{\equiv} 1 \pmod{n}. \end{aligned}$$

This seems reasonable because we've already shown that the above statement holds, at least when p is prime, because $\phi(p) = p-1$. So the above equation is really just Fermat's Little Theorem:

³This is because composite numbers factor. For example, suppose $n = jk$ for $j, k \in \mathbb{N}$ such that $1 < j, k < n$. Therefore, $\gcd(n, j) = j > 1$, and thus, $j \notin S_{\phi(n)}$. This means that we cannot cancel j out from both sides of the congruence.

Theorem 12.1: Fermat's Little Theorem (Using Euler's Totient Function)

Let p be prime and let $\gcd(a, p) = 1$, then

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

Where we used that $a \not\equiv 0 \pmod{p}$ if and only if $\gcd(a, p) = 1$. (This follows from the fact that p is prime.⁴) So, the question becomes: Is it true that $a^{\phi(n)} \equiv 1 \pmod{n}$ for non-prime $n \in \mathbb{N}$?

Time For Experimental Mathematics

Experimental mathematics in this context means: *computing examples in order to (i) build intuition and (ii) see if a conjecture is plausible.*

Let's try $n = 12$ and $a = 5$. The conditions of the conjecture are met since $\gcd(12, 5) = 1$. Computing $a^{\phi(n)} \pmod{n}$ we have

$$5^{\phi(12)} = 5^4 = 625 \equiv 1 \pmod{12},$$

where we used $\phi(12) = 4$ and $624 = 12 \cdot 52$. The conjecture held! How amazing! Let's try again to make sure we didn't get lucky.

Let's set $n = 10$ and $a = 3$. Using that $\phi(10) = 4$ we have,

$$3^{\phi(10)} = 3^4 = 81 \equiv 1 \pmod{10}.$$

Woot! I'm convinced, how about you?

Conjecture 6. *Let $a, n \in \mathbb{N}$. If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

⁴This is because $\gcd(a, p) = 1$ or $\gcd(a, p) = p$. However, the assumption that $a \not\equiv 0 \pmod{p}$ implies that $p \nmid a$. It follows that $\gcd(a, p) \neq p$ and thus $\gcd(a, p) = 1$.

12.2. Euler's Little Theorem

Our proof for our conjecture 6, which is Euler's Little Theorem, will be similar to our proof for Fermat's Little Theorem. In the proof for Fermat's Little Theorem, we showed, through a lemma and a corollary, that the integers: $1a, 2a, 3a, \dots, (p-1)a$ form a complete set of residues. We will want to prove a similar statement regarding the integers $m_1a, m_2a, \dots, m_{\phi(n)}a$, where $m_i \in S_{\phi(n)}$. More precisely, we want to show the former list forms a *reduced set of residues* (mod n). What's a reduced set of residues, you ask? Good question!

Definition 12.1: Reduced Set of Residues.

We say that the list of integers $m_1, m_2, \dots, m_{\phi(n)}$ forms a reduced set of residues (mod n) if every element in the list has its residue (mod n) in the set $S_{\phi(n)}$. And every integer in $S_{\phi(n)}$ is congruent to an integer in the list.

Note, we could be loose without notation and write:

$$S_{\phi(n)} = \{m_1 \pmod{n}, m_2 \pmod{n}, \dots, m_n \pmod{n}\}$$

I'd say the definition of a reduced set of residues needs an example, huh?

Example 17. Recall that we showed back in example 13 on page 127 that,

$$S_{\phi(15)} = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

and hence $\phi(15) = 8$.

We claim the list 11, 22, 44, 77, 88, 121, 143, 154 is a reduced set of residues (mod 15), since

$$\begin{array}{lll} 11 \equiv 11 \pmod{15}, & 22 \equiv 7 \pmod{15}, & 44 \equiv 14 \pmod{15}, \\ 77 \equiv 2 \pmod{15}, & 88 \equiv 13 \pmod{15}, & 121 \equiv 1 \pmod{15}, \end{array}$$

$$143 \equiv 8 \pmod{15}, \quad 154 \equiv 4 \pmod{15}$$

contains all the elements in $S_{\phi(15)}$ with no duplicates.

Likewise, the list 53, 61, 67, 86, 88, 94, 104, 107 is also a reduced set of residues since,

$$\begin{aligned} 53 &\equiv 8 \pmod{15}, & 61 &\equiv 1 \pmod{15}, & 67 &\equiv 7 \pmod{15}, \\ 86 &\equiv 11 \pmod{15}, & 88 &\equiv 13 \pmod{15}, & 94 &\equiv 4 \pmod{15}, \\ 104 &\equiv 14 \pmod{15}, & 107 &\equiv 2 \pmod{15}. \end{aligned}$$

Thus, the reduced version of the list 53, 61, 67, 86, 88, 94, 104, 107 contains all the elements in $S_{\phi(15)}$ once and only once. ■

Our first task is to show that the following list,

$$m_1a, m_2a, \dots, m_{\phi(n)}a$$

forms a reduced set of residues modulo n . But, as we will see, we will require a few lemmas. So, let's get started!

Lemma 12.1: The integers m_1a are *incongruent* $\pmod{n}$

Let n and a be integers such that $\gcd(a, n) = 1$. Furthermore, let $S_{\phi(n)} = \{m_1, m_2, \dots, m_{\phi(n)}\}$. Then each of the integers

$$am_1, am_2, am_3, \dots, am_{\phi(n)}$$

are *incongruent* $\pmod{n}$.

Proof. Let n and a be relatively prime integers, that is $\gcd(a, n) = 1$. Also, let $S_{\phi(n)} = \{m_1, m_2, \dots, m_{\phi(n)}\}$. We want to prove that all the integers below,

$$am_1, am_2, am_3, \dots, am_{\phi(n)}$$

are *incongruent* (mod n). What we will prove is the contrapositive: if $am_i \equiv am_j \pmod{n}$, then $m_i = m_j$.

With this aim in mind, and without loss of generality,⁵ assume that $0 < m_j \leq m_i \leq n$. Rearranging the congruence $am_i \equiv am_j \pmod{n}$, we deduce,

$$a(m_i - m_j) \equiv 0 \pmod{n}.$$

Since $\gcd(a, n) = 1$, we can safely cancel a to deduce $m_i - m_j \equiv 0 \pmod{n}$ or that,

$$m_i - m_j = nt$$

for some integer t . By our assumption, $0 < m_j \leq m_i \leq n$, it follows that the difference $m_i - m_j$ is bounded in a similar way: $0 \leq m_i - m_j \leq n - 1$. Combining the former inequality with our equation for $m_i - m_j$ we get,

$$0 \leq m_i - m_j = nt < n,$$

and since t is an integer, it must be that $t = 0$. Altogether, we have shown $m_i = m_j$, thus concluding the proof.



Lemma 12.2: $\gcd(a, n) = \gcd(m, n) = 1$
 $\implies \gcd(am, n) = 1$

Let $n, a, m \in \mathbb{Z}$, where $\gcd(a, n) = 1$ and $\gcd(m, n) = 1$.
 Then, $\gcd(am, n) = 1$.

⁵The phrase ‘without loss of generality’ means ‘this assumption does not affect the generality of the proof’. Or, this assumption helps reduce the work of the proof because we no longer need to consider multiple equivalent cases. For our situation, we don’t need to prove the case when $0 < m_j \leq m_i \leq n$ and the case when $0 < m_i \leq m_j \leq n$. Since m_i and m_j are arbitrary anyway, there is nothing that distinguishes the two cases.

Proof. Let $n, a, m \in \mathbb{Z}$ be such that $\gcd(a, n) = \gcd(m, n) = 1$. We aim to prove that $\gcd(am, n) = 1$. Assume, for the hope a contradiction, that $\gcd(am, n) \neq 1$, i.e., $\gcd(am, n) = d \geq 2$. Using the Fundamental Theorem of Arithmetic on page 91, there is a prime p that divides d . This implies that $p \mid am$ and $p \mid n$. By Euclid's lemma on page 90, $p \mid am$ implies that $p \mid a$ or $p \mid m$. We will show that either case leads to a contradiction.

Case 1: $p \mid a$. Since $p \mid a$ and $p \mid n$, it follows $\gcd(a, n) = p > 1$. However, this contradicts that $\gcd(a, n) = 1$.

Case 2: $p \mid m$. In a similar manner to case 1, we have $p \mid m$ and $p \mid n$, it follows $\gcd(m, n) = p > 1$ which contradicts that $\gcd(m, n) = 1$.

In either case, we have found a contradiction, hence we conclude $\gcd(am, n) = 1$.



We're now ready to find our reduced set of residues. I encourage you to try to make a conjecture regarding what our reduced set of residues is and then check it by reading the following proposition. After you do that, try to use our lemmas to prove the proposition yourself! Then you can continue reading to check your work. Keep in mind, if your proof isn't the same as mine, your proof may still be correct. Who knows, your proof might be a better proof than mine! How great would that be?

Proposition 12.1: $aS_{\phi(n)}$ is a Reduced Set of Residues

Let $\gcd(a, n) = 1$. Then, the set of integers $\{am_1, am_2, \dots, am_{\phi(n)}\}$ is a reduced set of residues $(\text{mod } n)$. Furthermore, we denote this set $aS_{\phi(n)}$. Thus,

$$aS_{\phi(n)} = \{am_1, am_2, \dots, am_{\phi(n)}\}$$

is a reduced set of residues $(\text{mod } n)$.

Proof. Let n and a be integers such that $\gcd(a, n) = 1$ and let $S_{\phi(n)} = \{m_1, m_2, \dots, m_{\phi(n)}\}$. Since we are interested in the residues of the am_i 's, let's denote the residue of am_i by $\overline{am_i}$.⁶ Using this new notation, what we want to prove can be restated in the following way,

$$S_{\phi(n)} = \{\overline{am_1}, \overline{am_2}, \dots, \overline{am_{\phi(n)}}\}.$$

First, by lemma 12.1 it follows that $\overline{am_i} \neq \overline{am_j}$ for all $i \neq j$.

Next, by lemma 12.2, we know that every am_i for $m_i \in S_{\phi(n)}$ is relatively prime to n . This means that the residue $\overline{am_i}$ is also relatively prime to n , that is $\gcd(\overline{am_i}, n) = 1$, by our Lemmanade Lemma (page 130). Hence, $\overline{am_i} \in S_{\phi(n)}$ for all $m_i \in S_{\phi(n)}$.

Lastly, when we combine the results from the previous two paragraphs with the fact that $|S_{\phi(n)}| = |aS_{\phi(n)}|$, we conclude,

$$S_{\phi(n)} = \{\overline{am_1}, \overline{am_2}, \dots, \overline{am_{\phi(n)}}\}.$$

(Can you see why?) Hence, the set

$$aS_{\phi(n)} = \{am_1, am_2, \dots, am_{\phi(n)}\}$$

is a reduced set of residues (mod n).



If you take a look back at our example 17 you might notice that the reduced set of residues 11, 22, 44, 77, 88, 121, 143, 154 (mod 15) is the list you'd get by choosing $a = 11$ in the former proof. That is,

$$11 S_{\phi(15)} = \{11, 22, 44, 77, 88, 121, 143, 154\}.$$

IT'SSSSS TIMEEEEEEEEEEE

⁶For example, let $am_1 = 26$ and $n = 15$. Then $\overline{26} = 11$ since 11 is the residue of 26 (mod 15).

Theorem 12.2: Euler's Little Theorem

Let n and a be positive integers such that $\gcd(n, a) = 1$, then

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

Proof of Euler's Little Theorem. Let n and a be positive integers such that $\gcd(n, a) = 1$. Consider the two sets,

$$S_{\phi(n)} = \{m_1, m_2, m_3, \dots, m_{\phi(n)}\}.$$

and

$$aS_{\phi(n)} = \{am_1, am_2, am_3, \dots, am_{\phi(n)}\}.$$

We know from our previous proposition that the set $aS_{\phi(n)}$ forms a reduced set of residues. This means that the two products are congruent:

$$am_1 \cdot am_2 \cdots am_{\phi(n)} \equiv m_1 \cdot m_2 \cdots m_{\phi(n)} \pmod{n}.$$

Since each m_i is relatively prime to n we can use the cancellation rule (Your Corollary on page 112) to deduce that we can make the following cancellations,

$$a \cdot \cancel{m_1} \cdot a \cdot \cancel{m_2} \cdots a \cdot \cancel{m_{\phi(n)}} \equiv \cancel{m_1} \cdot \cancel{m_2} \cdots \cancel{m_{\phi(n)}} \pmod{n}.$$

which implies,

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

Boom!



12.3. An example

Let's see what we can use Euler's Little Theorem for. Consider the following puzzle.

What are the last two digits (the ones and tens place value) of 123^{81} ?

Give this a go! As a hint, don't multiply 121 by itself 81 times, all you'll need is Euler's Little Theorem!

Solution. Consider that if you only wanted to know the one's digit of some integer n , you only need to compute $n \pmod{10}$. Similarly, to find the ones and the tens digits of n , you only need to determine $n \pmod{100}$. This is where Euler's Little Theorem comes into play.

To use Euler's theorem, we must first find $\phi(100)$. We make use of our results from Chapter 10, more specifically the question at the end of the chapter on page 134 (solution on page 189) to conclude $\phi(100) = 40$.

Employing some exponent rules, we conclude that the last two digits of 123^{81} are:

$$\begin{aligned} 123^{81} &= 123^{40+40+1} \\ &= 123^{40} \cdot 123^{40} \cdot 123^1 \\ &\equiv 1 \cdot 1 \cdot 123 && \text{using Euler's Little Theorem} \\ &\equiv 23 \pmod{100}. \end{aligned}$$

So that the last two digits of 123^{81} are 23. How much easier was this compared to having to multiply 123 by 123 eighty-one times!



12.4. Big Things Come in Little Packages

Euler's Little Theorem is a beautiful generalization of Fermat's Little Theorem. This might be enough to pique your interest, as the reader, in the result. However, for those with a more pragmatic interest in mathematics, you'll be happy to know that modern cryptography utilizes Euler's Little Theorem! Which is

wonderful and surprising! If you are interested, I recommend looking up some books and videos on the subject. You'll be happy to see a lot of what we learned show up there! Here are some problems/puzzles for you to have fun with!⁷

- (1) What are the last two digits of 3^{84} ?
- (2) Prove that for any integer a , the last digit of a and a^{4n+1} have are the same.
- (3) Research: How is Euler's Little Theorem used in RSA encryption?

⁷See page 191 for the solutions!!

Commencement 2.0!

“Once a Wildcat, always a Wildcat!”

– Troy Bolton’s (Zac Efron) Commencement Speech
in *High School Musical 3*

You’re Still Reading????

We have come to the end of our journey together. I hope you’ve had some fun, but if not, at least I know that I’ve had a lot of fun writing this! If you’ve made it this far, I cannot express my gratitude that you used your most precious resource, time, reading my book. But I will try:

My Gratitude = Largest Natural Number (∞)

Wait, did I just say that my gratitude doesn’t exist? Because that’s not what I meant to say!!! Let me try again.

My Gratitude = Number of Primes (∞)

There we go!

Commencement 2.0

The reason why this chapter is called **Commencement 2.0** is because your—and my—journey learning mathematics never ends. This book is just one step of many.

Now that you've finished this book, it's up to you to find another source of information to enjoy. I highly highly highly recommend “*Proofs: A Long-Form Mathematics Textbook (The Long-Form Math Textbook Series)*”, “*Real Analysis: A Long-Form Mathematics Textbook (The Long-Form Math Textbook Series)*”, and/or “*Math History: A Long-Form Mathematics Textbook (The Long-Form Math Textbook Series)*” all by Jay Cummings. These books inspired me to pursue mathematics in graduate school. I don't think I could give any book a better compliment!

But now it's time to end this book, so I wish you luck, joy, success, and confusion on your journey! And remember,

“Whoever who has the most fun, wins.”

— James Clear.

Chapter A

Induction and Well-Ordering

“Everything should be made as simple as possible, but not simpler”

– Albert Einstein.

Okay, forewarning: this will cover some really deep mathematics. I recommend you refresh yourself on the Principle of Induction (page 17) and the Well-ordering Principle (page 51) before you begin.

A.1. The Connection

Our goal for this chapter is to determine the connection between the two principles: Induction and Well-Ordering. But, before I tell you what the connection is, what might you guess? Does Induction imply Well-Ordering? Or maybe Well-Ordering implies Induction? Or maybe the connection is something altogether different.

Try to form an opinion so you can test your intuition. The good thing about testing intuition is that it doesn't matter if your

right or wrong! In either case you are building intuition which you can use later!

Seriously, keep thinking!

What if I told you that induction and well-ordering are (logically) equivalent! Recall this means that they imply each other! Neither is *deeper* than the other! They are one and the same (only in disguise!!!!)

What?!?

How?!?

Huh?!?

I know, I know it's awesome!

Let's see why!

Theorem A.1: Well-Ordering $\iff$ Induction

Well-Ordering $\iff$ Induction

Sketch.

Forward: Well-Ordering Implies Induction

For this direction, we are assuming well-ordering holds: *Every non-empty subset of number(s) from $\mathbb{N}$ contains a smallest number.* And we are aiming to prove: *For any statement $P(n)$ that has the property that: (i) $P(1)$ is true and (ii) “ $P(n)$ is true” implies “ $P(n+1)$ is true”, then it must be that $P(n)$ is true for all natural numbers in $\mathbb{N}$.*

Let's begin.

Let $P(n)$ be a statement such that (i) $P(1)$ is true and (ii) “ $P(n)$ is true” implies “ $P(n+1)$ is true”. And let's focus our attention on the set of numbers n where $P(n)$ is true and the set of n where $P(n)$ is false,

$$T := \{n \in \mathbb{N} : P(n) \text{ is True}\},$$

$$F := T^c = \{n \in \mathbb{N} : P(n) \text{ is False}\}.$$

*****Where T^c the *complement* of T , which is a fancy and mathy way of saying that: (i) T and T^c have no overlapping elements and (ii) every natural number is in either T or T^c . A succinct way of saying this is: any natural number is either in T or $F = T^c$ but not both!¹*****

First, observe that we know at the very minimum that $1 \in T$, since we assumed that $P(1)$ is true. We also know, $T \subseteq \mathbb{N}$ since any $n \in T$ is also in $\mathbb{N}$. Likewise, $F \subseteq \mathbb{N}$.

Using our newly minted sets T and F , we are aiming to prove that $T = \mathbb{N}$ and $F = \emptyset$. This would imply that $P(n)$ is true for all natural numbers.

How might we do this? We will assume that F is not empty and see if we can find a contradiction.

So, assume for the hope of a contradiction that F is not empty. Now guess what? We already knew that $F \subseteq \mathbb{N}$ and now we have that F is non-empty. Seems like the right time to use well-ordering, huh?

By the well-ordering principle, there must be a smallest natural number in F , call it $m \in F$. But, $m \in F$ means that $P(m)$ is false. Or, that $m \notin T$. It follows that $m - 1$ is not in T either, for if it was, then $(m - 1) \in T$ would imply that $m \in T$ (recall we assumed $P(n)$ implies $P(n + 1)$, that is with $n = m - 1$ we have $m - 1 \in T \implies m \in T$). But we know that $m \notin T$, a contradiction. We conclude $m - 1$ is not in T , so $m - 1 \in F$.

We have concluded that $m - 1 \in F$, which contradicts that m was the smallest element in F since $m - 1 < m$. Wahooooo we found our contradiction. Our assumption that F was nonempty is therefore false. Thus, F is empty, and every natural number is in T . Thus $P(n)$ is true for all natural numbers. i.e., the principle of induction works.

Backward: Induction Implies Well-Ordering

¹An even more succinct way of stating this is: $T \cup T^c = \mathbb{N}$ and $T \cap T^c = \emptyset$, or $T \cup F = \mathbb{N}$ and $T \cap F = \emptyset$ (recall the empty set on page 2).

We are assuming: For any statement $P(n)$ where (i) $P(1)$ is true and (ii) “ $P(n)$ is true” implies “ $P(n+1)$ is true”, then it must be that $P(n)$ is true for all natural numbers in $\mathbb{N}$. And are trying to prove: Every non-empty subset of number(s) from $\mathbb{N}$ contains a smallest number. In other words, we’re going to do a proof by induction to show that every non-empty subset of $\mathbb{N}$ contains a smallest element.

Let’s begin.

Suppose some set S is both non-empty and a subset of $\mathbb{N}$. Recall these are the two assumptions used in well-ordering.

hmmm... How might we go about showing that there is a least element?

This is hard to do. A much simpler thing to show is a contradiction if S did not have a least element!

So, in a similar way as in the above forward direction proof, assume for the hope of a contradiction that S **does not have a least element**. Our guiding light in this proof is to use induction.

To use induction, we need to find a statement that has the properties that $P(1)$ is true, and $P(n)$ implies $P(n+1)$. A first guess for what $P(n)$ might be is something along the lines of: let $P(n)$ be true if $n \in S$. However, this cannot be the case, since we want $P(1)$ to be true, and this would imply that $1 \in S$, and since 1 is the smallest natural number, in general, 1 would have to be the smallest element in S . But we assumed that S did not have a smallest element. So $1 \notin S$. Since we want $P(1)$ to be true, maybe $P(n)$ has to do with numbers not in S . However, we also want to somehow capture the fact that there is no minimum element in S . For these reasons, it turns out to be more useful to consider the statement:

❓ $P(n)$ is true when all natural numbers, m , smaller than or equal to n are not in S , (i.e. all natural numbers m where $m \leq n$ are such that $m \notin S$).

The same statement, but positive, is

☞ $P(n)$ is true when all natural numbers, m , smaller than or equal to n are in S^c (i.e. all natural numbers m where $m \leq n$ are such that $m \in S^c$).

Where the set S^c is the complement of S (the set S^c contains all numbers that are not in S and in $\mathbb{N}$).

Using $P(n)$, observe that if, say $P(10)$ is true, then it must be that $P(1), P(2), \dots, P(9)$ are all true too. Since $P(10)$ implies that every number less than or equal to 10 is in S^c . Therefore, $P(n)$ has the property that if $P(n)$ is true, then $P(m)$ is also true for all numbers m less than n too.

Base Case: Let's check $P(1)$. Since we already concluded that 1 is not in S we know 1 is in S^c , and there are no natural numbers smaller than 1. Thus, $P(1)$ is true! Boom Base Case Done!

Induction Hypothesis: So, let's assume that $P(n)$ is true, this implies all integers m such that $m \leq n$ are also in S^c .

Inductive Step: We aim to prove that $n+1 \in S^c$. For the hope of a contradiction, suppose that $n+1$ was not in S^c . This would imply that $n+1 \in S$, and by our inductive hypothesis, no number less than $n+1$ is in S , since every number m less than or equal to n is in S^c . Thus, $n+1$ is the smallest number in S . BOOOOOM contradiction since we assumed there was no smallest number in S ! Thus, $n+1 \notin S$, or $n+1 \in S^c$, which tells us $P(n+1)$ is true.

We just showed $P(n)$ implies $P(n+1)$. Boom Inductive Step DONE!

We conclude by induction that $P(n)$ is true for all natural numbers $n \in \mathbb{N}$. Therefore, every natural number is in S^c , or no numbers are in S . Thus, S is empty! BOOM ROASTED ... oops I meant BOOM CONTRADICTION! Since our assumption from the start was that S is nonempty. We conclude that S must have a minimum element!



Now, let's condense what we just wrote into a single, elegant proof!

Proof

Forward. Assume that the natural numbers are well-ordered. Consider a statement on the natural numbers $P(n)$ that has the two properties: (i) $P(1)$ is true and (ii) “ $P(n)$ is true” implies “ $P(n+1)$ is true”. We will prove that $P(n)$ is true for all $n \in \mathbb{N}$.

To this end, define the two sets,

$$T := \{n \in \mathbb{N} : P(n) \text{ in True}\}$$

$$F := T^c = \{n \in \mathbb{N} : P(n) \text{ in False}\}.$$

Note that F is the complement of T and hence $T \cup F = \mathbb{N}$ and $T \cap F = \emptyset$. Furthermore, observe that we have $1 \in T$ and “ $n \in T$ ” $\implies$ “ $n+1 \in T$ ” (by assumption, since $P(1)$ is true and “ $P(n)$ is true” implies “ $P(n+1)$ is true”). Furthermore, we have both $T \subseteq \mathbb{N}$ and $F \subseteq \mathbb{N}$.

Since we want to prove $P(n)$ is true for all $n \in \mathbb{N}$, we want to prove $T = \mathbb{N}$ and $F = \emptyset$. So, assume for the hope of a contradiction that $F \neq \emptyset$. It follows from Well-Ordering that F must have a least element. Let's denote this minimum element $m \in F$.

Since $m \in F$, we know $P(m)$ is false so that $m \notin T$. It follows that $m-1 \notin T$, since if it were, we'd have a contradiction, as $m-1 \in T$ implies $m \in T$. Thus, $m-1 \notin T$ and hence $m-1 \in F$, which contradict that $m \in F$ was the least element in F .



Backward. Assume that any statement $P(n)$ with the properties (i) $P(1)$ is true and (ii) “ $P(n)$ is true” implies “ $P(n+1)$ is true”, then it must be that $P(n)$ is true for all natural numbers in $\mathbb{N}$.

Let S be a non-empty subset of $\mathbb{N}$. We aim to prove that there is a least element in S . We will do so using a proof by contradiction.

To this end, assume that S does not have a minimum element. Observe that if $1 \in S$, then we'd be done since 1 is the smallest natural number, $1 \in S$ would also be the least element in S , a contradiction. Hence, $1 \notin S$. We will use induction, on n , using the following statement:

💡 $P(n)$ is true when all natural numbers, m , smaller than or equal to n are not in S , (i.e. all natural numbers m where $m \leq n$ are such that $m \notin S$).

Which is the same statement as

💡 $P(n)$ is true when all natural numbers, m , smaller than or equal to n are in S^c (i.e. all natural numbers m where $m \leq n$ are such that $m \in S^c$).

Where S^c is the complement of S .

Base Case: Consider $P(1)$. We already showed that $1 \notin S$ or $1 \in S^c$, hence $P(1)$ is true.

Induction Hypothesis: Assume that $P(n)$ is true for some $n \in \mathbb{N}$. That is, all the integers $1, 2, 3, \dots, n \in S^c$.

Inductive Step: Consider $P(n+1)$. We are aiming to show $P(n+1)$ is true or that $n+1 \in S^c$. For the hope of a contradiction, suppose that $n+1 \notin S^c$, or that $n+1 \in S$. It follows that $n+1$ is the least element in S since, by our induction hypothesis $1, 2, 3, \dots, n \notin S$. This contradicts the assumption that S does not have a least element, thus it must be the case that $n+1 \notin S$ or that $P(n+1)$ is true. Note we have just shown that $P(n)$ implies $P(n+1)$.

We conclude by induction that $P(n)$ is true for all $n \in \mathbb{N}$, which implies that no natural numbers are in S , hence $S = \emptyset$. This contradicts the assumption that S was non-empty. Thus, our assumption that S did not have a minimum element is false, or that S does have a minimum element!



A.2. Closing Remarks

Wow, that was a journey, huh? Let's recap what we proved. We proved that the Well-Ordering Principle and the Principle of Induction are logically one and the same. What does this mean exactly? It means that they both imply each other. "Okay? So?"

I hear you say. The upshot is that you can take either as your starting point and prove the other. So, if you were trying to build a mathematical theory, you could take either to be a law of math (an axiom for those who know that word) and deduce the other.

One of the key takeaways I got from this fact was that there can be many starting points for building a mathematical theory. One way may be incredibly obvious and almost not worth stating (cough cough, I'm looking at you, well-ordering). And the other, very strange upon first encounter (induction, anyone?). But in the end, sometimes they are the same. They carry the same weight, so to speak.

So, next time you use induction, remember that you might really be relying on the fact that all non-empty subsets of $\mathbb{N}$ have a least element!

Chapter B

Irrational Numbers

“I’m not crazy, my mother had me tested.”

– Sheldon Cooper in the *Big Bang Theory*.

Today, we are going to discuss a new type of number called irrational numbers. I know, this is strange, since this a book on number theory—which focuses on integers—but since our goal is to understand numbers in general, so we should be familiar with all the types of numbers that exist.

B.1. What are rational and irrational numbers????

Let’s start with Natural Numbers $\mathbb{N}$ and work our way up to more abstract sets of numbers. We could argue that natural numbers make the most intuitive sense, since we’ve used them to describe the real world since childhood. For example, when

we say things like: there are 2 apples left on the tree, I have 10 fingers on my right hand, this book is 197 pages long, I ate 3 slices of pizza for dinner; we all understand that all of those numbers describe a *quantity*. More than this, real-world situations motivate the concepts of addition, subtraction, multiplication, and division (sometimes), e.g., I ate 4 more slices of pizza for dessert, therefore I ate $3 + 4 = 7$ total slices of pizza today.

As time goes on, we expand our set of numbers to include negative numbers and zero. Thus, forming the integers $\mathbb{Z}$. When we first learn about the integers, the negative numbers seem less useful and more abstract than their positive counterparts. In spite of this, I bet if I said that I owe you \$15 it would make total sense to say that I have -\$15, because I'm in debt.

The integers eventually become intuitive to us, and we've learned to use them to describe everyday situations, like with debts. And again, we can motivate the concepts of addition, subtraction, multiplication, and division (in some cases) with these numbers.

When we become even more advanced, we eventually expand our set of numbers to include fractions. In the process, we are inventing what are called *rational numbers*, which we denote $\mathbb{Q}$. Rational numbers are numbers that can be written as a fraction of two integers (as long as the bottom number isn't 0).

Definition B.1: Rational Numbers $\mathbb{Q}$ (An Informal and Flawed Definition)

The rational numbers are the set of integer fractions, that is, r is a rational number if it is a ratio of two integers: $\frac{m}{n}$ where $n \neq 0$,

$$\mathbb{Q} := \left\{ \frac{m}{n} : m, n \in \mathbb{Z} \text{ and } n \neq 0 \right\}.$$

Remark. This definition is informal and flawed for a few reasons.

First, because we need to be more precise. After all, we have two different representations of the same fraction—for instance $\frac{1}{2} = \frac{2}{4}$ —which isn't addressed in the above definition. Unfortunately, we don't have the tools necessary to give the proper definition. The good news is, as a first pass, that our informal definition is good enough.

Example 18. For example, $\frac{1}{2} \in \mathbb{Q}$ since 1 and 2 are integers. likewise $\frac{-1}{2}$ is rational since -1 and 2 are integers. ■

Example 19. Every integer is a rational number, too! For example,

$$\frac{10}{1} = 10 \in \mathbb{Q}.$$

So $\mathbb{Z}$ is a subset of $\mathbb{Q}$ in much the same way that $\mathbb{N} \subseteq \mathbb{Z}$,

$$\mathbb{N} \subseteq \mathbb{W} \subseteq \mathbb{Z} \subseteq \mathbb{Q}.$$

■

Example 20. Fractions of rational numbers are also rational numbers! For instance $\frac{1.5}{2}$ is a rational number since

$$\frac{1.5}{2} = \frac{1.5 \times 2}{2 \times 2} = \frac{3}{4}.$$

The takeaway from this example is that sometimes it's not obvious that a number is rational. For example, 3.1415926535 is rational since

$$3.1415926535 = \frac{31\,415\,926\,535}{10\,000\,000\,000}.$$

■

Rational numbers also describe everyday situations: I have eaten 7 slices of pizza out of the 8 total slices, so I have eaten $\frac{7}{8}$ of the pizza. Or, I have 50 cents, which is equal to $\frac{1}{2}$ of a dollar. And again, it makes sense to add, subtract, multiply, and divide (never by zero!) these rational numbers.

People used to think that all numbers were rational. This was probably because rational numbers could describe pretty much everything that numbers were expected to. (What would it mean for a number to **not** be a rational number? What would the non-rational number describe?) This bias was so strong that a guy named Pythagoras,¹, built a religion based on the idea that rational numbers are sacred.

The disciples of Pythagoras were called the Pythagoreans. They believed that every number could be written as a fraction of whole numbers, i.e., that all numbers are rational numbers. Long story short, yada yada yada, the Pythagoreans were wrong! There are so-called irrational numbers that cannot be written as a fraction of whole numbers.

A Pythagorean named Hippasus is rumored to have been the first person to discover and prove that irrational numbers exist. And we now have the tools necessary to prove, using modern mathematics, what Hippasus discovered. However, let's define what we mean by an irrational number first.

Definition B.2: Irrational Numbers

A number r that cannot be written as a fraction of whole numbers is called irrational. In other words, a number that is not rational is called irrational.

We will also need to recall what it means for a fraction to be in *simplest form*. Just to make sure we are on the same page, I give you definition B.3

Definition B.3: Simplest Form Fraction

We say that $\frac{a}{b} \in \mathbb{Q}$ is in *simplest form* if $\gcd(a, b) = 1$.

¹Yes, the same guy from the Pythagorean Theorem!

Example 21. Consider the fraction $\frac{10}{15}$. Since $\gcd(10, 15) = 5 \neq 1$, our fraction is not in simplest form. However, by canceling out a factor of 5 from the numerator and denominator, we get

$$\frac{10}{15} = \frac{2 \cdot \cancel{5}}{3 \cdot \cancel{5}} = \frac{2}{3}$$

which is in simplest form since $\gcd(2, 3) = 1$. ■

Theorem B.1: There are irrational numbers

The number $\sqrt{2}$ is irrational.

It's very hard to prove statements such as, "there does not exist blah blah..." or in this case "there are no integers a and b such that $\sqrt{2} = \frac{a}{b}$." It's much easier to write a proof by contradiction and assume "there does exist blah blah" because this gives us a place to start, and then try to find a contradiction.

Proof. Let's assume for the hope of a contradiction that $\sqrt{2}$ was rational. This means that there are integers a and b such that $\sqrt{2} = \frac{a}{b}$. Moreover, we can assume that $\frac{a}{b}$ is in simplest form because if $\frac{a}{b}$ weren't in simplest form of the fraction, we could cancel a factor of $\gcd(a, b)$ from the numerator and denominator resulting in a fraction in simplest form.

Since square roots and fractions are messy, let's square both sides of $\sqrt{2} = \frac{a}{b}$ and then solve for a^2 ,

$$(\sqrt{2})^2 = \left(\frac{a}{b}\right)^2 \iff 2b^2 = a^2.$$

Recall Euclid's Lemma Corollary on page 91. Since 2 is prime and $2 \mid a^2$, it follows by Euclid's Lemma Corollary that $2 \mid a$. Thus, $a = 2m$ where m is some integer. Plugging this back into our previous result and canceling a factor of 2 gives,

$$2b^2 = a^2$$

$$\begin{array}{ll} 2b^2 = 4m^2 & \text{substitute } a = 2m \\ b^2 = 2m^2 & \text{cancel 2 from both sides} \end{array}$$

Now we see that $2 \mid b^2$. Which by Euclid's lemma Corollary (again) $2 \mid a$.

Wait!

We have concluded both $2 \mid a$ and $2 \mid b$. So 2 is a common divisor of a and b , hence $\gcd(a, b) \geq 2$. Which contradicts our assumption that our fraction was in simplest form so that $\gcd(a, b) = 1$.

We conclude that our assumption that $\sqrt{2}$ is rational was incorrect, and hence $\sqrt{2}$ is irrational!



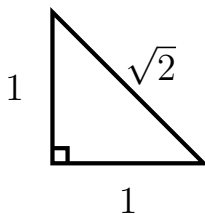
How awesome is that! You can modify the proof above to show that $\sqrt{p}$ for any prime p is irrational.

B.1.1 A Quick Comment

We began by discussing how natural numbers, integers, and rational numbers are intuitive because they can be used to describe the real world. This begs the question: Do irrational numbers describe the real world?

Well... yes and no. As we now know, $\sqrt{2}$ is irrational. And $\sqrt{2}$ shows up as the hypotenuse of a right triangle with side lengths 1 and 1.²

² Why's that? Recall the Pythagorean theorem states: $a^2 + b^2 = c^2$ where a and b are the legs of a right triangle and c is the hypotenuse. Using $a = 1$ and $b = 1$ we see that $1^2 + 1^2 = 2 = c^2$. Thus, $c = \sqrt{2}$.



So it seems like $\sqrt{2}$ does show up in the real world, at least when working with triangles.

But there's a catch.

Perfect 1-by-1 right triangles don't really show up in nature... The sides of any triangle will change due to a few moving atoms, an extra pixel, quantum uncertainty, or simply because the lines themselves have nonzero thickness. So the 'issue' is more subtle than we might have thought.

It gets worse (or better), if we want to use irrational numbers to perform calculations such as finding $10\sqrt{2} + 2$ in decimal form, we can't use $\sqrt{2}$ in decimal form when carrying out our calculations. This is because irrational numbers have an infinite non-repeating decimal expansion. We (and computers) cannot handle infinity! So, we round $\sqrt{2}$ to 1.4 or maybe 1.414 or maybe we need more accuracy and use 1.41421356237309504880168872420969807. But there's a problem. When we round, we're turning an irrational number into a rational number because only rational numbers can have a finite decimal expansion.

So you pick. Do irrational numbers describe the real world?

B.2. Don't be Irrational

There are so many beautiful proofs to show that different numbers like π and e are irrational. Many of them are quite technical, but there are a few that don't require advanced mathematics. And there are so many open questions out there. For example, we don't yet know if π^e or $\pi + e$ are irrational! Keep learning and discovering, and maybe you, the reader, will solve these problems!

Chapter C

Some Solutions

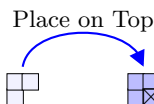
C.1. From Chapter 2

Prove that you can tile any $2^n \times 2^n$ checkerboard with one square removed using an L-shaped tile.

I hope that you gave this problem a go! It's so much fun to think about!

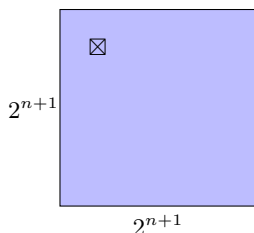
Proof. We proceed by induction on n .

To show our base case, we want to tile a $2^1 \times 2^1$ checkerboard with one tile removed using the tile. Note that we can simply place the tile  on the checkerboard, ,

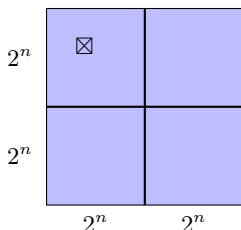


Now, assume that we can tile a $2^n \times 2^n$ checkerboard with one tile removed using the tile L-tile. We aim to find a tiling of a $2^{n+1} \times 2^{n+1}$ checkerboard.

Consider the following checkerboard with one tile removed.

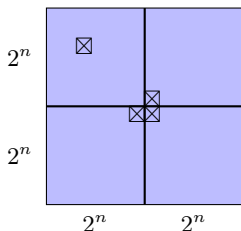


Here's the key idea: We can break the $2^{n+1} \times 2^{n+1}$ checkerboard up into *four* $2^n \times 2^n$ checkerboards, which we know can be tiled when one piece is missing:



This helps because now we can tile the upper left square—since there is one tile missing. However, our induction hypothesis does not yet help with the other three $2^n \times 2^n$ boards. We need to remove one tile from each of those three $2^n \times 2^n$ boards. Can you think of a way to remove a tile from all three boards so that you make an empty L-tile?

How about:



Now, by our induction hypothesis, every $2^n \times 2^n$ board with one square removed can be tiled. Furthermore, the entire board can be tiled, because the empty spots in the center form an L-tile, completing the induction step.

Therefore, by induction, we can tile any $2^n \times 2^n$ checkerboard with one square removed using an L-shaped tile.



C.2. From Chapter 6

(1) What are the integer solutions to $7x + 26y = 15$? This is the equation in the introduction.

Solution. First, we must check to see if there are any solutions to $7x + 26y = 15$. We know using Bézout's Identity Generalized on page 77 that there is a solution iff $\gcd(7, 26) \mid 15$. We can see (and will show using the Euclidean algorithm) that $\gcd(7, 26) = 1$. And $1 \mid 15$, so there are solutions! Woo!

Our game plan is to solve the equation $7x + 26y = 1$, and use the same argument we used to prove Bézout's Identity Generalized.

To begin, let's complete the Euclidean algorithm with $a = 26$ and $b = 7$,

$$26 = 3(7) + 5$$

$$7 = 1(5) + 2$$

$$5 = 2(2) + \boxed{1}$$

$$2 = 1(2) + 0$$

Therefore, $\gcd(7, 26) = 1$, as we said earlier. Now we will use the above steps to determine our solutions x_0 and y_0 to $7x + 26y = 1$.

First, we solve for $\gcd(7, 26) = 1$ in the third line: $\gcd(7, 26) = 1 = 5 + (-2)(2)$.

Next, we will solve for the second line's remainder: $2 = 7 + (-1)(5)$. And now we plug our expression into the expression for $\gcd(7, 26)$,

$$\begin{aligned}\gcd(7, 26) = 1 &= 5 + (-2)(2) \\ &= 5 + (-2)(7 + (-1)(5)) \\ &= (3)(5) + (-2)(7)\end{aligned}$$

We're almost there! Let's now solve for the first line's remainder: $5 = 26 + (-3)(7)$. And now let's plug this into the last expression we found for $\gcd(7, 26)$,

$$\begin{aligned}\gcd(7, 26) = 1 &= (3)(5) + (-2)(7) \\ &= (3)(26 + (-3)(7)) + (-2)(7) \\ &= (3)(26) + (-11)(7)\end{aligned}$$

BOOOOOOM!

Our solutions to x_0 and y_0 to $7x + 26y = 1$ are: $x_0 = -11$ and $y_0 = 3$. But, since we wanted a solution to $7x + 26y = 15$, we must multiply $x_0 = 3$ and $y_0 = -11$ by 15. This gives us a solution: $x_1 = -165$ and $y_1 = 45$,

$$7(15 \cdot -11) + 26(15 \cdot 3) = 7(-165) + 26(45) = 15$$

We're not done just yet! Using equation  on page 84 we have the infinite family of solutions (note that x_0 and y_0 will be replaced with x_1 and y_1):

$$x = -165 - \left(\frac{26}{1}\right)k \quad \text{and} \quad y = 45 + \left(\frac{7}{1}\right)k$$

$$= -165 - 26k$$

and

$$= 45 + 7k$$



(2) We showed our solution set is given by $x = x_0 - \left(\frac{b}{d}\right)k$ and $y = y_0 + \left(\frac{a}{d}\right)k$. Would $x = x_0 + \left(\frac{b}{d}\right)k$ and $y = y_0 - \left(\frac{a}{d}\right)k$ work too?

Yes! Since $k \in \mathbb{Z}$, whether or not you add or subtract does not matter! The only thing that matters is that the expressions for x and y have the opposite sign.

(3) If you restrict x and y to be greater than or equal to 0, that is $x, y \in \mathbb{N}$, what different numbers n can you get as a solution to: $ax + by = n$.

The wonderful YouTube channel *Numberphile* has a great video that answers this question, and it came out the day after I wrote the content for this chapter! I cannot do better than a Numberphile video, so I will outsource my work to them. I recommend you search: *Numberphile the Frobenius Problem*. Or you can search scan the QR code on the next page.¹

C.3. From Chapter 8

(1) If $3 \nmid c$, then $c^2 \equiv 1 \pmod{3}$.

Proof. First, note that $1^2 \equiv 2^2 \equiv 1 \pmod{3}$. That is, the only square number (mod 3) is congruent to 1.

Let $3 \nmid c$. Then, it must be that $c \not\equiv 0 \pmod{3}$. It follows that $c \equiv 1 \pmod{3}$ or $c \equiv 2 \pmod{3}$. In either case, $c^2 \equiv 1 \pmod{3}$.



¹Again, if you don't want to scan the QR here's the link: https://youtu.be/be8BGCLuC54?si=aRBh5ywoiPZLCL_R or



(2) What is the remainder when you divide $1! + 2! + 3! + \cdots + 100!$ by 5?

Proof. Asking for the remainder after dividing by 5 is equivalent to asking for the *residue mod 5*. Using our modular arithmetic rules in theorem 8.1 (i) on page 112 we deduce,

$$1! + 2! + 3! + \cdots + 100! \equiv 1! + 2! + 3! + 4! + 0 + 0 \cdots + 0 \pmod{5}$$

since every factorial larger than $4!$ is a multiple of 5. Furthermore, $1! \equiv 1 \pmod{5}$, $2! \equiv 2 \pmod{5}$, $3! = 6 \equiv 1 \pmod{5}$, and $4! = 24 \equiv 4 \pmod{5}$. Thus,

$$\begin{aligned} 1! + 2! + 3! + \cdots + 100! &\equiv 1! + 2! + 3! + 4! \\ &\equiv 1 + 2 + 1 + 1 + 4 \\ &\equiv 4 \pmod{5} \end{aligned}$$



(3) Prove: If $a \equiv 1 \pmod{n}$, then $\gcd(a, n) = 1$.

Proof. Let $a \equiv 1 \pmod{n}$. By definition 8.2 on page 100, this is equivalent to $(a-1) = nk$ for some $k \in \mathbb{Z}$. After some algebra this

is the same as the equation: $a - nk = a + (-k)n = 1$. Note that this equation has the same form as $ax + by = 1$ with $x = 1$, $b = n$, and $y = -k$. By theorem 6.2 on page 79, $\gcd(a, b) = \gcd(a, n) = 1$.



C.4. From Chapter 9

(1) Compute $3^{24} \pmod{11}$ and $7^{115} \pmod{29}$.

Solution: Observe that both 11 and 29 are prime. Using some exponent rules we deduce:

$$3^{24} = 3^{6+6+6+6} = 3^6 \cdot 3^6 \cdot 3^6 \cdot 3^6 \equiv 1 \cdot 1 \cdot 1 \cdot 1 = 1 \pmod{11}$$

Where we used Fermat's Little Theorem on page 120 to conclude $3^6 \equiv 1 \pmod{11}$. Similarly,

$$\begin{aligned} 7^{115} &= 7^{28+28+28+28+3} = 7^{28} \cdot 7^{28} \cdot 7^{28} \cdot 7^{28} \cdot 7^3 \\ &\equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 7^3 \pmod{29} \end{aligned}$$

After using Fermat's Little Theorem to deduce $7^{28} \equiv 1 \pmod{29}$. Now we just need to simplify $7^3 \pmod{29}$. We do so in two steps,

$$7^3 \equiv 49 \cdot 7 \equiv 20 \cdot 7 \equiv 140 \equiv 24 \pmod{29}.$$



(2) Find $1^{25} + 2^{25} + 3^{25} + \cdots + 100^{25} \pmod{7}$.

This one is a good one!

Solution: Since 7 is prime, by Fermat's Little Theorem we know: $a^6 \equiv 1 \pmod{7}$. Thus,

$$a^{25} = a^{4 \cdot 6 + 1} = (a^6)^4 \cdot a^1 \equiv 1^4 \cdot a \equiv a \pmod{7}.$$

Thus,

$$1^{25} + 2^{25} + 3^{25} + \cdots + 100^{25} \equiv 1 + 2 + \cdots + 100 \pmod{7}.$$

We know from our first theorem 2.1 on page 20 that the sum equals $100(101)/2 = 5,050$. Which, upon reducing mod 7, gives 3. Or, we could have done the following:

$$\begin{aligned} 1^{25} + 2^{25} + 3^{25} + \cdots + 100^{25} &\equiv 1 + 2 + \cdots + 100 \pmod{7} \\ &\equiv 1 + 2 + 3 + 4 + 5 + 6 + 0 \\ &\quad + 1 + 2 + 3 + 4 + \cdots + 0 + 1 + 2 \\ &\equiv 14(1 + 2 + 3 + 4 + 5 + 6) + (1 + 2) \\ &\equiv 0 + 3 \\ &\equiv 3 \pmod{7}. \end{aligned}$$

We used a lot of tricks! In going from the second line to the third, we reduce each term (mod 7). To transition from the third to the fourth, we reasoned that there would be $100 \div 7$ rounded down, groups of $(1 + 2 + 3 + 4 + 5 + 6)$.



(3) A googol is 10^{100} . What day of the week will it be in a googol days? (from whatever day you are reading this on)

Solution: This problem is equivalent to asking: What is $10^{100} \pmod{7}$? Which reduces to using Fermat's Little Theorem:

$$10^{100} = 10^{16 \cdot 6 + 4} = (10^6)^{16} \cdot 10^4 \equiv (1)^{16} \cdot 10^4 \pmod{7} \equiv 10^4 \pmod{7}$$

Which can be further reduced to show $10^4 = 10000 \equiv 4 \pmod{7}$.

Today, the day I'm writing this, is a Monday. If we let Sunday = 0, Monday = 1, ..., Saturday = 6, then Monday + 4 = 5 which is a Friday!



C.5. From Chapter 10

(1) What is $\phi(100)$?

Solution. Note that $100 = 2^2 \cdot 5^2$. Thus, by proposition 10.1 part 4 back on page 128, we have,

$$\begin{aligned}\phi(100) &= 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) \\ &= 40\end{aligned}$$

Not too shabby!



(2) Prove that for every integer n greater than 2, $\phi(2)$ is even.

Proof. Let $n > 2$ be an integer. There are two stations to consider: (i) n is a power of 2, that is $n = 2^k$ for some positive $k \in \mathbb{Z}$; (ii) n has an odd prime factor p .

In the first case, using proposition 10.1 part 4, we have,

$$\phi(n) = \phi(2^k) = 2^k \left(1 - \frac{1}{2}\right) = 2^{k-1}.$$

However, since $n > 2$ it must be that $k > 1$ or that $k - 1 > 0$. Thus, 2^{k-1} is an even integer.

In the second situation, there is some odd prime that divides n . Then, n 's prime factorization will be of the form: $n = kp^t$, where $p \nmid k$ (which implies $\gcd(p, k) = 1$). Again, using proposition 10.1 parts 3 and 4 we have,

$$\begin{aligned}\phi(n) &= \phi(kp^t) \\ &= \phi(k)\phi(p^t) && \text{by part 3} \\ &= \phi(k)p^t \left(1 - \frac{1}{p}\right) && \text{by part 4}\end{aligned}$$

$$\begin{aligned}
 &= \phi(k)p^t \left(\frac{p-1}{p} \right) \\
 &= \phi(k)p^{t-1}(p-1).
 \end{aligned}$$

Since p is an odd prime, $p \geq 3$ and thus $p-1 \geq 2$ is an even integer; and an even times any integer is even, concluding the proof.



(3) Prove the two statements: (i) If n is odd, then $\phi(2n) = \phi(n)$, and (ii) If n is even, then $\phi(2n) = 2\phi(n)$.

Proof of (i). Let n be odd. It follows that $\gcd(2, n) = 1$. using proposition 10.1 (yet again!) we deduce,

$$\phi(2n) = \phi(2)\phi(n) = \phi(n)$$

where we used that $\phi(2) = 1$ as you can verify.



Proof of (ii). Let n be even. Then, $n = 2^m k$ where k is odd. Since k is odd, it follows that $\gcd(2^m, k) = \gcd(2^{m+1}, k) = 1$ and hence,

$$\phi(2n) = \phi(2^{m+1}k) = \phi(2^{m+1})\phi(k) = 2^k\phi(k)$$

Where we used that $\phi(2^{m+1}) = 2^m$ as you can verify, again. Also, we have,

$$\phi(n) = \phi(2^m k) = \phi(2^m)\phi(k) = 2^{m-1}\phi(k).$$

Comparing the expression we got for $\phi(2n)$ and $\phi(n)$ we see that $\phi(2n) = 2\phi(n)$.



C.6. From Chapter 12

(1) What are the last two digits of 3^{84} ?

This is a similar problem to the one we solved together in the chapter. We want to find $3^{84} \pmod{100}$. We will utilize that $\phi(100) = 40$.

$$3^{84} = 3^{40+40+4} = 3^{40} \cdot 3^{40} \cdot 3^4 \equiv 1 \cdot 1 \cdot 81 \equiv 81 \pmod{100}$$

Thus, the last two digits are an 8 and a 1 to make 81.

(2) Prove that for any integer a , the last digit of a and a^{4n+1} have are the same.

Proof. Let $a \in \mathbb{Z}$. We are concerned with $a \pmod{10}$ and in order to apply Euler's Little Theorem, we need $\phi(10)$. I'll let you work it out, but it's 4 haha! Thus,

$$a^{4n+1} = (a^4)^n \cdot a^1 \equiv 1^n \cdot a \equiv a \pmod{10}.$$



(3) How is Euler's Little Theorem used in RSA encryption?

Look it up!

No, seriously, there is too much to cover here in any detail. I recommend two references: (1) Brilliant.org and (2) *Elementary number theory* by Burton, D. M. [2].

Index

- $\mathbb{N}$, 2
 $\mathbb{Z}$, 3
'is an element of', 3
- Albert Einstein, ix, xxvi,
164, 165
- Bertrand's Theorem, x
Binary Numbers, xii
Bruce Barton, 117
Buzz Lightyear, 13
Bézout's Identity, 71, 77,
78, 82, 141, 183
Bézout's Identity
Generalized, 77,
141
- Chinese Proverb, 137
Clock Algebra, 102
Complement, 167
Composite, 88
Congruence, 98
Contrapositive, 11, 119
- Converse, 10
Coprime, 71
- Diophantine Equation, 85
Dirichlet, 95
Dirichlet's Theorem about
Arithmetic
Progressions, 95
Division Algorithm, 42, 44
division algorithm, 58,
60–65, 89, 101,
145
Divisor, 54
Donald Knuth, 53
- Empty Set, 2
Ernest Hemingway, 39
Euclid's Lemma, 90
Euclidean Algorithm, 53
Euler, 126
Euler's Lemma, 81
Euler's Little Theorem, 151,
155, 160, 161, 191

-
- Euler's Totient Function, 126
 - Euler's Totient Theorem, 151
 - Experimental Mathematics, 154
 - Factorial, 121
 - Fermat's Last Theorem, 118
 - Fermat's Little Theorem, 115, 122, 123, 134, 151, 161, 187, 188
 - Fibonacci, xvi–xix, xxiv
 - Fundamental Theorem of Arithmetic, 89
 - Greatest Common Divisor, 53
 - Implication, 9
 - Inclusive Or, 5
 - Induction and Well-Ordering, 42
 - Infinite Number of Primes, 33
 - Integers, ix, x, 3, 4, 31–34, 38, 42, 44, 46, 50, 52–60, 62–65, 68, 70, 71, 73, 77–79, 82, 83, 90, 92, 98, 100, 102, 104, 107–110, 113, 118–122, 125, 126, 129–133, 140–143, 146, 148, 155, 156, 160, 173–175, 177, 178
 - Integers (Set), 3
 - Intersection of Sets, 5
 - Irrational Numbers, 173
 - Maryam Mirzakhani, 67
 - Mod, 98
 - Modular Arithmetic, 98
 - Modular Congruence, 137
 - Multiple, 54
 - Multiplicative, 133
 - Natural Numbers, 2, 4, 17, 31, 42, 44–47, 50, 126, 166–171, 173, 178
 - Pascal's Triangle, xx
 - Paul Erdős, 95
 - Paul R. Halmos, 1
 - Perfect Numbers, x
 - Phil Dunphy, 29
 - Pierre-Simon Laplace, 125
 - Powers of 2, xv, xxii–xxiv
 - Prime Factorization, 91
 - Prime Number Theorem, 95
 - Prime Numbers, 88
 - Principle of Induction, 165
 - Proof by Contradiction, 29
 - Quotient, 45
 - Rational Numbers, 174
 - Recursive, xvii
 - Reducing, 101
 - Relatively Prime, 71

-
- Remainder, 45
 - Residue mod n , 101
 - Set Definition, 2
 - Sheldon Cooper, 173
 - Snazzy, 121
 - Square Numbers, 22
 - Strong Induction, 25
 - Subset, 6
 - Tanzanian proverb, 151
 - The Principle of
 - Mathematical Induction, 17
 - The Well-Ordering
 - Principle, 44, 51
 - Timothy Gowers, Fields Medalist, 87
 - Triangular Numbers, xix, xx, xxiii, 20, 24
 - Troy Bolton (Zac Efron), 163
 - Truth Table, 9
 - Union of Sets, 5
 - Well-Ordering, 42
 - Well-ordering Principle, 165
 - Whole Numbers, 44
 - William Dunham, 125
 - Woody, 28

Bibliography

- [1] Guy, R. K. Unsolved problems in number theory; Springer: New York, 2014.
- [2] Burton, D. M. Elementary number theory; McGraw-Hill: New York, 2011.
- [3] Cummings, J. Proofs: A long-form mathematics textbook; LongFormMath.com: Sacramento, CA, 2023.
- [4] Lewis Carroll Quotes. (n.d.). BrainyQuote.com. Retrieved July 31, 2025, from BrainyQuote.com Web site: https://www.brainyquote.com/quotes/lewis_carroll_107140
- [5] Integers. Brilliant.org. Retrieved 17:28, July 31, 2025, from <https://brilliant.org/wiki/integers/>
- [6] Su, F. Real Analysis, Lecture 6: Principle of Induction <https://youtu.be/D3qVXZd-ONo?si=evxxF9sKOdx5YV48> (accessed Aug 20, 2025).
- [7] Spiegel, M. R.; Lipschutz, S.; Liu, J. Mathematical Handbook of Formulas and tables; 5th ed.; McGraw-Hill Education: New York, 2018.
- [8] High school musical 3: Senior year; Walt Disney home entertainment: Milano, 2009.