“Mathematics is the Queen of the Sciences, and Number Theory is the Queen of Mathematics.”
– Carl Friedrich Gauss (1777-1855)

aBa Mbirika and Rita Post

Spring 2019
Creative Commons License (CC BY-NC-SA): This text, including the art and illustrations, are available under the Creative Commons license (CC BY-NC-SA), allowing anyone to reuse, revise, remix and redistribute the text.

To view a copy of this license, visit

https://creativecommons.org/licenses/by-nc-sa/4.0/
Contents

0 Preliminaries 9
  0.1 Math Symbols Used In This Book 9
  0.2 What Is Number Theory and What Is Its Purpose? 12
    0.2.1 Some Beautiful Conjectures Awaiting Proofs 22
    0.2.2 Some Beautiful Results That Have Been Proven 23
    0.2.3 Number Theory Flourishes In Hollywood Films 27
  0.3 Examples of the Beauty and Power of Number Theory 29

1 Proofs – An Introduction 37
  1.1 Statements and Truth Tables 38
  1.2 Implications 42
  1.3 Predicates and Quantifiers 46
  1.4 Writing Formal Proofs 56
  1.5 Quick Review of Set Theory and Some Set Theory Proofs 63
  1.6 Butternut Squash 69

2 Mathematical Induction 71
  2.1 Motivation 71
  2.2 The Principle and Method of Mathematical Induction 74
  2.3 Exercises 77

3 Pascal’s Triangle and Binomial Coefficients 81
  3.1 Motivation 81
  3.2 Constructing Pascal’s Triangle 84
  3.3 16 Rows of Pascal’s Triangle 86
  3.4 Binomial Coefficients 87
  3.5 Exercises 88

4 Primes, Prime Factorization, and Some Consequences 93
  4.1 Motivation 93
  4.2 Density of Primes and the Celebrated Prime Number Theorem 94
  4.3 A Smörgåsbord of Types of Primes 99
  4.4 The Fundamental Theorem of Arithmetic and Some Consequences 106
  4.5 The Goldbach Conjecture 112
  4.6 Exercises 114
5 Divisibility Theory 119
5.1 Motivation .......................................................... 119
5.2 Divisibility ............................................................ 120
5.3 The Division Algorithm ............................................. 126
5.4 GCD and LCM ....................................................... 127
5.5 The Euclidean Algorithm and Bézout’s Identity .......... 129
5.6 The Diophantine Equation ........................................ 134
5.7 Exercises ............................................................ 135

6 Congruence Theory (a Number Theory Perspective) 141
6.1 Motivation ............................................................ 141
6.2 Gauss and Congruence Properties ............................... 142
6.3 Solving Linear Congruences ...................................... 148
6.4 Chinese Remainder Theorem (CRT) ......................... 153
6.5 Exercises ............................................................ 159

7 Arithmetic Functions 167
7.1 Motivation ............................................................ 167
7.2 Sigma and Tau Functions ......................................... 171
7.3 Perfect Numbers .................................................... 178
7.4 The Omega Functions $\omega$ and $\Omega$ ...................... 182
7.5 Euler’s Phi Function ............................................... 183
7.6 Möbius Inversion Formula ....................................... 188
7.7 Exercises ............................................................ 195

8 Euler, Fermat, and Wilson 205
8.1 Motivation ............................................................ 205
8.2 Fermat’s Little Theorem and Pseudoprimes ............... 206
8.3 Wilson’s Theorem .................................................. 212
8.4 Euler’s Theorem .................................................... 214
8.5 Exercises ............................................................ 215

9 Congruence Theory (a Group Theory Perspective) 223
9.1 Motivation ............................................................ 223
9.2 The Groups $\mathbb{Z}_n, \oplus$ and $\mathbb{U}(n), \circ$ ............ 226
9.3 Group Homomorphisms and Isomorphisms ............... 235
9.4 The Order of an Element in a Group and Primitive Roots . 239
10 Quadratic Reciprocity 251
  10.1 Motivation ......................................................... 251
  10.2 The Many Masks of Quadratic Reciprocity (QR) ............. 255
  10.3 Solving Quadratic Congruences ................................. 256
  10.4 Euler’s Criterion .................................................... 256
  10.5 The Legendre Symbol and Its Properties ..................... 256

Index 258
**Preface:** This is an introductory course to both proofs and number theory. No mathematics beyond Calculus I is assumed. As such, Chapters 0 and 1 are dedicated to introducing the beauty and power of number theory proofs and teaching the foundations of logic and set theory which will be useful for the rest of the book contents. If you are holding the student version, then there are multiple blanks throughout the book. Together in class we will be creating the missing contents of this book. In the words of mathematician Paul Halmos (1916–2006):

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

To that end, we will also have one homework assignment (with proofs and/or computations and/or conceptual questions) for each section in addition to occasional computational WeBWorK homeworks. Each written homework will be done in LaTeX and a template will be provided for each of those homeworks.

**Acknowledgments:** Co-authors aBa and Post would like to express their sincere appreciation to the following people\(^1\) for their useful comments and suggestion in earlier drafts of this book:

1. Niels Abel
2. Claude Gaspar Bachet de Merziriac
3. Étienne Bézout
4. Richard Dedekind
5. Diophantus of Alexandria
6. Lejeune Dirichlet
7. Paul Erdős
8. Eratosthenes
9. Euclid of Alexandria
10. Leonhard Euler
11. Pierre de Fermat
12. Leonardo Fibonacci
13. Carl Friedrich Gauss
14. Sophie Germain
15. Christian Goldbach
16. G.H. Hardy
17. David Hilbert
18. Hypatia of Alexandria
19. Carl Jacobi
20. Sofia Kovalevskaya
21. Leopold Kronecker
22. Ernst Kummer
23. Joseph-Louis Lagrange
24. Adrien-Marie Legendre
25. Joseph Liouville
26. Ada Lovelace
27. Marin Mersenne
28. Hermann Minkowski
29. Sir Isaac Newton
30. Emmy Noether
31. Blaise Pascal
32. Pythagoras of Samos
33. Srinivasa Ramanujan
34. Bernhard Riemann
35. Pafnuty Lvovich Chebyshev.

---

\(^1\)The authors do indeed realize that every person on their list of acknowledgments is deceased. But that mortality status did not prevent any of these 35 people from giving thoughtful comments and spiritual inspiration to co-authors aBa and Post in the writing of this book!
**About the authors:** Co-author aBa received his PhD from the University of Iowa and then completed a 3-year postdoctoral position at Bowdoin College in Maine. He is now an associate professor at the University of Wisconsin-Eau Claire (UWEC). His mathematical interests include combinatorics as related to areas such as representation theory and algebraic geometry/topology. His research interests with UWEC undergraduates have included lattice point visibility, complex reflection groups, and number theory in the Eisenstein integer ring. Co-author Post received her Bachelors degree in Mathematics at UWEC with a minor in Computer Science. She is currently exploring the computer science industry as an associate developer. Her research interests include combinatorics as related to permutation statistics in the hyperoctahedral group and topology as related to knot theory focusing on virtual spatial trivalent graphs.

![Post and aBa (in Summer 2018 at Math In The Woods)](image)
0 Preliminaries

0.1 Math Symbols Used In This Book

Below is a list of symbols with their associated meanings that we will come across in this course.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>( N )</td>
<td>set of natural numbers (we exclude 0)</td>
</tr>
<tr>
<td>( \mathbb{Z} )</td>
<td>set of integers</td>
</tr>
<tr>
<td>( \mathbb{Q} )</td>
<td>set of rational numbers</td>
</tr>
<tr>
<td>( \mathbb{R} )</td>
<td>set of real numbers</td>
</tr>
<tr>
<td>( \mathbb{C} )</td>
<td>set of complex numbers</td>
</tr>
<tr>
<td>( \cup )</td>
<td>union</td>
</tr>
<tr>
<td>( \cap )</td>
<td>intersection</td>
</tr>
<tr>
<td>( \biguplus )</td>
<td>disjoint union</td>
</tr>
<tr>
<td>( n! )</td>
<td>( n ) factorial</td>
</tr>
<tr>
<td>( \binom{n}{k} )</td>
<td>binomial coefficient</td>
</tr>
<tr>
<td>( T_n )</td>
<td>( n^{th} ) triangular number</td>
</tr>
<tr>
<td>( a \mid b )</td>
<td>( a ) divides ( b )</td>
</tr>
<tr>
<td>( a \nmid b )</td>
<td>( a ) does not divide ( b )</td>
</tr>
<tr>
<td>( \gcd(a,b) )</td>
<td>greatest common divisor of ( a ) and ( b )</td>
</tr>
<tr>
<td>( \text{lcm}(a,b) )</td>
<td>least common multiple of ( a ) and ( b )</td>
</tr>
<tr>
<td>( a \equiv b \pmod{n} )</td>
<td>( a ) is congruent to ( b ) modulo ( n )</td>
</tr>
<tr>
<td>( M_n )</td>
<td>( n^{th} ) Mersenne number</td>
</tr>
<tr>
<td>( F_n )</td>
<td>( n^{th} ) Fermat number</td>
</tr>
<tr>
<td>( \tau(n) )</td>
<td>number of positive divisors of ( n )</td>
</tr>
<tr>
<td>( \sigma(n) )</td>
<td>sum of positive divisors of ( n )</td>
</tr>
<tr>
<td>( \phi(n) )</td>
<td>Euler’s phi function</td>
</tr>
<tr>
<td>( \omega(n) )</td>
<td>omega function</td>
</tr>
<tr>
<td>( \Omega(n) )</td>
<td>Omega function</td>
</tr>
<tr>
<td>( \sum_{d</td>
<td>n} )</td>
</tr>
<tr>
<td>( \mu(n) )</td>
<td>Möbius mu function</td>
</tr>
<tr>
<td>( (\mathbb{Z}_n, \oplus) )</td>
<td>set of integers modulo ( n )</td>
</tr>
<tr>
<td>( (\mathbb{U}(n), \odot) )</td>
<td>group of units in ( \mathbb{Z}_n )</td>
</tr>
</tbody>
</table>
| \( (a \bmod{b}) \) | Legendre symbol (pronounced “\( a \) on \( b \)”)


We also have some common abbreviations used in proofs for the most part as follows.

<table>
<thead>
<tr>
<th>Abbreviations</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>∀</td>
<td>for all</td>
</tr>
<tr>
<td>∃</td>
<td>there exists</td>
</tr>
<tr>
<td>∈</td>
<td>is an element of</td>
</tr>
<tr>
<td>BWOC</td>
<td>by way of contradiction</td>
</tr>
<tr>
<td>WLOG</td>
<td>without loss of generality</td>
</tr>
<tr>
<td>TFAE</td>
<td>the following are equivalent</td>
</tr>
<tr>
<td>s.t.</td>
<td>such that</td>
</tr>
<tr>
<td>: or equivalently</td>
<td>such that (used in set-theoretic notation)</td>
</tr>
<tr>
<td>⇒</td>
<td>implies</td>
</tr>
<tr>
<td>ELFS</td>
<td>exercise left for students</td>
</tr>
<tr>
<td>WWTS</td>
<td>we want to show</td>
</tr>
<tr>
<td>Q.E.D.</td>
<td>quod erat demonstrandum [end of proof]</td>
</tr>
</tbody>
</table>

**WARNING!!!!: Caution Alert!**

Often, it is very inappropriate to use abbreviations or math symbols to replace English words. For example, here are some atrocities in math writing:

- In the monomial $x^2$, the exponent of $x = 2$.
- There exists an $x \in \mathbb{R}$ s.t. $x^2 = x$.
- If $\exists$ two numbers (WLOG $x$ and $y$) that are even $\in \mathbb{Z}$, then $x + y$ being odd $\implies$ a contradiction.

That last example is enough to make unborn babies cry in the womb.

A variety of ways ELFS (Exercise Left For Students) may appear:

- [You Do!] – generally we will all do this together.
- [You Verify] or equivalently [Confirm This!], usually for minor calculations.
- [Let’s Discuss!] – meaning of this is obvious.
Throughout the text the following two characters will arise at times to make certain observations or ask poignant questions. We call them the expressionless people.

Lastly, a very important symbol we will use in proofs is what we call the WWTS bubble. When doing a proof, it forces you to place your thoughts of what you want show at the beginning of the proof, but the BUBBLE around it reminds you that this is not true yet. Often students make the mistake of using what they want to show in their proof and taking for granted its truth. The bubble may help. For example, if we were tasked with proving the following theorem:

**Theorem 0.1.** For every real number $x$, there exists a real number $y$ such that $x + y = 0$.

The proof would begin like so:

*Proof.* Let $x \in \mathbb{R}$.

\[
\text{WWTS: } \exists y \in \mathbb{R} \text{ s.t. } x + y = 0.
\]

Then you continue on with the rest of your proof.

*Q.E.D.*
0.2 What Is Number Theory and What Is Its Purpose?

Definition 0.2. Pure mathematics is the study of mathematical concepts independently of any application outside mathematics.

Question 0.3. Who is G.H. Hardy?

- Godfrey Harold Hardy (1877—1947), England
- Known for his achievements in number theory and mathematical analysis.
- Was mentor to the Indian mathematician Srinivasa Ramanujan.
- Was an atheist.
- Detested the way mathematics was applied to war and the military.
- Preferred his work to be considered pure mathematics.

Definition 0.4. Number theory is a branch of pure mathematics devoted primarily to the study of the integers.

Number theory has the reputation of being a field in which many of whose results can be stated to the layperson. At the same time, the proofs of these results may not be particularly accessible, in part due to the vast range of tools they use within mathematics.
Quotes from G.H. Hardy

Four quotes from the famous number theorist G.H. Hardy in his famous 1940 essay titled *A Mathematician’s Apology*:

“**A mathematician, like a painter or a poet, is a maker of patterns. If his patterns are more permanent than theirs, it is because they are made with ideas.**”

“The mathematician’s patterns, like the painter’s or the poet’s must be beautiful; the ideas like the colours or the words, must fit together in a harmonious way. Beauty is the first test: there is no permanent place in the world for ugly mathematics.”

“I am interested in mathematics only as a creative art.”

“**Pure mathematics is on the whole distinctly more useful than applied. [...] For what is useful above all is technique, and mathematical technique is taught mainly through pure mathematics.**”

Blurry Line Between Pure and Applied Mathematics

The number-theorist Leonard Dickson (1874–1954) said “Thank God that number theory is unsullied by any application.” Such a view is no longer applicable to number theory especially since number theory is at the HEART of **public key cryptography**. In 1974, Donald Knuth said “...virtually every theorem in elementary number theory arises in a natural, motivated way in connection with the problem of making computers do high-speed numerical calculations.”

---

What is the Purpose of Number Theory?

Some Possible Answers:

- The beauty and elegance of the statements of the claims,
- The beauty and elegance of the proofs of the claims,
- The pleasure one receives from understanding the proofs,
- Beauty (said once more) because indeed beauty is a purpose.

A Related Question: What is the purpose of the Mona Lisa painting by Leonardo da Vinci (1452–1519)?
“An equation for me has no meaning unless it expresses a thought of God.” - Srinivasa Ramanujan

Question 0.5. Who is Srinivasa Ramanujan?

- Ramanujan’s series for $\pi$ namely

$$\pi = \frac{9801}{2\sqrt{2}} \left( \sum_{k=0}^{\infty} \frac{(4k)! \cdot (1103 + 26390k)}{(k!)^4 \cdot 396^{4k}} \right)^{-1}$$

converges extraordinarily rapidly (exponentially) and forms the basis of some of the fastest algorithms currently used to calculate $\pi$. Truncating the sum to the first term also gives the approximation $\frac{9801\sqrt{2}}{4412}$ for $\pi$, which is correct to six decimal places [Confirm This!]. Truncating the sum to the first two terms gives a value correct to 14 decimal places. [Confirm This!]

- Ramanujan’s tantalizing continued fraction in a letter to Hardy in 1913

$$\frac{1}{e^{-2\pi} + \frac{1}{e^{-4\pi} + \frac{1}{e^{-6\pi} + \frac{1}{e^{-8\pi} + \ldots}}}} = \left( \frac{\sqrt{5 + \sqrt{5}}}{2} - \frac{1 + \sqrt{5}}{2} \right)^{5\sqrt{e^{2\pi}}}$$
Ramanujan’s tantalizing nested radical

\[
\sqrt{1 + 2\sqrt{1 + 3\sqrt{1 + 4\sqrt{1 + 5\sqrt{1 + \cdots}}}}}
\]

which equals the number 3. He might have recognized this by observing

\[
3 = \sqrt{9} = \sqrt{1 + 8} = \sqrt{1 + 2 \cdot 4} = \sqrt{1 + 2\sqrt{16}} = \sqrt{1 + 2\sqrt{1 + 3 \cdot 5}} = \sqrt{1 + 2\sqrt{1 + 3\sqrt{25}}} = \sqrt{1 + 2\sqrt{1 + 3\sqrt{1 + 4 \cdot 6}}} = \cdots
\]

**Theorem 0.6** (Ramanujan’s Second Notebook, Chapter XII, entry 4). The following identity holds

\[
x + n + a = \sqrt{ax + (n + a)^2 + x\sqrt{a(x + n) + (n + a)^2 + (x + n)\sqrt{\cdots}}}
\]

**Question:** How does the theorem above prove, in particular, the special case that the nested radical at the top of the page equals 3?

**Answer:** Set \( x = 2, \ n = 1, \) and \( a = 0. \) Q.E.D.

**G.H. Hardy Reflecting on Ramanujan’s Letters**

“I had never seen anything in the least like them before. A single look at them is enough to show that they could only be written by a mathematician of the highest class. They must be true because, if they were not true, no one would have the imagination to invent them.”
Some Typical Number Theory Questions

Question 0.7. Can a sum of two squares be a square?

Answer: Yes, consider $3^2 + 4^2 = 5^2$. In general there are infinitely many so-called Pythagorean triples $(a, b, c)$ via the formula $a^2 + b^2 = c^2$.

Question 0.8. Can a sum of two cubes be a cube?

Answer: No, this is Fermat’s Last Theorem which says that there exist no integers $a$, $b$, and $c$ such that $a^n + b^n = c^n$ if $n \geq 3$.

Question 0.9. Regarding prime numbers (positive integers $p$ such that its only divisors are 1 and $p$ itself):

1. Are there infinitely many primes?
2. Are the infinitely many primes of the form $4k + 1$ where $k$ is an integer?
3. Are the infinitely many primes of the form $4k + 3$ where $k$ is an integer?

Answer: Yes to all three questions.

Question 0.10. Are there infinitely many twin primes? That is, are there infinitely many primes $p$ such that $p + 2$ is also prime?

Here is a list of the first few pairs:

$(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139), \ldots$

Answer: This is a very famous unsolved problem.
Recall the list of the first few twin prime pairs:

\[(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61),
(71, 73), (101, 103), (107, 109), (137, 139), \ldots\]

**Question 0.11.** What, if anything, is significant about the even integer lying between each pair, excluding the first pair \((3,5)\)?

**Answer:** All are multiples of 6:

\[6, 12, 18, 30, 42, 60, 72, 102, 106, 138, \ldots\]

Thus the twin prime pairs are of the form \((6q - 1, 6q + 1)\) for some \(q \in \mathbb{Z}\).

**Prove Your Conjecture:** Consider any integer \(n\) greater than 3, and divide it by 6. That is, write \(n = 6q + r\) where \(q\) is a non-negative integer and the remainder \(r\) is one of 0, 1, 2, 3, 4, or 5.

- If the remainder is 0, 2 or 4, then \(n\) is divisible by 2, and can not be prime.
- If the remainder is 3, then \(n\) is divisible by 3, and can not be prime.

So if \(n\) is prime, then the remainder \(r\) is either

- 1 and \(n = 6q + 1\) is one more than a multiple of six, or
- 5 and \(n = 6q + 5 = 6(q + 1) - 1\) is one less than a multiple of six.

Thus if \((p, p + 2)\) is a twin prime pair, then both primes are adjacent to a multiple of 6.

Q.E.D.
**Question 0.12.** Is $\sqrt{2}$ irrational?

**Answer:** Yes and we prove this in the next section.

**Question 0.13.** Is $i^i$ a real number where $i = \sqrt{-1}$?

**Answer:** Yes but we need tools from complex analysis. By a well-known formula of Euler we have $e^{i\theta} = \cos \theta + i \sin \theta$ and hence

$$e^{i\frac{\pi}{2}} = \cos \frac{\pi}{2} + i \sin \frac{\pi}{2} = i.$$  

So $i^i = (e^{i\frac{\pi}{2}})^i = e^{i^2\frac{\pi}{2}} = e^{-\frac{\pi}{2}} = \frac{1}{e^{\frac{\pi}{2}}}$ which is clearly a real number.

Q.E.D.

**Question 0.14.** Are there infinitely many primes of the form $n^2 + 1$?

Observe that if $n$ is odd, then $n^2 + 1$ is even and hence $n^2 + 1$ is not prime (excluding the trivial case when $n = 1$), so this is not an interesting question unless $n$ is even. Here is a list of the values $n^2 + 1$ for all even $n$ between 2 and 24.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$n^2 + 1$</th>
<th>Is Prime?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$2^2 + 1 = 5$</td>
<td>True</td>
</tr>
<tr>
<td>4</td>
<td>$4^2 + 1 = 17$</td>
<td>True</td>
</tr>
<tr>
<td>6</td>
<td>$6^2 + 1 = 37$</td>
<td>True</td>
</tr>
<tr>
<td>8</td>
<td>$8^2 + 1 = 65$</td>
<td>False</td>
</tr>
<tr>
<td>10</td>
<td>$10^2 + 1 = 101$</td>
<td>True</td>
</tr>
<tr>
<td>12</td>
<td>$12^2 + 1 = 145$</td>
<td>False</td>
</tr>
<tr>
<td>14</td>
<td>$14^2 + 1 = 197$</td>
<td>True</td>
</tr>
<tr>
<td>16</td>
<td>$16^2 + 1 = 257$</td>
<td>True</td>
</tr>
<tr>
<td>18</td>
<td>$18^2 + 1 = 325$</td>
<td>False</td>
</tr>
<tr>
<td>20</td>
<td>$20^2 + 1 = 401$</td>
<td>True</td>
</tr>
<tr>
<td>22</td>
<td>$22^2 + 1 = 485$</td>
<td>False</td>
</tr>
<tr>
<td>24</td>
<td>$24^2 + 1 = 577$</td>
<td>True</td>
</tr>
</tbody>
</table>

**Answer:** No one knows the answer to this question.
A Little History About the $n^2 + 1$ Problem

At the 1912 International Congress of Mathematicians, Edmund Landau (1877–1938) listed four basic problems about prime numbers. These problems were characterised in his speech as “unattackable at the present state of mathematics” and are now known as Landau’s problems. They are as follows:

1. Goldbach’s conjecture: Can every even integer greater than 2 be written as the sum of two primes?

2. Twin prime conjecture: Are there infinitely many primes $p$ such that $p + 2$ is prime?

3. Legendre’s conjecture: Does there always exist at least one prime between consecutive perfect squares?

4. Landau’s conjecture?: Are there infinitely many primes $p$ such that $p - 1$ is a perfect square? In other words: Are there infinitely many primes of the form $n^2 + 1$?

Although the last problem above is commonly known as Landau’s conjecture, its first appearance hails from a letter in 1752 from Euler to Goldbach\(^3\). Here is snippet. [Can anyone translate the German?]. Full letter linked in footnote below.

\(^{3}\)Leonard Euler, *Lettre CXLIX (Euler à Goldbach)*, The Euler Archive, [http://eulerarchive.maa.org/correspondence/letters/000877.pdf](http://eulerarchive.maa.org/correspondence/letters/000877.pdf)
The Famous Sum of Two Squares Problem

Question 0.15. Which positive integers are the sum of two squares?

For example, among the integers 1, 2, ..., 99, there are exactly 42 numbers which are the sum of two squares. [Verify a few of these]

\[
\begin{array}{ccccccccccccccc}
1 & 2 & 4 & 5 & 8 & 9 & 10 & 13 & 16 & 17 & 18 \\
20 & 25 & 26 & 29 & 32 & 34 & 36 & 37 & 40 & 41 & 45 \\
49 & 50 & 52 & 53 & 58 & 61 & 64 & 65 & 68 & 72 & 73 \\
74 & 80 & 81 & 82 & 85 & 89 & 90 & 97 & 98 \\
\end{array}
\]

Conjecture Time Again: Can you formulate any hypothesis of why a number is on the list above, and then use that hypothesis to predict the numbers \( n > 99 \) such that \( n \) is a sum of two squares? [You Do!] (It’s totally OK if you cannot come up with any reasonable hypothesis!)

Answer: An integer \( n > 0 \) is representable as a sum of two squares if and only if each prime factor \( p \) of \( n \) such that \( p \) is of the form \( 4k + 3 \) for some integer \( k \) occurs to an even power in the prime factorization of \( n \).

That is, if \( n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r} \) is a prime factorization of \( n \), then \( n = a^2 + b^2 \) for some \( a, b \in \mathbb{Z} \) if and only if for each prime \( p_i \) of the form \( 4k_i + 3 \) for some \( k_i \in \mathbb{Z} \) we have the exponent \( n_i \) is even.

Corollary Conjecture: Circle the prime numbers above. Conjecture a hypothesis of when a prime number is a sum of two squares. [You Do!]

Answer: An prime \( p > 2 \) is representable as a sum of two squares if and only \( p \) is of the form \( 4k + 1 \) for some \( k \in \mathbb{Z} \).
0.2.1 Some Beautiful Conjectures Awaiting Proofs

\textbf{Erdős-Straus Conjecture:} For all integers \( n \geq 2 \), the rational number \( \frac{4}{n} \) can be expressed as the sum of three positive unit fractions. For example,

\[
\text{for } n = 5, \text{ we have } \frac{4}{5} = \frac{1}{2} + \frac{1}{5} + \frac{1}{10}.
\]

Computer searches have verified the truth of the conjecture up to \( n \leq 10^{17} \).

\textbf{Brocard’s Problem:} This is a problem asks us to find integer values of \( n \) and \( m \) for which \( n! + 1 = m^2 \). It was posed by Henri Brocard in a pair of articles in 1876 and 1885, and independently in 1913 by Srinivasa Ramanujan. \[\text{Verify } n = 4, 5, 7 \text{ give solutions!}\]

\[
\begin{align*}
4! + 1 &= 24 + 1 = 25 = 5^2 \\
5! + 1 &= 120 + 1 = 121 = 11^2 \\
7! + 1 &= 5040 + 1 = 5041 = 71^2 
\end{align*}
\]

Hence the 3 pairs \( (n, m) \) satisfying \( n! + 1 = m^2 \) are \( (4, 5) \), \( (5, 11) \), and \( (7, 71) \).

It is conjectured that there are no other solutions.

\textbf{Brocard’s Conjecture:} There are at least four prime numbers between \( (p_n)^2 \) and \( (p_{n+1})^2 \), for \( n \geq 2 \), where \( p_n \) is the \( n^{\text{th}} \) prime number. \[\text{Verify } n = 2, 3.\]

\[
3^2 = 9 < 11, 13, 17, 19 < 25 = 5^2 \quad \text{and} \quad 5^2 = 25 < 29, 31, 37, 41 < 49 = 7^2
\]

\textbf{Riemann Hypothesis:} The Riemann zeta function is defined for complex numbers \( s \) with real part greater than 1 by the absolutely convergent infinite series

\[
\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots
\]

It can be continued analytically to be defined for ALL \( s \in \mathbb{C} \) except \( s = 1 \). The trivial zeros of \( \zeta(s) \) occur at the negative even values of \( s \). It is conjectured that all the non trivial zeros \( s = a + bi \) have real part \( a = \frac{1}{2} \).
0.2.2 Some Beautiful Results That Have Been Proven

**Fermat’s Last Theorem:** In 1637, Pierre de Fermat was studying a Latin translation of an old Greek text *Arithmetica*, a 3rd century A.D. work by Diophantus which had an enormous impact on number theory. In the margin of this book, Fermat scribbles the following in Latin:

“Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.”

In English, this translates as follows:

“It is impossible for a cube to be the sum of two cubes, a fourth power to be the sum of two fourth powers, or in general for any number that is a power greater than the second to be the sum of two like powers. I have discovered a truly marvelous demonstration of this proposition that this margin is too narrow to contain.”

But no proof was found by Fermat and hence was born the famous conjecture:

**Conjecture 0.16** (Fermat, c. 1637). The equation \( a^n + b^n = c^n \) has no integer solutions \((a, b, c)\) if \( n \geq 3 \).

More than 350 years pass before the first and only proof is found!

Andrew Wiles spends 7 years working alone in his attic and eventually proves FLT in 1995. [How?] a **VERY abridged summary is as follows**:

(a) **Fact:** The general equation for FLT can be put into an elliptical form.

(b) **Taniyama-Shimura-Weil (TSW) Conjecture, 1967:** Each rational elliptical curve is also a modular form (seen in a different way).

(c) **Frey’s Conjecture, 1986:** Any counterexample to FLT would also imply that a semistable elliptic curve existed that was not modular.

(d) **Ribet, 1990:** Ribet proves that Frey’s conjecture holds.

(e) **Wiles, 1995:** Wiles proves that TSW’s conjecture holds (in the semistable elliptic setting).
\textbf{e is irrational}

\textbf{Fact:} (From Calculus II) The Maclaurin series expansion of $e^x$ is $\sum_{n=0}^{\infty} \frac{x^n}{n!}$. Thus
\[ e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots. \]

\textbf{Theorem 0.17} (Euler, 1737). \textit{The number $e$ is irrational.}

\textit{Proof.} [Hardy and Wright, 1960]\footnote{G.H. Hardy and E.M. Wright, \textit{An Introduction to the Theory of Numbers}, 4th Ed., Oxford University Press, London, 1960.} Assume by way of contradiction that $e$ is rational. Then since $e$ is positive, we may write it as $\frac{p}{q}$ for some positive integers $p$ and $q$. It follows that
\[ \frac{p}{q} = \sum_{n=0}^{q} \frac{q}{n!} + \sum_{n=q+1}^{\infty} \frac{1}{n!}. \] [Why?]

Thus we have
\[ \frac{p - \sum_{n=0}^{q} \frac{1}{n!}}{q} = \sum_{n=q+1}^{\infty} \frac{1}{n!}. \]

Multiplying both sides by $q!$, we get
\[ p \cdot (q - 1)! - \sum_{n=0}^{q} \frac{q!}{n!} = \sum_{n=q+1}^{\infty} \frac{q!}{n!}. \]

The LHS of Equation (1) is as follows: [You Verify!]
\[ p \cdot (q - 1)! - [q! + q! + (q \cdot (q - 1) \cdots 2) + (q \cdot (q - 1) \cdots 3) + \cdots + (q \cdot (q - 1)) + q + 1], \]
which is clearly an integer. Denote this integer by $M$. Meanwhile, the RHS of Equation (1) is as follows: [You Verify!]
\[ \frac{1}{q + 1} + \frac{1}{(q + 1)(q + 2)} + \frac{1}{(q + 1)(q + 2)(q + 3)} + \cdots. \]

Denote this infinite series above by $N$. So Equation (1) becomes $M = N$. Observe
that we have the following:

\[ M = N \]
\[ < \frac{1}{q + 1} + \frac{1}{(q + 1)^2} + \frac{1}{(q + 1)^3} + \cdots \]  
\[ = \frac{1}{1 - \left(\frac{1}{q+1}\right)} - 1 \]  
\[ = \frac{1}{q}. \]

Hence \( M < \frac{1}{q} \) which gives a contradiction. [Why?] Thus it cannot be the case that \( e \) is rational. So we conclude that \( e \) is irrational.

Q.E.D.

**HINT:** To answer that last [Why?], it may be helpful to recall that \( M \) is an integer and also equal to \( e - \sum_{n=0}^{q} \frac{1}{n!} \) [And so what?] and that \( q \) is a positive integer.

**Definition 0.18.** An **algebraic number** is a number that is a root of a nonzero polynomial with rational coefficients. A number which is not algebraic is called a **transcendental number**.

---

Hermite proved \( \pi \) is transcendental in 1873. And Lindemann proved \( e^\pi \) is transcendental in 1882. Moreover, \( e^e \) is too!!

Big Deal. No one knows yet if any of the following are transcendental:
\[ \pi^e, e^\pi, \pi^\pi, \pi + e, \pi e, \pi^e \]

\(^5\)In fact, to this date no one even knows whether any of the values in the right cartoon person’s list is irrational or not.
Which is larger: $\pi^e$ or $e^\pi$?

Observe the following sequence of inequalities:

\[
\begin{align*}
1^2 &< 2^1 \\
2^3 &< 3^2 \\
\text{"LIMBO LAND"} &\\
3^4 &> 4^3 \\
4^5 &> 5^4
\end{align*}
\]

The values $e$ and $\pi$ lie between 2 and 4. So an inequality involving $e^\pi$ and $\pi^e$ lies in "limbo land".

The following is a recently published\(^6\) "proof without words" that $\pi^e < e^\pi$ holds:

\[\begin{align*}
\ln \pi - 1 = \int_e^\pi \frac{dx}{x} < \frac{1}{e} (\pi - e) = \frac{\pi - 1}{e} \\
\pi^e < e^\pi.
\end{align*}\]

**FILL IN DETAILS OF THIS PROOF:** [You Do!] The area under the curve $y = \frac{1}{x}$ from $x = e$ to $x = \pi$ being $\ln \pi - 1$ is simply integral calculus. Moreover, this area is clearly smaller than the area of the rectangle $PQRS$. Thus, it follows that

\[
\begin{align*}
\ln \pi - 1 < \frac{\pi}{e} - 1 &\implies \ln \pi < \frac{\pi}{e} &\implies e^{\ln \pi} < e^{\frac{\pi}{e}} &\implies \cdots \\
\cdots &\implies \pi < e^{\frac{\pi}{e}} &\implies \pi^e < \left(e^{\frac{\pi}{e}}\right)^e &\implies \pi^e < e^\pi.
\end{align*}
\]

Q.E.D.

\(^6\)B. Chakraborty, A visual proof that $\pi^e < e^\pi$, appeared online in August 2018 in *Mathematical Intelligencer*. 
0.2.3 Number Theory Flourishes In Hollywood Films

In an English nursery-rhyme poem, dating back as far as 1730\(^7\), a number theory riddle was presented. A modern version of the poem goes as follows:

As I was going to St. Ives,
I met a man with seven wives,
Each wife had seven sacks,
Each sack had seven cats,
Each cat had seven kits:
Kits, cats, sacks, and wives,
How many were there going to St. Ives?

**SOLUTION ATTEMPT:** The following may be going to St. Ives:

- 1 man
- 7 wives
- \(7^2 = 49\) sacks (since there are 7 sacks for each wife)
- \(7^3 = 243\) cats (since there are 7 cats in each sack)
- \(7^4 = 2401\) kittens (since each cat had 7 kittens)

So the total is a sum of a finite geometric series easily computed by the formula

\[
1 + r + r^2 + \ldots r^{n-1} = \frac{r^n - 1}{r - 1}.
\]

So our total equals \(\frac{4^5-1}{4-1} = \frac{16806}{3} = 5602\). But if we include the narrator, then there could be as many as 5603 people and animals on their way to St. Ives.

This version made a comeback in the 1995 Hollywood film *Die Hard with a Vengeance*.

Let’s take a wee break and watch the scene in the movie. Click the link below:

https://www.youtube.com/watch?v=zcUJUOMtfHQ

---

The Goldbach Conjecture (in a movie)

**The Conjecture:** Every even number greater than 2 can be expressed as the sum of two primes. [Verify for \( n = 4, 6, 8, \ldots, 20 \).]

**Status of the Problem (as of the year 2019):** The conjecture has been verified for all even numbers less than \( 4 \times 10^{18} \) but still remains unsolved.

Below is the letter that Goldbach sent to Euler on June 7, 1747, which discusses a similarly stated conjecture of the above:

Let’s take a wee break and watch the scene in the movie\(^8\). Click the link below:

http://www.math.harvard.edu/~knill/mathmovies/swf/calculuslove.html

---

\(^8\)The weblink is attributed to Harvard mathematician Oliver Knill. He has tons of links to movies and TV shows where math pops up. He welcomes increasing his list. Co-author aBa has provided him with a number of these entries.
0.3 Examples of the Beauty and Power of Number Theory

Before we explore our first example of the beauty and power of number theory, we introduce two lemmas. The first of these is a very powerful and fundamental tool used in combinatorics, and it is made transparent by the following image:

CLAIM: If there 10 pigeons and only 9 holes, then if all 10 pigeons are to fly into the holes, then at least one hole will contain more than one pigeon.

Proof. Obvious.

\[ \text{Q.E.D.} \]

Lemma 0.19 (Pigeonhole Principle). If \( m \) and \( n \) are positive integers with \( m < n \), then if we are to place \( n \) objects into \( m \) containers, then at least one container will contain more than one object.

Lemma 0.20. If \( a, b \in \mathbb{Z} \) and leave the same remainder upon division by some \( d \in \mathbb{Z} \), then \( d \) divides their difference \( a - b \).

Proof. [You Do!] Suppose two number \( a, b \in \mathbb{Z} \) leave the same remainder \( r \) upon division by some \( d \in \mathbb{Z} \). Then \( a = md + r \) and \( b = nd + r \) for some \( m, n \in \mathbb{Z} \). Thus \( a - b = (md + r) - (nd + r) = (m - n)d \).

\[ \text{Q.E.D.} \]

Example 0.21. Set \( a = 51, b = 16 \), and \( d = 7 \). It is easy to verify that \( a \) and \( b \) leave a remainder of \( 2 \) upon division by \( d \). And clearly \( d \) divides \( a - b \) since

\[
51 = \boxed{7} \cdot 7 + \boxed{2} \\
16 = \boxed{2} \cdot 7 + \boxed{2}
\]

and \( 51 - 16 = 35 = \left( \frac{7}{2} - \frac{2}{2} \right) \cdot 7 \).
Our First Beautiful Theorem

Theorem 0.22. Consider the following sequence of integers with repeating digits:

1, 11, 111, 1111, 11111, 111111, \ldots

There is at least one term divisible by 2019.

Proof. [You Do!] We prove something stronger. We show at least one term in the sequence of the first 2019 terms is divisible by 2019. To set notation, let $y_i$ denote the $i$th term in the sequence (i.e., the term with exactly $i$ ones), and let $(y_i)_{i=1}^{2019}$ denote the sequence of the first 2019 terms.

Suppose BWOC that for each $1 \leq i \leq 2019$, none of the $y_i$ are divisible by 2019. Set $r_i$ to equal the remainder of $y_i$ upon division by 2019. Thus in the sequence $(r_i)_{i=1}^{2019}$, we observe the following:

- Each integer $r_i$ lies strictly between 0 and 2019. [WHY?]
- There must be at least two terms that are equal. [WHY?]

Let us denote these two equal remainders $r_j$ and $r_k$ for some indices $j, k$ with $1 \leq j < k \leq 2018$. Consider the difference $y_k - y_j$.

\[
y_k \leftrightarrow \underbrace{111 \cdots 11111 \cdots 111}_{k \text{ ones}}
\]
\[
y_j \leftrightarrow \underbrace{111 \cdots 111}_{j \text{ ones}}
\]
\[
y_k - y_j = \underbrace{111 \cdots 11000 \cdots 000}_{\text{clearly } j \text{ zeros and hence } k - j \text{ ones}}
\]

Observe the following:

- $y_k - y_j$ leaves a remainder of 0 upon division by 2019. [WHY?]
- $y_k - y_j$ equals $y_{k-j} \cdot 10^j$. [WHY?]
- Hence 2019 divides $y_{k-j} \cdot 10^j$ forcing 2019 to divide $y_{k-j}$. [WHY?]

This gives a contradiction. [WHY?] And we conclude that some term in the sequence $(y_i)_{i=1}^{2019}$ is divisible by 2019.

Q.E.D.
After Thoughts and Remarks/Questions

- Was there anything special about the ones? For example, does 2019 divide some term in the sequence

\[ 2, \ 22, \ 222, \ 2222, \ 22222, \ 222222, \ldots ? \]

- Was there anything special about the 2019? For example, can we replace the 2019 with 2018 and use the same proof?

- The proof although beautiful, does not tell us WHICH term in the sequence will be divisible by 2019. This type of proof is called an **existence proof**.

<table>
<thead>
<tr>
<th>( n )</th>
<th>the ( n^{th} ) term ( y_n )</th>
<th>Does 21 divide ( y_n )?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>False</td>
</tr>
<tr>
<td>2</td>
<td>11</td>
<td>False</td>
</tr>
<tr>
<td>3</td>
<td>111</td>
<td>False</td>
</tr>
<tr>
<td>4</td>
<td>1111</td>
<td>False</td>
</tr>
<tr>
<td>5</td>
<td>11111</td>
<td>False</td>
</tr>
<tr>
<td>6</td>
<td>111111</td>
<td>True</td>
</tr>
<tr>
<td>7</td>
<td>1111111</td>
<td>False</td>
</tr>
<tr>
<td>8</td>
<td>11111111</td>
<td>False</td>
</tr>
<tr>
<td>9</td>
<td>111111111</td>
<td>False</td>
</tr>
<tr>
<td>10</td>
<td>1111111111</td>
<td>False</td>
</tr>
<tr>
<td>11</td>
<td>11111111111</td>
<td>False</td>
</tr>
<tr>
<td>12</td>
<td>111111111111</td>
<td>True</td>
</tr>
<tr>
<td>13</td>
<td>1111111111111</td>
<td>False</td>
</tr>
<tr>
<td>14</td>
<td>11111111111111</td>
<td>False</td>
</tr>
<tr>
<td>15</td>
<td>111111111111111</td>
<td>False</td>
</tr>
<tr>
<td>16</td>
<td>111111111111111</td>
<td>False</td>
</tr>
<tr>
<td>17</td>
<td>1111111111111111</td>
<td>False</td>
</tr>
<tr>
<td>18</td>
<td>11111111111111111</td>
<td>True</td>
</tr>
</tbody>
</table>

**YOUR CONJECTURE:**\(^9\) [You Do!] 21 divides \( y_n \) if and only if \( n \) is a multiple of 6.

\(^9\)Later in the course, you will have the tools to prove a more general statement of your conjecture.
Our Second Beautiful Theorem

**Theorem 0.23.** The sum $1 + 2 + 3 + \cdots + n$ equals $\frac{n(n+1)}{2}$.

The proof is made perhaps crystal clear by just gazing at the image below.

![Image of square arrays demonstrating the theorem](image)

**The Gauss Child Prodigy Anecdote**

When the soon-to-be great number theorist Carl Friedrich Gauss was only 7 years old in an advanced math class, he was tasked with doing busy work of finding the sum:

$$1 + 2 + 3 + \cdots + 100.$$ 

Minutes later, Gauss presented his slate board to the teacher. It had only one number on it, namely the correct sum of 5050.

**QUESTION:** How did Gauss do this? [Let’s Discuss]
Our Third Beautiful Theorem  
(Ugly Version)

**Theorem 0.24.** The sum $1^3 + 2^3 + 3^3 + \cdots + n^3$ equals $\frac{n^4 + 2n^3 + n^2}{4}$.

**Hands Dirty Part:**

**QUESTION:** Do we even believe the statement? It certainly is ugly. But lots of ugly things are true (but beautiful deep down inside); for example\(^{10}\)

$$\pi = \frac{9801}{2\sqrt{2}} \left( \sum_{k=0}^{\infty} \frac{(4k)! \cdot (1103 + 26390k)}{(k!)^4 \cdot 396^{4k}} \right)^{-1}.$$  

So back to the theorem above, let us get our hands dirty and verify the statement for small values of $n$. [Fill out the table below!]

<table>
<thead>
<tr>
<th>$n$</th>
<th>$1^3 + 2^3 + 3^3 + \cdots + n^3$</th>
<th>$\frac{n^4 + 2n^3 + n^2}{4}$</th>
<th>Cool?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$1^3$ = 1</td>
<td>$\frac{1^4 + 2 \cdot 1^3 + 1^2}{4} = \frac{4}{4} = 1$</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>$1^3 + 2^3$ = 9</td>
<td>$\frac{2^4 + 2 \cdot 2^3 + 2^2}{4} = \frac{36}{4} = 1$</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>$1^3 + 2^3 + 3^3$ = 36</td>
<td>$\frac{3^4 + 2 \cdot 3^3 + 3^2}{4} = \frac{144}{4} = 1$</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>$1^3 + 2^3 + 3^3 + 4^3$ = 100</td>
<td>$\frac{4^4 + 2 \cdot 4^3 + 4^2}{4} = \frac{400}{4} = 1$</td>
<td>Yes</td>
</tr>
<tr>
<td>5</td>
<td>$1^3 + 2^3 + 3^3 + 4^3 + 5^3$ = 225</td>
<td>$\frac{5^4 + 2 \cdot 5^3 + 5^2}{4} = \frac{900}{4} = 1$</td>
<td>Yes</td>
</tr>
</tbody>
</table>

\(^{10}\)Truthfully, beauty is only skin deep. In this famous formula by the great Ramanujan, we see a rather displeasing-to-the-eye formula for $\pi$, yet it is also MESMERIZING!
Our Third Beautiful Theorem
(Ugly Version) - Continued

So it seems that we believe the statement holds. Now the big question is how to prove it. We want to show the following identity holds for all \( n \in \mathbb{N} \).

\[
1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^4 + 2n^3 + n^2}{4}
\]

1) **MUTILATE AND MUTATE STRATEGY:**

“Mess around” with the RHS until it looks less like a foe and more like a friend!

**[You Do!]**

By playing around with the RHS we can deduce the following:

\[
\frac{n^4 + 2n^3 + n^2}{4} = \frac{n^2(n^2 + 2n + 1)}{4} = \frac{n^2(n+1)^2}{4} = \left( \frac{n(n+1)}{2} \right)^2
\]

2) **TRANSFORM THE PROBLEM INTO A TOTALLY NEW PROBLEM:** **[You Do!]**

Gauss’ sum is \( 1 + 2 + 3 + \cdots + n = \frac{n(n + 1)}{2} \), so a new way to look at this problem is to change it into one of solving

\[
1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + 3 + \cdots + n)^2.
\]
Our Third Beautiful Theorem  
(Pretty Version)

**Theorem 0.25.** For all \( n \in \mathbb{N} \), we have
\[
\sum_{k=1}^{n} k^3 = \left( \sum_{k=1}^{n} k \right)^2.
\]

**HISTORICAL NOTE:** This problem dates back to the 1st Century A.D., in the time of the Pythagoreans\(^{11}\). One particular Pythagorean by the name of Nicomachus of Gerasa was aware of the following\(^{12}\):
\[
\begin{align*}
1 &= 1 \\
8 &= 3 + 5 \\
27 &= 7 + 9 + 11 \\
64 &= 13 + 15 + 17 + 19 \\
125 &= 21 + 23 + 25 + 27 + 29
\end{align*}
\]

**QUESTION:** How does Nicomachus’ observation relate directly to the theorem above? Or what kind of connection can you make if not directly with the theorem above?

**ANSWER:** [You Do!] The right hand side of Nicomachus’ observation are sums of consecutive odds. But hmmm. ...what do sums of consecutive odds have to do with the value \( (\sum_{k=1}^{n} k)^2 \)? Well they have a very intimate connection.

We omit the proof of the connection of Nicomachus’ right hand side of values with the value on the right hand side of the theorem above. And instead prove Theorem 0.25 in the most beautiful manner possible on the next page.

---

\(^{11}\)Pythagoreanism originated in the 6th Century B.C. and is based on the teachings and beliefs held by Pythagoras. The followers of Pythagoreanism are called Pythagoreans.

\(^{12}\)This is from Nicomachus’ text “Introduction to Arithmetic”, Book 2, Chapter XX, translated by Martin Luther D’Ooge and published by the Macmillan Company, New York, 1926.
Our Third Beautiful Theorem
(Pretty Version with the Most Beautiful Proof!)

Our goal is to prove Theorem 0.25 which states $\sum_{k=1}^{n} k^3 = (\sum_{k=1}^{n} k)^2$ or in a less “summy”-notation way, simply

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

A proof without words for this beautiful result of Nicomachus in the 1st Century A.D. was given in 1985 by Alan L. Fry\textsuperscript{13}. We give a variation of this proof in the illustration below.

QUESTION: How does this work? [Let’s Discuss]

1 Proofs – An Introduction

“The essential quality of a proof is to compel belief”
- Pierre de Fermat (1601–1665)

Committee on the Undergraduate Program (CUPM-2001) writes:

“All students should achieve an understanding of the nature of proof. Proof is what makes mathematics special.”

Of course, the CUPM does not recommend “theorem-proof” type courses for non-math majors, but they do write the following.

“The International Commission on Mathematical Instruction (2008) writes:

“Proof is much more than a sequence of correct steps, it is also and, perhaps most importantly, a sequence of ideas and insights, with the goal of mathematical understanding—specifically, understanding WHY a claim is true.”
1.1 Statements and Truth Tables

**Definition 1.1.** A *statement* (or proposition) is a declarative sentence that is true or false but not both.

**Question 1.2.** Which of the following are statements? Write *NS* if it is not a statement and *S* if it is. Also give the truth value if it is a statement.

- January is the first month of the year. *S* - True
- June is the first month of the year. *S* - False
- The Packers is the best football team. *NS* - “Sorry, Packer fans.”
- $6x + 3 = 17$. *NS* - It depends on what $x$ is.
- The equation $6x + 3 = 17$ has more than one solution. *S* - False
- This statement is false. *NS* - Let’s discuss why.

**Definition 1.3.** A *truth table* is a mechanism for determining the truth values of compound statements.

Complete filling out the tables below for negations, conjunctions, disjunctions, and implications. [You Do!]

**(i) NEGATION:** “not” symbol $\sim$

<table>
<thead>
<tr>
<th>$A$</th>
<th>$\sim A$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

The rule is: “Not” reverses the truth value.
(ii) **CONJUNCTION**: “and” symbol $\land$

<table>
<thead>
<tr>
<th>$A$</th>
<th>$B$</th>
<th>$A \land B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

The rule is: An “and” is true ONLY WHEN both sides are true.

(iii) **DISJUNCTION**: “or” symbol $\lor$

<table>
<thead>
<tr>
<th>$A$</th>
<th>$B$</th>
<th>$A \lor B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

The rule is: An “or” is false ONLY WHEN both side are false.

(iv) **IMPLICATION**: “if-then” symbol $\Rightarrow$

<table>
<thead>
<tr>
<th>$A$</th>
<th>$B$</th>
<th>$A \Rightarrow B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

The rule is: An “if-then” is false ONLY WHEN the hypothesis holds but the conclusion fails.

**Definition 1.4.** A **vacuously true statement** is an “if-then” statement in which the “if”-part (i.e., hypothesis) is false. Hence the statement will be true regardless of the truth value of the “then”-part (i.e., the conclusion).

Equivalently, a vacuous truth is a statement that asserts that all members of an empty set possess a certain property. [Give some examples!]
Definition 1.5. (Tautology versus Contradiction)

- A **tautology** is a statement that is always true.
- A **contradiction** is a statement that is always false.

Example 1.6. Is the statement \((A \lor \neg B) \lor \neg A\) a tautology, contradiction, or neither? [You Do!]

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>\sim B</th>
<th>A \lor \sim B</th>
<th>\sim A</th>
<th>(A \lor \sim B) \lor \sim A</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

We conclude that \((A \lor \sim B) \lor \sim A\) is a: **Tautology!**

Definition 1.7. Two statements are **logically equivalent** if they have the same truth tables. We use the symbol \(\equiv\) to denote this.

Example 1.8. Show that \(\sim (A \lor B) \equiv \sim A \land \sim B\). [You Do!]

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>A \lor B</th>
<th>\sim (A \lor B)</th>
<th>\sim A</th>
<th>\sim B</th>
<th>\sim (A \lor B) \equiv \sim A \land \sim B</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

We conclude that: \(\sim (A \lor B)\) is logically equivalent to \(\sim A \land \sim B\).

Definition 1.9. **De Morgan’s Laws** assert the following logical equivalencies:

- \(\sim (A \lor B)\) is logically equivalent to \(\sim A \land \sim B\).
- \(\sim (A \land B)\) is logically equivalent to \(\sim A \lor \sim B\).
Converting Sentences Into Formal Logic

**EXERCISE:** Convert the following sentences into formal logic. [You Do!]

(i) If it rains, then I get wet.
   - Let $P$ equal “it is raining”.
   - Let $Q$ equal “I get wet”.
Then the formal logic statement is: $P \implies Q$

(ii) I hate math, but I like this course.
   - Let $P$ equal “I hate math”.
   - Let $Q$ equal “I like this course”.
Then the formal logic statement is: $P \land Q$

**CAREFUL!** Sometimes the word “but” is used in place of “and” when the part of the independent clause that follows the “but” is unexpected.

(iii) Katie Sue does not like Jammo, or Zhang Li likes Edith.
   - Let $P$ equal “Katie Sue likes Jammo”.
   - Let $Q$ equal “Zhang Li likes Edith”.
Then the formal logic statement is: $\sim P \lor \sim Q$

(iv) If I study hard, then I will rock this course!
   - Let $P$ equal “I study hard”.
   - Let $Q$ equal “I will not rock this course”.
Then the formal logic statement is: $P \implies \sim Q$
1.2 Implications

First recall the “If-Then” truth table below:

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>A ⇒ B</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

**EXERCISE:** Compute the truth table for ~B ⇒ ~A. [You Do!]

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>∼ A</th>
<th>∼ B</th>
<th>∼ B ⇒ ∼ A</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

**QUESTION:** Is A ⇒ B logically equivalent to ∼B ⇒ ∼A? [Hell Yah!]

**Definition 1.10.** The **contrapositive** of the statement A ⇒ B is the statement ∼B ⇒ ∼A.

**EXERCISE:** Compute the truth table for B ⇒ A. [You Do!]

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>B ⇒ A</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

**QUESTION:** Is A ⇒ B logically equivalent to B ⇒ A? [Nope!]

**Definition 1.11.** The **converse** of the statement A ⇒ B is the statement B ⇒ A.
**EXERCISE:** Compute the truth table for $\sim A \implies \sim B$. [You Do!]

<table>
<thead>
<tr>
<th>$A$</th>
<th>$B$</th>
<th>$\sim A$</th>
<th>$\sim B$</th>
<th>$\sim A \implies \sim B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

**QUESTION:** Is $A \implies B$ logically equivalent to $\sim A \implies \sim B$? [Nope!]

**Definition 1.12.** The **inverse** of the statement $A \implies B$ is the statement $\sim A \implies \sim B$.

**EXERCISE:** Consider the statement “If $n$ is divisible by 10 or divisible by 12, then $n$ is even.” [Answer the following!]

**Contrapositive and truth value?:** If $n$ is odd, then $n$ is not divisible by 10 and not divisible by 12. **NOTE:** It is more colloquial in English to say “$n$ is neither divisible by 10 nor 12”. - TRUE.

**Converse and truth value?:** If $n$ is even, then $n$ is divisible by 10 or divisible by 12. - FALSE, let $n = 4$.

**Inverse and truth value?:** If $n$ is neither divisible by 10 nor 12, then $n$ is odd. - False, let $n = 8$. 
The Or-Form of an Implication

**EXERCISE:** Compute the truth table for $\sim A \lor B$ and compare it to $A \implies B$.

[You Do!]

<table>
<thead>
<tr>
<th>$A$</th>
<th>$B$</th>
<th>$\sim A$</th>
<th>$\sim A \lor B$</th>
<th>$A \implies B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

**QUESTION:** Is $A \implies B$ logically equivalent to $\sim A \lor B$? [Hell Yah!]

**EXERCISE:** Consider the statement “If I don’t study, then I fail.” [Answer the following!]

Write the Or-Form: I study or I fail.

**NOTE:** This is a very true statement, so STUDY DILIGENTLY everyone!

The Negation of an Implication

Since we know that $A \implies B$ logically equivalent to $\sim A \lor B$, then it is simple to find the negation of $A \implies B$. We simply take the negation of its equivalent form $\sim A \lor B$.

**EXERCISE:** Using De Morgan’s Law, what is the negation of $\sim A \lor B$? $A \land \sim B$ Verify this is indeed $\sim (A \implies B)$ via the truth table. [You Do!]

<table>
<thead>
<tr>
<th>$A$</th>
<th>$B$</th>
<th>$\sim B$</th>
<th>$A \land \sim B$</th>
<th>$A \implies B$</th>
<th>$\sim (A \implies B)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
</tbody>
</table>

Observe that the 4th column we just computed, could easily have been done by just negating the 3rd column of the table at the top of the page!
EXERCISE: Consider the statement “If I have a baby, then my life will suck.”  
[Answer the following!]

Write the negation: I have a baby, but my life doesn’t suck.

EXERCISE: Write a sequence of logical equivalencies to prove again (but without truth tables that the negation of $A \implies B$ is indeed $A \land \neg B$. [You Do!]

$$
\neg (A \implies B) \equiv \neg (\neg A \lor B) \equiv \neg \neg A \land \neg B \equiv A \land \neg B
$$

EXERCISE: Consider the statement: “Today is not Easter, or tomorrow is Monday.”

Discuss the truth value of this statement: [You Do!]

NOTE: Do not assume today is this very day.

HINT: Consider all possible cases of the day of the week it can be, and whether today is Easter or tomorrow is Monday holds in each case.

If today is Monday, then it is DEFINITELY not Easter. The same goes for the cases of Tuesday through Saturday. Now on the final case when it is Sunday, then we don’t know if it is Easter Sunday; however, it is certain that “tomorrow is Monday” will definitely hold. So the OR-STATEMENT is true.

Write down the If-Then form of the Or-Statement: [You Do!]

If today is Easter, then tomorrow is Monday.

---

14 This is an image of authors Post and aBa, respectively, when they were little babies in a parallel universe obviously since baby aBa arrived to Earth many gestation periods before Post arrived.
1.3 Predicates and Quantifiers

**Definition 1.13.** A **predicate** (or propositional function) is a sentence that contains a finite number of variables and becomes a proposition when specific values are substituted for the variables.

The **domain of a predicate** is the set of all values that may be substituted in place of the variable.

**Example 1.14.** Let $D$ be the set of all animals. Let $P(x)$ be the predicate 

“$x$ is a mammal”.

**QUESTION:** For which $x$ in the subset \{sharks, whales, kangaroos\} $\subseteq D$ is the predicate $P(x)$ true? [You Do!] **Whales and kangaroos are mammals.**

**Definition 1.15.** A **quantifier** is a logical symbol which makes an assertion about the set of values which make one or more predicates true.

**QUESTION:** What are two VERY WELL-KNOWN quantifiers that you use a lot in mathematics? [You Do!]

**ANSWER:** “for all” $\forall$ and “there exists” $\exists$

**Note:** “there exists” is usually followed by a “such that”. We sometimes abbreviate “such that” by “s.t.”.

**EXERCISE:** Let $P(x, y)$ be the predicate $xy \in \mathbb{Z}$ [Answer the following!]

- If $D = \mathbb{N}$, is $P(x, y)$ true $\forall x, y \in D$? Yes.
- If $D = \mathbb{Z}$, is $P(x, y)$ true $\forall x, y \in D$? Yes.
- If $D = \mathbb{Q}$, is $P(x, y)$ true $\forall x, y \in D$? No, set $x = \frac{1}{2}$ and $y = 3$.
- If $D = \mathbb{N}$, is $P(x, y)$ true $\forall x, y \in D$? No, set $x = \pi$ and $y = e$. 
Universal and Existential Statements

**REMARK:** In the following, let $Q(x)$ be a predicate with domain $D$.

**Definition 1.16.** A **universal statement** is a statement using a **universal quantifier** $\forall$ as follows:

$$\forall x \in D, Q(x).$$

An **existential statement** is a statement using an **existential quantifier** $\exists$ as follows:

$$\exists x \in D \text{ s.t. } Q(x).$$

**How to (Dis)Prove a Universal and Existential Statements:**

- **To Prove:** $\forall x \in D, Q(x)$
  
  Let $x \in D$. Then show that $Q(x)$ holds.

- **To Disprove:** $\forall x \in D, Q(x)$
  
  Find a counterexample (i.e., show $\exists x \in D \text{ s.t. } Q(x)$ fails).

- **To Prove:** $\exists x \in D \text{ s.t. } Q(x)$
  
  Find at least one $x \in D$ such that $Q(x)$ holds.

- **To Disprove:** $\exists x \in D \text{ s.t. } Q(x)$
  
  Show that for all $x \in D$, the statement $Q(x)$ fails.
**EXERCISE:** Let $D = \mathbb{Z}$ and consider the universal statement:

$$
\forall x \in D, \text{ we have } \frac{x}{x^2 + 1} < \frac{1}{2}.
$$

Is the predicate $P(x) = \ " \frac{x}{x^2 + 1} < \frac{1}{2} "$ true for all $x \in D$?

**ANSWER:** Setting $x = 1$, we have $\frac{x}{x^2 + 1}$ equals $\frac{1}{2}$, so the predicate is not true for all $x \in D$.

**EXERCISE:** Let $D = \{2, 5, 9, 10\}$ and consider the universal statement:

$$
\forall x \in D, \text{ we have } x^2 > x + 1.
$$

Is the predicate $P(x) = \ " x^2 > x + 1 "$ true for all $x \in D$?

**ANSWER:** Setting $x = 2$, we get $2^2 > 2 + 1$. Setting $x = 5$, we get $5^2 > 5 + 1$. Setting $x = 9$, we get $9^2 > 9 + 1$. Setting $x = 10$, we get $10^2 > 10 + 1$. So the predicate is true for all $x \in D$.

Remark 1.17. The proof technique used above is called a proof by exhaustion for obvious reasons. ☺

**EXERCISE:** Let $D = \mathbb{R}$ and consider the universal conditional\(^\text{15}\)

$$
x < y \text{ and } w < z \implies xw < yz.
$$

Is the predicate $P(x, y, w, z) = \ " x < y \text{ and } w < z \implies xw < yz "$ true for all $x \in D$?

**ANSWER:** Setting $x = w = -10$ and $y = z = 0$, we have $-10 < 0$ and $-10 < 0$, but $xw < yz$ does not hold since

$$
(-10) \cdot (-10) = 100 < 0 = 0 \cdot 0 \text{ is false.}
$$

So the predicate is not true for all $x \in D$.

\(^{15}\)This term “universal conditional” will be explained on the next page in Remark 1.18.
Remark 1.18. The statement in the previous example is called a \textbf{universal conditional statement} since it is understood to mean

\[ \forall x, y, w, z \in \mathbb{R}, \ P_1(x, y, w, z) \implies P_2(x, y, w, z) \]

where \( P_1(x, y, w, z) \) is \( x < y \) and \( w < z \), and \( P_2(x, y, w, z) \) is \( xw < yz \).

**EXERCISE:** Universal conditional statements in informal English are quite often implied rather than specific. Rewrite the following statements formally. [You Do!]

- All real numbers are positive when squared.
  
  \[ \text{For all numbers } x, \text{ if } x \in \mathbb{R} \text{ then } x^2 \geq 0. \]

- If a polygon has 3 sides, it must be a triangle. \textbf{Maybe replace with a “more NT” example}
  
  \[ \text{For all polygons } p, \text{ if } p \text{ has 3 sides then } p \text{ is a triangle}. \]

- A girl has got to be crazy to date that psycho killer.
  
  \[ \text{For all girls } g, \text{ if } g \text{ dates that psycho killer then } g \text{ is crazy}. \]

\begin{tcolorbox}
\textbf{A Helpful Proof Tip (using negations)}

To prove a statement is true, it is often helpful (or easier) to instead consider proving the NEGATION of the statement is false.
\end{tcolorbox}

**EXERCISE:** We will formally learn how to take the negations on the next page, but for now attempt to write an “informal” negation for each of the three universal conditional statements above. [You Do!]

- There is a real number that is not positive when squared.

- A 3-sided polygon exists and is not a triangle.

- Some non-crazy girl dates that psycho killer.
Negations of Universal and Existential Statements

How to Negate Universal and Existential Statements:

- **To negate a universal statement:** [You Do!]
  \[
  \sim (\forall x \in D, \, Q(x)) \equiv \exists x \in D \text{ s.t. } \sim Q(x)
  \]

- **To negate an existential statement:** [You Do!]
  \[
  \sim (\exists x \in D \text{ s.t. } Q(x)) \equiv \forall x \in D, \sim Q(x)
  \]

**EXERCISE:** Negate “there is a natural number that is even and prime”.

**ANSWER:** Every natural number is odd or composite.

**EXERCISE:** Negate “all dogs go to heaven”.

**ANSWER:** There exists a dog that does not go to heaven.

**NOTE:** This negation is false because it is well known that it is indeed true that ALL dogs go to heaven as can be seen in the image below\(^{16}\). And hence the universal statement is true.

---

\(^{16}\)This painting was done by artist Jim Warren and appears with his permission. You can see more of his work at [https://jimwarren.com/](https://jimwarren.com/).
**Statements with Multiple Quantifiers**

Many statement mix $\forall$ and $\exists$, it is important to note the following:

- Order of the symbols $\forall$ and $\exists$ matters!!
- Order does not matter if there are two $\forall$'s or two $\exists$'s.

**Example 1.19.** Let the domain $D$ be the set of all people. And let $P(x, y)$ be the predicate “$x$ loves $y$”.

- **Interpret the following:** $\forall x \in D, \exists y \in D \text{ s.t. } P(x, y)$
  
  Everyone loves at least one person.

- **Interpret the following:** $\exists x \in D \text{ s.t. } \forall y \in D, P(x, y)$
  
  There exists a person whom everyone loves.

---

**How to Negate Multiply-Quantified Statements:**

- **To negate a universal-existential statement:** [You Do!]
  
  $\sim (\forall x \in D, \exists y \in E \text{ s.t. } P(x, y))$ is logically equivalent to $\exists x \in D \text{ s.t. } \forall y \in E, \sim P(x, y)$

- **To negate an existential-universal statement:** [You Do!]
  
  $\sim (\exists x \in D \text{ s.t. } \forall y \in E, P(x, y),)$ is logically equivalent to $\forall x \in D, \exists y \in E \text{ s.t. } \sim P(x, y)$
How to Prove a Universal-Existential Statement:

- **To Prove:** $\forall x \in D, \exists y \in E \text{ s.t. } P(x, y)$

  Let $x \in D$. And find a $y \in E$ such that $P(x, y)$ holds.

How to Prove an Existential-Universal Statement:

- **To Prove:** $\exists x \in D \text{ s.t. } \forall y \in E, P(x, y)$

  Find an $x \in D$ for which no matter what choice of $y \in E$, we have $P(x, y)$ holds.

The Calculus I definition of continuity is a multiply-quantified statement!

A function $f : \mathbb{R} \rightarrow \mathbb{R}$ is continuous at point $c \in \mathbb{R}$ if

$$\forall \epsilon > 0, \exists \delta > 0 \text{ such that } 0 < |x - c| < \delta \implies |f(x) - f(c)| < \epsilon.$$ 

**EXERCISE:** Negate the continuity definition above (using English and not $\forall-\exists$ symbols).

**ANSWER:** There exists an $\epsilon > 0$ such that for all $\delta > 0$, no matter which $x$ we pick near $c$ inside the $\delta$-tunnel of $c$ (i.e., $0 < |x - c| < \delta$), it follows that $f(x)$ is outside the $\epsilon$-tunnel of $f(c)$ (i.e., $|f(x) - f(c)| \geq \epsilon$).
**EXERCISE:** Prove the function

\[ f(x) = \begin{cases} 
2 & \text{if } x = 1 \\
1 & \text{if } n \neq 1 
\end{cases} \]

is discontinuous at \( x = 1 \).

**HINT:** draw the function and consider the “epsilon tunnel” around \( f(1) \) with \( \epsilon = \frac{1}{2} \).

**Proof.** Set \( \epsilon := \frac{1}{2} \).

**WWTS:** \( \forall \delta > 0, \text{ we have } 0 < |x - 1| < \delta, \text{ but } |f(x) - f(1)| \geq \frac{1}{2} \).

Observe that no matter what \( \delta \) is, for any \( x \neq 1 \) with \( |x - 1| < \delta \), we claim that \( |f(x) - f(1)| \geq \frac{1}{2} \). This follows since \( f(x) = 1 \) whenever \( x \neq 1 \) and \( f(1) = 2 \), so we have

\[
|f(x) - f(1)| = |1 - 2| = 1 \geq \frac{1}{2}.
\]

Thus \( f \) is discontinuous at \( x = 1 \).

Q.E.D.
**EXERCISE:** Prove the following:
\[ \forall x \in \mathbb{R}, \exists y \in \mathbb{R} \text{ such that } x + y = 0. \]

*Proof.* Let \( x \in \mathbb{R} \).

**WWTS:** \( \exists y \in \mathbb{R} \text{ s.t. } x + y = 0. \)

Set \( y := -x \). Observe that \( y \in \mathbb{R} \) and it follows that
\[
    x + y = x + (-x) = 0
\]
as desired. Thus the claim holds.

\[ \text{Q.E.D.} \]

---

**EXERCISE:** Prove that the following statement is false:
\[ \exists x \in \mathbb{R} \text{ such that } \forall y \in \mathbb{R}, \text{ we have } x + y = 0. \]  

(2)

**RECALL:** To prove a statement is false either find a counterexample, OR prove that the statement’s negation is false. Statement (1) does not lend itself to finding a counterexample, so let’s prove the negation is true. **WHAT IS THE NEGATION OF STATEMENT (1)? [You Do!]**

\[ \forall x \in \mathbb{R}, \exists y \in \mathbb{R} \text{ such that } x + y \neq 0. \]

Now prove the negation.

*Proof.* Let \( x \in \mathbb{R} \).

**WWTS:** \( \exists y \in \mathbb{R} \text{ s.t. } x + y \neq 0. \)

Choose \( y := -x + 1 \). Observe that \( y \in \mathbb{R} \) and it follows that
\[
    x + y = x + (-x + 1) = 1 \neq 0
\]
as desired. Thus the negation of Statement (1) is true, so we conclude that Statement (1) is false.

\[ \text{Q.E.D.} \]
Group Work on Multiply-Quantified Statements

In groups, discuss your assigned problem. If the statement is true, provide a proof (but a “justification” might be fine for now if you can’t prove it.). If false, then negate the statement and prove/justify the negation’s truth value.

(1) \( \forall y \in \mathbb{R}, \exists x \in \mathbb{R} \text{ such that } x^2 < y + 1. \)

(2) \( \exists x \in \mathbb{R} \text{ such that } \forall y \in \mathbb{R}, \text{ we have } x^2 + y^2 = 9. \)

(3) \( \forall x \in \mathbb{R} \text{ and } \forall y \in \mathbb{R}, \text{ we have } x^2 + y^2 \geq 0. \)

(4) \( \forall x \in \mathbb{R}, \exists y \in \mathbb{R} \text{ such that } x^2 + y^2 \leq 0. \)

(5) \( \exists x \in \mathbb{R} \text{ such that } \forall y \in \mathbb{R}, \text{ we have } x^2 + y^2 < 0. \)

(6) \( \exists x \in \mathbb{R} \text{ and } \exists y \in \mathbb{R} \text{ such that } x^2 + y^2 \leq 0. \)

(7) \( \exists x \in \mathbb{Z} \text{ such that } \forall y \in \mathbb{Z}, \text{ we have } x + y = 0. \)

(8) \( \forall x \in \mathbb{Z}, \exists y \in \mathbb{R} \text{ such that } x \cdot y = 1. \)
1.4 Writing Formal Proofs

The Four Types of Proofs:

- (I) Direct Proofs
- (II) Proof by Cases
- (III) Proof by Contradiction
- (IV) Proof by Contrapositive

Tips and best starting points for a proof:

1. Start by writing what hypothesis (i.e., assumptions) are given. (e.g., $x \in \mathbb{Q}$)
2. Write down your WWTS in the proof RIGHT AFTER stating the assumptions, and put it in a bubble like so:

   **WWTS**: Blah Blah Blah.

3. Mathematically/Symbolically say what that means. (e.g., $x = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$). This may be done at times right before the WWTS.
4. Some things NOT to do!!!!!!!:
   
   (a) NEVER replace English words with math blackboard slang.
   (b) Do not put mathmode symbols both before [AND] after a comma.

   Do not write garbage like: “Choose a $\mathbb{R}$ $x$ s.t. $\forall y, y > x.$”

**EXERCISE**: Rewrite the garbage in the box above, so that it is less “trashy”.

Choose a real number $x$ such that for all $y$, we have $y > x.$

\[17\] Of course, this statement though written very pretty, is not true. [WHY?]
How to Prove the Four Types of Proofs

(I) DIRECT PROOF:

How to Prove the Universal Conditional Statement:

\[ \text{For all } x \in D, \text{ we have } P(x) \text{ implies } Q(x). \]

- If the statement is not already in the form above, then write it in this form.
- *FIRST SENTENCE OF PROOF*
  
  Assume \( x \in D \) and suppose \( P(x) \) holds.

- *SECOND SENTENCE OF PROOF*

  \( \text{WWTS: } Q(x) \text{ holds.} \)

  \text{NOTE: The exact words of } Q(x) \text{ need not be in the bubble. Sometimes you put there only what it suffices to show.}

- *BODY OF PROOF*

- *LAST LINE OF PROOF* We conclude that \( Q(x) \) holds.

- Put a Q.E.D. or just a \( \square \).

(II) PROOF BY CASES:

How to Prove the Conditional Statement:

\[ \text{If } A_1 \text{ or } A_2 \text{ or } A_3 \text{ or } \ldots \text{ or } A_n, \text{ then } B. \]

- (CASE 1) Assume \( A_1 \) holds.  \( \text{WWTS: } B \text{ holds.} \) Then prove this.

- (CASE 2) Assume \( A_2 \) holds.  \( \text{WWTS: } B \text{ holds.} \) Then prove this.

- \( \vdots \) etc...

- (CASE n) Assume \( A_n \) holds.  \( \text{WWTS: } B \text{ holds.} \) Then prove this.

- *LAST LINE OF PROOF* We conclude that \( B \) holds.

- Put a Q.E.D. or just a \( \square \).
(III) PROOF BY CONTRADICTION:
How to Prove the Conditional Statement:

\[ \text{If } A, \text{ then } B. \]

- Assume \( A \) holds.
- Suppose by way of contradiction (BWOC) that \( B \) is false.
- **THERE IS NO WWTS IN THIS TYPE OF PROOF!!!**
- Derive any contradiction.
- Hence it cannot be that \( B \) is false.
- *LAST LINE OF PROOF* We conclude that \( B \) holds.
- Put a Q.E.D. or just a \( \square \).

(IV) PROOF BY CONTRAPOSITIVE:
How to Prove the Conditional Statement:

\[ \text{If } A, \text{ then } B. \]

- Restate it in its contrapositive form. [You Do!]
  \[ \text{If } \sim B, \text{ then } \sim A. \]

**NOTE:** You don’t write this contrapositive form in your formal proof.

- *FIRST SENTENCE OF PROOF*
  Assume \( \sim B \) holds.

- *SECOND SENTENCE OF PROOF*
  \[ \text{WWTS: } \sim A \text{ holds.} \]

**NOTE:** The exact words of \( \sim A \) need not be in the bubble. Sometimes you put there only what it suffices to show.

- *BODY OF PROOF*

- *LAST LINE OF PROOF* We conclude that \( \sim A \) holds.
- Put a Q.E.D. or just a \( \square \).
An Example of a Direct Proof

**Theorem 1.20.** The set of rational numbers is closed under addition.

**Proof.** [You Do!] Let \( x, y \in \mathbb{Q} \).

**WWTS:** \( x + y \in \mathbb{Q} \)

Since \( x, y \in \mathbb{Q} \), then there exists \( a, b, c, d \in \mathbb{Z} \) with \( b \neq 0 \) and \( d \neq 0 \) such that \( x = \frac{a}{b} \) and \( y = \frac{c}{d} \). Observe that

\[
x + y = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}.
\]

By closure of addition and multiplication in \( \mathbb{Z} \), we know \( ad + bc \in \mathbb{Z} \) since \( a, b, c, d \in \mathbb{Z} \). Also, since \( b \neq 0 \) and \( d \neq 0 \), then \( bd \neq 0 \). Thus \( x + y \in \mathbb{Q} \) as desired.

**Q.E.D.**
An Example of a Proof by Contrapositive

This lemma below literally CANNOT be proven directly!!

Think about it. Give it a shot! Your proof would start as follows:

Proof. Assume \( n^2 \) is even.

\[ \textbf{WWTS: } n \text{ is even.} \]

Since \( n^2 \) is even, then \( n^2 = 2k \) for some \( k \in \mathbb{Z} \).

THERE IS LITERALLY NOWHERE TO GO FROM HERE! THINK ABOUT IT!

Lemma 1.21. If \( n^2 \) is even, then \( n \) is even.

Proof. [You Do!] Let \( n \) be an odd integer.

\[ \textbf{WWTS: } n^2 \text{ is odd.} \]

Since \( n \) is odd, then \( n = 2k + 1 \) for some \( k \in \mathbb{Z} \). Squaring \( n \) we get the following sequence of equalities

\[
\begin{align*}
n^2 &= (2k + 1)(2k + 1) = 4k^2 + 4k + 1 \\
&= 2(2k^2 + 2k) + 1 \\
&= 2M + 1,
\end{align*}
\]

where we set \( M := 2k^2 + 2k \). Observe that \( M \in \mathbb{Z} \) by closure of multiplication and addition in \( \mathbb{Z} \). Hence \( n^2 \) is odd. Therefore we conclude

\[ \text{If } n^2 \text{ is even, then } n \text{ is even.} \]

Q.E.D.

NOTE: It is nice to end a proof by contrapositive by stating the statement as originally written. But it is not necessary too; ending with “\( n^2 \) is odd” is fine too.
An Example of a Proof by Contradiction

The so-called FIRST CRISIS IN MATH!!

Long ago, in the 6th century BC, the followers of the school of Pythagoras, the Pythagoreans, came to a crisis in math. It was a long held view that all numbers are the ratio of two integers. However, the Pythagorean member Hippasus is thought to be the one to discover that there is a length that cannot be the ratio of two integers – a Greek Crisis! This length was the $\sqrt{2}$.

It is rumored that the drowning of Hippasus was the punishment from the gods for divulging this secret\textsuperscript{18}.

\textbf{Theorem 1.22.} The value $\sqrt{2}$ is irrational.

\textit{Proof.} [You Do!] Assume by way of contradiction that $\sqrt{2} \in \mathbb{Q}$. Then $\sqrt{2} = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ with $b \neq 0$, and we may assert that $\text{gcd}(a, b) = 1$. Then we have the following sequence of implications

\[
\sqrt{2} = \frac{a}{b} \implies \sqrt{2}b = a \\
\implies 2b^2 = a^2 \quad \text{by squaring both sides} \\
\implies a^2 \text{ is even} \\
\implies a \text{ is even} \quad \text{by Lemma 1.21.}
\]

Hence $a = 2k$ for some $k \in \mathbb{Z}$. Substituting this value $a$ in the equality $\sqrt{2}b = a$, we have $\sqrt{2}b = 2k$ and the following sequence of implications

\[
\sqrt{2}b = 2k \implies 2b^2 = 4k^2 \quad \text{by squaring both sides} \\
\implies b^2 = 2k^2 \\
\implies b^2 \text{ is even} \\
\implies b \text{ is even} \quad \text{by Lemma 1.21.}
\]

However, both $a$ and $b$ being even contradicts the fact that $\text{gcd}(a, b) = 1$. Therefore we conclude that $\sqrt{2}$ is irrational.

\textbf{Q.E.D.}

\textsuperscript{18}We would provide a reference for this, but there is a lot of documented debate with historians about the first Greek discoverer of the irrationality of $\sqrt{2}$. But for sure, the drowning of Hippasus is certain.
An Example of a Proof by Cases

An Important Consequence of the Division Algorithm

In Section 5 on divisibility, we will learn the very fundamental result:

**Theorem.** Given integers $a$ and $b$, with $b > 0$, there exist unique integers $q$ and $r$ satisfying

$$a = qb + r \quad \text{such that} \quad 0 \leq r < b.$$ 

A consequence of this theorem is one super well-known result that every integer is even (i.e., in $2\mathbb{Z}$) or odd (i.e. in $2\mathbb{Z} + 1$). The 2 is replaceable here. For instance, every integer lies in ONE AND ONLY one of the sets $3\mathbb{Z}$ or $3\mathbb{Z} + 1$ or $3\mathbb{Z} + 2$. [Proof? Obvious! Especially after covering Section 5.]

**Theorem 1.23.** If $n$ is an integer not divisible by 3, then $n^2 \in 3\mathbb{Z} + 1$.

**Proof.** [You Do!] Assume $n$ is an integer not divisible by 3. Then either $n$ lies in $3\mathbb{Z} + 1$ or $3\mathbb{Z} + 2$.

**CASE 1:** Assume $n \in 3\mathbb{Z} + 1$.

WWTS: $n^2 \in 3\mathbb{Z} + 1$.

Since $n \in 3\mathbb{Z} + 1$ then $n = 3m + 1$ for some $m \in \mathbb{Z}$. Thus we have

$$n^2 = (3m + 1)^2 = 9m^2 + 6m + 1 = 3(3m^2 + 2m) + 1 = 3M + 1$$

setting $M := 3m^2 + 2m$. Clearly $M \in \mathbb{Z}$, and hence $n^2 \in 3\mathbb{Z} + 1$.

**CASE 2:** Assume $n \in 3\mathbb{Z} + 2$.

WWTS: $n^2 \in 3\mathbb{Z} + 2$.

Since $n \in 3\mathbb{Z} + 2$ then $n = 3m + 2$ for some $m \in \mathbb{Z}$. Thus we have

$$n^2 = (3m + 2)^2 = 9m^2 + 12m + 4 = 3(3m^2 + 4m + 1) + 1 = 3M + 1$$

setting $M := 3m^2 + 4m + 1$. Clearly $M \in \mathbb{Z}$, and hence $n^2 \in 3\mathbb{Z} + 1$.

Q.E.D.
1.5 Quick Review of Set Theory and Some Set Theory Proofs

The following are numerical sets that will arise in this course:

<table>
<thead>
<tr>
<th>Set Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>natural numbers</td>
<td>$\mathbb{N} = {1, 2, 3, \ldots}$</td>
</tr>
<tr>
<td>integers</td>
<td>$\mathbb{Z} = {\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots}$</td>
</tr>
<tr>
<td>rational numbers</td>
<td>$\mathbb{Q} = \left{ \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ and } b \neq 0 \right}$</td>
</tr>
<tr>
<td>real numbers</td>
<td>$\mathbb{R} = {\text{rational and irrational numbers}}$</td>
</tr>
<tr>
<td>complex numbers</td>
<td>$\mathbb{C} = {a + bi \mid a, b \in \mathbb{R} \text{ and } i = \sqrt{-1}}$</td>
</tr>
<tr>
<td>Gaussian integers</td>
<td>$\mathbb{Z}[i] = {a + bi \mid a, b \in \mathbb{Z} \text{ and } i = \sqrt{-1}}$</td>
</tr>
<tr>
<td>Eisenstein integers</td>
<td>$\mathbb{Z}[\rho] = {a + b\rho \mid a, b \in \mathbb{Z} \text{ and } \rho = e^{\frac{2\pi i}{3}}}$</td>
</tr>
<tr>
<td>even integers</td>
<td>$2\mathbb{Z} = {2k \mid k \in \mathbb{Z}}$</td>
</tr>
<tr>
<td>odd integers</td>
<td>$2\mathbb{Z} + 1 = {2k + 1 \mid k \in \mathbb{Z}}$</td>
</tr>
<tr>
<td>arithmetic progression</td>
<td>$a\mathbb{Z} + b = {ak + b \mid k \in \mathbb{Z}}$ where $a, b$ fixed</td>
</tr>
</tbody>
</table>

**CULTURAL QUESTION 1:** Why are the integers denoted $\mathbb{Z}$?

**ANSWER:** The German word for “numbers” is *Zahlen*. Germans contributed much to Zahlentheorie (number theory).

**CULTURAL QUESTION 2:** Why are the rationals denoted $\mathbb{Q}$?

**ANSWER:** It was first denoted $\mathbb{Q}$ in 1895 by Giuseppe Peano after *quoziente*, Italian for “quotient”.

---

19We do not consider the number 0 to be a natural number, though it is common in fields such as computer science where loops and array elements start with the 0\textsuperscript{th} counter.
Some Essential Definitions in Set Theory


- Repetition of objects is ignored. For instance \( \{x, x, y\} = \{x, y\} \).
- Order does not matter. For instance \( \{x, y\} = \{y, x\} \).

A member of a set is called an element. It is customary to use a capital letter to denote a set.

Definition 1.25. The cardinality of a set is the number of elements in the set. We use the symbols \( N(A) \), \( n(A) \), or \( |A| \) to denote this “size” of a set \( A \).

Two types of infinity \( \infty \) that will arise in this class are \( \aleph_0 \) (aleph-naught) and \( \aleph_1 \) (aleph-one). The former is the cardinality of the natural numbers, while the latter is the cardinality of the real numbers.

Definition 1.26. The nullset, or empty set, is the set that contains no elements. It is denoted \( \emptyset \) or equivalently \( \{\} \).

**EXERCISE:** Compute the following cardinalities. [You Do!]

\[
\begin{align*}
A = \{a, b, c\} & \implies |A| = 3 \\
A = \{\{a, b\}, a, b\} & \implies |A| = 3 \\
A = \{\{\{a\}, a\}, a\} & \implies |A| = 2 \\
A = \mathbb{Z} & \implies |A| = \aleph_0 \\
A = 2\mathbb{Z} & \implies |A| = \aleph_0 \\
A = \mathbb{Q} & \implies |A| = \aleph_0 \\
A = \mathbb{C} & \implies |A| = \aleph_1 \\
A = \{\emptyset\} & \implies |A| = 1
\end{align*}
\]
WARNING! Two Easily Confused Symbols: $\in$ versus $\subseteq$

**Definition 1.27.** The notation $x \in A$ means "$x$ is an element of $A$".

**Definition 1.28.** The notation $A \subseteq B$ means "$A$ is a subset of $B$".

$A \subseteq B$ if and only if (For every $x \in A$, we have $x \in B$).

**EXERCISE:** Let $A = \{\{a, b\}, a, c\}$. Answer the following. [True or False?]

- $a \in A$ \hspace{1cm} True
- $b \in A$ \hspace{1cm} False
- $\{a, c\} \subseteq A$ \hspace{1cm} True
- $\{a, b\} \subseteq A$ \hspace{1cm} False
- $\{a, b\} \in A$ \hspace{1cm} True
- $\{\{a, b\}\} \subseteq A$ \hspace{1cm} True
- $\emptyset \subseteq A$ \hspace{1cm} True

**QUESTION:** Why is the nullset a subset of any set $A$?

**ANSWER:** Consider the statement $\emptyset \subseteq A$. Since there are no elements in $\emptyset$, it is clear that ALL of the elements in $\emptyset$ are contained in $A$, regardless of what set $A$ is. This is called a vacuously true statement.

**How to prove two sets are equal?**

**Claim 1.29.** Let $A$ and $B$ be sets. Then

$$A = B \quad \text{if and only if} \quad A \subseteq B \text{ and } B \subseteq A.$$
Definition 1.30. The **universal set** is a larger known set wherein a given set lives. We denote it \( U \). This set is generally understood in context or deliberately stated.

**EXERCISE:** Find the universal sets. [You Do!]

\[
A = \{\text{dogs}\} \implies U = \text{animals}
\]

\[
A = \{\text{even integers}\} \implies U = \text{integers}
\]

Definition 1.31. Let \( A \) and \( B \) be sets. Then the **intersection** of \( A \) and \( B \) (denoted \( A \cap B \)) is the set of elements in \( U \) that lie in both \( A \) and \( B \). Set-theoretically,

\[
A \cap B := \{x \in U \mid x \in A \text{ and } x \in B\}.
\]

Definition 1.32. Let \( A \) and \( B \) be sets. Then the **union** of \( A \) and \( B \) (denoted \( A \cup B \)) is the set of elements in \( U \) that lie in \( A \) or \( B \) (or both). Set-theoretically,

\[
A \cup B := \{x \in U \mid x \in A \text{ or } x \in B\}.
\]

Definition 1.33. Let \( A \) be a set. The **complement** of the set \( A \) (denoted \( A^c \) or \( A' \)) is the set of elements in \( U \) that do not lie in \( A \). Set-theoretically,

\[
A^c := \{x \in U \mid x \notin A\}.
\]

Definition 1.34. Let \( A \) and \( B \) be sets. The **difference** \( A \setminus B \) of \( A \) and \( B \) is defined as \( \{x \in A \mid x \notin B\} \).

**NOTE:** \( A \setminus B \) is sometimes written \( A - B \). Moreover \( A \setminus B = A \cap B^c \).
Just as we have De Morgan’s Laws for logic symbols $\lor$ and $\land$ (recall Definition 1.9), we have De Morgan’s Law for $\cup$ and $\cap$, respectively, as follows:

**Definition 1.35.** Let $A$ and $B$ be sets. Then **De Morgan’s Laws** assert the following set equalities:

- $(A \cup B)^c$ is equal to $A^c \cap B^c$.
- $(A \cap B)^c$ is equal to $A^c \cup B^c$.

## Set Theory on Collections of Sets

Let $J$ be any indexing set of any size (finite or infinite). Suppose for each $j \in J$, we have a set $A_j$. Consider the collection of sets $\{A_j \mid j \in J\}$.

**Definition 1.36.** We have the following:

- **“Big Union”:** $\bigcup_{j \in J} A_j = \{x \in U \mid x \in A_j \text{ for some } j \in J\}$
- **“Big Intersection”:** $\bigcap_{j \in J} A_j = \{x \in U \mid x \in A_j \text{ for every } j \in J\}$
- Let $A_1, A_2, \ldots, A_n$ be a finite collection of sets. The **Cartesian product** of the collection is denoted $A_1 \times A_2 \times \cdots A_n$ and is defined as $\{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ for } i = 1, 2, \ldots, n\}$.
- Two sets $A$ and $B$ are **disjoint** if $A \cap B = \emptyset$. Moreover the collection of sets $\{A_j \mid j \in J\}$ is **pairwise disjoint** of $A_i \cap A_j = \emptyset$ for $i, j \in J$ such that $i \neq j$.
- A collection of sets $\{A_j \mid j \in J\}$ is a **partition of a set** $X$ if and only if
  1. $X = \bigcup_{j \in J} A_j$, and
  2. the collection is pairwise disjoint.

We use the notation $X = \bigsqcup_{j \in J} A_j$ to denote this pairwise disjoint union.
Set Theory Proof Exercise 1

Claim 1.37. The sets $3\mathbb{Z}$, $3\mathbb{Z} + 1$, and $3\mathbb{Z} + 2$ form a partition of $\mathbb{Z}$.

Proof. Consider the sets $3\mathbb{Z}$, $3\mathbb{Z} + 1$, and $3\mathbb{Z} + 2$.

WWTS: $\mathbb{Z} = \bigsqcup_{j=0,1,2} 3\mathbb{Z} + j$.

By the division algorithm (which we’ll cover in Section 5), every integer $n$ can be represented in exactly one of three forms:

$$n = 3k \quad \text{or} \quad n = 3k + 1 \quad \text{or} \quad n = 3k + 2$$

for some integer $k$, and hence $\mathbb{Z} = 3\mathbb{Z} \cup 3\mathbb{Z} + 1 \cup 3\mathbb{Z} + 2$. This also implies that the three sets are pairwise disjoint and hence $\mathbb{Z} = \bigsqcup_{j=0,1,2} 3\mathbb{Z} + j$.

Q.E.D.

Set Theory Proof Exercise 2

Claim 1.38. Prove that $10\mathbb{Z} + 7 \subseteq 5\mathbb{Z} + 2$ but $10\mathbb{Z} + 7 \nsubseteq 5\mathbb{Z} + 2$.

Proof. We first show the $\subseteq$ containment holds. Let $x \in 10\mathbb{Z} + 7$.

WWTS: $x \in 5\mathbb{Z} + 2$.

Since $x \in 10\mathbb{Z} + 7$ then $x = 10k + 7$ for some $k \in \mathbb{Z}$. Thus

$$x = 10k + 5 + 2 = 5(2k + 1) + 2 = 5M + 2$$

where $M := 2k + 1$. Observe that $M \in \mathbb{Z}$ and so $x \in 5\mathbb{Z} + 2$. Thus $10\mathbb{Z} + 7 \subseteq 5\mathbb{Z} + 2$ as desired. We now show $\nsubseteq$ containment does not hold. Set $y = 12 = 5 \cdot 2 + 2 \in 5\mathbb{Z} + 2$. If $y \in 10\mathbb{Z} + 7$, then

$$12 = 10k + 7 \text{ for some } k \in \mathbb{Z} \implies 10k = 12 - 7 \implies k = \frac{5}{10} \in \mathbb{Z}$$

which gives a contradiction so $10\mathbb{Z} + 7 \nsubseteq 5\mathbb{Z} + 2$.

Q.E.D.
1.6 Butternut Squash

Here are solutions to the Group Work problems earlier in this section. The book authors Post on the left and aBa on the right owe these solutions to the Butternut Squash Gods which we are holding. If you look closely, you may notice a person’s eyes\(^\text{20}\) in the handle of the whiteboard.

\(^{20}\)These eyes belong to Emily Gullerud, a mathematics graduate student at the University of Minnesota. She too is a fan of the Butternut Squash Gods.
2 Mathematical Induction

2.1 Motivation

Using only 3 and 5 cent stamps, can we produce any postage value greater than 7 cents? **Yes!!**

Let us look at some examples:

\[
\begin{align*}
8\text{¢} & = 3\text{¢} + 5\text{¢} \\
9\text{¢} & = 3\text{¢} + 3\text{¢} + 3\text{¢} \\
10\text{¢} & = 5\text{¢} + 5\text{¢} \\
11\text{¢} & = 5\text{¢} + 3\text{¢} + 3\text{¢} \\
12\text{¢} & = 3\text{¢} + 3\text{¢} + 3\text{¢} + 3\text{¢}
\end{align*}
\]

How would you go about answering this question? Mathematical induction is a perfectly good method. And in Section 5 on Diophantine equations, we will see a purely number theoretic method also! The *Diophantine* approach is to ask the following question:

**Question 2.1.** For each integer \( n \geq 8 \), does there always exist integers \( r, s \geq 0 \) such that \( n = 3r + 5s \)?

We will wait until the section on divisibility properties to answer the question in the number theoretic manner. For now let us explore the method of mathematical induction.
The Falling Dominoes Analogy

Imagine that we want to prove that an infinite number of statements $S_1$, $S_2$, $S_3$, etc. are all true. The dominoes analogy of math induction is the following:

- Visualize each statement as a domino. And visualize the act of the $n^{th}$ domino falling to mean that statement $S_n$ is proven true.
- Suppose you can knock over the first domino (i.e., you can prove $S_1$).
- Suppose you can show that if any $k^{th}$ domino falling will definitely force the $(k + 1)^{th}$ domino to fall.
- We can conclude that $S_1$ falls and knocks down $S_2$. Next $S_2$ falls and knocks down $S_3$. Then $S_3$ knocks down $S_4$, etc.
- Hence all dominoes fall!!!  **Q.E.D.**
(nonrigorous) **Induction Proof of the Stamp Problem**

First recall the question:

**Question 2.2.** Using only 3 and 5 cent stamps, can we produce any postage value greater than 7 cents?

**Base Case:** The first domino clearly falls since we can get 8¢ of postage simply by using these two stamps:

![Stamps](image)

**Induction Hypothesis:** Assume for some $k \geq 8$, we can use 3 and 5 cent stamps to produce the value $k$.

**Induction Step:** We must prove that we can use 3 and 5 cent stamps to produce the value $k + 1$. Below we give a visual example of how we may do this. Since $k \geq 8$, there are clearly two cases: either the $k$ cents has at least one 5 cent stamp or it doesn’t.

**Case 1:** $k$ cents contain at least one 5¢ stamp.

**Case 2:** $k$ cents do not contain any 5¢ stamp.

Then there are at least three 3¢ stamp.
2.2 The Principle and Method of Mathematical Induction

The Principle of Mathematical Induction

Let $P(n)$ be a property defined on the integers $n$. Let $a \in \mathbb{N}$ be a fixed integer. Suppose the following two statements are true:

1. $P(a)$ is true
2. For every $k \geq a$, we have $P(k)$ implies $P(k + 1)$.

Then $P(n)$ is true for all $n \geq a$.

The Method of Mathematical Induction

PROVE: For all $n \geq a$, it follow that $P(n)$ is true.

(Proof)

- **Step 1:** (Base Case) Show that $P(a)$ is true.

- **Step 2:** (Induction Hypothesis) Assume $P(k)$ holds for some $k \geq a$. **WARNING!**: The word “some” is VERY IMPORTANT! This existential quantifying word asserts that the $k$ is a PARTICULAR (i.e., fixed) but arbitrarily chosen integer.

- **Step 3:** Show that $P(k + 1)$ holds. **WARNING!**: If you manage to prove $P(k + 1)$ without ever using the fact that $P(k)$ holds, then your proof is DEFINITELY wrong.

- **Step 4:** Conclude that $P(n)$ is true for all $n \geq a$. 


The Canonical Example: Triangular Numbers

**Definition 2.3.** The $n^{th}$ triangular number $T_n$ is defined to be the sum $1 + 2 + \cdots + n$. That is,

$$T_n = \sum_{i=1}^{n} i$$

**Well Known Fact:** Recall the Gauss sum from Theorem 0.23 in Section 0.

$$1 + 2 + \cdots + n = \binom{n + 1}{2} = \frac{(n + 1)!}{((n + 1) - 2)! \cdot 2!} = \frac{n \cdot (n + 1)}{2}$$

(“Proof” by one example) Let us count handshakes between $n + 1$ people.

Imagine the $n = 5$ case by considering the following image:

- A shakes hands with B, C, D, E, and F. (5 handshakes)
- B shakes hands with C, D, E, and F. (4 handshakes)
- C shakes hands with D, E, and F. (3 handshakes)
- D shakes hands with E and F. (2 handshakes)
- E shakes hands with F. (1 handshake)

Thus there are $1 + 2 + 3 + 4 + 5$ handshakes. But this is equivalent to the number of ways to choose two of the six vertices in the graph above. Hence $1 + 2 + 3 + 4 + 5 = \binom{5+1}{2}$ as desired.

“Q.E.D.”
Geometric View of $T_n$

\[
\begin{array}{cccc}
1 & 3 & 6 & 10 \\
T_1 & T_2 & T_3 & T_4
\end{array}
\]

Cool Fact: $T_{n-1} + T_n = n^2$ for all $n \geq 2$.
[You Do!] Draw the $n = 4$ case.
(Hint: Think Geometrically)

Rotate the $T_3$-diagram to 180 and place in the upper-right part of the $T_4$-diagram and we get

\[
4^2
\]
2.3 Exercises

Induction Exercise 1

PROVE: $T_{n-1} + T_n = n^2$ for all $n \geq 2$. [You Do!]

(Base Case): $n = 2$

- LHS is $T_1 + T_2 = 1 + 3 = 4$
- RHS is $2^2 = 4$

(Induction Hypothesis): Assume $T_{k-1} + T_k = k^2$ for some $k \geq 2$.

WWTS: $T_k + T_{k+1} = (k + 1)^2$

[Complete the proof!]

\[
T_k + T_{k+1} = (1 + 2 + \cdots + k) + (1 + 2 + \cdots + (k + 1)) \\
= (T_{k-1} + k) + (T_k + (k + 1)) \\
= T_{k-1} + k + (k + (k + 1)) \\
= k^2 + (k + (k + 1)) \text{ by Induction Hypothesis} \\
= k^2 + 2k + 1 \\
= (k + 1)^2
\]

as desired. Hence $T_{n-1} + T_n = n^2$ for all $n \geq 2$.

Q.E.D.
Induction Exercise 2

**PROVE:** 3 divides \( n^3 - n \) for all \( n \geq 1 \). [You Do!]

**(Base Case):** \( n = 1 \)

[You Verify and finish the proof!]

\[ 1^3 - 1 = 0 \] and yes 3 divides 0.

**(Induction Hypothesis):**
Assume 3 | \( k^3 - k \) for some \( k \geq 1 \).

**WWTS:** 3 | \((k + 1)^3 - (k + 1)\)

It suffices to show that \((k + 1)^3 - (k + 1) = 3M\) for some \( M \in \mathbb{Z} \). Consider the following sequence of equalities:

\[
(k + 1)^3 - (k + 1) = (k^3 + 3k^2 + 3k + 1) - (k + 1) \\
= k^3 + 3k^2 + 3k - k - 1 \\
= k^3 + 3k^2 + 3k \\
= (k^3 - k) + 3k^2 + 3k \\
= 3N + 3k^2 + 3k \text{ by Induction Hypothesis} \\
= 3[N + k^2 + k].
\]

Note that the 2nd last line holds since the induction hypothesis implies that \((k^3 - k) = 3N\) for some \( N \in \mathbb{Z} \). Set \( M = N + k^2 + k \) and observe that \( M \in \mathbb{Z} \). Thus \((k + 1)^3 - (k + 1) = 3M\) as desired. Hence 3 divides \( n^3 - n \) for all \( n \geq 1 \).

Q.E.D.
Induction Exercise 3

**PROVE:** $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ for all $n \geq 1.$

[You Do!]

**(Base Case):** $n = 1$

- **LHS** is 1
- **RHS** is $1^2$

Thus LHS = RHS so the base case holds.

**(Induction Hypothesis):**

Assume $1 + 3 + 5 + \cdots + (2k - 1) = k^2$ for some $k \geq 1.$

Let $LHS = 1 + 3 + 5 + \cdots + (2k - 1) + (2k + 1)$, consider the following sequence of equalities:

$LHS = [1 + 3 + 5 + \cdots + (2k - 1)] + (2k + 1)$

$= k^2 + (2k + 1)$ by Induction Hypothesis

$= (k + 1)^2$

as desired. Hence $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ for all $n \geq 1.$

**Q.E.D.**

**Question 2.4.** Can you think of an easier “geometric view” proof like we did for the sum of consecutive triangular numbers being a square? **HINT:** Draw each of the odd numbers as equal-armed length L’s and arrange them suggestively to construct a square.
A Tantalizing Image

The following appears in a blog post by author Chris Hunter on the sum of consecutive odds. We reproduce the image below with his permission:\(^{21}\):

\(^{21}\)This blog post can be found at the following address
https://reflectionsinthewhy.wordpress.com/2011/09/14/running-naked-through-the-streets/
3 Pascal’s Triangle and Binomial Coefficients

3.1 Motivation

Ponder the following VERY RELATED questions?

- How many ways can we select 2 objects from a set of 6 distinct objects?
- How many ways are there to distinguishably rearrange the letters in the word “BOOBOO”?
- In the binomial expansion of \((x + y)^6\), what is the coefficient of the term \(x^2y^4\)?
- In a group of 7 people, how many distinct pairs of people are possible?
- What is the sum \(1 + 2 + 3 + 4 + 5\)?
- What is the atomic number of the element phosphorous?

The answer to all six questions:

15
Preliminary Counting Definitions

**Definition 3.1.** The number of arrangements of \( n \) distinct objects is \( n \)-factorial and is given by the formula

\[
  n! = n \cdot (n - 1) \cdot (n - 2) \cdots 3 \cdot 2 \cdot 1.
\]

Does order matter? **Yes**

**Note:** We set 0! to equal 1.

Cool number theory related factoids involving factorials:

- \( n! \) is divisible by ALL PRIME NUMBERS up to and including \( n \). [WHY?]
- As a consequence of the above, \( n > 5 \) is composite if and only if \( n \) divides \( (n - 1)! \). [WHY?]
- A stronger result is Wilson’s Theorem (which we’ll learn later in the semester) which states

\[
p \text{ divides } (p - 1)! + 1 \text{ if and only if } p \text{ is prime.}
\]

In laymen’s terms, this says “A number \( n > 1 \) is a prime number if and only the product of all positive integers less than \( n \) is ONE LESS than a multiple of \( n \).” [Ponder this!]

**Definition 3.2.** The number of ways to choose \( r \) objects from \( n \) distinct objects is the **binomial coefficient** \( n \) choose \( r \) and is given by the formula

\[
  \binom{n}{r} = \frac{n!}{r! \cdot (n - r)!}.
\]

Does order matter? **No**

**Example 3.3** \((n = 5 \text{ and } r = 3)\). The number of ways to choose 3 objects from 5 distinct objects is

\[
  \binom{5}{3} = \frac{5!}{3! \cdot (5 - 3)!} = \frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{(3 \cdot 2 \cdot 1)(2 \cdot 1)} = \frac{5 \cdot 4}{2 \cdot 1} = 10.
\]
Question 3.4. Who is Blaise Pascal? And what was his wager?

Pascal’s Wager: the argument that it is in one’s own best interest to behave as if God exists, since the possibility of eternal punishment in hell outweighs any advantage of believing otherwise.

Pascal did NOT discover Pascal’s triangle!

Remark 3.5. Though Blaise Pascal is attributed to the famous triangle bearing his name, the triangle was studied by mathematicians centuries before him in India, Persia, China, and Germany. In particular, the triangle above is known as Yang Hui’s triangle after the late-Song dynasty Chinese mathematician Yang Hui (1238–1298). This image appears in a publication in 1303 A.D.
3.2 Constructing Pascal’s Triangle

Pascal’s Identity

**Theorem 3.6** (Pascal’s Identity). For any natural number \( n \), we have

\[
\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}
\]

for \( 1 \leq k \leq n \)

where \( \binom{n}{k} \) is a binomial coefficient.

**Combinatorial Proof (by example for \( n = 5 \) and \( k = 3 \)):**

\[
\text{WWTS: } \binom{4}{2} + \binom{4}{3} = \binom{5}{3}
\]

Count the number of subsets of 3 superheroes from the 5 superheroes below.

In any subset of 3 superheroes, clearly the Hulk will be in it OR not be in it.

**CASE 1:** (Hulk is in the subset) How many possible subsets of this type?

There are \( \binom{4}{2} = 6 \) ways to choose the other 2.

**CASE 2:** (Hulk is NOT in the subset) How many possible subsets of this type?

There are \( \binom{4}{3} = 4 \) ways to choose the 3 people.

We conclude that there are \( 6 + 4 = 10 \) ways to have a size-3 subset of a set with 5 distinct objects (that is, the value \( \binom{5}{3} \)). Q.E.D.
Using Pascal’s Identity to construct Pascal’s Triangle

QUESTION: How is Pascal’s identity used to construct the triangle above?

ANSWER: The identity \( \binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k} \) says that the entry \( \binom{n}{k} \) in row \( n \) is the sum of the two numbers above it in row \( n - 1 \), namely \( \binom{n-1}{k-1} \) and \( \binom{n-1}{k} \). If \( k = 0 \) or \( k = n \), then set \( \binom{n-1}{-1} = 0 \) or \( \binom{n-1}{n} = 0 \), respectively.

QUESTION: Explain the rows in the triangle above and to the right.

ANSWER: The polynomial in row \( n \) is the expansion of the binomial \((x + y)^n\).
3.3 16 Rows of Pascal’s Triangle

QUESTION 1: Use the triangle above to find \( \binom{14}{5} \)

We count 6 boxes from the left on the 14th row. Don’t count 5 boxes. Also don’t forget that the first row is the 0th row. It follows that

\[
\binom{14}{5} = 1001.
\]

QUESTION 2: Explain why \( \binom{14}{5} \) is the same as \( \binom{14}{9} \).

This follows because of the easily provable identity:

\[
\binom{n}{k} = \binom{n}{n-k}.
\]

This is trivial. Whenever you are choosing a subset of size \( k \) from a set of size \( n \), then you are IGNORING a subset of size \( n-k \); that is, the “unchosen” elements.

QUESTION 3: Darn it! The table only goes to the 16th row. How can we use the triangle to compute \( \binom{17}{4} \) for instance?

Pascal’s Identity (Theorem 3.6) says that \( \binom{17}{4} \) is the sum of the two entries above it. Those entries are \( \binom{16}{3} \) and \( \binom{16}{4} \). Hence \( \binom{17}{4} = 560 + 1820 = 2380.\)
3.4 Binomial Coefficients

The Binomial Theorem and Some Cool Triangle Identities

Theorem 3.7. If \( n \geq 0 \) is an integer, then

\[
(x + y)^n = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n.
\]

More compactly, we write

\[
= \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k
\]

Below are a host of BEAUTIFUL identities. Explain what the first three identities mean by considering how they are visually related to the entries in Pascal’s triangle. [You Do!]

1. \( \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n \) [This is Exercise 1] (3)
2. \( \binom{n}{0} + \binom{n+1}{1} + \binom{n+2}{2} + \cdots + \binom{n+r}{r} = \binom{n+r+1}{r} \) (4)
3. \( \binom{n}{0} + 2\binom{n}{1} + 3\binom{n}{2} + \cdots + n\binom{n}{n} = n2^n \) [This is a HW Problem] (6)
4. \( \sum_{k=0}^{r} \binom{M}{k} \binom{W}{r-k} = \binom{M+W}{r} \) (7)

A simple combinatorial proof of Identity (7): Imagine there are \( M \) men and \( W \) women. We want to form a committee of \( r \) people. It is clear that there are \( r \) cases.

Case 1: The committee has no men. This happens in \( \binom{M}{0} \binom{W}{r} \) ways. [WHY?]
Case 2: The committee has only one man. This happens in \( \binom{M}{1} \binom{W}{r-1} \) ways. [Why? And do you see how the other cases would go?]

Q.E.D.
3.5 Exercises

Cool Triangle Identity Exercise 1

PROVE: \( \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n \quad \forall n \geq 0 \)

Combinatorial Proof: (The Light Switch Analogue)

Let \( X = \{a_1, a_2, a_3, \ldots, a_n\} \). How many possible subsets are there for \( X \)?

The light switch analogue says the following:

- The element \( a_i \) corresponds to the \( i \)th light switch.
- Let us build a subset \( A \) of \( X \). If the \( i \)th light switch is on, put \( a_i \) in \( A \).
  - e.g., all light switches on means \( A = X \)
  - e.g., all light switches off means \( A = \emptyset \)
  - e.g., the first two on but all others off means \( A = \{a_1, a_2\} \)
- The Analogue: There exists a one-to-one correspondence between the subsets of \( A \) and all possible light switch settings.
- There are \( n + 1 \) distinct cases: each depends on the cardinality (i.e., size) of the subset \( A \).
Case 0: (size 0 subsets) $\emptyset$ is the only one. \( \binom{n}{0} = 1 \) of these

Case 1: (size 1 subsets) \{a_1\}, \{a_2\}, \{a_2\}, \ldots, \{a_n\}. \( \binom{n}{1} = n \) of these

Case 2: (size 2 subsets) \{a_1, a_2\}, \{a_1, a_3\}, \ldots, \{a_1, a_n\}, \{a_2, a_3\}, \{a_2, a_4\}, \ldots
\binom{n}{2} \) of these

Case \( n \): (size \( n \) subsets) \( \{a_1, a_2, \ldots, a_n\} \) is the only one.
\( \binom{n}{n} = 1 \) of these

Total = \( \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} \)

Next we show that this total equals \( 2^n \). If \( A \subseteq X \), then \( a_i \) is either an element of \( A \) or not for each \( i \). So for each \( a_i \) there are TWO choices. Hence there are 2 choices for each \( a_i \), so there are \( 2^n \) possible lightswitch settings.

Q.E.D.

A Connection to Power Sets

Remark 3.8. This method used to prove the identity gives the following fundamental set theory result:

\[ X \text{ is a set with } n \text{ elements } \implies \mathcal{P}(X) = 2^{\lvert X \rvert}. \]

[Why is this?] This is clear.

Algebraic Proof: (via Binomial Theorem)

[You Do!] Use the Binomial Theorem 3.7 and set \( x = 1 \) and \( y = 2 \).

Then by the binomial theorem with \( x = 1 \) and \( y = 1 \) we have

\[ 2^n = (1 + 1)^n = \binom{n}{0} 1^n + \binom{n}{1} 1^{n-1} \cdot 1 + \binom{n}{2} 1^{n-2} \cdot 2^1 + \cdots + \binom{n}{n} 1^n \]
\[ = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} \]

as desired.

Q.E.D.
Pascal’s Triangle Exercise 2 Part a

**QUESTION:** How many different pizza pies can be ordered if a pizza parlor offers 6 different possible toppings? (Not including cheese and crust)

\[
\begin{align*}
\binom{6}{0} & \quad \text{plain pizza} \\
\binom{6}{1} & \quad \text{1 topping} \\
\binom{6}{2} & \quad \text{2 toppings} \\
\binom{6}{3} & \quad \text{3 toppings} \\
\binom{6}{4} & \quad \text{4 toppings} \\
\binom{6}{5} & \quad \text{5 toppings} \\
\binom{6}{6} & \quad \text{6 toppings}
\end{align*}
\]

- **(CASE 1)** Choose 0 toppings (i.e., a plain pizza): 1 choice
- **(CASE 2)** Choose 1 topping: 6 choices
- **(CASE 3)** Choose 2 toppings: 15 choices
- **(CASE 4)** Choose 3 toppings: 20 choices
- **(CASE 5)** Choose 4 toppings: 15 choices
- **(CASE 6)** Choose 5 toppings: 6 choices
- **(CASE 7)** Choose 6 toppings: 1 choice

Thus there are \(1 + 6 + 15 + 20 + 15 + 6 + 1 = 64\) or \(2^6 = 64\) different pizza pies that can be ordered for 6 different toppings.
**Pascal’s Triangle Exercise 2 Part b**

**QUESTION:** Suppose a pizza place has 20 different possible toppings. (Not including cheese and crust) How many different pizza pies can be ordered if you are allowed only to have AT MOST 17 toppings?

---

**Remark 3.9.** It may be handy to think about the complement rule in set theory. Recall that if we have a set $E$ that is a subset of some universal set $U$. And we want to calculate the cardinality $|E|$ of $E$. It maybe easier to calculate the size of the complement $E'$ of $E$. We know that $U = E \cup E'$ and also the intersection $E \cap E'$ is empty. Thus we have

$$U = E \dot{\cup} E'$$

where $\dot{\cup}$ denotes a disjoint union

$$|U| = |E| + |E'|.$$  

The complement rule then says that if it is hard to compute $|E|$ but easier to compute $|E'|$ and $|U|$ then you can use the formula above to find $|E|$.

So let us apply that to our new pizza problem.

- Let $U$ be the set of all possible pizza orders if 20 toppings are available.
  $$|U| = 2^{20} = 1,048,576.$$

- Let $E$ be the set of the pizza orders if you are allowed only to have AT MOST 17 toppings. We want to compute $|E|$.

It is a LOT EASIER to compute $|E'|$ than $|E|$. What is the set $E'$ (in words)?

- $E'$ is the set of pizza orders if you MUST have at least 18 toppings.

Clearly, there are 3 cases.

- **(CASE 1)** Choose 18 toppings: $\binom{20}{18} = 190$ choices

- **(CASE 2)** Choose 19 toppings: $\binom{20}{18} = 18$ choices

- **(CASE 3)** Choose 18 toppings: $\binom{20}{18} = 1$ choice

Thus $|E'| = 190 + 18 + 1 = 209$. Thus by the complement rule, the number of possible pizza orders with at most 17 toppings is

$$|E| = |U| - |E'| = 1,048,576 - 209 = 1,048,367.$$
Binomial Theorem Exercise

Recall Theorem 3.7, which we reproduce below but change the $x$ and $y$ to $a$ and $b$ respectively. If $n \geq 0$ is an integer, then

\[(a + b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n.\]

**QUESTION 1:** Use the binomial theorem to expand $(-2x + 3y)^4$.

Set $a = -2x$ and $b = 3y$ and $n = 4$, and make the appropriate substitutions in the formula above. We get

\[
(-2x + 3y)^4 = \binom{4}{0}(-2x)^4 + \binom{4}{1}(-2x)^3(3y) + \binom{4}{2}(-2x)^2(3y)^2 + \cdots + \binom{4}{4}(-2x)(3y)^3 + \binom{4}{4}(3y)^4
\]

\[= 1(-2)^4 \cdot x^4 + 4(-2)^3(3) \cdot x^3y + 6(-2)^23^2 \cdot x^2y^2 + \cdots + 4(-2)^3 \cdot xy^3 + 1(3)^4 \cdot y^4
\]

\[= 16x^4 - 96x^3y + 216x^2y^2 - 216xy^3 + 81y^4.
\]

**QUESTION 2:** Find the coefficient of $x^{13}y^3$ in the expansion of $(3x - y)^{16}$.

**[HINT]:** It may be helpful to use the big triangle in Subsection 3.3. It’s quicker than a calculator ☺.

Recall the more compact summation form of the binomial theorem above

\[(a + b)^n = \sum_{k=0}^{n} \binom{n}{k}a^{n-k}b^k.
\]

Set $a = 3x$ and $b = -y$ and $n = 16$, we seek the following summand $\binom{16}{3}(3x)^{13}(-y)^3$. This equals $560 \cdot 3^{13} \cdot (-1)^3 \cdot x^{13}y^3 = 892,820,880x^{13}y^3$. Thus the coefficient of $x^{13}y^3$ is

\[892,820,880\].
4 Primes, Prime Factorization, and Some Consequences

4.1 Motivation

Ponder the following questions

- What is the greatest integer value of $n$ such that $2^n$ is a factor of $200^6$?
- What is so special about the number $2^{82,589,933} - 1$ and was it really just discovered on Dec. 21, 2018? (FUN FACT: This number contains almost 25 million digits!)
- What is satanic about Belphegor’s prime?
- What is the Goldbach conjecture and why has nobody proved it?
- What are safe primes and what is their connection to the imminent female mathematician Sophie Germain?

All the questions above will be answerable by the end of this section.
4.2 Density of Primes and the Celebrated Prime Number Theorem

Below we give a spiral representation\textsuperscript{22} of the first 1200 integers in 30 concentric circles of 40 integers each. Shaded blue are the squares of primes; coincidentally all but 4 and 25 lie in the 1st and 9th columns (Hmm?). Shaded red are the primes.

\textbf{QUESTION:} Guess at what percentage of the 1200 numbers are prime?

\textbf{ANSWER:} There are 196 primes and \( \frac{196}{1200} = .16\bar{3} \). So \( 16\frac{1}{3}\% \) of the positive integers less than 1200 are prime.

\textsuperscript{22}This image is made with software under a creative commons license CC BY-NC-SA 2.5 and may be shared. More info on how it is constructed at http://alphapixel.com/prime-number-diagrams-in-python-and-svg/
**Definition 4.1.** An integer $n > 1$ whose only positive divisors are 1 and itself is called a **prime number**. If $n$ is not prime, then it is called a **composite number**.

Here is a list of primes up to 100. Observe that there are 25 primes between 1 and 100. So exactly 25% of the integer interval $[1, 100]$ are prime numbers.

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

**Definition 4.2.** Let $\pi : \mathbb{N} \to \mathbb{Z}$ be the **prime counting function** defined by $\pi(n)$ equals the number of primes less than or equal to $n$.

**Density of the Primes**

- Compute $\pi(100)$ and $\pi(1200)$. [You Do!]

  $$
  \pi(100) = 25 \quad \text{and} \quad \pi(1200) = 196.
  $$

- Use the results above to compute $\frac{\pi(100)}{100}$ and $\frac{\pi(1200)}{1200}$. [You Do!]

  $$
  \frac{\pi(100)}{100} = .25 \quad \text{and} \quad \frac{\pi(1200)}{1200} = .1633.
  $$

We define the **density of primes** in the set of positive integers to be

$$
\lim_{n \to \infty} \frac{\pi(n)}{n}.
$$

**QUESTION:** Do you think this proportion $\frac{\pi(n)}{n}$ of primes in the interval $[1, n]$ continues to decrease as $n$ increases? That is, do you think the density is exactly zero?

---

*aA rigorous answer to this question involves the celebrated **prime number theorem** we give on the next page but whose proof is beyond the scope of this course.*
The Prime Number Theorem

**Definition 4.3.** Two functions $f$ and $g$ are said to be **asymptotic functions** if \( \lim_{n \to \infty} \frac{f(n)}{g(n)} = 1 \). We denote this as \( f(n) \sim g(n) \).

**Theorem 4.4** (Prime Number Theorem). *The following relationship holds*

\[
\pi(n) \sim \frac{n}{\log(n)}.
\]

**Note:** We write \( \log \) to mean the natural logarithm.

<table>
<thead>
<tr>
<th>( n )</th>
<th>( \pi(n) )</th>
<th>( \frac{n}{\log(n)} )</th>
<th>( \frac{n}{\log(n)} - 1.08366 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>168</td>
<td>144.765</td>
<td>171.7</td>
</tr>
<tr>
<td>2000</td>
<td>303</td>
<td>263.127</td>
<td>306.878</td>
</tr>
<tr>
<td>3000</td>
<td>430</td>
<td>374.702</td>
<td>433.356</td>
</tr>
<tr>
<td>4000</td>
<td>550</td>
<td>482.273</td>
<td>554.755</td>
</tr>
<tr>
<td>5000</td>
<td>669</td>
<td>587.048</td>
<td>672.628</td>
</tr>
<tr>
<td>6000</td>
<td>783</td>
<td>689.694</td>
<td>787.83</td>
</tr>
<tr>
<td>7000</td>
<td>900</td>
<td>790.633</td>
<td>900.9</td>
</tr>
<tr>
<td>8000</td>
<td>1007</td>
<td>890.155</td>
<td>1012.21</td>
</tr>
<tr>
<td>9000</td>
<td>1117</td>
<td>988.47</td>
<td>1122.01</td>
</tr>
<tr>
<td>10000</td>
<td>1229</td>
<td>1085.74</td>
<td>1230.51</td>
</tr>
</tbody>
</table>

Notice that the far-right column gives a better estimate for \( \pi(n) \). This was observed in the late 1700s by Adrien-Marie Legendre who conjectured that

\[
\pi(n) \sim \frac{n}{\log(n) - B}
\]

with \( B = 1.08366 \).

Notice that since \( \pi(n) \sim \frac{n}{\log(n) - B} \) [We will show this later!] no matter what choice is made for \( B \) it makes sense to find the \( B \) that makes the best estimate\(^\text{23}\).  

\(^\text{23}\)In their 2005 book *Prime Number - A Computational Perspective*, authors Crandall and Pomerance note that \( B = 1 \) is “attractive for estimations with a pocket calculator.”
**The Coolest Estimator of $\pi(n)$**

**Definition 4.5.** The **logarithmic integral** $\text{li}(x)$ is the function defined as

$$\text{li}(x) = \int_{0}^{x} \frac{1}{\log(t)} \, dt \text{ for all } x \in \mathbb{R}^+ \setminus \{1\}.$$ 

The **Eulerian logarithmic integral** $\text{Li}(x)$ is the function defined as

$$\text{Li}(x) = \int_{2}^{x} \frac{1}{\log(t)} \, dt = \text{li}(x) - \text{li}(2).$$

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\pi(n)$</th>
<th>$\frac{n}{\log(n) - 1.08366}$</th>
<th>$\text{Li}(n)$</th>
<th>$\frac{\pi(n)}{\text{Li}(n)}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^3$</td>
<td>168</td>
<td>172</td>
<td>177</td>
<td>0.951494</td>
</tr>
<tr>
<td>$10^4$</td>
<td>1229</td>
<td>1231</td>
<td>1245</td>
<td>0.987076</td>
</tr>
<tr>
<td>$10^5$</td>
<td>9592</td>
<td>9588</td>
<td>9629</td>
<td>0.996182</td>
</tr>
<tr>
<td>$10^6$</td>
<td>78498</td>
<td>78543</td>
<td>78627</td>
<td>0.998366</td>
</tr>
<tr>
<td>$10^7$</td>
<td>664579</td>
<td>665140</td>
<td>664917</td>
<td>0.999491</td>
</tr>
<tr>
<td>$10^8$</td>
<td>5761455</td>
<td>5768004</td>
<td>5762208</td>
<td>0.999869</td>
</tr>
<tr>
<td>$10^9$</td>
<td>50847534</td>
<td>50917519</td>
<td>50849234</td>
<td>0.999967</td>
</tr>
<tr>
<td>$10^{10}$</td>
<td>455052511</td>
<td>455743004</td>
<td>455055614</td>
<td>0.999993</td>
</tr>
</tbody>
</table>

**QUESTION:** What can you say about the $\text{Li}(n)$ estimator in comparison to Legendre’s estimator for $\pi(n)$?

**ANSWER:** The function $\text{Li}(x)$ is a MUCH BETTER estimator for $\pi(x)$. 
Quirky Facts and Questions

1. **QUESTION:** Use the PNT result \( \pi(n) \sim \frac{n}{\log(n)} \) to show that the density of primes, namely \( \frac{\pi(n)}{n} \), tends to zero as \( n \) tends to infinity. [You Do!]

**ANSWER:** Since \( \pi(n) \sim \frac{n}{\log(n)} \), then \( \frac{\pi(n)}{n} \sim \frac{1}{\log(n)} \). And thus

\[
\lim_{n \to \infty} \frac{\pi(n)}{n} = \lim_{n \to \infty} \frac{1}{\log(n)} = 0.
\]

2. **QUESTION:** A few pages ago, we said \( \pi(n) \sim \frac{n}{\log(n) - B} \) no matter what choice for \( B \). Give a justification for this. [You Do!]

**ANSWER:** It suffices to show that \( \lim_{n \to \infty} \frac{\pi(n)}{n/(\log(n) - B)} = 1 \).

Observe that

\[
\frac{\pi(n)}{n/(\log(n) - B)} = \frac{\pi(n) \cdot (\log(n) - B)}{n} = \frac{\pi(n) \cdot \log(n)}{n} - \frac{\pi(n) \cdot B}{n}.
\]

Hence it follows that

\[
\lim_{n \to \infty} \frac{\pi(n)}{n/(\log(n) - B)} = \lim_{n \to \infty} \frac{\pi(n) \cdot \log(n)}{n} - B \cdot \lim_{n \to \infty} \frac{\pi(n)}{n} = 1 - B \cdot 0
\]

which equals 1, so \( \pi(n) \sim \frac{n}{\log(n) - B} \). ✓

3. It is **VERY HARD** to know the value of \( \pi(n) \) for large \( n \). For example, the largest \( k \) for which \( \pi(10^k) \) is known\(^{24}\) is \( k = 27 \). The exact value is

\[
\pi(10^{27}) = 16,352,460,426,841,680,446,427,399.
\]

4. Astonishingly, the Li-function estimator delivers this startling close estimate

\[
\text{Li}(10^{27}) = 16,352,460,426,842,189,113,085,404.
\]

\(^{24}\)This was discovered in 2015 by David Baugh and Kim Walisch. They announced their finding at the website [https://www.mersenneforum.org/showthread.php?t=20473](https://www.mersenneforum.org/showthread.php?t=20473)
4.3 A Smörgåsbord of Types of Primes

In the literature there are many different types of primes. Indeed, the following Wikipedia page


gives over 70 different types of primes. We will take a look at a few of these.

**Definition 4.6.** A left-truncatable prime is a prime number which remains prime when each leading (“left”) digit is successively removed. Whereas, a right-truncatable prime is a prime which remains prime when each last (“right”) digit is successively removed.

- 9137 is a left-truncatable prime since 9137, 137, 37, and 7 are all prime.
- 7393 is a right-truncatable prime since 7393, 739, 73, and 7 are all prime.
- 357,686,312,646,216,567,629,137 is the largest known left-truncatable prime.
- 73,939,133 is the largest known right-truncatable prime.

**Definition 4.7.** A palindromic prime is a prime number that is also a palindromic number. Here is a list of the first 20 of them:

2, 3, 5, 7, 11, 101, 131, 151, 181, 191, 313, 353, 373, 383, 727, 757, 787, 797, 919, 929

**QUESTION:** Besides 11, all palindromic numbers have an odd number of digits. [WHY?] **HINT:** Consider the divisible-by-11 test in Subsection 5.1.

**ANSWER:** If a palindromic number has an even number of digits, then it is necessarily divisible by 11. For example, consider a number of the form \(abccba\). Then the reverse alternating sum of its digits is

\[
a - b + c - c + b - a = 0
\]

and 11 divides 0, so hence \(abccba\) is also divisible by 11, so \(abccba\) cannot be prime.
Fact: The largest known\textsuperscript{25} palindromic prime as of Nov 2014 is (474,501 digits):
\[ 10^{474500} + 999 \cdot 10^{237249} + 1. \]

**QUESTION:** The following palindromic prime is called \textit{Belphegor’s prime}:

1,000,000,000,000,066,600,000,000,000,001

The name Belphegor refers to one of the Seven Princes of Hell\textsuperscript{26}. What is particularly demonic about this number? (\textit{Give at least two devilish reasons!})

**ANSWER:** The center of the number is 666, the \textit{Number of the Beast}, and is flanked on its left and right sides by 13 zeroes. Lastly it has 31 digits and 31 is the reverse of 13.

**Mersenne Numbers and a Future Homework Problem**

A \textbf{Mersenne number} is a number of the form \(2^m - 1\) for some positive integer \(m\).

**HOMEWORK EXERCISE:** Prove that if \(m \in \mathbb{N}\) is composite (that is, \(m = ab\) for some integers \(a, b > 1\)), then \(2^m - 1\) is divisible by both \(2^a - 1\) and \(2^b - 1\).

Thus if a Mersenne number is prime, then \(m\) must be prime. Note that the converse does not hold since \(m = 11\) is prime yet \(2^{11} - 1 = 2047 = 23 \cdot 89\) is composite.

---

\textsuperscript{25}This palindromic prime was discovered by Serge Batalov. See \textit{The Prime Pages} website by Chris Caldwell at https://primes.utm.edu/top20/page.php?id=53

\textsuperscript{26}The Seven Princes of Hell and their \textit{devilishly evil} correspondences are:

(i) \textbf{Lucifer}: pride, (ii) \textbf{Mammon}: greed, (iii) \textbf{Asmodeus}: lust, (iv) \textbf{Leviathan}: envy, (v) \textbf{Beelzebub}: gluttony, (vi) \textbf{Satan}: wrath, and (vii) \textbf{Belphegor}: sloth.
Question 4.8. Who is Marin Mersenne?

- Marin Mersenne (1588—1648), France
- He studied theology and Hebrew in Paris and was ordained a priest in 1613.
- He studied mathematics with René Descartes, Étienne Pascal (father of Blaise Pascal), and others.
- He corresponded with Galileo Galilei and was a staunch defender of Galileo’s controversial heliocentric view of the Earth revolving around the sun and not vice-versa.
- He is MOST FAMOUS in mathematics for what we now call Mersenne primes.

Definition 4.9. Let $p_n$ denote the $n^{\text{th}}$ prime number and consider the sequence $\{M_{p_n}\}_{n=1}^\infty$ where

$$M_{p_n} = 2^{p_n} - 1.$$  

A Mersenne prime is a Mersenne number $M_{p_n}$ which is itself prime.

The first twenty terms of this Mersenne number sequence $\{M_{p_n}\}$ are given in the tables below. Recall that $p_n$ is the $n^{\text{th}}$ prime. We highlight the particular $M_{p_n}$ values which are Mersenne primes.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$p_n$</th>
<th>$M_{p_n} = 2^{p_n} - 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>31</td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td>127</td>
</tr>
<tr>
<td>5</td>
<td>11</td>
<td>2047</td>
</tr>
<tr>
<td>6</td>
<td>13</td>
<td>8,191</td>
</tr>
<tr>
<td>7</td>
<td>17</td>
<td>131,071</td>
</tr>
<tr>
<td>8</td>
<td>19</td>
<td>524,287</td>
</tr>
<tr>
<td>9</td>
<td>23</td>
<td>8,388,607</td>
</tr>
<tr>
<td>10</td>
<td>29</td>
<td>536,870,911</td>
</tr>
<tr>
<td>11</td>
<td>31</td>
<td>2,147,483,647</td>
</tr>
<tr>
<td>12</td>
<td>37</td>
<td>137,438,953,471</td>
</tr>
<tr>
<td>13</td>
<td>41</td>
<td>2,199,023,255,551</td>
</tr>
<tr>
<td>14</td>
<td>43</td>
<td>8,796,093,022,207</td>
</tr>
<tr>
<td>15</td>
<td>47</td>
<td>140,737,488,355,327</td>
</tr>
<tr>
<td>16</td>
<td>53</td>
<td>9,007,199,254,740,991</td>
</tr>
<tr>
<td>17</td>
<td>59</td>
<td>576,460,752,303,423,487</td>
</tr>
<tr>
<td>18</td>
<td>61</td>
<td>2,305,843,009,213,693,951</td>
</tr>
<tr>
<td>19</td>
<td>67</td>
<td>147,573,952,589,676,412,927</td>
</tr>
<tr>
<td>20</td>
<td>71</td>
<td>2,361,183,241,434,822,606,847</td>
</tr>
</tbody>
</table>

**QUESTION TO PONDER:** Do you think it is a coincidence that all these numbers end in 1, 3 or 7? Why don’t any end in 5 or 9? **HINT:** Consider the last digit of powers of 2.
Mersenne’s mistake

Conjecture 4.10. In his book Cogita Physica-Mathematica in 1644, Marin Mersenne states that the numbers $M_p = 2^p - 1$ are prime for the following prime $p$ values:

$$2, 3, 5, 7, 13, 17, 19, 31, 67, 127, \text{ and } 257$$

and is composite for all other primes $p < 257$.

In the 1600s, Mersenne as well as his colleagues did not have the primality-testing abilities to confirm his assertion above. Some history:

- In 1772, Euler verified $M_{31}$ is prime by brute force dividing by a sufficient set of primes less than $\sqrt{M_{31}} \approx 46341$. However, $M_{67}, M_{127},$ and $M_{257}$ were beyond the great Euler’s reach!

- In 1876, Édouard Lucas proves that $M_{127}$ is prime. This number remains to be LARGEST KNOWN prime number for the next 75 years!

- In 1876, Lucas is also able to give an existence proof that $M_{67}$ is composite. This refutes Mersenne’s claim that $M_{67}$ is prime. However, he is UNABLE to produce any actual factors of $M_{67}$.

- In 1883, Ivan Mikheevich Pervushin proves that $M_{61}$ is prime. This refutes Mersenne’s claim that $M_{61}$ is composite. $M_{61}$ remains the second largest known prime number until 1911.

- In 1903 (27 years after Lucas fails to find $M_{67}$’s factors), Frank Nelson Cole gives a famous talk at the AMS meeting. Without speaking a word, he raises 2 to the 67th power on the blackboard and then subtracts 1. On the other side of the board, he multiplies $193,707,721 \times 761,838,257,287$ and gets the same number. He returns to his seat (to applause) without speaking.\(^c\)

\(^{b}\)Euler proves that if $M_{31}$ has a prime divisor $p$, then $p$ is congruent to 1 or 63 (mod 248). The constraint on the prime divisors is an immediate consequence of the (now) well-known Mersenne factor theorem [This might be a good HW or exam problem!]: for odd primes $p, q$ we have

$$p \mid M_q \implies p \equiv 1 \pmod{q}, \quad p \equiv \pm 1 \pmod{8}.$$ 

Mersenne’s mistake (continued)

- After his famous 1903 talk, Cole tells a friend that it took him 20 years of Sunday afternoons to find the factors of

\[ M_{67} = 147,573,952,589,676,412,927. \]

- In 1911 and 1914, Ralph Ernest Powers proves that \( M_{89} \) and \( M_{107} \), respectively, are prime. This refutes Mersenne’s claim that \( M_{89} \) and \( M_{107} \) are composite.

- In 1930, Derrick Lehmer gives an existence proof that \( M_{257} \) is composite but cannot find any factorization. This refutes Mersenne’s claim that \( M_{67} \) is prime.

- In 1980 (50 years after Lehmer’s dilemma), the prime factorization of \( M_{257} \) is finally found!

**MERSENNE’S MISTAKE:** He erroneously concludes \( M_{67} \) and \( M_{257} \) are prime and excludes \( M_{61} \), \( M_{89} \), and \( M_{107} \) from his “list of primes”.

**THE BIG “BUTT”:** He made some mistakes, but Marin Mersenne is still a bad ass!!! See what the expressionless person has to say below!

- The largest known prime number (as of January 2019) is \( 2^{82,589,933} - 1 \), a number with 24,862,048 digits. It was found by the Great Internet Mersenne Prime Search (GIMPS)\(^{27} \) on December 21, 2018.

- As of January 2019, the eight largest known primes are Mersenne primes.

- The last seventeen record primes were Mersenne primes.

\(^{27}\)See the webpage: [https://www.mersenne.org/primes/?press=M82589933](https://www.mersenne.org/primes/?press=M82589933)
The following type of prime is attributed to Pierre de Fermat (1607–1665). We wait until Subsection 8 on his “Little Theorem” to give a history box on him.

**Definition 4.11.** For $n \in \mathbb{N} \cup \{0\}$, a **Fermat number** is a number of the form

$$F_n = 2^{2^n} + 1.$$ 

If $F_n$ is a prime number, then we call it a **Fermat prime**.

**Fermat’s mistake**

**Conjecture 4.12.** In writing to Marin Mersenne, Fermat states: “I have a found that numbers of the form $2^{2^n} + 1$ are always prime numbers and have long since signified to analysts the truth of this theorem.”

Fermat observed that

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad \text{and} \quad F_4 = 65,537.$$ 

And these are all prime numbers.

**QUESTION:** What do you think Fermat’s mistake is?

**ANSWER:** Primality testing was very difficult in the time of Fermat’s life. But apparently not for Euler who in 1732 found that

$$F_5 = 4,294,967,297 = 2^{2^5} + 1 = 641 \cdot 6,700,417.$$ 

This disproves Fermat’s conjecture.

**SOME VERY COOL/SURREAL FACTS:**

1. No one has yet to find a Fermat prime larger than $F_4 = 65,537$.

2. As of 2014, the numbers $F_n$ for $5 \leq n \leq 32$ were known to be composite, but of these, complete factorizations were only known for $5 \leq n \leq 11$.

3. Ironically, even though we know $F_{20}$ and $F_{24}$ are composite, to this date\(^{28}\) NO ONE knows any prime factors of either number. **That is so weird!!**

\(^{28}\)See [http://www.prothsearch.com/fermat.html](http://www.prothsearch.com/fermat.html) Almost 300 Fermat numbers as of 2019 are known to be composite, yet $F_{33}$ still remains a mystery. Ha! The largest known composite number is $F_{3329780}$. 
Question 4.13. Who is Sophie Germain?

- Sophie Germain (1776—1831), France
- She was a mathematician, physicist, and philosopher.
- Her work on Fermat’s Last Theorem provided a foundation for mathematicians exploring the subject for hundreds of years after.
- Because of prejudice against her sex, she was unable to make a career out of mathematics, but she worked independently corresponding by letter to math greats such as Lagrange and Gauss under the male name Monsieur Antoine-Auguste Le Blanc.

“How can I describe my astonishment and admiration on seeing my esteemed correspondent M. Le Blanc metamorphosed into this celebrated person. . . when a woman, because of her sex, our customs and prejudices, encounters infinitely more obstacles than men in familiarizing herself with [number theory’s] knotty problems, yet overcomes these fetters and penetrates that which is most hidden, she doubtless has the most noble courage, extraordinary talent, and superior genius.” - Gauss (after realizing the true identity of Monsieur Le Blanc)

Definition 4.14. A prime number \( p \) is a Sophie Germain prime if \( 2p + 1 \) is also prime. The number \( 2p + 1 \) associated with a Sophie Germain prime is called a safe prime.

The first few Sophie Germain primes are

\[
2, 3, 5, 11, 23, 29, 41, 53, 83, \ldots
\]

and their corresponding safe primes are

\[
5, 7, 11, 23, 47, 59, 83, 107, 167, \ldots
\]

There are many more types of primes, but the idea is that primes are important, and they show up a lot! Now that we have a good idea at what a prime is, we look at some properties of prime numbers.
4.4 The Fundamental Theorem of Arithmetic and Some Consequences

Before we look at the fundamental theorem of arithmetic (FTA), we look at an important axiom and Euclid’s lemma, which are pivotal in helping us show WHY FTA holds.

**The Well-Ordering Principle Axiom (WOP)**

**Axiom 4.15.** Every nonempty set of non-negative integers has a smallest member.

**Fact:** WOP is logically equivalent to induction. WOP is also used to prove the division algorithm.

**Lemma 4.16** (Euclid’s Lemma). Let $p$ be a prime.

(i) If $p | mn$ where $m, n \in \mathbb{Z}$, then $p | m$ or $p | n$.

(ii) If $p | m_1m_2 \cdots m_r$ where $m_i \in \mathbb{Z}$ for all $i$, then $p | m_i$ for some $i$.

**Theorem 4.17** (Prime Factorization Theorem). The following holds.

(i) Every integer $n \geq 2$ is a product of (one or more) primes.

(ii) This factorization is unique (up to order of the prime factors). That is, if $n = p_1p_2 \cdots p_r$ and $n = q_1q_2 \cdots q_s$ then $r = s$ and each $q_j$ can be relabeled so that $p_i = q_i$ for $i = 1, 2, \ldots, r$.

**Proof of (1)** Strong induction [see an abstract algebra textbook]

**Proof of (2)** Suppose BWOC that (ii) fails. Then by WOP there exists a smallest integer $m$ such that

$$m = p_1p_2 \cdots p_r = q_1q_2 \cdots q_s$$

are two distinct prime factorizations of $m$. Thus $m$ is not prime. [Why?]

Two distinct factorizations does not allow $r = s = 1$. 
So \( r \geq 2 \) and \( s \geq 2 \). Hence \( p_1 \mid q_1 q_2 \cdots q_s \) and so \( p_1 \mid q_j \) for some \( j \) with \( 1 \leq j \leq s \) [Why? by Euclid’s Lemma (ii)]. By relabeling we can let \( p_1 \mid q_1 \). Observe that \( p_1 = q_1 \). [Why? because \( q_1 \) is prime.] Since \( m = p_1 p_2 \cdots p_r \) and \( m = q_1 q_2 \cdots q_s \) and \( p_1 = q_1 \), then

\[
\frac{m}{p_1} = p_2 p_3 \cdots p_r \quad \text{and} \quad \frac{m}{p_1} = q_2 q_3 \cdots q_s
\]

are two distinct factorizations of the integer \( \frac{m}{p_1} \). [Why is this in \( \mathbb{Z} \)?]

The integer \( \frac{m}{p_1} \) is strictly less than \( m \) and has two distinct prime factorizations. This contradicts the fact that \( m \) is the smallest number with this property.

Hence (2) follows.

Q.E.D.

**Corollary 4.18.** Two integers are relatively prime if there exists no prime that divides them both.

**A Very Cool Number Theory Fact**

**Remark 4.19.** By the Prime Factorization Theorem, each \( n \in \mathbb{N}_{\geq 2} \) can be written uniquely as \( n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r} \) where the \( p_i \) are distinct primes and \( n_i \geq 1 \) for all \( i \).

**Theorem 4.20.** Let \( n \) be an integer with prime factorization \( n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r} \) (\( p_i \) distinct primes and \( n_i \geq 1 \)). Then \( d \mid n \) implies that \( d = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r} \) where \( d > 0 \) and \( 0 \leq d_i \leq n_i \ \forall i \).

In Section 7, we will learn the \( \tau \) function which counts the number of divisors of \( n \) in Theorem 7.9. This \( \tau \) will rely on Theorem 4.20. It is in that section where we will prove this theorem.
Remark 4.21. The “first” given proof of the infinitude of primes was given by Euclid in 300 B.C. His proof is given below in the following proposition found in Euclid’s *Elements* (see Heath\(^e\)) Book IX Proposition 20. At the current moment, there are at least 183 different proofs for the infinitude of primes. For a survey article on these proofs see Romeo Meštrović’s 2018 paper, *Euclid’s theorem on the infinitude of primes: a historical survey of its proofs (300 B.C.–2017) and another new proof*, on the arXiv:

https://arxiv.org/pdf/1202.3670


Theorem 4.22 (Euclid). *There are infinitely many primes.*

Many erroneously believe that Euclid’s original proof was a proof by contradiction. However, what he does prove in his *Elements* is that there are more primes than found in any finite list of primes. That is what we prove below truer to Euclid’s original proof.

Proof. Let \(p_1, p_2, \ldots, p_k\) be any finite list of primes. And set \(P\) equal to \(p_1 p_2 \cdots p_k + 1\). Then \(P\) is either prime or it is not.

- If \(P\) is prime, then it is a prime not on our list. [WHY?]

- If \(P\) is not prime, then it is divisible by some prime, call it \(p\). Notice \(p\) cannot be any of the \(p_1, p_2, \ldots, p_k\) otherwise it would divide 1. [WHY?] So \(p\) is some prime that was not in our original list.

Either way, the original list is incomplete.

Q.E.D.

Now take a break [AND] sing “a product of powers of primes, oh my!” to the tune of “lions and tigers and bears, oh my!” from the Wizard of Oz. 😊
Liar Liar Pants on Fire!

Published in *The American Mathematical Monthly*, Vol. 122, No. 5 (May 2015), p. 466, the following one-line proof for the infinitude of primes appeared:

![A One-Line Proof of the Infinitude of Primes](image)

This proof and a subsequent video on YouTube that went viral has placed this flawed proof in the public attention. Hence, we will address this issue because this does indeed happen in mathematics.

**QUESTION:** What is true about the “proof”?

**ANSWER:** [You Do!] Denote $P = \prod_{p'} p'$. Since each prime $p$ is greater than or equal to 2, then $\sin\left(\frac{\pi}{p}\right) > 0$ follows. So $0 < \prod_p \sin\left(\frac{\pi}{p}\right)$ holds. Also the 1st equality holds too since

$$
\sin\left(\frac{\pi \cdot (1 + 2P)}{p}\right) = \sin\left(\frac{\pi}{p} + 2\pi P\right) = \sin\left(\frac{\pi}{p} + 2\pi k_p\right)
$$

where $k_p$ is the integer that remains when $P$ is divided by $p$. Thus, the $2\pi$-periodicity of sine confirms that Northshield’s 2nd equality holds.

**QUESTION:** What is the flaw? [Let’s Discuss]

---

29In their paper of arXiv (See [https://arxiv.org/abs/1710.07633](https://arxiv.org/abs/1710.07633)), Karamzadeh does a thorough job of addressing the flaws in this proof.
Example 4.23. Write 60 as a “product of powers of primes” (Oh My!) and then use Theorem 4.20 to find the number of positive divisors of 60.

First draw the factor-tree. [You finish]

Using Theorem 4.20, we find [You Finish!]

\[ d \mid 60 \implies d = 2^{d_1} \times 3^{d_2} \times 5^{d_3} \]

where

\[
\begin{align*}
0 \leq d_1 \leq 2 & \implies \text{3 choices for } d_1 \\
0 \leq d_2 \leq 1 & \implies \text{2 choices for } d_2 \\
0 \leq d_3 \leq 1 & \implies \text{2 choices for } d_3
\end{align*}
\]

12 possible divisors of 60

A Thought Exercise (in Combinatorics)

How many positive divisors does \( n = p_1^{n_1}p_2^{n_2} \cdots p_r^{n_r} \) have?

**YOUR CONJECTURE AND JUSTIFICATION:** Any positive divisor of \( n \) will be of the form \( d = p_1^{d_1}p_2^{d_2} \cdots p_r^{d_r} \) with \( 0 \leq d_i \leq n_i \) for each \( i \). There are \( d_i + 1 \) choices for the exponent of the prime \( p_i \). And hence there is a total of \( \prod_{i=1}^{r} (d_i + 1) \) possible divisors of \( n \). ✓
Quickie GCD and LCM Calculations

NOTE: We leave the formal definitions of the greatest common divisor and least common multiple in the next section in Definitions 5.14 and 5.16, respectively. But we presume all are well aware of their numerical meaning.

**Theorem 4.24** (GCD and LCM via Prime Factorization). Let \( \{a, b, c, \ldots\} \) be a set of positive integers and write

\[
a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}
\]
\[
b = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}
\]
\[
c = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}
\]

where an exponent is zero if the prime does not occur. Then \( \gcd(a, b, c, \ldots) \) and \( \text{lcm}(a, b, c, \ldots) \) are computed as follows:

\[
\gcd(a, b, c, \ldots) = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \text{ where } k_i = \min(a_i, b_i, c_i, \ldots) \text{ for each } i
\]
\[
\text{lcm}(a, b, c, \ldots) = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r} \text{ where } m_i = \max(a_i, b_i, c_i, \ldots) \text{ for each } i.
\]

**EXERCISE:** Let \( a = 28,665 = 3^2 \cdot 5 \cdot 7^2 \cdot 13 \) and \( b = 22,869 = 3^3 \cdot 7 \cdot 11^2 \). Compute \( \gcd(a, b) \) and \( \text{lcm}(a, b) \).

**ANSWER:**

\[
\gcd(a, b) = 3^2 \cdot 5^0 \cdot 7^1 \cdot 11^0 \cdot 13^0 = 63
\]
\[
\text{lcm}(a, b) = 3^3 \cdot 5^1 \cdot 7^2 \cdot 11^2 \cdot 13^1 = 10,405,395
\]
4.5 The Goldbach Conjecture

**Conjecture 4.26 (The Goldbach Conjecture).** *Every even integer greater than two is the sum of two prime numbers.*

**EXERCISE:** Clearly 4, 6, and 8 can be written as sum of two primes in one way only. Find ALL the ways to write each of the following as a sum of two primes. [You Do!]

\[
egin{align*}
10 &= 5 + 5 \text{ or } 3 + 7 \\
12 &= 5 + 7 \\
14 &= 3 + 11 \text{ or } 7 + 7 \\
16 &= 3 + 13 \text{ or } 5 + 11 \\
18 &= 5 + 13 \text{ or } 7 + 11 \\
20 &= 3 + 17 \text{ or } 7 + 13
\end{align*}
\]
Status of the problem (as of 2019)

The conjecture has been shown to hold for all even integers less than 4,000,000,000,000, but it remains unproven despite considerable effort.

Pictorially we can view Goldbach’s conjecture as follows:\textsuperscript{30}:

- Even integers corresponding to the black horizontal lines.
- For each prime, there are two one red and one blue.
- The sums of the two primes are intersections of one red and one blue line, marked by a circle.

\textsuperscript{30}This image is by Adam Cunningham and John Ringland and is on Wikimedia Commons and is free to share under the license https://creativecommons.org/licenses/by-sa/3.0/deed.en
Prime Factorization Exercise 1

**Question 4.27.** The product of $360 \cdot 200 \cdot 81$ is the cube of what integer?

We first draw a prime factor tree for each factor.
Thus the prime factorization of 360, 200, and 81 is as follows

\begin{align*}
360 &= 2^3 \cdot 3^2 \cdot 5 \\
200 &= 2^3 \cdot 5^2 \\
81 &= 3^4.
\end{align*}

Hence we have

\begin{align*}
60 \cdot 200 \cdot 81 &= (2^3 \cdot 3^2 \cdot 5) \cdot (2^3 \cdot 5^2) \cdot (3^4) \\
&= 2^6 \cdot 3^6 \cdot 5^3 \\
&= 2^3 \cdot 3^2 \cdot 3^4 \cdot 5^3 \\
&= (2^2)^3 \cdot (3^2)^3 \cdot 5^3 \\
&= (2^2 \cdot 3^2 \cdot 5)^3 \\
&= 180^3.
\end{align*}

Thus the product of 360 \cdot 200 \cdot 81 is the cube of 180.
Fermat’s Last Theorem Proof Exercise 2

Fermat’s last theorem says that for all integers \( n > 2 \), the equation \( x^n + y^n = z^n \) has no positive integer solution \((x, y, z \in \mathbb{N})\).

Prove the following version of Fermat’s last theorem: If \( x^p + y^p = z^p \) has no positive integer solution for all prime numbers \( p > 2 \), then for all \( n > 2 \) with \( n \neq 2^k \) for any \( k \) we have \( x^n + y^n = z^n \) has no positive integer solution.

Proof. Suppose by way of contradiction that there is an integer \( n > 2 \) that is not a power of 2 for which \( x^n + y^n = z^n \) has a positive integer solution. Call the solution \( x = x_0, y = y_0 \) and \( z = z_0 \).

**WWTS:** There exists a prime \( p > 2 \) such that \( x^p + y^p = z^p \) for \( x, y, z \in \mathbb{Z}^+ \).

There are two cases: when \( n \) is prime and when \( n \) is not prime.

**CASE 1:** (\( n \) is prime) Since \( n \) is prime, then for some prime \( p \) (namely \( p = n \)), \( x^p + y^p = z^p \) has a positive integer solution, and we are done.

**CASE 2:** (\( n \) is not prime) Using Remark 4.19, since \( n \) is not prime, then \( n \) is divisible by a prime. Since \( n \) is not a power of 2, there exist a prime number \( p > 2 \) such that \( n = kp \) for some integer \( k \). Since \( x = x_0, y = y_0 \) and \( z = z_0 \) is a positive integer solution to \( x^n + y^n = z^n \), then

\[
x_0^n + y_0^n = z_0^n.
\]

Substituting \( n = kp \), we have

\[
x_0^{kp} + y_0^{kp} = z_0^{kp} \text{ or equivalently } (x_0^k)^p + (y_0^k)^p = (z_0^k)^p.
\]

Note \( x_0^k, y_0^k, \) and \( z_0^k \) are all positive integers (because they are integer powers of positive integers). Consequently, the equation

\[
x^p + y^p = z^p
\]

has a positive integer solution (namely \( x_0^k, y_0^k, \) and \( z_0^k \)).

Q.E.D.
Prime Number Proof Exercise 3

Prove that for all integers $n$, if $n > 2$ then there is a prime number $p$ such that $n < p < n!$.

**Hands Dirty Part:**

$$
\begin{align*}
  n &= 3 & 3 &< &5 &< 3! &= 6 \\
  n &= 4 & 4 &< &7, 11, 13, 17, 19, 23 &< 4! &= 24 \\
  n &= 5 & 5 &< &11, 13, \cdots, 109, 113 &< 5! &= 120 \\
\end{align*}
$$

**Proof.** Let $n > 2$ be any integer.

**WWTS:** There is a prime number $p$ such that $n < p < n!$

** Attempt 1:** Given $n!$ there exists a prime $p$ such that $p \mid n!$ [Why?] thus $p \leq n!$ is forced. [Why?] Since $n!$ is not prime, we have $p < n!$. Therefore it suffices to show $p > n$.

**Question 4.28.** This $p$ is not **forced** to be greater than $n$. For example, what is a $p$ such that $p \leq n$ and $p \mid n!$ for all $n > 2$?

** Attempt 2:** [You Do!] Consider $n! - 1$. Then there exists a $p$ such that $p \mid n! - 1$. Since $n! - 1 < n!$ and $p \mid n! - 1$, we have $p < n!$. It suffices to show that $p > n$ is forced. Suppose by way of contradiction that $p \leq n$. If $p \leq n$, then $p \mid n!$ [WHY?]. But $p \mid n!$ and $p \mid n! - 1$ implies $p \mid n! - (n! - 1)$ which forces $p = 1$. So $p \leq n$ cannot happen. Thus $p > n$ holds. Therefore $n < p < n!$ as desired.

Q.E.D.
Prime Number Proof Exercise 4

Prove that if \( p_1, p_2, \ldots, p_n \) are distinct prime numbers with \( p_1 = 2 \) and \( n > 1 \), then \( p_1 p_2 \cdots p_n + 1 \) can be written in the form \( 4k + 3 \) for some integer \( k \).

**Question 4.29.** Why is \( p_1 p_2 \cdots p_n + 1 \) necessarily odd?

**Answer:** Since \( p_1 \) is even, then \( p_1 p_2 \cdots p_n \) is even and thus it follows that \( p_1 p_2 \cdots p_n + 1 \) is odd.

**Question 4.30.** Why is every odd integer of the form \( 4k + 1 \) or \( 4k + 3 \)
for some \( k \in \mathbb{Z} \)?

**Answer:** SHORT ANSWER: Divide a number by 4 using long division. What do you know of the remainder? LONG ANSWER: (Section 5) The division algorithm asserts that if \( n \in \mathbb{Z} \) then there exists a \( q, r \in \mathbb{Z} \) such that \( n = q4 + r \) where \( 0 \leq r < 4 \). Thus \( n \) odd forces \( r = 1 \) or \( r = 3 \) only.

**Question 4.31.** Consider the numbers \( p_1, p_2, \cdots p_n \) for \( n = 2, 3, 4, 5 \).

<table>
<thead>
<tr>
<th>( n )</th>
<th>( p_1 p_2 \cdots p_n + 1 )</th>
<th>( 4k + 3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>( 2 \cdot 3 + 1 = 7 )</td>
<td>( 4 \cdot 1 + 3 )</td>
</tr>
<tr>
<td>3</td>
<td>( 2 \cdot 3 \cdot 5 + 1 = 31 )</td>
<td>( 4 \cdot 7 + 3 )</td>
</tr>
<tr>
<td>4</td>
<td>( 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211 )</td>
<td>( 4 \cdot 52 + 3 )</td>
</tr>
<tr>
<td>5</td>
<td>( 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311 )</td>
<td>( 4 \cdot 577 + 3 )</td>
</tr>
</tbody>
</table>

**Question 4.32.** Isn’t it totally weird that \( p_1 p_2 \cdots p_n + 1 \) is always in \( 4\mathbb{Z} + 3 \) if \( n \geq 2 \)?

We leave this problem as a HW exercise.
5 Divisibility Theory

5.1 Motivation

Mahāvīra (or Mahāviracharya, “Mahavira the Teacher”) was a 9th-century Jain mathematician from Karnataka, India. Highly respected among Indian mathematicians, he is the author of Ganita Sara Samgraha, the earliest Indian text devoted to mathematics. (Mahaviracharya, 850 A.D.). There are 63 piles of plantain fruit put together and 7 single fruits. They were divided equally among 23 travelers. What is one possible number of fruits in each pile? [We solve this at the end of this section.]

\[
p_1 + p_2 + p_3 + \ldots + p_{63}
\]

\[
x = \text{number of fruits in a pile of plantains}
\]

\[
x = 1 \quad \Rightarrow \quad \text{Does 23 divide } 1 \cdot 63 + 7 = 70 \text{ ?} \quad \text{No}
\]

\[
x = 2 \quad \Rightarrow \quad \text{Does 23 divide } 2 \cdot 63 + 7 = 133 \text{ ?} \quad \text{No}
\]

\[
x = 3 \quad \Rightarrow \quad \text{Does 23 divide } 3 \cdot 63 + 7 = 196 \text{ ?} \quad \text{No}
\]

THE GOAL: We seek a positive integer \( x \) such that 23 divides \( 63x + 7 \).
5.2 Divisibility

To understand divisibility theory, we must first understand what divisibility is.

**Definition 5.1.** A nonzero integer \( d \) divides \( n \) (symbolically \( d \mid n \)) if and only if there exists a \( k \in \mathbb{Z} \) such that \( n = d \cdot k \). Equivalently,

\[
d \mid n \iff n \text{ is a multiple of } d
\iff d \text{ is a factor of } n
\iff d \text{ is a divisor of } n
\]

We say \( n \) is **divisible** by \( d \). A positive divisor that is not \( n \) itself is called a **proper divisor** of \( n \).

This leads to a well-known definition that is based on divisibility.

**Definition 5.2.** An integer \( n \) is **even** if 2 divides \( n \); otherwise \( n \) is **odd**.

---

**Some Obvious But Important Results on the Arithmetic of Even and Odd Integers**

**Lemma 5.3.** The following results hold on the sets \( 2\mathbb{Z} \) and \( 2\mathbb{Z} + 1 \).

(i) \( 2\mathbb{Z} \) is closed under addition, subtraction, and multiplication.

(ii) \( x, y \in 2\mathbb{Z} + 1 \implies x + y \in 2\mathbb{Z} + 1 \).

(iii) \( x, y \in 2\mathbb{Z} + 1 \implies xy \in 2\mathbb{Z} + 1 \).  \([\text{Let’s prove this one on the board.}]\)

(iv) \( x \in 2\mathbb{Z} \text{ and } y \in 2\mathbb{Z} + 1 \implies xy \in 2\mathbb{Z} \).

(v) \( x \in 2\mathbb{Z} \text{ and } y \in 2\mathbb{Z} + 1 \implies x + y \in 2\mathbb{Z} + 1 \).

(vi) \( x \in 2\mathbb{Z} \text{ and } y \in 2\mathbb{Z} + 1 \implies x - y \in 2\mathbb{Z} + 1 \text{ and } x - y \in 2\mathbb{Z} + 1 \).
A Simple Divisibility Proof

Use Lemma 5.3 on the previous page to prove the theorem below.

Theorem 5.4. If $a$ is even and $b$ is odd, then $\frac{a^2+b^2+1}{2}$ is an integer.

Proof. Assume $a$ is even and $b$ is odd.

\[ \text{WWTS: } \frac{a^2+b^2+1}{2} \text{ is an integer.} \]

It suffices to show that $a^2 + b^2 + 1$ is divisible by 2. Since $a$ is even, then $a^2$ is even by part (i) of the lemma. Since $b$ is odd, then $b^2$ is odd by part (iii) of the lemma. Hence $a^2 + b^2$ is odd by part (v) of the lemma. Therefore adding 1, we get $a^2 + b^2 + 1$ is even, and hence divisible by 2. And we conclude that $\frac{a^2+b^2+1}{2}$ is an integer.

Q.E.D.

A Very Not Simple Divisibility Proof

EXERCISE: Prove that 19 divides $2^{6k+2} + 3$ for all $k = 0, 1, 2, \ldots$

What makes this problem challenging?

As $k$ increases, the numbers $2^{6k+2} + 3$ get FREAKISHLY LARGE very fast.

$k = 0 \implies 2^{6k+2} + 3 = 2^2 + 3 = 2^4 + 3 = 19.$

And the claim holds for $k = 0$. But consider what happens when $k = 1$:

$2^{6k+2} + 3 = 2^{6\cdot1+2} + 3 = 2^8 + 3 = 2^{256} + 3.$

Using Mathematica software, we find that this is a number with 78 digits; it is the following number:


We leave this proof as an EXAM problem.
A Somewhat Easier Problem than the Previous One, but Still Highly Non-Trivial

**EXERCISE:** Prove that 7 divides $1^{47} + 2^{47} + 3^{47} + 4^{47} + 5^{47} + 6^{47}$.

It is helpful to first prove the following lemma.

**Lemma 5.5.** If $n$ is an odd positive integer, then the following holds

$$r + s \text{ divides } r^n + s^n.$$

We leave these proofs also as EXAM problems.

Some More Divisibility Problems

Ahhhhh, yes, it’s the famous divisibility by 9 trick!! We all learn this “cheat” when we are young. There are many other “cheats” too. Turn the page!

**Question 5.6.** Is $987,654,321$ divisible by 9? Why or why not?
Divisibility Rules

An integer $n$ is divisible: [Fill in the Rule and give nontrivial examples (i.e., not $n$ itself)]

- by 2 if \text{its last digit is even.}
  \[ 2 \mid 58 \text{ but } 2 \nmid 67. \]

- by 3 if \text{the sum of its digits is a multiple of 3.}
  \[ 3 \mid 28,554 \text{ since } 2 + 8 + 5 + 5 + 4 = 24 \text{ and } 3 \mid 24. \]

- by 4 if \text{its last two digits form a number that is a multiple of 4.}
  \[ 4 \mid 756 \text{ because } 4 \mid 56. \]

- by 5 if \text{its last digit is a 0 or a 5.}
  \[ 5 \mid 85 \text{ but } 5 \nmid 84. \]

- by 6 if \text{it is passes the 2 and 3 divisibility checks.}
  \[ 6 \mid 6,498 \text{ since it is even and } 3 \mid 6 + 4 + 9 + 8 = 27. \]

- by 8 if \text{its last three digits form a number that is a multiple of 8.}
  \[ 8 \mid 4,895,064 \text{ since } 8 \mid 064 = 64. \]

- by 9 if \text{the sum of its digits is a multiple of 9.}
  \[ 9 \mid 4,895,064 \text{ since } 9 \mid 4 + 8 + 9 + 5 + 0 + 6 + 4 = 36. \]

- by 10 if \text{its last digit is 0.}
  \[ 567,890 \text{ is divisible by 10 but } 98,765 \text{ is not.} \]

- by 11 if \text{the reverse alternating sum of its digits is a multiple of 11.}
  \[ 11 \mid 8,470,803 \text{ since } 3 - 0 + 8 - 0 + 7 - 4 + 8 = 22 \text{ is a multiple of 11.} \]
Is There a Divisibility Rule for 7?

**QUESTION:** Is 1764 divisible by 7? Let’s “discover” the 7-divisibility rule.

- Write 1764 in its decimal representation (see Definition 5.7 below) as
  
  \[(1 \times 10^3) + (7 \times 10^2) + (6 \times 10^1) + (4 \times 1).\]

- We claim 1764 is divisible by 7 if and only if
  
  \[(1 \times 3^3) + (7 \times 3^2) + (6 \times 3^1) + (4 \times 1).\]

  [Verify that 7 divides the sum above!]

- Similarly we could have checked the divisibility of 112 by the same means:

  \[
  7 \mid (1 \times 10^2) + (1 \times 10^1) + (2 \times 1) \iff 7 \mid (1 \times 3^2) + (1 \times 3^1) + (2 \times 1).
  \]

  [Perform the highly trivial verification!]

---

**Conjecture for the Divisibility by 7 Rule**

The following definition may be helpful first.

**Definition 5.7.** The **decimal representation** of a positive integer \(n\) having \(r+1\) decimal places for some \(r \geq 0\) is \(n = n_r n_{r-1} \ldots n_2 n_1 n_0\). Then we can write

\[
n = (n_r \times 10^r) + (n_{r-1} \times 10^{r-1}) + \cdots + (n_2 \times 10^2) + (n_1 \times 10^1) + (n_0 \times 10^0).
\]

**YOUR CONJECTURE:** The number \(n = n_r n_{r-1} \ldots n_2 n_1 n_0\) written in decimal representation is divisible by 7 if and only if [You Finish!]

\[
(n_r \times 3^r) + (n_{r-1} \times 3^{r-1}) + \cdots + (n_2 \times 3^2) + (n_1 \times 3^1) + (n_0 \times 3^0)
\]

is divisible by 7.

Congruence Theory in the future Section 6 will help us prove this conjecture.
Divisibility Properties

The rule for divisibility by 6 illustrates a basic result about divisibility in general (this is Corollary 5.25 which you prove in HW):

If \( n \) is divisible by \( a \) and \( b \) with \( \gcd(a, b) = 1 \) (that is, \( a \) and \( b \) are relatively prime), then \( n \) is divisible by \( ab \).

Thus if \( n \) is divisible by both 2 and 3, then \( n \) is divisible by \( 2 \cdot 3 = 6 \). This result is true only if \( a \) and \( b \) have no common divisors (other than 1). For example, 20 is divisible by both 2 and 4, but 20 is not divisible by \( 2 \cdot 4 = 8 \). This leads to some more general properties of divisibility.

**Divisibility Properties**

The following divisibility properties hold:

- If \( a \mid b \) and \( a \mid c \), then for any integers \( m \) and \( n \) we have \( a \mid (mb + nc) \).
- If \( n \neq 0 \), then \( an \mid bn \) if and only if \( a \mid b \).
- If \( a \mid b \) and \( b \mid c \), then \( a \mid c \).
- If \( a \mid b \) and \( b \mid a \), then \( a = \pm b \).

---

What is the Opposite of Divisible?
5.3 The Division Algorithm

The following theorem is SUPER fundamental to the foundations of number theory, so we place it in an “IMPORTANT BOX”!!

**Theorem 5.8** (Division Algorithm). Given integers \( a \) and \( b \), with \( b > 0 \), there exist unique integers \( q \) and \( r \) satisfying

\[ a = qb + r \quad \text{such that} \quad 0 \leq r < b. \]

**Definition 5.9.** The integers \( q \) and \( r \) in the division algorithm are called, respectively, the **quotient** and **remainder** in the division of \( a \) by \( b \).

However, \( b \) does not have to be positive. If we get rid of the restriction that \( b > 0 \), then we have the following corollary.

**Corollary 5.10.** If \( a \) and \( b \) are integers with \( b \neq 0 \), then there exist unique integers \( q \) and \( r \) satisfying

\[ a = qb + r \quad 0 \leq r < |b|. \]

**Example 5.11.** Let us take \( b = -4 \). Then let us pick \( a = 34 \), \( 23 \), \( -23 \).

Using the division algorithm, we have

\[
\begin{align*}
34 & = -8 \cdot (-4) + 2 \\
23 & = -5 \cdot (-4) + 3 \\
-23 & = 6 \cdot (-4) + 1
\end{align*}
\]

**Question 5.12.** Why do we care about the division algorithm?

The division algorithm allows us to prove assertions about all of the integers by only considering a finite number of cases! (Recall Theorem 1.23 in Section 1)
5.4 GCD and LCM

**Question 5.13.** What happens when the remainder \( r \) in the division algorithm turns out to be zero?

Hmm... this looks familiar to our definition of divisibility (see Definition 5.1)!

**Definition 5.14.** Let \( a \) and \( b \) be given integers with at least one of them different from zero. The **greatest common divisor** of \( a \) and \( b \), denoted \( \gcd(a,b) \), is the positive integer \( d \) satisfying the following:

- \( d \mid a \) and \( d \mid b \)
- If \( c \mid a \) and \( c \mid b \), then \( c \leq d \).

**Definition 5.15.** If the \( \gcd(a, b) = 1 \), then \( a \) and \( b \) are **relatively prime**.

**REMARK:** In Corollary 5.24, we will give a criterion for relative primality of two integers \( a \) and \( b \) (not both zero): \( a \) and \( b \) are relatively prime if and only if there exists integers \( x \) and \( y \) such that \( 1 = ax + by \).

**Definition 5.16.** The **least common multiple** of two nonzero integers \( a \) and \( b \), denoted \( \text{lcm}(a, b) \), is the positive integer \( m \) satisfying the following:

- \( a \mid m \) and \( b \mid m \)
- If \( a \mid c \) and \( b \mid c \), with \( c > 0 \), then \( m \leq c \).
Using Factor Trees

Example 5.17. Find the lcm of 81, 231, and 3465.

First, let us start by creating a factor tree for each number.

![Factor Trees](image)

Prime Factors

<table>
<thead>
<tr>
<th></th>
<th>3</th>
<th>3</th>
<th>3</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>81</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>231</td>
<td>3</td>
<td>7</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>3465</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>11</td>
</tr>
</tbody>
</table>

\[\text{LCM} = 3 \times 3 \times 3 \times 3 \times 5 \times 7 \times 11 = 31,185\]
5.5 The Euclidean Algorithm and Bézout’s Identity

**Question 5.18. Who is Euclid?**

- Euclid (around 300 B.C.), Greece
- The “father of geometry”
- Deduced theorems of Euclidean geometry
- Little is known about his life, and few references of his work have survived

- “The laws of nature are but the mathematical thoughts of God.” - Euclid
- “If Euclid failed to kindle your youthful enthusiasm, then you were not born to be a scientific thinker.” - Albert Einstein

**Definition 5.19.** The **Euclidean Algorithm** is a method for computing gcd($a, b$) (suppose for simplicity that $a \geq b > 0$ since gcd($|a|, |b|$) = gcd($a, b$), we do not lose generality). Note that by the **Division Algorithm**, we know we can write

\[
\begin{align*}
a &= q_0 b + r_1 & 0 < r_1 < b \\
b &= q_1 r_1 + r_2 & 0 < r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3 & 0 < r_3 < r_2 \\
r_2 &= q_3 r_3 + r_4 & 0 < r_4 < r_3 \\
& \vdots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n & 0 < r_n < r_{n-1} \\
r_{n-1} &= q_n r_n + 0.
\end{align*}
\]

The process terminates because $r_1 < b$, so $r_1 \leq b - 1$. Then $r_2 < r_1$, so $r_2 \leq b - 2$, and so on. Since the numbers are decreasing and they are positive integers, at some point the process cannot continue (i.e., you reach 0).

**FACT:** The last nonzero remainder $r_n$ is equal to the gcd($a, b$).
Example 5.20. Compute gcd(1767, 11571).

\[
\begin{align*}
11571 &= 6 \cdot 1767 + 969 \\
1767 &= 1 \cdot 969 + 798 \\
969 &= 1 \cdot 798 + 171 \\
798 &= 4 \cdot 171 + 114 \\
171 &= 1 \cdot 114 + 57 \\
114 &= 2 \cdot 57
\end{align*}
\]

Hence gcd(1767, 11571) = 57.

Example 5.21. Compute gcd(15, 49) using the Euclidean algorithm. [You Do!]

\[
\begin{align*}
49 &= 3 \cdot 15 + 4 \\
15 &= 3 \cdot 4 + 3 \\
4 &= 1 \cdot 3 + 1 \\
3 &= 3 \cdot 1 + 0
\end{align*}
\]

Hence gcd(15, 49) = 1.

**QUESTION:** Can we write gcd(15, 49) as a linear combination of a and b?

For example, one might be able get lucky and observe that

- $4 \times 49 = 196$ and $-13 \times 15 = -195$
- Hence $1 = 15 \cdot (-13) + 49 \cdot 4$.

But there MUST be a better way other than getting lucky to find integers $x$ and $y$ such that $1 = 15x + 49y$.

**ANSWER:** Bézout’s Identity will SAVE THE DAY!!!
Bézout’s Identity

Question 5.22. Who is Bézout?

- Étienne Bézout (1730—1783), France
- Famed for being a writer of textbooks
- He also did important work on the use of determinants in solving equations
- He married young and happily and was also a father

Like the division algorithm, the following theorem is also SUPER fundamental to the foundations of number theory, so we place it in an “IMPORTANT BOX”!!

Theorem 5.23 (Bézout’s Identity). For any integers $a, b$ (not both zero), there exist integers $x$ and $y$ such that

$$\text{gcd}(a, b) = ax + by$$

(that is, the gcd of $a$ and $b$ can be written as a linear combination of $a$ and $b$). Moreover, $\text{gcd}(a, b)$ is the smallest positive integer that can be expressed in this form.

**QUESTION:** What is the $\text{gcd}(12, 30)$? **ANSWER:** $6$

Can you write this gcd as a linear combination of 12 and 30?

$$\text{gcd}(12, 30) = 6 = 12 \cdot (-2) + 30 \cdot 1$$

This is not always an easy task. For example, $\text{gcd}(172, 20) = 4$. But could you have guessed easily that $4 = 172 \cdot 2 + 20 \cdot (-17)$. In Exercise 1 at the end of the section, we will find a nice way to do this.
Proof of Bézout’s Identity

First we need recall the very important axiom we first encountered in the previous section. This was Axiom 4.15 called the Well-Ordering Principle.

**Well Ordering Principle**

Every non-empty set $S$ of positive integers contains a least element. That is, there exists an $a \in S$ such that $a \leq b$ for all $b \in S$.

We first restate Bézout’s Identity, and then write a proof below it.

**Theorem** (Bézout’s Identity). For any integers $a, b$ (not both zero), there exist integers $x$ and $y$ such that $\gcd(a, b) = ax + by$. Moreover, $\gcd(a, b)$ is the smallest positive integer that can be expressed in this form.

**Proof.** Given any nonzero integers $a$ and $b$, define a set $S$ as follows:

$$S := \{ax + by \mid x, y \in \mathbb{Z} \text{ and } ax + by > 0\}.$$ 

The set $S$ is nonempty since it contains $a$ or $-a$ [WHY? - choose $x = \pm 1$ and $y = 0$ so that $ax + by > 0$]. By WOP, $S$ has a least element--call it $d$. So $d = as + bt$ for some $s, t \in \mathbb{Z}$. We claim that $d$ equals $\gcd(a, b)$.

**WWTS:** $d \mid a$ and $d \mid b$, and if $\exists c \text{ s.t. } c \mid a$ and $c \mid b$, then $c \leq d$.

By the division algorithm on $a$ and $d$, we know there exists $q, r \in \mathbb{Z}$ such that $a = dq + r$ with $0 \leq r < d$. The remainder $r$ is in $S \cup \{0\}$ because

$$r = a - qd = a - q(as + bt) = a \cdot (1 - qs) - b \cdot qt.$$ 

As $d$ is the smallest positive integer in $S$, then $r = 0$ and hence $d \mid a$. By analogous reasoning, we can show $d \mid b$. Now suppose that $c$ is another common divisor of $a$ and $b$. Then $a = cu$ and $b = cv$ for some $u, v \in \mathbb{Z}$. Thus we have

$$d = as + bt = cu \cdot s + cv \cdot t = c \cdot (us + vt)$$

implies $c \mid d$ and hence $c \leq d$.

**Q.E.D.**
Corollary 5.24. Let $a$ and $b$ be integers (not both zero). Then $a$ and $b$ are relatively prime if and only if there exists integers $x$ and $y$ such that $1 = ax + by$.

We prove this in Exercise 3 at the section’s end.

Corollary 5.25. Prove that if $m | x$ and $n | x$ and $\text{gcd}(m, n) = 1$, then $mn | x$.

We leave this proof as a HW exercise.

Ponder on This!

EXERCISE: Use Corollary 5.25 above to prove that the product of any three consecutive integers is divisible by 6. [You Do!]

PROOF SKETCH: Consider the integers $a$, $a + 1$, and $a + 2$. At least one integer is even, and exactly one integer is divisible by three [WHY?]. Hence the product $N = a_1 \cdot a_2 \cdot a_3$ is divisible by both 2 and 3. Thus $6 \mid N$ by the corollary.

EXERCISE: Use Corollary 5.25 above to prove that the product of any four consecutive integers is divisible by 24. [You Do!]

PROOF SKETCH: Consider the integers $a$, $a + 1$, $a + 2$, and $a + 3$. One integer $a + j$ is even (but not divisible by 4) for some $0 \leq j \leq 3$, and exactly one other integer different than $a + j$ is divisible by 4 [WHY?]. Also at least one is divisible by 3. Hence the product $N = a_1 \cdot a_2 \cdot a_3 \cdot a_4$ is divisible by both 8 and 3. Thus $24 \mid N$ by the corollary.

YOUR CONJECTURE: Conjecture a general statement for the product of $n$ consecutive integers, $N = \prod_{i=0}^{n-1} a + i$.

$N$ is divisible by $n!$.³¹

³¹Mathematician Tim Gowers has much to say on this theorem and its proof. See his blog entry at the website https://gowers.wordpress.com/2010/09/18/are-these-the-same-proof/. Many other famous mathematicians like Terence Tao, Gil Kalai, Igor Pak, and others left comments on this blog entry.
5.6 The Diophantine Equation

Definition 5.26. A **Diophantine equation** is any equation with one or more unknowns whose solution is an integer.

Question 5.27. *Who is Diophantus?*

- Diophantus (210—294), Greece
- The “father of algebra”
- He was the first Greek mathematician to recognize fractions as numbers
- He was the first person known to use algebraic notation and symbolism

The simplest type of Diophantine equation is the linear Diophantine equation $ax + by = c$, which has two unknowns. A given linear Diophantine equation can have a number of solutions, but can also have no solution.

Question 5.28. *How do we know if a linear Diophantine equation has a solution?*

This leads us to the next theorem.

Theorem 5.29. The linear Diophantine equation $ax + by = c$ has a solution if and only if $d | c$, where $d = \gcd(a, b)$. If $x_0, y_0$ is any particular solution of this equation, then all other solutions are given by

$$x = x_0 + \left(\frac{b}{d}\right) t \quad y = y_0 - \left(\frac{a}{d}\right) t.$$
5.7 Exercises

Diophantine Exercise 1

Find all integer solutions to the equation

\[ 15x + 49y = 8. \]

We need to find \( \text{gcd}(15, 49) \). Recall that in Example 5.21 we used the Euclidean algorithm to find this.

\[
\begin{align*}
49 &= 3 \cdot 15 + 4 \\
15 &= 3 \cdot 4 + 3 \\
4 &= 1 \cdot 3 + 1 \\
3 &= 3 \cdot 1 + 0
\end{align*}
\]

Since \( \text{gcd}(15, 49) = 1 \), this equation will indeed have solutions. (Recall that in general, if \( a \) and \( b \) are relatively prime, then the equation \( ax + by = c \) will have integer solutions.) To find these solutions, we will work our way back up by rewriting each step of the Euclidean algorithm that we used above and substituting it into our expression. So rewriting what we just did above backwards, starting from the second line from the bottom and working our way up will produce:

\[
\begin{align*}
1 &= 4 - 3 \cdot 1 \\
&= 4 - (15 - 3 \cdot 4) \cdot 1 \\
&= 4 \cdot 4 - 1 \cdot 15 \\
&= 4 \cdot (49 - 3 \cdot 15) - 15 \\
&= 15 \cdot (-13) + 49 \cdot 4
\end{align*}
\]

Therefore, the greatest common divisor of 15 and 49 can be written as a linear combination (with integer coefficients) of 15 and 49:

\( 15 \cdot (-13) + 49 \cdot 4 = 1 \quad \text{Yay, Bézout’s Identity holds!} \)

Then, since our original equation has the integer 8 on the right hand side of the equality, we will multiply both sides by 8 giving us

\[ 15 \cdot (-104) + 49 \cdot (32) = 8. \]

So one solution of our original equation is \( x_0 = -104 \) and \( y_0 = 32 \). Therefore, all of the solutions of the equation are given by the formulas

\[ x = -104 + 49t \quad \text{and} \quad y = 32 - 15t \]

for any integer \( t \).
A Graphical View of Exercise 1

The Graphical Diophantine Picture

To solve the Diophantine Equation $ax + by = c$, this amounts to finding the integer solutions $(x, y)$ to the linear equation

$$y = -\frac{a}{b}x + \frac{c}{b}.$$  

[WHY?]

We call this the “Diophantine line” corresponding to $ax + by = n$.

Example 5.30. Recall Exercise 1 on the previous page asked us to find ALL solutions to the Diophantine Equation

$$15x + 49y = 8.$$  

So we found ONE solution at first, namely $(-104, 32)$. But the Diophantine Equation is equivalent to the Diophantine line in $y = mx + b$ form:

$$y = -\frac{15}{49}x + \frac{8}{49}.$$  

So moving according to the slope rules: “rise down 15 units” and “run right 49 units”, we get our next point solution $(-55, 17)$. And repeating this, we get $(−6, 2)$ and then $(43, −13)$, and then $(92, −28)$, etc. Moreover, these latter four points correspond to the points we get if let $t = 1, 2, 3, 4$ in the equations at the bottom of the previous page. Here is an illustration:
Divisibility Exercise 2

Determine all $n$ for which $2^n + 1$ is divisible by 3.

**Hands Dirty Part:** For ease of notation, let $M_n$ denote $2^n + 1$. Let’s compute $M_n$ for the values 1, \ldots, 11.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$M_n$</th>
<th>Does 3</th>
<th>$M_n$?</th>
<th>If so, $M_n = 3 \times$ what?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$2^1 + 1 = 3$</td>
<td>Yes</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>$2^2 + 1 = 5$</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>$2^3 + 1 = 9$</td>
<td>Yes</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>$2^4 + 1 = 17$</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>$2^5 + 1 = 33$</td>
<td>Yes</td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>6</td>
<td>$2^6 + 1 = 65$</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>$2^7 + 1 = 129$</td>
<td>Yes</td>
<td></td>
<td>43</td>
</tr>
<tr>
<td>8</td>
<td>$2^8 + 1 = 257$</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>$2^9 + 1 = 513$</td>
<td>Yes</td>
<td></td>
<td>171</td>
</tr>
<tr>
<td>10</td>
<td>$2^{10} + 1 = 1025$</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>$2^{11} + 1 = 2049$</td>
<td>Yes</td>
<td></td>
<td>684</td>
</tr>
</tbody>
</table>

**YOUR CONJECTURE:** What do you conjecture is happening here?

[You Do!]

- When $n$ is odd, then 3 divides $M_n$.
- When $n$ is even, then 3 does not divide $M_n$.

We leave this proof as a HW exercise.\footnote{We will eventually learn a \textit{VERY} slick way to prove our conjectures, but that will require congruence theory. In the divisibility HW, you are NOT allowed to use congruence theory to solve this problem!}
Important Corollary to Bézout’s Identity

Exercise 3

First we recall the statement of Corollary 5.24:

Corollary 5.24. Let \( a \) and \( b \) be integers (not both zero). Then \( a \) and \( b \) are relatively prime if and only if there exists integers \( x \) and \( y \) such that \( 1 = ax + by \).

Proof. Assume that \( a \) and \( b \) are integers (not both zero).

\((\implies)\) Suppose that \( a \) and \( b \) are relatively prime. [You Finish]

\[ \text{WWTS: } \exists x, y \in \mathbb{Z} \text{ s.t. } 1 = ax + by. \]

Since \( a \) and \( b \) are relatively prime, then \( \gcd(a, b) = 1 \) by definition. By Bézout’s Identity, we know then that there exists integers \( x \) and \( y \) such that \( 1 = \gcd(a, b) = ax + by \) as desired.

\((\iff)\) Suppose there exists integers \( x \) and \( y \) such that \( 1 = ax + by \). [You Finish]

\[ \text{WWTS: } \exists x, y \in \mathbb{Z} \text{ s.t. } 1 = ax + by. \]

Let \( d = \gcd(a, b) \). Then by definition of \( \gcd \), we know that \( d \mid a \) and \( d \mid b \). In particular, by Proof Problem 2 in the Divisibility HW, we know that \( d \mid ax + by \). But by assumption, \( ax + by = 1 \). So \( d \mid 1 \). That forces \( d = 1 \) [Why can’t \( d = -1 \)?]. Thus \( 1 = \gcd(a, b) \), and hence by definition \( a \) and \( b \) are relatively prime as desired.

Q.E.D.

\[ \text{33In completing this direction, you may assume the following is true. If } d \in \mathbb{Z} \text{ such that } d \mid a \text{ and } d \mid b, \text{ then } d \mid (ax + by) \text{ for any integers } x, y. \text{ This is Proof Problem 2 in the Divisibility HW} \]
Plantain Diophantine Exercise 4

First let us recall the Mahaviracharya’s problem from 850 A.D.:

There are 63 piles of plantain fruit put together and 7 single fruits. They were divided equally among 23 travelers. What is one possible number of fruits in each plantain fruit pile?

We seek an \( x \in \mathbb{N} \) such that 23 divides \( x \cdot 63 + 7 \). [Why?] It may be helpful to go back to Subsection 5.1 and review why this is so.

CLAIM: It suffices to solve \( 23y = 63x + 7 \), or equivalently, the Diophantine equation \( -63x + 23y = 7 \). NOTE: We care only for the \( x \)-solution.

SOLUTION: [You Do!] First we do the Euclidean Algorithm to find \( \gcd(-63, 23) \).

\[
-63 = -3 \cdot 23 + 6 \\
23 = 3 \cdot 6 + 5 \\
6 = 1 \cdot 5 + 1 \\
5 = 5 \cdot 1 + 0,
\]

and hence \( \gcd(-63, 23) = 1 \). Now we show Bézout’s Identity holds by running Euclid’s algorithm backwards.

\[
1 = 6 - 1 \cdot 5 \\
= 6 - 1 \cdot (23 - 3 \cdot 6) \\
= 6 - 23 + 3 \cdot 6 \\
= 4 \cdot 6 - 23 \\
= 4(-63 + 3 \cdot 23) - 23 \\
= 4(-63) + 12 \cdot 23 - 1 \\
= 4(-63) + 11(23)
\]

Thus \(-63(4)+23(11) = 1\). Multiplying by 7, we get \(-63(28)+23(77) = 7\). Hence \( x = 28 \) is one solution for the possible number of fruits in each plantain pile. We confirm this on the top of the next page. ✓
Optional Exercise 5  
Addendum to the Plantain Pile Problem

So we know from the previous exercise that there can be 28 plantains in each of the 63 plantain fruit piles. Hence the 23 people above can each have an equal portion of the total of $28 \times 63 = 1764$ plantains and 7 single other fruits. So there’s a total of $1764 + 7 = 1771$ fruits, and $1771 = 23 \times 77$.

(NOTE: 77 is the $y$-value that we said we didn’t care about.)

Optional Exercise 5: How many ways can we distribute the 1771 fruits amongst the 23 people given that the plantains are indistinguishable from each other?

SOLUTION: Since the plantains all look alike, it suffices to show how many ways we can distribute the 7 other single fruits amongst the 23 people. [You Do!]

HINT: This is a typical stars and bars problem from discrete mathematics. If you do not know this method, then aBa can quickly teach it right now.

This is equivalent to finding all the solutions to the equation

$$x_1 + x_2 + x_3 + \cdots + x_{23} = 7$$

subject to the constraint that $x_i \geq 0$ for each $1 \leq i \leq 23$. There are 7 stars and 22 bars, so the total number of solutions to the equation above is $\binom{29}{7} = 1,560,780$. Hence there are 1,560,780 ways to distribute the 1771 fruits amongst the 23 people. ✓
6 Congruence Theory (a Number Theory Perspective)

6.1 Motivation

Ponder the following VERY HARD questions?

- Consider $1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$. What is this number’s remainder when you divide it by 4?  
  **ANSWER:** 0

- Consider the ridiculously large number $53^{103} + 103^{53}$.  
  **Note:** It is 177 digits long! Is it divisible by 39?  
  **ANSWER:** Yes!

- Consider the even more ridiculously large number $111^{333} + 333^{111}$.  
  **Note:** It is a whopping 682 digits long! Is it divisible by 7?  
  **ANSWER:** Yes!

- (Sun-Tsu, 1st Century A.D.) Find a number that leaves a remainder of 2, 3, and 2 when divided by 3, 5, and 7, respectively.  
  **ANSWER:** T.B.D.

- (Brahmagupta, 7th Century A.D.) Suppose that when eggs in a basket are removed 2, 3, 4, 5, and 6 at a time, there remain 1, 2, 3, 4, and 5 eggs, respectively. But when taken out 7 at a time, none are left over. Find the smallest number of eggs that could have been in the basket.  
  **ANSWER:** 119

All the questions above are a piece of cake with congruence theory. You will find this out perhaps in homework problems!
6.2 Gauss and Congruence Properties

**Question 6.1. Who is Gauss?**

- Carl Friedrich Gauss (1777—1855), German
- This man was an *ABSOLUTE MATH GIANT*! His peers regarded him as *Princeps Mathematicorum* (Prince of Mathematicians), on a par with Archimedes and Isaac Newton.
- In his monumental work *Disquisitiones Arithmeticae*, he introduced a whole new discipline of mathematics with his theory of congruences. He wrote this at age 24.
- In addition to the amazing advances he made in mathematics, his greatest achievement was in theoretical physics, calculating the orbit of the dwarf planet Ceres (between Mars and Jupiter) with amazing accuracy.

"Mathematics is the Queen of the Sciences, and Number Theory is the Queen of Mathematics. She often condescends to render service to astronomy and other natural sciences, but in all relations she is entitled to the first rank." - Gauss

In 1801, Carl Friedrich Gauss introduces the congruence theory in his publication *Disquisitiones Arithmeticae*.

**Definition 6.2.** Let \( n \geq 1 \). Two integers \( a \) and \( b \) are congruent modulo \( n \) if \( n \mid a - b \); that is, \( a - b = kn \) for some \( k \in \mathbb{Z} \). If so, we write \( a \equiv b \pmod{n} \).

**Note:** Any two integers are congruent modulo 1, so generally we only consider \( n > 1 \). For \( n = 2 \), two integers are congruent if and only if they are both odd or both even.

**Example 6.3.** Recalling the division algorithm from Subsection 5.3, for all integers \( a \) and \( b \), with \( b > 0 \), there exists a unique quotient \( q \) and remainder \( r \) such that \( a = qb + r \) and \( 0 \leq r < b \). For example,

\[
5 = 1 \cdot 3 + 2 \quad (8)
\]
\[
-5 = -2 \cdot 3 + 1 \quad (9)
\]

Hence we have the following:
- Equation (8) implies
  \[5 - 2 = 1 \cdot 3 \implies 3 \mid 5 - 2 \implies 5 \equiv 2 \pmod{3}.
  
- Equation (9) implies
  \[(-5) - 1 = -2 \cdot 3 \implies 3 \mid (-5) - 1 \implies -5 \equiv 1 \pmod{3}.

**NOTE:** The relation \(\equiv\) preserves many of the properties that the relation = has. For example, exponentiation is preserved:

- Is \(5^2 \equiv 2^2 \pmod{3}\)?
  Yes since \(5^2 = 25\) and \(2^2 = 4\). So \(25 - 4 = 21\) and \(3 \mid 21\).

- Is \(5^3 \equiv 2^3 \pmod{3}\)? [You verify!]
  Yes since \(5^3 = 125\) and \(2^3 = 8\). So \(125 - 8 = 117\) and \(3 \mid 117\).

It turns out that in general, we have

If \(a \equiv b \pmod{n}\) and \(k \geq 1\), then \(a^k \equiv b^k \pmod{n}\).

We will prove this shortly. For now let us use it to answer the following question.

**Question 6.4.** What is the remainder of the B.I.G. (“big ass number”) \(5^{777}\) when divided by 3?

[You Do!] Observe that \(5 \equiv 2 \pmod{3}\). So we have \(5^{777} \equiv 2^{777} \pmod{3}\). But clearly \(2 \equiv -1 \pmod{3}\) [Why?], and hence \(2^{777} \equiv (-1)^{777} \pmod{3}\) which implies \(2^{777} \equiv -1 \pmod{3}\) [Why?]. Thus we have

\[5^{777} \equiv 2^{777} \pmod{3}\] and \(2^{777} \equiv -1 \pmod{3}\),
So we can conclude \(5^{777} \equiv 2 \pmod{3}\) [Why?].
The divisibility-by-9 rule was given earlier in Section 5, but we are now prepared to rigorously prove the result.

**Theorem 6.5.** An integer \( n \) is divisible by 9 if and and only if the sum of its digits is divisible by 9.

**Proof.** Let \( n \) be an integer. We can assume \( n > 0 \) since 9 divides 0 and a positive integer \( n \) is divisible by \( n \) if and only if \( -n \) is divisible by \( n \). We first write \( n \) in its decimal representation \( n = n_r n_{r-1} \ldots n_2 n_1 n_0 \) presuming \( n \) has \( r + 1 \) decimal places where \( r \geq 0 \). Then we can write

\[
n = (n_r \times 10^r) + (n_{r-1} \times 10^{r-1}) + \cdots + (n_2 \times 10^2) + (n_1 \times 10^1) + (n_0 \times 10^0).
\]

Observe that \( 10 \equiv 1 \pmod{9} \) [Why?]. And hence \( 10^k \equiv 1^k = 1 \pmod{9} \) for all \( k \geq 0 \). Applying congruence modulo 9 to both sides of the decimal representation of \( n \) above we get

\[
n \equiv (n_r \times 1^r) + (n_{r-1} \times 1^{r-1}) + \cdots + (n_2 \times 1^2) + (n_1 \times 1) + n_0 \pmod{9} \quad \text{[Why?]}
\]

\[
\equiv n_r + n_{r-1} + \cdots + n_2 + n_1 + n_0 \pmod{9}.
\]

Therefore we conclude that

\[
9 \text{ divides } n \iff 9 \text{ divides } \sum_{i=0}^{r} n_i \quad \text{[Why?]}
\]

as desired.

\[Q.E.D.\]

Let’s take a wee break and listen to the Count sing about the number of the day, which is 9. Click the link below:

[https://www.youtube.com/watch?v=25SsCCCGwz8](https://www.youtube.com/watch?v=25SsCCCGwz8)
Some Important Properties of $\equiv (\text{mod } n)$

**Similarities between the symbols $=$ and $\equiv (\text{mod } n)$**

**Remark 6.6.** Many of the properties of the equal symbol, $=$, which you are familiar with still hold in the setting of the congruence modulo $n$ symbol, $\equiv (\text{mod } n)$. This is because both symbols denote something we call an equivalence relation. Which we will explore soon. The first three properties below, in particular, guarantee that $\equiv (\text{mod } n)$ is indeed an equivalence relation.

**Theorem 6.7.** Let $n, a, b, c, d \in \mathbb{Z}$ with $n > 1$. The following properties hold:

(i) **(Reflexive Property)**

$$a \equiv a \ (\text{mod } n)$$

(ii) **(Symmetric Property)**

$$a \equiv b \ (\text{mod } n) \quad \text{implies} \quad b \equiv a \ (\text{mod } n)$$

(iii) **(Transitive Property)**

$$a \equiv b \ (\text{mod } n) \quad \text{and} \quad b \equiv c \ (\text{mod } n) \quad \text{implies} \quad a \equiv c \ (\text{mod } n)$$

(iv) **(“Adding or Multiplying Two Congruences” Property)**

$$a \equiv b \ (\text{mod } n) \quad \text{and} \quad c \equiv d \ (\text{mod } n) \quad \text{implies} \quad \begin{cases} 
  a + c \equiv b + d \ (\text{mod } n) \\
  ac \equiv bd \ (\text{mod } n)
\end{cases}$$

(v) **(“Adding or Multiplying a Number to a Congruence” Property)**

$$a \equiv b \ (\text{mod } n) \quad \text{implies} \quad a + c \equiv b + c \ (\text{mod } n) \quad \text{and} \quad ac \equiv bc \ (\text{mod } n)$$

(vi) **(“Exponentiation of a Congruence” Property)**

$$a \equiv b \ (\text{mod } n) \quad \text{implies} \quad a^k \equiv b^k \ (\text{mod } n) \quad \text{for all } k \geq 1$$
More Important Properties of $\equiv (\mod n)$

Cancellation Property for Congruences?

**QUESTION:** The multiplication part of property (v) on the previous page states

$$a \equiv b \pmod{n} \implies ac \equiv bc \pmod{n}.$$ 

Does the converse hold? For example, $18 \equiv 12 \pmod{6}$ clearly holds. But can we cancel 3s and conclude $6 \equiv 4 \pmod{6}$?

**ANSWER:** Certainly not, but it is true that $6 \equiv 4 \pmod{2}$. This leads to a more general theorem

Let $a, b, c, n \in \mathbb{N}$ such that $ac \equiv bc \pmod{n}$ and $d = \gcd(c, n)$. Then $a \equiv b \pmod{n/d}$.

The following theorem will have a very simple proof once we learn about inverses modulo $n$. [Why?] $\gcd(c, n) = 1 \implies \exists c^{-1}$ such that $cc^{-1} \equiv 1 \pmod{n}$

**Theorem 6.8.** Let $a, b, c, n \in \mathbb{N}$ such that $ac \equiv bc \pmod{n}$ and $\gcd(c, n) = 1$. Then $a \equiv b \pmod{n}$.

**Theorem 6.9.** Let $m_1, m_2, \ldots, m_r \in \mathbb{N}$. Then following are equivalent.

(i) $a \equiv b \pmod{m_i}$ for $i = 1, 2, \ldots, r$.

(ii) $a \equiv b \pmod{n}$ where $n = \text{lcm}(m_1, m_2, \ldots, m_r)$.

**Proof.** Let $m_1, m_2, \ldots, m_r \in \mathbb{N}$ and set $n = \text{lcm}(m_1, m_2, \ldots, m_r)$. Then we have

$$a \equiv b \pmod{m_i} \text{ for all } i \iff m_i \mid a - b \text{ for all } i$$

$$\iff n \mid a - b$$

$$\iff a \equiv b \pmod{n}. \quad \text{See footnote}^{34}$$

Thus the claim holds.

Q.E.D.

---

$^{34}$This “if and only if” is a homework problem in the Divisibility Homework Set.
Theorem 6.9 can be useful by taking one linear congruence and changing it to a system of smaller congruences.

Solve $5x \equiv 9 \pmod{666}$.

**EXERCISE:** Use Theorem 6.9 to change the linear congruence into a system of three easier to handle congruences. [You Do!]

**SOLUTION:** Prime factorization of 666 is $2 \cdot 3^2 \cdot 37$, and $\text{lcm}(2, 3^2, 37) = 666$. By Theorem 6.9, the congruence $5x \equiv 9 \pmod{666}$ is equivalent to

$$
\begin{cases}
5x \equiv 9 \pmod{2} \\
5x \equiv 9 \pmod{3^2} \\
5x \equiv 9 \pmod{37}
\end{cases}
$$

But we can say that this is equivalent to [You Finish!]

$$
\begin{cases}
x \equiv 1 \pmod{2} \quad [\text{WHY?}] \\
5x \equiv 0 \pmod{3^2} \quad [\text{WHY?}] \\
5x \equiv 9 \pmod{37}
\end{cases}
$$

The first congruence says that $x$ is odd [WHY?]. And the second congruence says that $9 \mid 5x$, and hence $9 \mid x$ [WHY?]. Hence, so far we know that $x = 9J$ for some $J \notin 2\mathbb{Z}$. Substituting this into the third congruence gives

$$5 \cdot 9J \equiv 9 \pmod{37} \implies 5J \equiv 1 \pmod{37}$$

since $\gcd(9, 37) = 1$ allows us to cancel the 9s by the cancellation theorem (Theorem 6.8). This last congruence will be EASY to solve by methods in the next subsection. For now, just verify the $J = 15$ works [You Do!].

We conclude that $x = 9J = 9 \cdot 15 = 135$ is the desired solution to the original system [You Verify!].
6.3 Solving Linear Congruences

Recall the good ole days of high school algebra.

Now for the number theory analogue in this course . . .

Example 6.10. Verify that 6, 13, and 20 are all valid solutions [You Do!].

\[
\begin{align*}
x = 6 & \implies 6x = 6 \cdot 6 = 36 = 1 \cdot 21 + 15 \equiv 15 \pmod{21} \\
x = 13 & \implies 6x = 6 \cdot 13 = 78 = 3 \cdot 21 + 15 \equiv 15 \pmod{21} \\
x = 20 & \implies 6x = 6 \cdot 20 = 120 = 5 \cdot 21 + 15 \equiv 15 \pmod{21}
\end{align*}
\]
Section 6  CONGRUENCE THEORY (A NUMBER THEORY PERSPECTIVE)  Page 149

When a Linear Congruence Has a Solution

First we recall an important theorem on a necessary and sufficient condition for a Diophantine equation to have a solution. We change the names of some of the variables as written in Theorem 5.29 and rewrite that theorem as follows

**Theorem 6.11.** The linear Diophantine equation \( ar + ns = b \) has a solution \((r, s)\) if and only if \( d | b \) where \( d = \gcd(a, n) \).

**Theorem 6.12.** The linear congruence \( ax \equiv b \pmod{n} \) has a solution if and only if \( d | b \) where \( d = \gcd(a, n) \).

**Proof.**

(\(\implies\)) Assume that the linear congruence \( ax \equiv b \pmod{n} \) has a solution. Denote this solution \( x_0 \).

\[
\text{WWTS: } d | b \text{ where } d = \gcd(a, n)
\]

Observe that

\[
ax \equiv b \pmod{n} \implies ax - b = nk \text{ for some } k \in \mathbb{Z} \implies ax - nk = b.
\]

So the Diophantine equation \( ar + ns = b \) has solution \((r, s)\) if we set \( r := x_0 \) and \( s := k \). But by Theorem 6.11, we conclude \( d | b \) where \( d = \gcd(a, n) \) as desired.

(\(\impliedby\)) Suppose \( d | b \) where \( d = \gcd(a, n) \).

\[
\text{WWTS: } ax \equiv b \pmod{n} \text{ has a solution.}
\]

Since \( d | b \) then by Theorem 6.11, \( ar + ns = b \) has a solution—call it \((r, s) = (r_0, s_0)\). Then \( ar_0 + ns_0 = b \implies ar_0 - b = n(-s_0) \). That implies \( ar_0 \equiv b \pmod{n} \) so \( ax \equiv b \pmod{n} \) has a solution.

Q.E.D.
**Mutually Incongruent Solutions**

**Remark 6.13.** If \( d \mid b \), then \( ax \equiv b \pmod{n} \) has \( d \) mutually incongruent solutions modulo \( n \).

**EXERCISE:** Verify that the remark above holds in Example 6.10–the problem of solving the linear congruence \( 6x \equiv 15 \pmod{21} \). [**You Do!**]

**SOLUTION:** Since \( d = \gcd(a,n) \), then in our case \( d = \gcd(6,21) = 3 \). And yes, \( 6x \equiv 15 \pmod{21} \) has 3 mutually incongruent solutions.

---

**How to solve the linear congruence** \( ax \equiv b \pmod{n} \)

Recall the image two pages ago:

We solved the equation by first finding the inverse of 6 and then multiplying it on both sides of the equality \( 6x = 15 \) to get \( x \) alone on the left hand side.

**QUESTION:** Can we use the SAME EXACT reasoning as above to solve \( 6x \equiv 15 \pmod{21} \)? **Hint:** does 6 have an inverse modulo 21? That is, does there exist a number \( t \) such that \( 6t \equiv 1 \pmod{21} \)?

**ANSWER:** The inverse does not exist. But how do we know this? [**You Do!**]

Recall \( ax \equiv b \pmod{n} \) has a solution if and only if \( \gcd(a,n) \mid b \). For \( 6t \equiv 1 \pmod{21} \) to have a solution, \( \gcd(6,21) \) must divide 1. But that is impossible. Hence 6 has no inverse modulo 21.

**BOTTOMLINE:** \( ax \equiv b \pmod{n} \) can have a solution WITHOUT there existing an inverse of \( a \) modulo \( n \).
How to solve $ax \equiv b \pmod{n}$ (continued)

The five steps to solve $6x \equiv 15 \pmod{21}$:

1. First verify $\gcd(6, 21)$ divides 15, otherwise there are no solutions. [You Do!]

   It is clear $\gcd(6, 21) = 3$ and divides 15. ✓

2. Convert $6x \equiv 15 \pmod{21}$ to a Diophantine equation. [You Do!]

   $6x \equiv 15 \pmod{21} \implies 6x - 15 = 21$ for some $y \in \mathbb{Z}$
   \[ \implies 6x + 21(-y) = 15 \]

   The latter is our Diophantine equation.

3. Use the Euclidean algorithm to compute $\gcd(6, 21)$. [You Do!]

   
   $21 = 3 \cdot 6 + 3$
   $6 = 2 \cdot 3$.

   So $\gcd(6, 21) = 3$.

4. Run Euclid’s algorithm backwards to attain values $r, s \in \mathbb{Z}$ such that Bézout’s Identity holds: $\gcd(6, 21) = 6r + 21s$. [You Do!]

   \[ 3 = 6 \cdot (-3) + 21 \cdot 1 \]

   So setting $r := -3$ and $s := 1$, we have $\gcd(6, 21) = 6r + 21s$.

5. Multiply both sides of Bézout’s Identity you’ve just computed by an appropriate integer to solve our Diophantine equation $6x + 21(-y) = 15$.

   We multiply both side of $3 = 6 \cdot (-3) + 21 \cdot 1$ by 5, and we get

   \[ 15 = 6 \cdot (-15) + 21 \cdot 5. \]

   So a solution is $x = -15$ and $y = “\text{whatever}”$ since we don’t care about $y$. Modding up by 21’s, we get $x = 15 \equiv 6 \pmod{21}$ so $x_0$ is a solution. The others are $x = x_0 + \frac{21}{\gcd(6, 21)} \cdot t$ as $t = 1, 2$. (Review the Diophantine Theorem 5.29.)
The method to solve \( ax \equiv b \pmod{n} \)

1. Verify \( \gcd(a, n) \) divides \( b \).
2. Convert \( ax \equiv b \pmod{n} \) to a Diophantine equation:
   \[
   ax + n(-y) = b.
   \]
3. Use the Euclidean algorithm to compute \( \gcd(a, n) \).
4. Run Euclidean algorithm’s backwards to find \( r, s \in \mathbb{Z} \) such that Bézout’s Identity holds:
   \[
   \gcd(a, n) = ar + ns.
   \]
5. Multiply the above by an appropriate integer to find a solution \( x_0 \pmod{n} \) to our Diophantine equation.
6. By Remark 6.13, there are \( d \) mutually incongruent solutions modulo \( n \) where \( d = \gcd(a, n) \). These \( d \) solutions are \( x = x_0 + \frac{n}{d} \cdot t \) as \( t \) varies from 0 to \( d - 1 \).

**Conceptual Question 1:** How many solutions modulo \( n \) are there to the linear congruence \( ax \equiv b \pmod{n} \) if \( a \) and \( n \) are relatively prime?

Exactly 1 solution!

**Conceptual Question 2:** If Diophantus and Bézout morphed and became one person, what would the person be called?

Diout Bézantus!
6.4 Chinese Remainder Theorem (CRT)

**History of the name “Chinese Remainder Theorem”:** This result was so named after a description of some congruence problems appeared in one of the first reports in the West on Chinese mathematics, articles by Alexander Wylie published in 1852 in the North China Herald, which were soon translated into both German and French and republished in European journals.\(^{35}\)

**Question 6.14. (Sun-Tsu, 1\(^{st}\) Century A.D.)** Find a number that leaves a remainder of 2, 3, and 2 when divided by 3, 5, and 7, respectively.

Rephrased in congruence language, the question above becomes the following.

**Question 6.15.** What is the unique integer \(x \in \{0, 1, 2, \ldots, n-1\}\) where \(n = 3 \cdot 5 \cdot 7 = 105\) that solves the system of congruences:

\[
\begin{align*}
    x &\equiv 2 \pmod{3} \\
    x &\equiv 3 \pmod{5} \\
    x &\equiv 2 \pmod{7}
\end{align*}
\]

*Can anyone guess a solution?*

\(^{35}\)This is taken from pg. 222 of Victor Katz’s book “A History of Mathematics: An Introduction”.
The “less eloquent” (non-CRT) way to solve Sun-Tsu’s Problem

Example 6.16. [You Do!] Let us try a purely algebraic way to solve the system:

\[
\begin{align*}
    x &\equiv 2 \pmod{3} \\
    x &\equiv 3 \pmod{5} \\
    x &\equiv 2 \pmod{7}
\end{align*}
\]

First consider the first two congruences \( \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases} \).

By the first congruence we have

\[ x \equiv 2 \pmod{3} \implies x - 2 = 3k \implies x = 3k + 2. \]

By the second congruence we have

\[ x \equiv 3 \pmod{5} \implies 3k + 2 \equiv 3 \pmod{5} \quad \text{since } x = 3k + 2 \]
\[ \implies 3k \equiv 1 \pmod{5} \]
\[ \implies 2 \cdot 3k \equiv 2 \pmod{5} \]
\[ \implies k \equiv 2 \pmod{5} \quad \text{since } 2 \cdot 3 \equiv 1 \pmod{5} \]
\[ \implies k = 5j + 2 \]
\[ \implies x = 3(5j + 2) + 2 \quad \text{since } x = 3k + 2 \]
\[ \implies x = 15j + 8 \]
\[ \implies x \equiv 8 \pmod{15}. \]

Thus the first two congruences of Sun-Tsu’s have the same solution as the ONE congruence \( x \equiv 8 \pmod{15} \). So combining this new congruence with the 3rd Sun-Tsu congruence, it suffices to solve the system

\[
\begin{cases} 
    x \equiv 8 \pmod{15} \\
    x \equiv 2 \pmod{7}
\end{cases}
\]
The “less eloquent” Solution (continued)

Following a similar manner that we did we with Sun-Tsu’s first two congruences, we solve this new system \( \begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 2 \pmod{7} \end{cases} \) of congruences in the same manner. By the first congruence we have

\[ x \equiv 8 \pmod{15} \implies x - 8 = 15r \implies x = 15r + 8. \]

By the second congruence we have

\[ x \equiv 2 \pmod{7} \implies 15r + 8 \equiv 2 \pmod{7} \quad \text{since } x = 15r + 8 \]
\[ \implies 15r \equiv -6 \equiv 1 \pmod{7} \]
\[ \implies r \equiv 1 \pmod{7} \quad \text{since } 15 \equiv 1 \pmod{7} \]
\[ \implies r = 7s + 1 \]
\[ \implies x = 15(7s + 1) + 8 \quad \text{since } x = 15r + 8 \]
\[ \implies x = 210s + 23 \]
\[ \implies x \equiv 23 \pmod{210}. \]

We conclude that \( x = 23 \) is the UNIQUE solution modulo 210 for the system \( \begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 2 \pmod{7} \end{cases} \) and hence is ALSO the unique solution modulo 210 for Sun-Tsu’s original system

\[ \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7}. \end{cases} \]

Q.E.D.
The Statement [AND] a Constructive Proof of the Chinese Remainder Theorem

**Theorem 6.17** (Chinese Remainder Theorem). Consider the following system of linear congruences

\[
\begin{align*}
  x &\equiv a_1 \pmod{n_1} \\
  x &\equiv a_2 \pmod{n_2} \\
  & \vdots \\
  x &\equiv a_r \pmod{n_r}.
\end{align*}
\]

If the moduli are all pairwise relatively prime (i.e., \(\gcd(n_i,n_j) = 1\) for all \(i \neq j\)), then the system admits a unique solution \(x\) modulo \(m\) where \(m = n_1 \cdot n_2 \cdots n_r\).

(Proof.) Suppose that \(n_1,n_2,\ldots,n_r\) are pairwise relatively prime, and set \(m\) to the product \(n_1 \cdot n_2 \cdots n_r\). Define \(N_i\) as follows:

\[
N_i = n_1 \cdot n_2 \cdots n_{i-1} \cdot \hat{n}_i \cdot n_{i+1} \cdots n_r
\]

where \(\hat{n}_i\) means to omit this multiplicand from the product.

- It follows that \(\gcd(N_i,n_i) = 1\) for each \(i\). [Why?]
- Therefore \(N_i\) has a multiplicative inverse mod \(n_i\). That is, for each \(i\) there is a solution \(x_i\) to the congruence \(N_i x_i \equiv 1 \pmod{n_i}\). [WHY?]
- Define \(x\) to be the following sum

\[
x = \sum_{i=1}^{r} a_i N_i x_i = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r.
\]

- We claim that \(x \pmod{m}\) is a solution modulo \(m\) for the system.

**QUESTION:** Why does \(x \equiv a_j \pmod{n_j}\) hold for each \(j = 1, 2, \ldots, r\)?

**ANSWER:** For each \(i \neq j\), we have \(N_i \equiv 0 \pmod{n_j}\) [WHY?], and hence \(a_i N_i x_i \equiv 0 \pmod{n_j}\). Thus

\[
x \equiv \sum_{i=1}^{r} a_i N_i x_i \pmod{n_j}
\]

\[
\equiv a_j N_j x_j \quad \text{since } a_i N_i x_i \equiv 0 \pmod{n_j} \text{ for all } i \neq j
\]

\[
\equiv a_j \quad \text{since } N_j x_j \equiv 1 \pmod{n_1}.
\]
We now prove that this $x$ is unique modulo $m$. To this end it would be helpful to reproduce the following lemma below (which first appeared as Corollary 5.25 and whose proof is a homework exercise in the Divisibility Homework).

**Lemma 6.18.** Prove that if $m \mid x$ and $n \mid x$ and $\gcd(m, n) = 1$, then $mn \mid x$.

**Conclusion of the C.R.T. Proof**

We know that $x = \sum_{i=1}^{r} a_i N_i x_i \pmod{m}$ is a solution to the system of congruences. Suppose that $x'$ is another solution to the system.

**QUESTION:** What does it suffice to show?

**ANSWER:** It suffices to show that $x \equiv x' \pmod{m}$.

Since $x$ and $x'$ are solutions to the system, then for each $i = 1, 2, \ldots, r$, we have

$$x \equiv a_i \equiv x' \pmod{n_i} \quad \text{[WHY?]}. $$

And thus for each $i$, we have $n_i$ divides $x - x'$ [WHY?]. And therefore by recalling $m = n_1 \cdot n_2 \cdots n_r$ and by *inductive use* of the lemma above, we have $m$ divides $x - x'$ [Huh? What do we mean by “inductive use”]. We conclude

$$x \equiv x' \pmod{m}$$

and hence the solution $x$ is unique modulo $m$ as desired.

Q.E.D.

---

36 Cartoon artist is Ian VanderSchee who is currently teaching International Baccalaureate math in Texas. And it is taken with his permission from his webpage https://blueshirtkhakipants.com/.
Chinese Remainder Theorem Solution to Sun-Tsu’s Problem

Solve the following linear congruence using C.R.T.:

\[
\begin{align*}
    x &\equiv 2 \pmod{3} \\
    x &\equiv 3 \pmod{5} \\
    x &\equiv 2 \pmod{7}
\end{align*}
\]

Recalling the notation from the proof C.R.T. given in Theorem 6.17, we fill out the following table as follows:

<table>
<thead>
<tr>
<th></th>
<th>(a_i)</th>
<th>(n_i)</th>
<th>(N_i)</th>
<th>The (N_i x_i \equiv 1 \pmod{n_i}) to solve</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>35</td>
<td>35(x_1 \equiv 1 \pmod{3})</td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>5</td>
<td>21</td>
<td>21(x_2 \equiv 1 \pmod{5})</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>7</td>
<td>15</td>
<td>15(x_3 \equiv 1 \pmod{7})</td>
</tr>
</tbody>
</table>

Since \(\gcd(N_i, n_i) = 1\), each congruence \(N_i x_i \equiv 1 \pmod{n_i}\) has a unique solution \(x_i\) modulo \(n_i\). Solve these three congruences in the far-right column. [You Do!]

- \(35x_1 \equiv 1 \pmod{3}\) simplifies to \(2x_1 \equiv 1 \pmod{3}\) and it is easily deduced that \(x_1 = 2\) is the unique solution modulo 3.
- \(21x_2 \equiv 1 \pmod{5}\) simplifies to \(x_2 \equiv 1 \pmod{5}\) the unique solution!
- \(15x_3 \equiv 1 \pmod{7}\) simplifies to \(x_3 \equiv 1 \pmod{7}\) the unique solution!

Now compute \(x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3\). [You Do!]

\[
x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 140 + 63 + 30 = 233.
\]

Finally, verify that \(x \pmod{3 \cdot 5 \cdot 7}\) is solution to the system. [You Do!]

Since \(3 \cdot 5 \cdot 7 = 210\), then \(x = 233 \equiv 23 \pmod{210}\). Observe that \(23 \equiv 2 \pmod{3}\), \(23 \equiv 3 \pmod{5}\), and \(23 \equiv 2 \pmod{7}\).
6.5 Exercises

**Congruence Exercise 1**

**PROVE:** If $a$ is odd, then $a^2$ leaves a remainder of 1 when divided by 8. That is,

$$a \in 2\mathbb{Z} + 1 \implies a^2 \in 8\mathbb{Z} + 1.$$

First let’s check some small values of $a$. [You Do!].

<table>
<thead>
<tr>
<th>$a$</th>
<th>$a^2$</th>
<th>$8(?) + 1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$1^2 = 1$</td>
<td>$8(0) + 1$</td>
</tr>
<tr>
<td>3</td>
<td>$3^2 = 9$</td>
<td>$8(1) + 1$</td>
</tr>
<tr>
<td>5</td>
<td>$5^2 = 25$</td>
<td>$8(3) + 1$</td>
</tr>
<tr>
<td>7</td>
<td>$7^2 = 49$</td>
<td>$8(6) + 1$</td>
</tr>
<tr>
<td>9</td>
<td>$9^2 = 81$</td>
<td>$8(10) + 1$</td>
</tr>
<tr>
<td>11</td>
<td>$11^2 = 121$</td>
<td>$8(15) + 1$</td>
</tr>
<tr>
<td>13</td>
<td>$13^2 = 169$</td>
<td>$8(21) + 1$</td>
</tr>
</tbody>
</table>

**QUESTION 1:** Do the values in the parentheses in the 3\textsuperscript{rd} column look familiar?

**ANSWER:** These are the so-called triangular numbers given in Definition 2.3. Recall the $n$\textsuperscript{th} triangular number is given by $T_n = \sum_{i=1}^{n} i$.

**QUESTION 2:** Given the observation made above from Question 1, can you rewrite the statement we are trying to prove. That is, write a formula for $a^2$ given that $a$ is the $k$\textsuperscript{th} odd integer $2k - 1$.

**ANSWER:** Let $k \geq 1$. Then

$$a = 2k - 1 \implies a^2 = 8 \cdot T_{k-1} + 1.$$
Congruence Exercise 1 (continued)

**PROVE:** Let \( k \geq 1 \). Then

\[
a = 2k - 1 \implies a^2 = 8 \cdot T_{k-1} + 1.
\]

**PROOF \#1 of 3 (the algebraic proof):**

- **LHS** of \( a^2 = 8 \cdot T_{k-1} + 1 \) is

\[
(2k - 1)^2 = (2k - 1)(2k - 1)
= 4k^2 - 4k + 1
\]

- **RHS** of \( a^2 = 8 \cdot T_{k-1} + 1 \) is

\[
8 \cdot T_{k-1} + 1 = 8 \cdot (1 + 2 + \cdots + (k + 1)) + 1
= 8 \cdot \frac{(k - 1)k}{2} + 1 \quad [\text{Why?}]
= 4(k^2 - k) + 1
= 4k^2 - 4k + 1
\]

Q.E.D.

The algebraic proof above works but it sucks since it only works for positive odd integers [and] you need to know triangular numbers!
PROOF #2 of 3 (the congruence proof):

PROVE: If $a$ is odd, then $a^2$ leaves a remainder of 1 when divided by 8.

Proof. Let $a \in 2\mathbb{Z} + 1$. [You Finish!]

WWTS: \( a^2 \equiv 1 \pmod{8} \)

Since $a \in 2\mathbb{Z} + 1$, then $a = 2k + 1$ for some $k \in \mathbb{Z}$. Observe we have the following sequence of equalities:

\[
\begin{align*}
a^2 &= (2k - 1)^2 \\
&= 4k^2 - 4k + 1 \\
&= 4(k^2 - k) + 1 \\
&= 4(k \cdot (k - 1)) + 1 \\
&= 4(2M) + 1 \\
&= 8M + 1 \\
&\equiv 1 \pmod{8},
\end{align*}
\]

where the fifth equality holds since $k \cdot (k - 1)$ is a product of two consecutive integers and hence one of these two will surely be even. Since $a^2 \equiv 1 \pmod{8}$, we know $a^2$ leaves a remainder of 1 when divided by 8.

Q.E.D.

PROOF #3 of 3 (the proof by picture):

Question 6.19. Let $a = 2k - 1$ for some $k \in \mathbb{N}$. Can you arrange eight triangles (where each one represents the $(k - 1)^{\text{th}}$ triangular number) and add one additional point to make an $a \times a$ square of points?
Congruence Exercise 2

**PROVE:** Let $a \in \mathbb{Z}$. Show that either $a^4 \equiv 0 \pmod{5}$ or $a^4 \equiv 1 \pmod{5}$.

First let’s check some small values of $a$.

<table>
<thead>
<tr>
<th>$a$</th>
<th>$a^4$</th>
<th>$a^4 \equiv 0 \pmod{5}$?</th>
<th>$a^4 \equiv 1 \pmod{5}$?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$1^4 = 1$</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>$2^4 = 16$</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>$3^4 = 81$</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>$4^4 = 256$</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>5</td>
<td>$5^4 = 625$</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>6</td>
<td>$6^4 = 1296$</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>7</td>
<td>$7^4 = 2401$</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**QUESTION:** What would these five cases be?

**ANSWER:** Case 1 would be to suppose $a \equiv 0 \pmod{5}$. Case 2 would be to suppose $a \equiv 1 \pmod{5}$. Continue in this manner up to the fifth case: Case 5 would be to suppose $a \equiv 4 \pmod{5}$.

*We leave this problem as a HW exercise.*
Congruence Exercise 3

PROVE: 41 divides $2^{20} - 1$.

QUESTION:

ANSWER: Show that $2^{20} \equiv 1 \pmod{41}$.

Proof. By brute force we calculate the first few powers of 2 modulo 41. The first five powers of 2 are all less than 41:

$2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, and $2^5 = 32$.

The next few power modulo 41 are as follows:

\[
2^6 = \frac{64}{23} \equiv 23 \pmod{41}
\]

\[
2^7 = \frac{2^6 \cdot 2}{23 \cdot 2} \equiv 23 \cdot 2 \pmod{41} = 46 \equiv 5 \pmod{41}
\]

\[
2^8 = \frac{2^7 \cdot 2}{5 \cdot 2} \equiv 5 \cdot 2 \pmod{41} \equiv 10 \pmod{41}
\]

\[
2^9 = \frac{2^8 \cdot 2}{10 \cdot 2} \equiv 10 \cdot 2 \pmod{41} \equiv 20 \pmod{41}
\]

\[
2^{10} = \frac{2^9 \cdot 2}{20 \cdot 2} \equiv 20 \cdot 2 \pmod{41} \equiv 40 \pmod{41}
\]

However, now that we just computed that $2^{10} \equiv 40 \pmod{41}$, we know that $2^{10} \equiv -1 \pmod{41}$ [Why? Also, you finish the proof]!

Since $2^{10} \equiv -1 \pmod{41}$, then by squaring both sides of the congruence we get $2^{20} \equiv 1 \pmod{41}$. Thus by definition of congruence, we have that 41 divides the difference $2^{20} - 1$ which is what was to be shown.

Q.E.D.
Congruence Exercise 4

Recall in Divisibility Exercise 2, we asked you to consider the following:

Determine all $n$ for which $2^n + 1$ is divisible by 3.

After getting our hands dirty with examples, you conjectured the following:

(i) When $n$ is odd, then 3 divides $2^n + 1$.

(ii) When $n$ is even, then 3 does not divide $2^n + 1$.

And in the Divisibility HW you were asked to prove only the first conjecture (and NOT to use congruence theory, which we had not learned yet). We now attempt the super slick congruence theory proof of both conjectures. [You Do!]

Proof.

**Proof of (i):** Suppose $n$ is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$.

**WWTS:** $2^{2k+1} + 1 \equiv 0 \pmod{3}$

Observe the following sequence of equalities and congruences modulo 3:

$$2^{2k+1} + 1 = (2^2)^k \cdot 2 + 1 \equiv 1^k \cdot 2 + 1 \equiv 0 \pmod{3}.$$

**Proof of (ii):** Suppose $n$ is even. Then $n = 2k$ for some $k \in \mathbb{Z}$.

**WWTS:** $2^{2k} + 1 \not\equiv 0 \pmod{3}$

Observe the following sequence of equalities and congruences modulo 3:

$$2^{2k} + 1 = (2^2)^k + 1 \equiv 1^k + 1 \equiv 2 \not\equiv 0 \pmod{3}.$$

Q.E.D.
Congruence Exercise 5

Recall the following problems from Subsection 6.1 at the beginning of this section.

- Consider $1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$. What is this number’s remainder when you divide it by 4? \textbf{ANSWER: 0}

- Consider the ridiculously large number $53^{103} + 103^{53}$. \textbf{Note:} It is 177 digits long! Is it divisible by 39? \textbf{ANSWER: Yes!}

- Consider the \textbf{even more} ridiculously large number $111^{333} + 333^{111}$. \textbf{Note:} It is a whopping 682 digits long! Is it divisible by 7? \textbf{ANSWER: Yes!}

- \textbf{(Brahmagupta, 7th Century A.D.)} Suppose that when eggs in a basket are removed 2, 3, 4, 5, and 6 at a time, there remain 1, 2, 3, 4, and 5 eggs, respectively. But when taken out 7 at a time, none are left over. Find the smallest number of eggs that could have been in the basket. \textbf{ANSWER: 119}

\begin{center} We leave some of these problems as HW exercises. \end{center}
7 Arithmetic Functions

7.1 Motivation

PoaBast was an ancient society where the royals had specific rules for bequeathing their possessions. The rules were that given \( n \) items to bequeath, the maximum number of heirs they could give their possessions to was equal to the number of proper divisors of \( n \) and the amount of items given away to each heir was a unique proper divisor of \( n \); meaning that no two heirs would receive the same proper divisor number of items.

---

\(^9\)Authors Post and aBa thank Burger King™ for the complimentary royal crowns they are wearing in this image taken at the BK fast food joint in Eau Claire, WI.

Consider this scenario: Queen Rita has 12 goats, and would like to give away these goats to her heirs.

**Question 7.1.** What is the maximum number of heirs Rita can give her goats to?
Question 7.2. How many goats can Queen Rita give Katie Sue? How about Jammo?

Queen Rita can give Katie Sue 1, 2, 3, 4, 6 and Jammo 1, 2, 3, 4, 6, as long as it is NOT the same number of goats that Katie Sue received.

Question 7.3. Can Queen Rita give away all of her goats to all of her heirs?

No, she cannot [WHY?]. The maximum heirs she could give goats to is 4, and it would be possible to give 12 goats to these four heirs [WHY?].
Question 7.4. What is the number $n$ of goats needed for Queen Rita to bequeath upon her 5 heirs? *Hint:* $n$ must have exactly 5 proper divisors.

Multiple answers work here, but 18 is one answer.

Question 7.5. For what numbers $n$ could Queen Rita give away all of her goats to all of her heirs?

Multiple answers work here, but 28 is one answer.

We will discover in this section that these numbers fall into the category of *perfect numbers* and *semi-perfect numbers*!
Definition 7.6. An arithmetic function $f$ is a function whose domain is the set of positive integers and whose range is a subset of the complex numbers.

We have already seen one example of an arithmetic functions. The greatest common divisor function, $\text{gcd}(n, k)$ where $k$ is a fixed integer is an arithmetic function. Some additional examples of arithmetic functions that we will see in this section include

- $\sigma(n)$ the sum of the positive divisors of $n$
- $\tau(n)$ the number of positive divisors of $n$
- $\phi(n)$ the number of positive numbers not exceeding $n$ and relatively prime to $n$
- $\omega(n)$ the number of distinct prime divisors of $n$.
- $\Omega(n)$ the number of primes dividing $n$, counting multiplicity.

Note that we can express $\sigma(n)$ and $\tau(n)$ in summation notation. It is simple to see that

$$\sigma(n) = \sum_{d|n} d \quad \text{and} \quad \tau(n) = \sum_{d|n} 1.$$ 

**EXERCISE:** Consider $n = 20$. Complete the following. [You Do!]

- What are its positive divisors? 1, 2, 4, 5, 10, and 20
- Compute $\sigma(n)$. 42
- Compute $\tau(n)$. 6
- Compute $\phi(n)$. 8
- Compute $\omega(n)$. 2
- Compute $\Omega(n)$. 3
7.2 Sigma and Tau Functions

Definition 7.7. The sum of divisors function, denoted by $\sigma$, is defined by setting $\sigma(n)$ equal to the sum of all of the positive divisors of $n$.

**EXERCISE:** Fill out the table below for all $n \leq 10$. [You Do!]

<table>
<thead>
<tr>
<th>$n$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sigma(n)$</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>7</td>
<td>6</td>
<td>12</td>
<td>8</td>
<td>15</td>
<td>13</td>
<td>18</td>
</tr>
</tbody>
</table>

Definition 7.8. The number of divisors function, denoted by $\tau$, is defined by setting $\tau(n)$ equal to the number of positive divisors of $n$.

**EXERCISE:** Fill out the table below for all $n \leq 10$. [You Do!]

<table>
<thead>
<tr>
<th>$n$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\tau(n)$</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

**EXERCISE:** Consider $n = 12$.

- What are the positive divisors of $n$? [You Do!]

\[1, 2, 3, 4, 6, \text{ and } 12\]

- Compute $\tau(n)$. [You Do!]

\[6\]

- Compute $\sigma(n)$. [You Do!]

\[1 + 2 + 3 + 4 + 6 + 12 = 28\]
The Tao of $\tau$

Like the famous book *The Tao of Pooh* which introduced the Eastern mysticism of Taoism to a Western audience through Winnie the Pooh allegory, so deep and profound is the Tao of $\tau$.

**EXERCISE:** Suppose $p$ is a prime number. [Contemplate the following!]

- What is $\tau(p)$? $2$
- What is $\tau(p^2)$? $3$
- What is $\tau(p^3)$? $4$
- What is $\tau(p^n)$? $n + 1$

- If $q$ is a prime different than $p$, write the divisors of $pq$ and compute $\tau(pq)$.

  
  $1, p, q, \text{ and } pq \text{ and hence } \tau(pq) = 4.$

- Write the divisors of $p^2q$ and compute $\tau(p^2q)$.

  
  $1, p, q, p^2, pq, \text{ and } p^2q \text{ and hence } \tau(p^2q) = 6.$

- Write the divisors of $p^2q^2$ and compute $\tau(p^2q^2)$.

  
  $1, p, q, p^2, pq, q^2, p^2q, pq^2, \text{ and } p^2q^2 \text{ and hence } \tau(p^2q^2) = 9.$

**CONJECTURE TIME:** What is $\tau(p^nq^m)$? Justify your reasoning.

If $d$ divides $p^nq^m$ then it is of the form $p^aq^b$ where $a$ and $b$ are integers with $0 \leq a \leq n$ and $0 \leq b \leq m$. So there are $n + 1$ choices for $a$ and $m + 1$ choices for $b$ and hence $(m + 1)(n + 1)$ possible divisors of $p^nq^m$. 
**Theorem 7.9.** Let \( n \) be an integer with prime factorization \( n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r} \) \((p_i \text{ distinct primes and } n_i \geq 1)\). Then the positive divisors \( d \) of \( n \) are of the form

\[
d = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r} \quad \text{where } d > 0 \text{ and } 0 \leq d_i \leq n_i \text{ for all } i.
\]

In particular, \( \tau(n) = (n_1 + 1)(n_2 + 1) \cdots (n_r + 1) \).

**Proof.** [You Do!] Let \( D \) be the set \( \{p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r} \mid 0 \leq d_i \leq n_i \text{ for all } i\} \).

And let \( E \) be the set of all positive divisors of \( n \).

\textbf{WWTS: } \( D = E \).

\((\subseteq)\) Let \( d = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r} \) be in \( D \). Then we claim that \( d \) is a divisor of \( n \). Clearly

\[
(p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}) \cdot (p_1^{n_1-d_1} p_2^{n_2-d_2} \cdots p_r^{n_r-d_r}) = n.
\]

Thus \( d \) is a divisor of \( n \) and hence \( D \subseteq E \).

\((\supseteq)\) Suppose \( d \in E \). That is, \( d \) is a divisor of \( n \). If some prime \( p \) divides \( d \), then \( p \) also divides \( n \). So each prime in the prime factorization of \( d \) must appear in the prime factorization of \( n \). Thus \( d \) is of the form

\[
d = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r}
\]

where some (or all) of the exponents may be zero. Moreover, no \( f_i \) can be larger than \( n_i \) for otherwise \( p_i^{f_i} \mid d \) and \( d \mid n \), which implies \( p_i^{f_i} \mid n \), but that is impossible if \( f_i > n_i \). Thus \( d \in D \) and hence \( D \supseteq E \).

Therefore \( D = E \).

Lastly, each \( d_i \) may take on \( n_i + 1 \) possible values. Thus we have

\[
\tau(n) = |D| = (n_1 + 1)(n_2 + 1) \cdots (n_r + 1)
\]

as desired.

\textbf{Q.E.D.}
Sum $\sum$ Time? Nope, It’s Some $\sigma$ Time!

Recall that $\sigma(n)$ is the sum of the positive divisors of $n$.

**EXERCISE:** Suppose $p$ is a prime number. [Contemplate the following!]

- What is $\sigma(p)$?
  
  $1 + p$

- What is $\sigma(p^2)$?
  
  $1 + p + p^2$

- What is $\sigma(p^3)$?
  
  $1 + p + p^2 + p^3$

- What is $\sigma(p^n)$?
  
  $1 + p + p^2 + \cdots + p^n$

- If $q$ is a prime different than $p$, write the divisors of $pq$ and compute $\sigma(pq)$.
  
  $1, p, q, \text{ and } pq \text{ and hence } \sigma(pq) = 1 + p + q + pq.$

Now write $\sigma(pq)$ as a product of two polynomials.

\[ \sigma(pq) = (1 + p)(1 + q). \]

- Write the divisors of $p^2q$ and compute $\sigma(p^2q)$.
  
  $1, p, q, p^2, pq, \text{ and } p^2q \text{ and hence } \sigma(p^2q) = 1 + p + q + p^2 + pq + p^2q.$

Now write $\sigma(p^2q)$ as a product of two polynomials.

\[ \sigma(p^2q) = (1 + p + p^2)(1 + q). \]

**CONJECTURE TIME:** What is $\sigma(p^nq^m)$? Justify your reasoning.

It seems like it should be the following product

\[ (1 + p + p^2 + \cdots + p^n) \ (1 + q + q^2 + \cdots + q^m) . \]

Multiplying this out we get all the possible divisors $p^aq^b$ (where $0 \leq a \leq n$ and $0 \leq b \leq m$) as unique summands in the expansion of the product above.
Now for a blast from the past from calculus. We learned that a finite geometric series \( \sum_{k=0}^{n-1} r^k \) converges as follows
\[
\sum_{k=0}^{n-1} r^k = \frac{r^n - 1}{r - 1}.
\]
[Should we prove this?]

**Theorem 7.10.** Let \( n \) be an integer with prime factorization \( n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r} \) (\( p_i \) distinct primes and \( n_i \geq 1 \)). Then
\[
\sigma(n) = \frac{p_1^{n_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{n_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{n_r+1} - 1}{p_r - 1}.
\]

**Proof.** Since the prime factorization of \( n \) is \( p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r} \), then the divisors of \( n \) will be of the form \( p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r} \). Consider the product
\[
(1 + p_1 + p_1^2 + \cdots + p_1^{n_1})(1 + p_2 + p_2^2 + \cdots + p_2^{n_2}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{n_r}).
\]
Expanding this we see that each positive divisor of \( n \) appears exactly once as a term and thus
\[
\sigma(n) = \prod_{i=0}^{r} \left( 1 + p_i + p_i^2 + \cdots + p_i^{n_i} \right).
\]
Applying the formula for the sum of a finite geometric series to each \( i \)th summand on the right-hand side we get
\[
1 + p_i + p_i^2 + \cdots + p_i^{n_i} = \frac{p_i^{n_i+1} - 1}{p_i - 1}.
\]
Therefore
\[
\sigma(n) = \frac{p_1^{n_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{n_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{n_r+1} - 1}{p_r - 1}.
\]
Q.E.D.

Given \( n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r} \) (\( p_i \) distinct primes and \( n_i \geq 1 \)), using “fattie product” notation, we have
\[
\tau(n) = \prod_{i=0}^{r} (n_i + 1) \quad \text{and} \quad \sigma(n) = \prod_{i=0}^{r} \frac{p_i^{n_i+1} - 1}{p_i - 1}.
\]
Multiplicative Functions

Definition 7.11. An arithmetic function $f$ is said to be multiplicative if

$$f(m \cdot n) = f(m) \cdot f(n)$$

whenever $\gcd(m, n) = 1$.

Theorem 7.12. The function $\tau$ is a multiplicative function.

Proof. Let $m = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ and $n = q_1^{n_1} q_2^{n_2} \cdots q_s^{n_s}$ and suppose $\gcd(m, n) = 1$.

WWTS: $\tau(mn) = \tau(m) \cdot \tau(n)$.

Since $\gcd(m, n) = 1$, then no $p_i = q_j$ for any indices $i, j$. So the prime factorization of $mn$ is given by

$$mn = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r} \cdot q_1^{n_1} q_2^{n_2} \cdots q_s^{n_s}.$$  

By repeated application of Theorem 7.9, it follows that

$$\tau(mn) = \prod_{i=0}^{r} (m_i + 1) \cdot \prod_{j=0}^{s} (n_j + 1)$$

$$= \prod_{i=0}^{r} \tau(p_i^{m_i}) \cdot \prod_{j=0}^{s} \tau(q_j^{n_j}) \quad \text{since } \tau(p^a) = a + 1 \text{ for } p \text{ prime}$$

$$= \tau(m) \cdot \tau(n)$$

Thus $\tau$ is a multiplicative function.

Q.E.D.
Theorem 7.13. The function \( \sigma \) is a multiplicative function.

The proof of this is VERY similar to the proof that \( \tau \) is multiplicative. The crux of the proof is to generalize the following to the \( \sigma \)-setting:

By repeated application of Theorem 7.9, it follows that

\[
\tau(mn) = \prod_{i=0}^{r} (m_i + 1) \cdot \prod_{j=0}^{s} (n_j + 1)
\]

\[
= \prod_{i=0}^{r} \tau(p_i^{m_i}) \cdot \prod_{j=0}^{s} \tau(q_j^{n_j}) \quad \text{since } \tau(p^a) = a + 1 \text{ for } p \text{ prime}
\]

\[
= \tau(m) \cdot \tau(n)
\]

**EXERCISE:** Use Theorem 7.10 to mimic the argument above in the \( \sigma \)-setting to prove \( \sigma \) is multiplicative. That is, \( \sigma(mn) = \sigma(m) \cdot \sigma(n) \). [You Do!]

By repeated application of Theorem 7.10, it follows that

\[
\sigma(mn) = \prod_{i=0}^{r} \frac{p_i^{m_i+1} - 1}{p_i - 1} \cdot \prod_{j=0}^{s} \frac{q_j^{n_j+1} - 1}{q_j - 1}
\]

\[
= \prod_{i=0}^{r} \sigma(p_i^{m_i}) \cdot \prod_{j=0}^{s} \sigma(q_j^{n_j}) \quad \text{see justification below}
\]

\[
= \sigma(m) \cdot \sigma(n)
\]

The second equality holds since for any prime \( p \) and \( a \in \mathbb{N} \), we have

\[
\sigma(p^a) = 1 + p + p^2 + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1}.
\]

“Q.E.D.”
7.3 Perfect Numbers

While perfect numbers are not arithmetic functions, they do relate to arithmetic functions. Particularly, they are related to the arithmetic function $\sigma$.

**Definition 7.14.** Let $n$ be a positive integer.

- $n$ is called an **abundant number** if the sum of its proper divisors is larger than $n$. That is $\sigma(n) - n > n$ (or equivalently, $\sigma(n) > 2n$).
- $n$ is called a **deficient number** if the sum of its proper divisors is smaller than $n$. That is $\sigma(n) - n < n$ (or equivalently, $\sigma(n) < 2n$).

**EXERCISE:** Classify the numbers 8 and 12 as abundant, deficient, or neither.

**ANSWER:** [You Do!] Since the proper divisors of 8 are 1, 2, and 4, and $1 + 2 + 4 = 7 < 8$, then 8 is deficient. And since the proper divisors of 12 are 1, 2, 3, 4, and 6, and $1 + 2 + 3 + 4 + 6 = 16 > 12$, then 12 is abundant.

**FACT:** Most numbers are either abundant or deficient. Perfection is rare.

“Perfect numbers like perfect men are very rare.”
- René Descartes\textsuperscript{37} (1596–1650)

**Definition 7.15.** A positive integer $n$ is said to be a **perfect number** if $n$ is equal to the sum of all its positive divisors, excluding $n$ itself.

**EXERCISE:** What is the connection to the Goldilocks fable?

\textsuperscript{37} Appears without citation by math historian Howard W. Eves, Mathematical Circles Squared (1972), 7, and it is noted with the fact that only 12 perfect numbers were known in Descartes’ time.
The sum of the positive divisors of an integer \( n \), each of them less than \( n \), is given by \( \sigma(n) - n \). Thus, the condition “\( n \) is perfect” is equivalent to saying \( \sigma(n) - n = n \), or

\[
\sigma(n) = 2n.
\]

For example, we have

\[
\sigma(6) = 1 + 2 + 3 + 6 = 2 \cdot 6.
\]

The smallest perfect number is 6 and is illustrated in the “patriotic” diagram:

\[
\begin{array}{cccccccc}
\text{6} & \text{1} & \text{6} \\
\text{6} & \text{2} & \text{3} \\
\text{6} & \text{3} & \text{2} \\
\text{1} & \text{2} & \text{3} \\
\end{array}
\]

The first four perfect numbers are 6, 28, 496, and 8128. These were the only perfect numbers known in the 4\(^{th}\) Century B.C. in the time of Euclid.

**COOL HISTORICAL FACTS**

- From the 4\(^{th}\) Century B.C. until A.D. 1456, no other perfect numbers were found. But in A.D. 1456, the next smallest perfect number after 8128 is found. It is number 33,550,336.
- Nicomachus of Gerasa (c. A.D. 60–120) conjectured that every perfect number is of the form \( 2^{p-1}(2^p - 1) \) where \( 2^p - 1 \) is prime.
- Hasan Ibn al-Haytham (c. A.D. 965–1040), a mathematician, astronomer, and physicist in the Islamic Golden Age, known as the “father of optics”, conjectured that every **EVEN** perfect number is of the form \( 2^{p-1}(2^p - 1) \) where \( 2^p - 1 \) is prime.
- Euler proved al-Haytham’s conjecture finally in the 18\(^{th}\) Century!!! This is known as the **Euclid-Euler Theorem**.
- To this date in 2019, no odd perfect numbers are known. It is a famous open problem whether any odd perfect numbers will ever be found.
The mystical properties of perfect numbers

For many centuries, philosophers were more concerned with the mystical or religious significance of perfect numbers than with their mathematical properties. Here are some of the notable theories.

- Saint Augustine explains that although God could have created the world all at once, He preferred to take 6 days because of the perfection of the work is symbolized by the perfect number 6.
- Early commentators on the Old Testament argued that the perfection of the universe is represented by 28, the number of days it takes the moon to circle the Earth.
- 8th century theologian Alcuin of York observed that the whole human race is descended from the 8 souls of Noah’s Ark and that this second Creation is less perfect than the first.

Recall that 8 is a deficient number. [Why?]

Euclid proved in the 4th Century B.C. that the number $2^{p-1}(2^p - 1)$ is an even perfect number whenever $2^p - 1$ is prime. Before we show his proof, let’s look at the evidence that he had back then, namely the ONLY four known perfect numbers at that time.

$$
6 = 2 \cdot 3 = 2(2^2 - 1) \\
28 = 2^2 \cdot 7 = 2^2(2^3 - 1) \\
496 = 2^4 \cdot 31 = 2^4(2^5 - 1) \\
8128 = 2^6 \cdot 127 = 2^4(2^7 - 1)
$$

**QUESTION:** What is significant about a number $2^n - 1$ being prime?

**ANSWER:** [You Do!] This type of number is called a Mersenne prime. And if $2^n - 1$ is prime then $n$ must be prime, but the converse does not necessarily hold.
Euclid’s Theorem on Perfect Numbers

In Euclid’s Book IX of his great work *The Elements* he proves in Proposition 36:

“If as many numbers as we please beginning from a unit are set out continuously in double proportion until the sum of all becomes prime, and if the sum multiplied into the last makes some number, then the product is perfect.”

**QUESTION:** What does that say in modern math language/notation?

**ANSWER:** [You Do!] He is saying for us to consider the sum of “consecutively doubled proportions” of the unit 1 as such:

\[ 1 + 2 + 2^2 + \cdots + 2^{n-1} \]

for some \( n \) for which the sum become prime. And then multiply that sum with the very last summand \( 2^{n-1} \). This product is a perfect number.

We can restate the theorem as follows. [Why?]

**Theorem 7.16** (Euclid, 4th Century B.C.). *If \( p \) and \( q = 2^p - 1 \) are prime, then \( 2^{p-1}q \) is a perfect number.*

**Proof.** [You Do!] Let \( p \) and \( q = 2^p - 1 \) be prime. Set \( N = 2^{p-1}q. \)

**WWTS:** \( \sigma(N) - N = N. \)

The proper divisors of \( 2^{p-1}q \) are 1, 2, 2\(^2\), \ldots, \( 2^{p-1}, q, 2q, 2^2q, \ldots, 2^{p-2}q, \) so summing them we get

\[
\sigma(N) - N = (1 + 2 + 2^2 + \cdots + 2^{p-1}) + q \left( 1 + 2 + 2^2 + \cdots + 2^{p-2} \right)
\]

\[
= \frac{2^p - 1}{2 - 1} + q \cdot \frac{2^{p-1} - 1}{2 - 1} \quad \text{by geometric series sum}
\]

\[
= (2^p - 1) + q2^{p-1} - q
\]

\[
= q2^{p-1} \quad \text{since } q = 2^p - 1
\]

\[
= N
\]

as desired. Thus \( 2^{p-1}q \) is a perfect number.

Q.E.D.
7.4 The Omega Functions \( \omega \) and \( \Omega \)

**Definition 7.17.** The prime **omega function** \( \omega(n) \) calculates the number of distinct prime divisors of \( n \) and the **Omega function** \( \Omega(n) \) calculates the number of primes dividing \( n \), counting multiplicity.

Note that for any number \( n \) with prime factorization \( n = p_1^{n_1}p_2^{n_2} \cdots p_r^{n_r} \) for distinct prime \( p_i \) with \( 1 \leq i \leq r \), we have \( \omega(n) = r \) and \( \Omega(n) = n_1 + n_2 + \cdots + n_r \).

**EXERCISE:** Calculate \( \omega(44100) \) and \( \Omega(44100) \). [You Do!]

- First write the prime factorization of 44100.
- Calculate \( \omega(44100) \).
- Calculate \( \Omega(44100) \).

```
2^2 \cdot 3^2 \cdot 5^2 \cdot 7^2
\omega(44100) = 4
\Omega(44100) = 8
```

**Definition 7.18.** An arithmetic function \( f \) is said to be **additive** if

\[
f(m \cdot n) = f(m) + f(n)
\]

whenever \( \gcd(m, n) = 1 \). It is **completely additive** if the property holds even when \( m \) and \( n \) are not necessarily coprime; in this case, \( f(1) = 0 \). [Why?]

**Properties of \( \omega(n) \) and \( \Omega(n) \)**

**Remark 7.19.** We have the following properties.

- \( \Omega(n) \) is a completely additive arithmetic function. That is,
  \[
  \Omega(mn) = \Omega(m) + \Omega(n), \quad m \geq 1, \quad n \geq 1. \quad \text{[Why?]}
  \]

- If \( n \) is a square-free integer, then \( \Omega(n) = \omega(n) \) [Why?], otherwise we have \( \Omega(n) > \omega(n) \).

As we will see later in the section, if \( n \) is squarefree then \( \omega(n) \) is related to the Möbius function \( \mu(n) \) by \( \mu(n) = (-1)^{\omega(n)} \).
7.5 Euler’s Phi Function

**Question 7.20. Who is Euler?**

- Leonhard Euler (1707—1783), Switzerland
- He is widely considered to be the most prolific mathematicians of all time
- He has worked in almost all areas of mathematics from calculus to geometry to number theory, and some areas of physics
- Has contributed 60 to 80 volumes worth of material in mathematics
- Euler has two numbers named after him (e and gamma)

**Definition 7.21.** For \( n \in \mathbb{N} \), we define \( \phi(n) \) to be the number positive integers up to a given integer \( n \) that are relatively prime to \( n \). That is,

\[
\phi(n) = |\{k \in \mathbb{N} : \gcd(k, n) = 1 \text{ and } k \leq n\}|.
\]

This function is called **Euler’s phi function** or Euler’s totient function.

**Example 7.22.** Find \( \phi(30) \).

To find \( \phi(30) \), we must find all of the positive numbers less than or equal to 30 that are relatively prime to 30.

\[
1, 7, 11, 13, 17, 19, 23, 29.
\]

Since there are 8 numbers that are relatively prime to 30, then \( \phi(30) = 8 \).

For the first few positive integers, it is known that

<table>
<thead>
<tr>
<th>( n )</th>
<th>( \phi(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
</tr>
</tbody>
</table>
In general, for $n > 1$,
\[ \phi(n) = n - 1 \iff n \text{ is prime} \quad \text{[Why?]} \]

**Question 7.23.** Wouldn’t it be great if we could derive a formula for $\phi(n)$ by only knowing the prime factorization of $n$?

**Answer:** Yes, we can! We just need to prove that $\phi$ is multiplicative and then apply the theorem below.

**Theorem 7.24.** If $p$ is a prime and $n > 0$, then
\[ \phi(p^n) = p^n - p^{n-1} = p^{n-1}(p - 1) = p^n \left(1 - \frac{1}{p}\right). \]

**Proof.** [You Do!] Let $X = \{a \in \mathbb{N} \mid \gcd(a, p^n) = 1 \text{ and } a \leq p^n\}$.

**WWTS:** $|X| = p^n - p^{n-1}$.

The numbers NOT relatively prime to $p^n$ are those values in $\{1, 2, \ldots, p^n\}$ that are multiples of $p$, namely, the set-complement:
\[ X^c = \{p, 2p, 3p, \ldots, (p^{n-1} - 1)p, p^{n-1}p\}. \]

Since clearly $|X^c| = p^{n-1}$, then we have $|X| = p^n - |X^c| = p^n - p^{n-1}$.

Q.E.D.

**Example 7.25.** Calculate $\phi(16)$ using Theorem 7.24. [You Do!]
\[ \phi(16) = \phi(2^4) = 2^4 - 2^3 = 16 - 8 = 8 \]
**GOAL:** To show that $\phi(90) = \phi(9) \cdot \phi(10)$.

<p>| | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>27</td>
<td>28</td>
<td>29</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>32</td>
<td>33</td>
<td>34</td>
<td>35</td>
<td>36</td>
<td>37</td>
<td>38</td>
<td>39</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>42</td>
<td>43</td>
<td>44</td>
<td>45</td>
<td>46</td>
<td>47</td>
<td>48</td>
<td>49</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>52</td>
<td>53</td>
<td>54</td>
<td>55</td>
<td>56</td>
<td>57</td>
<td>58</td>
<td>59</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>62</td>
<td>63</td>
<td>64</td>
<td>65</td>
<td>66</td>
<td>67</td>
<td>68</td>
<td>69</td>
<td>70</td>
<td></td>
</tr>
<tr>
<td>71</td>
<td>72</td>
<td>73</td>
<td>74</td>
<td>75</td>
<td>76</td>
<td>77</td>
<td>78</td>
<td>79</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>82</td>
<td>83</td>
<td>84</td>
<td>85</td>
<td>86</td>
<td>87</td>
<td>88</td>
<td>89</td>
<td>90</td>
<td></td>
</tr>
</tbody>
</table>

**Question 7.26.** If a column contains at least one number relatively prime to 10, then are all entries in that column are relatively prime to 10? Why, if so?

**Answer:** Every number in the $j^{th}$ column is of the form $i \cdot 10 + j$ for $0 \leq i \leq 9$. Moreover it is well known fact that $\gcd(cb + a, b) = \gcd(a, b)$ [WHY?]. So in our setting $\gcd(i \cdot 10 + j, 10) = \gcd(j, 10)$. That is, if the top entry in the column is relatively prime to 10, then all entries in the column are too. Observe that there are $\phi(10) = 4$ of these columns.

**Question 7.27.** In the columns that are relatively prime to 10, circle the numbers that are ALSO relatively prime to 9. How many are there in each column. Why?

**Answer:** There are exactly $\phi(9) = 6$ of them in each of these columns. This is what we will prove in generality in the following theorem.
Proof That $\phi$ is Multiplicative

**Theorem 7.28.** The function $\phi$ is a multiplicative function. That is, for $m, n \in \mathbb{N}$ such that $\gcd(m, n) = 1$, we have $\phi(mn) = \phi(m) \cdot \phi(n)$.

**Proof.** Let $m, n \in \mathbb{N}$ such that $\gcd(m, n) = 1$. The theorem holds trivially if $m = n = 1$, so suppose that $m > 1$ and $n > 1$.

**WWTS:** $\phi(mn) = \phi(m) \cdot \phi(n)$.

Consider a table of values $1, 2, \ldots, mn$ with $m$ rows and $n$ columns as follows:

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>\cdots</th>
<th>$j$</th>
<th>\cdots</th>
<th>$n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$n + 1$</td>
<td>$n + 2$</td>
<td>$n + 3$</td>
<td>\cdots</td>
<td>$n + j$</td>
<td>\cdots</td>
<td>$2n$</td>
</tr>
<tr>
<td>2</td>
<td>$2n + 1$</td>
<td>$2n + 2$</td>
<td>$2n + 3$</td>
<td>\cdots</td>
<td>$2n + j$</td>
<td>\cdots</td>
<td>$3n$</td>
</tr>
<tr>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
<td>\vdots</td>
</tr>
<tr>
<td>$(m - 1)n + 1$</td>
<td>$(m - 1)n + 2$</td>
<td>$(m - 1)n + 3$</td>
<td>\cdots</td>
<td>$(m - 1)n + j$</td>
<td>\cdots</td>
<td>$mn$</td>
<td></td>
</tr>
</tbody>
</table>

[You Finish!] By definition $\phi(mn)$ is the number of entries in the table above which are relatively prime to $mn$. But a number is relatively prime to $mn$ if and only if it is relatively prime to $m$ and $n$ [WHY?].

Observe the following facts:

- The values in the $j^{th}$ column are of the form $i \cdot n + j$ for $0 \leq i \leq m - 1$.
- For each $0 \leq i \leq m - 1$, we know $\gcd(i \cdot n + j, n) = \gcd(j, n)$ [WHY?].
- Hence all the numbers in column $j$ for which $\gcd(j, n) = 1$ will be relatively prime to $n$ [WHY?]. There are exactly $\phi(n)$ such columns.
Proof That $\phi$ is Multiplicative (continued)

[You Finish!] It remains to show that in each of these $\phi(n)$ columns, there are EXACTLY $\phi(m)$ entries which are ALSO relatively prime to $m$. Consider one such column $j$ such that $\gcd(j, n) = 1$. The $m$ entries are

$$j, n + j, 2n + j, \ldots, (m - 1)n + j.$$ 

Observe the following facts:

- No two of these $m$ integers are congruent mod $m$ for otherwise there exists $0 \leq r < s \leq m - 1$ such that $rn + j \equiv sn + j \pmod{m}$.
- But then $rn \equiv sn \pmod{m}$ [WHY?]
- Hence $r \equiv s \pmod{m}$ [WHY?] which forces $r = s$ [WHY is this a contradiction?].
- So reduced modulo $m$, the $m$ numbers in this column $j$ are just a rearrangement of the $m$ values $0, 1, 2, \ldots, m - 1$.
- The number of numbers in the list $0, 1, 2, \ldots, m - 1$ which are relatively prime to $m$ is EXACTLY the value $\phi(m)$.

**BOTTOMLINE:** Hence in any of the $\phi(n)$ columns which have numbers all numbers relatively prime to $n$, there are exactly $\phi(m)$ of the entries in that column which are ALSO relatively prime to $m$. Therefore, we conclude

$$\phi(mn) = \phi(m) \cdot \phi(n).$$

Q.E.D.

**Example 7.29.** Calculate $\phi(18000)$. **HINT:** $18000 = 2^4 \cdot 3^2 \cdot 5^3$. [You Do!]

$$\phi(18000) = \phi(2^4) \cdot \phi(3^2) \cdot \phi(5^3)$$

$$= (16 - 2) \cdot (9 - 3) \cdot (125 - 5) = 14 \cdot 6 \cdot 120 = 10,080$$
7.6 Möbius Inversion Formula

Question 7.30. Who is Möbius?

- August Ferdinand Möbius (1790—1868), Germany
- His father was a dancing teacher and his mother was a descendant of Martin Luther
- He made contributions to astronomy, mechanics, projective geometry, optics, statics, and number theory
- He is best known for his discovery of a surface with one side, known as the Möbius strip

Definition 7.31. For a positive integer \( n \), define the Möbius function \( \mu \) by the rules

\[
\mu(n) = \begin{cases} 
1 & \text{if } n = 1 \\
0 & \text{if } p^2 \mid n \text{ for some prime } p \\
(-1)^r & \text{if } n = p_1p_2\cdots p_r \text{ where } p_i \text{ are distinct primes}
\end{cases}
\]

Find the first few values of \( \mu(n) \). [You Do!]

<table>
<thead>
<tr>
<th>( n )</th>
<th>( \mu(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>-1</td>
</tr>
<tr>
<td>3</td>
<td>-1</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>-1</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>-1</td>
</tr>
</tbody>
</table>

CONCEPTUAL EXERCISE: Suppose you had a squarefree \( n \in \mathbb{N} \) such that \( \omega(n) = 17 \). Compute \( \mu(n) \). [You Do!]

\[-1\]
Below is a graph of $\mu(n)$ for $1 \leq n \leq 50$.

![Graph of $\mu(n)$ for $1 \leq n \leq 50$.]

---

**Proof That $\mu$ is Multiplicative**

**Theorem 7.32.** The function $\mu$ is a multiplicative function.

**Proof.** Suppose $m, n \in \mathbb{N}$ such that $\gcd(m, n) = 1$.

**WWTS:** $\mu(mn) = \mu(m) \cdot \mu(n)$.

There are three cases.

**CASE 1:** ($m = 1$ or $n = 1$) When $m = 1$, we see that both $\mu(mn)$ and $\mu(m)\mu(n)$ equal $\mu(n)$. The case is similar for $n = 1$.

**CASE 2:** ($m$ or $n$ is not squarefree) Then $p^2 \mid m$ or $p^2 \mid n$ for some prime $p$, and hence $p^2 \mid m \cdot n$. Thus it is clear that

$$\mu(mn) = 0 = \mu(m)\mu(n).$$

**CASE 3:** ($m$ and $n$ are square-free integers greater than 1) Let $m = p_1p_2\cdots p_r$ and let $n = q_1q_2\cdots q_s$. Since $\gcd(m, n) = 1$ then $p_i \neq q_j$ for all $i, j$. It follows that

$$\mu(mn) = (-1)^r(-1)^s = \mu(m) \cdot \mu(n).$$

Thus $\mu$ is multiplicative.

Q.E.D.
Brief Detour: How to Make New Multiplicative Functions From Old Ones

**Theorem 7.33.** If $f$ is a multiplicative function, then so is $F$ where $F$ is defined

$$F(n) := \sum_{d|n} f(d).$$

**Proof.** Suppose $m, n \in \mathbb{N}$ such that $\gcd(m, n) = 1$.

**WWTS:** $F(mn) = F(m) \cdot F(n)$.

We have the following sequence of equalities:

$$F(mn) = \sum_{d|m \cdot n} f(d)$$

$$= \sum_{d=d_1d_2 \atop d_1|m \atop d_2|n} f(d_1d_2)$$

$$= \sum_{d=d_1d_2 \atop d_1|m \atop d_2|n} f(d_1)f(d_2) \quad \text{since } f \text{ is multiplicative}$$

$$= \left( \sum_{d_1|m} f(d_1) \right) \left( \sum_{d_2|n} f(d_2) \right)$$

$$= F(m) \cdot F(n).$$

Hence $F$ is multiplicative, as desired.

**Q.E.D.**
Concrete Example Time! Yay!

**EXERCISE (Part 1 of 2):** Define \( f : \mathbb{N} \rightarrow \mathbb{C} \) by \( f(n) = n^s \) for some fixed \( s \in \mathbb{C} \). Prove that \( f \) is multiplicative.

**ANSWER:** [You Do!]

*Proof.* Suppose \( m, n \in \mathbb{N} \) such that \( \gcd(m, n) = 1 \).

**WWTS:** \( f(mn) = f(m) \cdot f(n) \).

It is clear that \( f(mn) = (mn)^s = m^s n^s = f(m) \cdot f(n) \).

Q.E.D.

---

**Completely Multiplicative Function**

**Remark 7.34.** The function \( f \) defined above is an example of a *completely multiplicative function*. While this is a rather trivial example of a completely multiplicative function, we will see in Subsection 10.5 a less trivial example called the Legendre symbol \( \left( \frac{a}{p} \right) \).

**EXERCISE (Part 2 of 2):** Define \( \sigma_s : \mathbb{N} \rightarrow \mathbb{C} \) by \( \sigma_s(n) = \sum_{d|n} d^s \) for some fixed \( s \in \mathbb{C} \). By Theorem 7.33, we know that \( \sigma_s \) is multiplicative. But verify this when \( n = 15 \) and \( s = 4 \).

**ANSWER:** [You Do!] Observe that

\[
\sigma_4(3) = \sum_{d|3} d^4 = 1^4 + 3^4 \quad \text{and} \quad \sigma_4(5) = \sum_{d|5} d^4 = 1^4 + 5^4.
\]

It follows that

\[
\sigma_4(3) \cdot \sigma_4(5) = (1^4 + 3^4) \cdot (1^4 + 5^4) = 1^4 + 3^4 + 5^4 + 15^4 = \sigma_4(15)
\]

as desired. ✓
**ANSWER:** Yes, but we need the Möbius Inversion Formula (MIF) below.

**Theorem 7.35** (Möbius Inversion Formula). If $F$ and $f$ are arithmetic functions (not necessarily multiplicative) satisfying

$$F(n) = \sum_{d|n} f(d),$$

then we have

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

We omit the proof of MIF, but let’s get our hands dirty and do an example.

**Example 7.36.** Recall the functions $f, \sigma_s : \mathbb{N} \rightarrow \mathbb{C}$ defined by $f(n) = n^s$ and $\sigma_s(n) = \sum_{d|n} d^s$ for some fixed $s \in \mathbb{C}$. Use MIF to write $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d)$.

[You Do!]

$$f(n) = n^s = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sigma_s(d)$$
Example (continued) Since $f$ is multiplicative, it suffices to check the MIF version of $f$ on a power of a prime $p$, namely, $p^k$ for some $k \in \mathbb{N}$. [You Do!]

By MIF we have

$$f(p^k) = \sum_{d|p^k} \mu\left(\frac{p^k}{d}\right) \sigma_s(d).$$

But the only divisors $d$ of $p^k$ that result in a nonzero $\mu\left(\frac{p^k}{d}\right)$ are $p^k$ and $p^{k-1}$ [WHY?]. Since $\mu\left(\frac{p^k}{p^k}\right) = 1$ and $\mu\left(\frac{p^k}{p^{k-1}}\right) = -1$, we have

$$f(p^k) = \sigma_s(p^k) - \sigma_s(p^{k-1})$$
$$= (1^s + p^s + (p^2)^s + \cdots + (p^k)^s) - (1^s + p^s + (p^2)^s + \cdots + (p^{k-1})^s)$$
$$= (p^k)^s.$$

Example 7.37. It is a well-known result by Gauss that the following holds

$$N = \sum_{d|N} \phi(d).$$

We may view the left hand side of the equality above as the image of $N$ under the identity function $F(n) = n$. Then MIF implies the corresponding result [Why?]

$$\phi(N) = \sum_{d|N} \mu\left(\frac{N}{d}\right) d.$$ 

Set $N = 20$ and verify the equality above. [You Do!]

<table>
<thead>
<tr>
<th>$d$</th>
<th>$\frac{N}{d}$</th>
<th>$\mu\left(\frac{N}{d}\right)$</th>
<th>$\mu\left(\frac{N}{d}\right) d$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>20</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>-1</td>
<td>-4</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>-1</td>
<td>-10</td>
</tr>
<tr>
<td>20</td>
<td>1</td>
<td>1</td>
<td>20</td>
</tr>
</tbody>
</table>

The right column sum equals $8$. And $\phi(20) = \phi(4)\phi(5) = 8$. ✓
Finally the Proof of $F$ Multiplicative Implies $f$ Multiplicative

Theorem 7.38. If $F$ is a multiplicative function, then so is $f$ where $F$ is defined

$$F(n) := \sum_{d|n} f(d).$$

Proof. [You Do!] Suppose $m, n \in \mathbb{N}$ such that $\gcd(m, n) = 1$.

WWTS: $f(mn) = f(m) \cdot f(n)$.

If $d \mid mn$ then $d$ can be uniquely written as $d = d_1 d_2$, where $d_1 \mid m$ and $d_2 \mid n$ with $\gcd(d_1, d_2) = 1$. The following equalities hold

$$f(mn) = \sum_{d \mid mn} \mu(d) F\left( \frac{mn}{d} \right) \quad \text{by MIF}$$

$$= \sum_{d_1 \mid m \atop d_2 \mid n} \mu(d_1 d_2) F\left( \frac{mn}{d_1 d_2} \right) \quad \text{since } d = d_1 d_2$$

$$= \sum_{d_1 \mid m \atop d_2 \mid n} \mu(d_1) \mu(d_2) F\left( \frac{m}{d_1} \right) F\left( \frac{n}{d_2} \right) \quad \text{since } \mu \text{ multiplicative}$$

$$= \sum_{d_1 \mid m} \mu(d_1) F\left( \frac{m}{d_1} \right) \cdot \sum_{d_2 \mid n} \mu(d_2) F\left( \frac{n}{d_2} \right)$$

$$= f(m) \cdot f(n). \quad \text{by MIF}$$

Hence $f$ is multiplicative, as desired.

Q.E.D.
7.7 Exercises

A Very Cool Theorem – Exercise 1

Theorem 7.39. For any positive integer \( n \), it follows that

\[
\sum_{d|n} \sigma(d) = \sum_{d|n} \frac{n}{d} \cdot \tau(d).
\]

**Hands Dirty Part:** Is that even true!!!?? Let’s do one example with \( n = 15 \). Compute the left hand and right hand sides separately and confirm that they are equal. [You Do!]

The LHS is as follows:

\[
\sum_{d|15} \sigma(d) = \sigma(1) + \sigma(3) + \sigma(5) + \sigma(15)
\]

\[
= 1 + (1 + 3) + (1 + 5) + (1 + 3 + 5 + 15)
\]

\[
= 1 + 4 + 6 + 24
\]

\[
= 35.
\]

The RHS is as follows:

\[
\sum_{d|15} \frac{15}{d} \cdot \tau(d) = \frac{15}{1} \cdot \tau(1) + \frac{15}{3} \cdot \tau(3) + \frac{15}{5} \cdot \tau(5) + \frac{15}{15} \cdot \tau(15)
\]

\[
= 15 \cdot 1 + 5 \cdot 2 + 3 \cdot 2 + 1 \cdot 4
\]

\[
= 15 + 10 + 6 + 4
\]

\[
= 35.
\]

So yes, the LHS = RHS in this one example. ✓
Recall that we want to prove Theorem 7.39, which states the following holds

\[ \sum_{d|n} \sigma(d) = \sum_{d|n} \frac{n}{d} \cdot \tau(d) \]

for all \( n \in \mathbb{N} \).

**GAME PLAN STRATEGY!!**

First we denote the left hand and right hand sides of the equality as follows:

\[
F(n) := \sum_{d|n} \sigma(d) \quad \text{and} \quad G(n) := \sum_{d|n} \frac{n}{d} \cdot \tau(d).
\]

Then we do the following four steps to prove Theorem 7.39:

- **[STEP 1]** Prove \( F(n) \) is multiplicative.
- **[STEP 2]** Prove \( G(n) \) is multiplicative.
- **[STEP 3]** Prove \( F(p^k) = G(p^k) \) where \( p \) is prime and \( k \in \mathbb{N} \).
- **[STEP 4]** Conclude \( F(n) = G(n) \) as desired.

**[STEP 1]** Prove \( F(n) := \sum_{d|n} \sigma(d) \) is multiplicative.

(HINT: Use Theorem 7.33.)

*Proof. [You Do!] By the theorem in the hint, it is super duper ridiculously clear that \( F(n) \) is definitely multiplicative 🧡.

Q.E.D.*
**[STEP 2]** Prove $G(n) := \sum_{d|n} \frac{n}{d} \cdot \tau(d)$ is multiplicative.

**Proof.** Suppose $m, n \in \mathbb{N}$ such that $\gcd(m, n) = 1$.

**WWTS:** $G(mn) = G(m) \cdot G(n)$.

If $d \mid mn$ then $d$ can be uniquely written as $d = d_1d_2$, where $d_1 \mid m$ and $d_2 \mid n$ with $\gcd(d_1, d_2) = 1$. The following equalities hold [You Finish!]

\[
G(mn) = \sum_{d\mid mn} \frac{mn}{d} \cdot \tau(d) = \sum_{d_1\mid m, d_2\mid n} \frac{mn}{d_1d_2} \cdot \tau(d_1d_2)
\]

\[
= \sum_{d_1\mid m, d_2\mid n} \frac{mn}{d_1d_2} \cdot \tau(d_1)\tau(d_2)
\]

\[
= \sum_{d_1\mid m, d_2\mid n} \frac{m}{d_1} \cdot \tau(d_1) \cdot \frac{n}{d_2} \cdot \tau(d_2)
\]

\[
= \left( \sum_{d_1\mid m} \frac{m}{d_1} \tau(d_1) \right) \cdot \left( \sum_{d_2\mid n} \frac{n}{d_2} \tau(d_2) \right)
\]

\[
= G(m) \cdot G(n)
\]

Therefore the function $G$ is multiplicative, as desired.

Q.E.D.
[STEP 3] Prove $F(p^k) = G(p^k)$ where $p$ is prime and $k \in \mathbb{N}$.

Proof. Let $p$ be a prime and let $k \in \mathbb{N}$.

WWTS: $F(p^k) = G(p^k)$.

Since the divisors of $p^k$ are $p^0, p^1, p^2, \ldots, p^k$, we can compute $F(p^k)$ and $G(p^k)$, respectively, as follows. [You Finish!]

Computing $F(p^k)$, we get

\[
F(p^k) = \sum_{d \mid p^k} \sigma(d) \\
= (p^0) + (p^0 + p^1) + \cdots + (p^0 + p^1 + \cdots + p^k) \\
= (k + 1) \cdot p^0 + (k) \cdot p^1 + \cdots + (2)p^{k-1} + (1) \cdot p^k \\
= 1 \cdot p^k + 2 \cdot p^{k-1} + \cdots + k \cdot p + (k + 1) \cdot p^0
\] (1)

and computing $G(p^k)$, we get

\[
G(p^k) = \sum_{d \mid p^k} \frac{p^k}{d} \tau(d) \\
= \left(\frac{p^k}{p^0} \cdot \tau(p^0)\right) + \left(\frac{p^k}{p^1} \cdot \tau(p^1)\right) + \cdots + \left(\frac{p^k}{p^k} \cdot \tau(p^k)\right) \\
= 1 \cdot p^k + 2 \cdot p^{k-1} + \cdots + k \cdot p + (k + 1) \cdot p^0
\] (2)

Since (1) = (2), we have $F(p^k) = G(p^k)$.

Q.E.D.
[STEP 4] Prove $F(n) = G(n)$ for all $n$ in $\mathbb{N}$.

Proof. Let $n \in \mathbb{N}$.

**WWTS:** $F(n) = G(n)$.

Write the prime factorization of $n$ as follows $n = p_1^{k_1}p_2^{k_2} \cdots p_r^{k_r}$. [You Finish!]

Then we have the following sequence of equalities:

$$
F(n) = F(p_1^{k_1}p_2^{k_2} \cdots p_r^{k_r})
= F(p_1^{k_1})F(p_2^{k_2}) \cdots F(p_r^{k_r}) \quad \text{since } F \text{ is multiplicative}
= G(p_1^{k_1})G(p_2^{k_2}) \cdots G(p_r^{k_r}) \quad \text{since } F(p^k) = G(p^k) \text{ by Step 3}
= G(p_1^{k_1}p_2^{k_2} \cdots p_r^{k_r}) \quad \text{since } G \text{ is multiplicative}
= G(n).
$$

Thus $F(n) = G(n)$ as desired.

Q.E.D.

At last, we have finally finished proving the very cool Theorem 7.39:

$$
\sum_{d \mid n} \sigma(d) = \sum_{d \mid n} \frac{n}{d} \cdot \tau(d).
$$

Now consider the following:

**Theorem 7.40.** For any positive integer $n$, it follows that

$$
\sum_{d \mid n} \frac{n}{d} \cdot \sigma(d) = \sum_{d \mid n} \tau(d).
$$

We leave this proof as a HW exercise.
Tau Exercise 2

Find all positive integers \( n \) such that \( \tau(n) = 6 \).

**Hands Dirty Part:** We start by showing that this is true for some smaller integers \( n \). Recall that if \( n = p_1^{n_1}p_2^{n_2} \cdots p_r^{n_r} \) is the prime factorization of \( n \), then using “fattie product” notation, we have

\[
\tau(n) = \prod_{i=0}^{r} (n_i + 1).
\]

Consider \( n = 18 \) and compute \( \tau(n) \). [You Do!]

Since \( 18 = 2 \cdot 3^2 \), then \( \tau(18) = \tau(2)\tau(3^2) = (1 + 1) \cdot (2 + 1) = 6. \) ✓

Consider \( n = 32 \) and compute \( \tau(n) \). [You Do!]

Since \( 32 = 2^5 \), then \( \tau(32) = 5 + 1 = 6. \) ✓

We are now ready to find all such \( n \) such that \( \tau(n) = 6 \).

**SOLUTION TO THE EXERCISE:** [You Do!] We know that

- \( \tau(n) = \prod_{i=0}^{r} (n_i + 1) \) for \( n = p_1^{n_1}p_2^{n_2} \cdots p_r^{n_r} \).
- So \( \tau(n) = 6 \implies \prod_{i=0}^{r} (n_i + 1) = 6. \)
- 6 is a product of integers in only two ways: \( 2 \cdot 3 \) and \( 6 \cdot 1 \).
- Hence \( n \) can have at most two distinct prime factors. [WHY?]

Thus \( n = p^kq^j \) where WLOG \( k \geq 1 \) and \( j \geq 0 \). If \( \tau(n) = 6 \), then

- \( j = 0 \implies n = p^k \implies k = 5 \) is forced.
- \( j > 0 \implies n = p^kq^j \implies \) WLOG \( k = 2 \) and \( j = 1 \) is forced.

Hence \( n \) must be of the form \( p^2q \) or \( p^5 \), where \( p, q \) are distinct primes. ✓
Perfect Numbers Exercise 3

Recall Theorem 7.16 proven by Euclid which goes:

**Theorem.** If \( p \) and \( q = 2^p - 1 \) are prime, then \( 2^{p-1}q \) is a perfect number.

It turns out that the converse holds. In other words, we have a necessary and sufficient criterion for number being perfect and even as follows:

**Theorem 7.41.** An even number is perfect if and only if it is of the form \( n = 2^{p-1}(2^p - 1) \) where \( 2^p - 1 \) and \( p \) are both primes.

**Proof.** We prove the two directions.

\((\iff)\) This is done by Euclid in Theorem 7.16.

\((\implies)\) Suppose \( n \) is an even perfect number.

**WWTS:** \( n = 2^{p-1}(2^p - 1) \) where \( 2^p - 1 \) and \( p \) primes.

To prove this direction, we need to recall some trivial lemmas. Then we will prove this direction on the next page.

- **(Lemma 1)** The finite geometric series sum states that
  \[
  \sum_{k=0}^{n-1} r^k = \frac{r^n - 1}{r - 1}.
  \]

- **(Lemma 3)** A number \( n \) is perfect if and only if \( \sigma(n) = 2n \).

- **(Lemma 3)** A number \( n \in \mathbb{N} \) is prime if and only if \( \sigma(n) = n + 1 \). [Why?]

- **(Lemma 4)** If \( 2^n - 1 \) is a Mersenne prime, then \( n \) must be prime. [Why?]
Let us recall the direction that we are proving:

\[ \implies \] Suppose \( n \) is an even perfect number.

**WWTS:** \( n = 2^{p-1}(2^p - 1) \) where \( 2^p - 1 \) and \( p \) primes.

[You Finish!] Since \( n \) is even, then \( n = 2^k m \) for some \( k \in \mathbb{N} \) and \( m \) odd. Since \( \sigma \) is multiplicative, we have \( \sigma(n) = \sigma(2^k) \cdot \sigma(m) \). Thus we have

- \( \sigma(2^k) = 1 + 2 + 2^2 + \cdots + 2^k = \frac{2^{k+1} - 1}{2 - 1} \) by Lemma 1.
- So \( \sigma(n) = (2^{k+1} - 1) \cdot \sigma(m) \).

Also since \( n \) is perfect, then \( \sigma(n) = 2n \) by Lemma 2. Thus we have \( \sigma(n) = 2n = 2 \cdot 2^k m = 2^{k+1} m \). and therefore it follows that

\[
(2^{k+1} - 1) \cdot \sigma(m) = 2^{k+1} m \implies 2^{k+1} \sigma(m) - \sigma(m) = 2^{k+1} m \\
\implies 2^{k+1} \sigma(m) - 2^{k+1} m = \sigma(m) \\
\implies 2^{k+1} (\sigma(m) - m) = \sigma(m) \\
\implies 2^{k+1} \text{ divides } \sigma(m) \\
\implies \sigma(m) = 2^{k+1} b \text{ for some } b \in \mathbb{N}.
\]

Substituting this last expression for \( \sigma(m) \) into the equality

\[
(2^{k+1} - 1) \cdot \sigma(m) = 2^{k+1} m,
\]

we get \( (2^{k+1} - 1) \cdot 2^{k+1} b = 2^{k+1} m \). By canceling \( 2^{k+1} \) on both sides, we deduce \( (2^{k+1} - 1) \cdot b = m \) and hence \( b \) divides \( m \). Moreover \( b \neq m \) [WHY?]. We propose that we can establish the following two claims:

- **(Claim 1)** \( b = 1 \) is forced and hence \( \sigma(m) = 2^{k+1} \) and \( m = 2^{k+1} - 1 \).
- **(Claim 2)** \( \sigma(2^{k+1} - 1) = 2^{k+1} \) and hence \( 2^{k+1} - 1 \) is prime [WHY?].

Thus \( 2^{k+1} - 1 \) is a Mersenne prime and hence \( k+1 \) is prime [WHY?].
Proof of Claim 1 and Claim 2 (continued)

(Proof of Claim 1) Since \((2^{k+1} - 1) \cdot b = m\) and \(\sigma(m) = 2^{k+1}b\), then we have

\[ b + m = b + ((2^{k+1} - 1) \cdot b) = b + 2^{k+1}b - b = 2^{k+1}b = \sigma(m). \]

Suppose BWOC that \(b \neq 1\), then since \(b \mid m\) then \(m\) has at least three distinct divisors: 1, \(b\), and \(m\). And hence \(\sigma(m) \geq 1 + b + m\) contradicting the fact that \(\sigma(m) = b + m\). Thus \(b = 1\) follows. ✓

(Proof of Claim 2) Since \((2^{k+1} - 1) \cdot b = m\) and \(\sigma(m) = 2^{k+1}b\) and \(b = 1\), then we have

\[ m = 2^{k+1} - 1 \quad \text{and} \quad \sigma(2^{k+1} - 1) = 2^{k+1}. \]

By Lemma 3 (\(\Longleftrightarrow\) direction), we deduce that \(2^{k+1} - 1\) must be prime. Moreover, it is a Mersenne prime. Thus by Lemma 4, the exponent \(k + 1\) must also be prime. ✓

Recall from first line of this proof, that \(n = 2^k m\) was assumed. And thus

\[ n = 2^k m = 2^k \cdot (2^{k+1} - 1) \implies n = 2^{p-1}(2^p - 1), \]

if we denote the prime \(k + 1\) by \(p\). Thus we conclude

If \(n\) is an even perfect number, then \(n\) is of the form \(2^{p-1}(2^p - 1)\) where \(2^p - 1\) and \(p\) are prime.

Q.E.D.
8 Euler, Fermat, and Wilson

8.1 Motivation

aBa owns a jewelry store and wants to make multi-colored earrings out of beads and strings for his customers.

If aBa has $a$ colors and $p$ beads where $p$ is prime, what is the number of possible unique earrings that aBa can make?

**Question 8.1.** If we start out with 3 beads and 2 colors, how many different earrings can we make?

However...

- aBa does not like earrings of the same color. Nor does he want earrings that look the same. So we must get rid of these choices.

- We will figure out this problem in an exercise at the end of the section!
8.2 Fermat’s Little Theorem and Pseudoprimes

Question 8.2. Who is Fermat?

- Pierre de Fermat (1607—1665), France
- Given credit for early developments that lead to infinitesimal calculus
- He has also made notable contributions to analytic geometry, probability, and optics
- First person known to have evaluated the integral of general power functions
- Despite claiming to have proven all of his arithmetic theorems, few records of his proofs have survived

Thought Exercise: Consider the powers $a^k \pmod{p}$ for $a = 1, \ldots, k - 1$ for each $k = 3, 5,$ and 7. Fill in the blanks in the tables below. [You Do!]

For $k = 3$, we have

<table>
<thead>
<tr>
<th>$a$</th>
<th>$a^2 \pmod{3}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$1^2 = 1$</td>
</tr>
<tr>
<td>2</td>
<td>$2^2 = 4 \equiv 1$</td>
</tr>
</tbody>
</table>

For $k = 5$, we have

<table>
<thead>
<tr>
<th>$a$</th>
<th>$a^2 \pmod{5}$</th>
<th>$a^3 \pmod{5}$</th>
<th>$a^4 \pmod{5}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$1^2 = 1$</td>
<td>$1^3 = 1$</td>
<td>$1^4 = 1$</td>
</tr>
<tr>
<td>2</td>
<td>$2^2 = 4$</td>
<td>$2^3 = 8 \equiv 3$</td>
<td>$2^4 = 16 \equiv 1$</td>
</tr>
<tr>
<td>3</td>
<td>$3^2 = 9 \equiv 4$</td>
<td>$3^3 = 27 \equiv 2$</td>
<td>$3^4 = 81 \equiv 1$</td>
</tr>
<tr>
<td>4</td>
<td>$4^2 = 16 \equiv 1$</td>
<td>$4^3 = 64 \equiv 4$</td>
<td>$4^4 = 256 \equiv 1$</td>
</tr>
</tbody>
</table>
QUESTION 1: By examining the row entries in each of the two tables, what conjecture do you make?

ANSWER 1: The values 1, 2 appear in row \( a = 2 \) of the first table. And the values 1, 2, 3, 4 appear in rows \( a = 2 \) and \( a = 3 \) in the second table.

QUESTION 2: By examining the last column in the two tables above for \( a^{p-1} \mod p \), when \( p = 3 \) and \( p = 5 \), what conjecture can you make for the values \( a^{p-1} \mod p \) and \( a^p \mod p \) for all primes \( p \)?

ANSWER 2: We conjecture that \( a^{p-1} \equiv 1 \mod p \) when \( a \nmid p \) and \( a^p \equiv a \mod p \) for all \( a \), provided that \( p \) is prime.

To give more belief in your conjecture let us examine the \( p = 7 \) setting. [You Do!]

<table>
<thead>
<tr>
<th></th>
<th>( a^2 \mod 7 )</th>
<th>( a^3 \mod 7 )</th>
<th>( a^4 \mod 7 )</th>
<th>( a^5 \mod 7 )</th>
<th>( a^6 \mod 7 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1² = 1</td>
<td>1³ = 1</td>
<td>1⁴ = 1</td>
<td>1⁵ = 1</td>
<td>1⁶ = 1</td>
</tr>
<tr>
<td>2</td>
<td>2² = 4</td>
<td>2³ ≡ _1</td>
<td>2⁴ ≡ _2</td>
<td>2⁵ ≡ _4</td>
<td>2⁶ ≡ _1</td>
</tr>
<tr>
<td>3</td>
<td>3² ≡ _2</td>
<td>3³ ≡ _6</td>
<td>3⁴ ≡ _4</td>
<td>3⁵ ≡ _5</td>
<td>3⁶ ≡ _1</td>
</tr>
<tr>
<td>4</td>
<td>4² ≡ _2</td>
<td>4³ ≡ _1</td>
<td>4⁴ ≡ _4</td>
<td>4⁵ ≡ _2</td>
<td>4⁶ ≡ _1</td>
</tr>
<tr>
<td>5</td>
<td>5² ≡ _4</td>
<td>5³ ≡ _6</td>
<td>5⁴ ≡ _2</td>
<td>5⁵ ≡ _3</td>
<td>5⁶ ≡ _1</td>
</tr>
<tr>
<td>6</td>
<td>6² ≡ _1</td>
<td>6³ ≡ _6</td>
<td>6⁴ ≡ _1</td>
<td>6⁵ ≡ _6</td>
<td>6⁶ ≡ _1</td>
</tr>
</tbody>
</table>

Theorem 8.3 (Fermat’s Little Theorem). For \( p \) prime and \( a \in \mathbb{Z} \), it follows that \( a^p \equiv a \mod p \). Alternatively, if \( \gcd(a, p) = 1 \), then \( a^{p-1} \equiv 1 \mod p \).

We prove this two pages from now!

The converse of Fermat’s Little Theorem is

If \( a^{n-1} \equiv 1 \mod n \) for some integer \( a \), then \( n \) is not necessarily prime.
Observe that the converse does not necessarily always hold. For example, let \( a = 2 \) and \( n = 341 \).

\[
2^{340} \equiv 1 \pmod{341} \text{ but } 341 = 11 \cdot 31 \implies \text{ not prime}
\]

**Definition 8.4.** A composite integer \( n \) is called **pseudoprime** whenever

\[
n \mid 2^n - 1.
\]

More generally, a composite integer \( n \) for which \( a^n \equiv a \pmod{n} \) is called a **pseudoprime to the base** \( a \).

There exist composite numbers \( n \) that are pseudoprimes to every base \( a \); that is, there are composite numbers \( n \) such that \( a^{n-1} \equiv 1 \pmod{n} \) for all integers \( a \) with \( \gcd(a, n) = 1 \). These numbers are called **absolute pseudoprimes** or **Carmichael numbers**.

**Example 8.5.** Show that 561 is an absolute pseudoprime.

To see that 561 = 3 \cdot 11 \cdot 17 must be an absolute pseudoprime, notice that \( \gcd(a, 561) = 1 \) gives

\[
gcd(a, 3) = gcd(a, 11) = gcd(a, 17) = 1.
\]

Using Fermat’s theorem leads to

\[
a^2 \equiv 1 \pmod{3} \quad a^{10} \equiv 1 \pmod{11} \quad a^{16} \equiv 1 \pmod{17}
\]

which implies

\[
a^{560} \equiv (a^2)^{280} \equiv 1 \pmod{3}
\]

\[
a^{560} \equiv (a^{10})^{56} \equiv 1 \pmod{11}
\]

\[
a^{560} \equiv (a^{16})^{35} \equiv 1 \pmod{17}
\]

Thus \( a^{560} \equiv 1 \pmod{561} \) where \( \gcd(a, 561) = 1 \). But then \( a^{561} \equiv a \pmod{561} \) for all \( a \), showing 561 to be an absolute pseudoprime.
Lemmas Used to Prove Fermat’s Little Theorem

To prove Fermat’s Little Theorem, we first need to recall Lemma 4.16 (i.e., Euclid’s Lemma).

**Lemma.** Let $p$ be a prime.

(i) If $p | mn$ where $m, n \in \mathbb{Z}$, then $p | m$ or $p | n$.

(ii) If $p | m_1 m_2 \cdots m_r$ where $m_i \in \mathbb{Z}$ for all $i$, then $p | m_i$ for some $i$.

The other necessary result is motivated by the following example.

**Example 8.6.** Consider the case where $a = 3$ and $p = 7$. Then $\gcd(a, p) = 1$. Fill in the missing blanks in the table below:

<table>
<thead>
<tr>
<th>$a$</th>
<th>$2a \pmod{7}$</th>
<th>$3a \pmod{7}$</th>
<th>$4a \pmod{7}$</th>
<th>$5a \pmod{7}$</th>
<th>$6a \pmod{7}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>6</td>
<td>28 $\equiv$ 1</td>
<td>10 $\equiv$ 3</td>
<td>12 $\equiv$ 5</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>9 $\equiv$ 2</td>
<td>12 $\equiv$ 5</td>
<td>15 $\equiv$ 1</td>
<td>18 $\equiv$ 4</td>
</tr>
<tr>
<td>4</td>
<td>8 $\equiv$ 1</td>
<td>12 $\equiv$ 5</td>
<td>16 $\equiv$ 2</td>
<td>20 $\equiv$ 6</td>
<td>24 $\equiv$ 3</td>
</tr>
<tr>
<td>5</td>
<td>10 $\equiv$ 3</td>
<td>15 $\equiv$ 1</td>
<td>20 $\equiv$ 6</td>
<td>25 $\equiv$ 4</td>
<td>30 $\equiv$ 2</td>
</tr>
<tr>
<td>6</td>
<td>12 $\equiv$ 5</td>
<td>18 $\equiv$ 4</td>
<td>24 $\equiv$ 3</td>
<td>30 $\equiv$ 2</td>
<td>36 $\equiv$ 1</td>
</tr>
</tbody>
</table>

**Question:** By examining the six rows of the values $a, 2a, \ldots, 6a$ for each $a \in \{1, 2, \ldots, 6\}$, what observation/conjecture do you make for all $a, p \in \mathbb{N}$ such that $\gcd(a, p) = 1$ and $p$ is prime?

**Answer:** We conjecture that the $p - 1$ numbers $a, 2a, \ldots, (p - 1)a$ reduced mod $p$ are a rearrangement of the numbers $1, 2, \ldots, p - 1$. We call this the **rearrangement property**.

Prove your conjecture on the next page. [You Do!]
Proof of conjecture from previous page: [You Do!]

Let $a, p \in \mathbb{N}$ such that $\gcd(a, p) = 1$ and $p$ is prime. Consider the $p - 1$ numbers $a, 2a, \ldots, (p - 1)a$.

**WWTS:** $a, 2a, \ldots, (p - 1)a$ reduced mod $p$ are a rearrangement of the numbers $1, 2, \ldots, p - 1$.

For each $k \in \{1, \ldots, p - 1\}$, observe that none of the numbers $ka$ in our list $a, 2a, \ldots, (p - 1)a$ is congruent to $0$ (mod $p$). For if $ka \equiv 0$ (mod $p$) then $p$ divides $ka$, but Euclid’s Lemma prevents this [WHY?]. Thus we know that the numbers $a, 2a, \ldots, (p - 1)a$ reduced mod $p$ are strictly between $1$ and $p - 1$. So it suffices to show that the $p - 1$ number reduced mod $p$ are all distinct numbers in the sequence $1, 2, \ldots, p - 1$.

Suppose BWOC that two of the distinct products $ka$ and $ma$ in the list $a, 2a, \ldots, (p - 1)a$ are not distinct mod $p$. That is,

$$1 \leq k, m \leq p - 1 \text{ such that } k \neq m \text{ and } ka \equiv ma \pmod{p}.$$  

The cancellation property (recall Theorem 6.8) implies $k \equiv m \pmod{p}$. But that is a contradiction [WHY?]. Thus the list $a, 2a, \ldots, (p - 1)a$ reduced mod $p$ are distinct members of the sequence $1, 2, \ldots, p - 1$. Since there are exactly $p - 1$ of these, the only possibility is that the former is a rearrangement of the latter.

Q.E.D.
Proof of Fermat’s Little Theorem

Theorem (Fermat’s Little Theorem). For \( p \) prime and \( a \in \mathbb{Z} \), it follows that \( a^p \equiv a \pmod{p} \). Alternatively, if \( \gcd(a,p) = 1 \), then \( a^{p-1} \equiv 1 \pmod{p} \).

Before we prove FLT, first note the following observations:

1. We want to prove that \( a^p \equiv a \pmod{p} \) for EVERY prime \( p \) and EVERY integer \( a \).

2. It suffices to consider \( 0 \leq a \leq p - 1 \) by laws of modular arithmetic. \([Why?]\) When reducing \( a^p \pmod{p} \) you may FIRST reduce \( a \pmod{p} \) then exponentiate.

3. It suffices to first prove that for \( a \) in the range \( 1 \leq a \leq p - 1 \) (and hence \( \gcd(a,p) = 1 \)) that \( a^{p-1} \equiv 1 \pmod{p} \) holds.

4. Thus FLT in the form \( a^p \equiv a \pmod{p} \) holds by multiplying both sides of \( a^{p-1} \equiv 1 \pmod{p} \) by \( a \). Note if \( a = 0 \), then \( a^p \equiv a \pmod{p} \) holds trivially.

So let us prove that if \( \gcd(a,p) = 1 \), then \( a^{p-1} \equiv 1 \pmod{p} \).

Proof. \([You do!]\) Let \( a, p \in \mathbb{N} \) such that \( \gcd(a,p) = 1 \) and \( p \) is prime.

\[ \text{WWTS: } a^{p-1} \equiv 1 \pmod{p}. \]

Consider the \( p - 1 \) numbers \( a, 2a, \ldots, (p - 1)a \). By the rearrangement lemma, we know that list \( a, 2a, \ldots, (p-1)a \pmod{p} \) is just a rearrangement of the sequence \( 1, 2, \ldots, p - 1 \). Therefore if we multiply together the numbers in each sequence, the results must be identical \( \pmod{p} \):

\[ a \times 2a \times 3a \times \cdots \times (p - 1)a \equiv 1 \times 2 \times 3 \times \cdots \times (p - 1) \pmod{p}. \]

And hence \( a^{p-1} \cdot (p - 1)! \equiv (p - 1)! \pmod{p} \) \([WHY?]\). And hence we conclude that \( a^{p-1} \equiv 1 \pmod{p} \) \([WHY \ CAN \ THE \ (p - 1)! \ CANCEL?]\).

Q.E.D.
8.3 Wilson’s Theorem

**Question 8.7. Who is Wilson?**

- John Wilson (1741—1793), England
- He was Fellow of the Royal Society (for making a huge contribution to mathematics)
- He was also a judge of the Court of Common Pleas and judged civil disputes
- He died 5 years after his marriage

**Theorem 8.8** (Wilson’s Theorem). For \( p \) prime, \((p - 1)! \equiv -1 \pmod{p}\).

Note that for \( p = 2 \) and \( p = 3 \), this theorem easily follows. For \( p = 2 \) we have \((2 - 1)! = 1 \equiv -1 \pmod{2}\) and for \( p = 3 \) we have \((3 - 1)! = 2 \equiv -1 \pmod{3}\). Thus the proof begins with the case where \( p > 3 \).

**NOTE:** Before we prove this for all \( p > 3 \), let’s look at a motivating example.

**Example 8.9.** Show that Wilson’s Theorem is true for \( p = 13 \).

Let’s find some products using 2, 3, . . . , 11 where each product is congruent to 1 modulo 13.

\[
\begin{align*}
2 \cdot 7 &\equiv 1 \pmod{13} \\
3 \cdot 9 &\equiv 1 \pmod{13} \\
4 \cdot 10 &\equiv 1 \pmod{13} \\
5 \cdot 8 &\equiv 1 \pmod{13} \\
6 \cdot 11 &\equiv 1 \pmod{13}
\end{align*}
\]

Multiplying these congruences gives the result

\[
11! = (2 \cdot 7)(4 \cdot 10)(5 \cdot 8)(6 \cdot 11) \equiv 1 \pmod{13}
\]

and so

\[
12! \equiv 12 \equiv -1 \pmod{13}
\]

Thus \((p - 1)! \equiv -1 \pmod{p}\) for \( p = 13 \).
Proof of Wilson’s Theorem

It may first be helpful to recall a MAJOR result (Theorem 6.12) in congruence theory. That theorem stated \( ax \equiv b \pmod{n} \) has a solution if and only if

\[
\gcd(a, n) = 1 \quad \text{[You Do!]} \]

Recall that since we know the Wilson’s Theorem holds for primes \( p = 2 \) and \( p = 3 \), we are proving the following:

For all primes \( p > 3 \), we have

\[(p - 1)! \equiv -1 \pmod{p}.\]

Proof. Suppose \( p \) is a prime greater than 3.

**WWTS:** \((p - 1)! \equiv -1 \pmod{p}.

We claim that each of the integers in the set \( \{1, 2, \ldots, p - 1\} \) has an inverse modulo \( p \). This follows since the equation \( ax \equiv 1 \pmod{p} \) has a solution if and only if \( \gcd(a, p) = 1 \). And each \( a \in \{1, 2, \ldots, p-1\} \) clearly satisfies this. Moreover, this inverse is unique; for suppose otherwise that \( b \) and \( c \) were both inverses for \( a \) then \( ab \equiv 1 \pmod{p} \) and \( ac \equiv 1 \pmod{p} \). And hence \( ab \equiv ac \pmod{p} \). By cancellation, then \( b \) and \( c \) are equivalent modulo \( p \). Thus inverses are unique. Moreover, the value 1 is clearly its own inverse. And \( p - 1 \) is also its own inverse since \( (p - 1)^2 = (p - 1)(p - 1) = p^2 - 2p + 1 \equiv 1 \pmod{p} \).

Thus we can partition the set \( \{2, 3, \ldots, p - 2\} \) into distinct pairs \( \{a, b\} \) such that \( ab \equiv 1 \pmod{p} \). Thus by rearrangement we have

\[
(2 \cdot 3 \cdot 4 \cdots (p - 2)) \equiv 1 \pmod{p}.
\]

Multiplying both sides by \( p - 1 \) gives \((p - 1)! \equiv p - 1 \equiv -1 \pmod{p} \).

Q.E.D.
8.4 Euler’s Theorem

Recall Theorem 8.3. Euler generalized this theorem from the case of a prime $p$ to an arbitrary positive integer $n$ using Euler’s phi function. This celebrated result is stated in the theorem below.

**Theorem 8.10** (Euler’s Theorem). If $n \geq 1$ and $\gcd(a, n) = 1$, then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$  

**Base Case:** ($n = 1$)
- **LHS** is $a^{\phi(1)} = a^1 = a$
- **RHS** is $1 \pmod{1}$

**Induction Hypothesis:** Assume $a^{\phi(p^k)} \equiv 1 \pmod{p^k}$ for some $k \geq 1$.

**WWTS:** $a^{\phi(p^{k+1})} \equiv 1 \pmod{p^{k+1}}$

[Complete the proof!]

$$a^{\phi(p^{k+1})} = a^{p^{k+1} - p^k} = a^{p(p^k - p^{k-1})}$$

$$= a^{p\phi(p^k)}$$

$$= (a^{\phi(p^k)})^p$$

$$= (1 + qp^k)^p \quad \text{by the Induction Hypothesis}$$

$$= 1 + \binom{p}{1}qp^k + \binom{p}{2}(qp^k)^2 + \cdots + \binom{p}{p-1}(qp^k)^{p-1} + (qp^k)^p$$

$$\equiv 1 + \binom{p}{1}qp^k \pmod{p^{k+1}}$$

But $p \mid \binom{p}{1}$ and so $p^{k+1} \mid (\binom{p}{1}qp^k)$. Thus $a^{\phi(p^{k+1})} \equiv 1 \pmod{p^{k+1}}$.

**Q.E.D.**
8.5 Exercises

Fermat’s Little Theorem Exercise 1

Recall the motivation exercise.

**Question 8.11.** How do we know that there are only two unique earring possible out of the 8 options?

First we removed the strings that were just odd colored.

But we can see that

**Observation:** The size of the group must be based on the amount of rotations it takes to get to the original!

**Question 8.12.** What does this mean?

The original set of all multi colored earrings divides evenly into groups of size three.
Let’s try this with 4 beads!

**Question 8.13.** Are any of these earrings identical?

**Question 8.14.** What about 5? Will they break equally?

*Yes, 5 can’t be broken into equal parts.*
Let’s try this with 5 beads!
Question 8.15. *What is special about the particular numbers 2, 3, 5?*
They are prime numbers!

Question 8.16. *What if we add more colors?*

*for any color, $p$ beads $\Rightarrow p$ rotations*

Question 8.17. *How does this relate to Fermat’s little theorem?*

- given $a$ number of colors, and $p$ beads per earring which are prime, the number of possible strings is $a \cdot a \cdot a \cdots a = a^p$.

- When we remove the mono-colored strings, we remove $a$ strings. So there are a total of $a^p - a$ strings.

- When we take the strings to form unique earrings, we find that the groups of strings are size $p$ since each earring must have $p$ rotations.

- Therefore $p$ divides $a^p - a$. In other words, if $p \mid a^p$, we will get some number $x$ with a remainder of $a$. Equivalently, this is

$$a^p \equiv a \pmod{p}.$$
Phi Function Exercise 2

**EXERCISE:** Prove that the following theorem holds for $n = 10$. [You Do!]

**Theorem 8.18.** For each positive integer $n \geq 1$,

$$n = \sum_{d \mid n} \phi(d)$$

the sum being extended over all positive divisors of $n$.

Recall that we saw the summation above in Example 7.37 in the previous section.

The integers between 1 and 10 can be separated into classes as follows: If $d$ is a positive divisor of 10, we put the integer $m$ into the class $S_d$ as shown

$$S_d = \{m \mid \gcd(m, 10) = d; 1 \leq m \leq 10\}.$$

So the classes of $S_d$ are

- $S_1 = \{1, 3, 7, 9\}$
- $S_2 = \{2, 4, 6, 8\}$
- $S_5 = \{5\}$
- $S_{10} = \{10\}$

These contain $\phi(1) = 1$, $\phi(2) = 1$, $\phi(5) = 4$, $\phi(10) = 4$ integers, respectively. Therefore

$$\sum_{d \mid 10} \phi(d) = \phi(10) + \phi(5) + \phi(2) + \phi(1)$$

$$= 4 + 4 + 1 + 1$$

$$= 10$$
Wilson’s Theorem Exercise 3

**EXERCISE:** Find the remainder of 53! when divided by 61. [You Do!]

**SOLUTION:** By Wilson’s Theorem, we know that

\[
60! \equiv -1 \pmod{61}.
\]

But how does that help us solve this problem? [You Finish!]

We have \(60! \equiv -1 \pmod{61}\), so this implies

\[
60 \cdot 59 \cdot 58 \cdot 57 \cdot 56 \cdot 55 \cdot 54 \cdot 53! \equiv -1 \pmod{61}
\]

\[
(-1)(-2)(-3)(-4)(-5)(-6)(-7) \cdot 53! \equiv -1 \pmod{61}
\]

\[
-1 \cdot (2 \cdot 5 \cdot 6) \cdot (3 \cdot 4 \cdot 7) \cdot 53! \equiv -1 \pmod{61}
\]

\[
-1 \cdot -1 \cdot (3 \cdot 4 \cdot 7) \cdot 53! \equiv -1 \pmod{61}
\]

\[
(3 \cdot 4 \cdot 7) \cdot 53! \equiv -1 \pmod{61}
\]

Now so far we have not needed any calculator, pen, or paper. To continue in this manner, perhaps notice that \(3 \cdot 4 = 12\) so if we multiply both sides by 5, we will get a 60 on the left side as follows.

\[
12 \cdot 7 \cdot 53! \equiv -1 \pmod{61}
\]

\[
5 \cdot 12 \cdot 7 \cdot 53! \equiv 5 \cdot -1 \pmod{61}
\]

\[
60 \cdot 7 \cdot 53! \equiv -5 \pmod{61}
\]

\[
-1 \cdot 7 \cdot 53! \equiv -5 \pmod{61}
\]

\[
7 \cdot 53! \equiv 5 \pmod{61}
\]

Notice that \(5 \equiv -56 \pmod{61}\). This is advantageous cuz we can write

\[
7 \cdot 53! \equiv -56 \pmod{61}
\]

So by “cancelling 7s” on both sides (a legal move since \(\gcd(7, 61) = 1\)), we get \(53! \equiv -8 \pmod{61}\). Equivalently \(53! \equiv 53 \pmod{61}\). So the answer is 53. ✓
**Euler’s Theorem Exercise 4**

**EXERCISE:** Solve the congruence $314^{164} \equiv x \pmod{165}$. [You Do!]

**SOLUTION:** We factorize 314 as $2 \times 157$, and 165 as $3 \times 5 \times 11$, so that tells us that $\gcd(314, 165) = 1$ so we may employ Euler’s Theorem and deduce

$$314^{\varphi(165)} \equiv 1 \pmod{165}.$$  

But how does that help us solve this problem? [You Finish!]

First we compute $\varphi(165)$ as follows:

$$\varphi(165) = \varphi(3) \cdot \varphi(5) \cdot \varphi(11) = 2 \cdot 4 \cdot 10 = 80,$$

and hence Euler’s Theorem yield $314^{80} \equiv 1 \pmod{165}$. By the division algorithm, we can write the exponent 164 as $80 \cdot 2 + 4$. Thus we can assert the following:

$$314^{164} = 314^{80 \cdot 2 + 4} = (314^{80})^2 \cdot 314^4 \equiv 1^2 \cdot 314^4 \pmod{165} \equiv 314^4 \pmod{165}.$$

So it suffices to compute by BRUTE FORCE the first four powers of 314 ‘modding out by 165’ each time to make sure the powers don’t get too large.

- $314^2 = 98596 \equiv 91 \pmod{165}$
- $314^3 = 314^2 \cdot 314 \equiv 91 \cdot 314 \equiv 28574 \equiv 29 \pmod{165}$
- $314^4 = (314^2)^2 \equiv 91^2 \equiv 8281 \equiv 31 \pmod{165}$

Thus the solution to our problem is $x = 31$.  

✓
QUESTION: What might the image below represent?

ANSWER: This appears to be the multiplication table for clocks. For example, 7 o’clock times 5 o’clock equals 35 o’clock (or equivalently, 11 o’clock).
The clock table on the previous page, did not represent what will eventually define to be a group. It had “issues” so to speak. The table below however has no “issues”. Below represents a group just fine.

\[
\begin{array}{c|cccccccccc}
\hline
& 1\text{ o’clock} & 2\text{ o’clock} & 3\text{ o’clock} & 4\text{ o’clock} & 5\text{ o’clock} & 6\text{ o’clock} & 7\text{ o’clock} & 8\text{ o’clock} & 9\text{ o’clock} & 10\text{ o’clock} & 11\text{ o’clock} \\
\hline
1\text{ o’clock} & 
& 
& 
& 
& 
& 
& 
& 
& 
& 
& \\
2\text{ o’clock} & 
& 
& 
& 
& 
& 
& 
& 
& 
& 
& \\
3\text{ o’clock} & 
& 
& 
& 
& 
& 
& 
& 
& 
& 
& \\
4\text{ o’clock} & 
& 
& 
& 
& 
& 
& 
& 
& 
& 
& \\
5\text{ o’clock} & 
& 
& 
& 
& 
& 
& 
& 
& 
& 
& \\
6\text{ o’clock} & 
& 
& 
& 
& 
& 
& 
& 
& 
& 
& \\
7\text{ o’clock} & 
& 
& 
& 
& 
& 
& 
& 
& 
& 
& \\
8\text{ o’clock} & 
& 
& 
& 
& 
& 
& 
& 
& 
& 
& \\
9\text{ o’clock} & 
& 
& 
& 
& 
& 
& 
& 
& 
& 
& \\
10\text{ o’clock} & 
& 
& 
& 
& 
& 
& 
& 
& 
& 
& \\
11\text{ o’clock} & 
& 
& 
& 
& 
& 
& 
& 
& 
& 
& \\
\hline
\end{array}
\]

**QUESTION:** What do you think are some good aspects that this clock table has that the clock table on the other page did not possess? [List them below]

- The operation here is addition.
- Each row and column has exactly all 12 different clocks. The table on the previous page did not have this feature.
- There is an “identity” clock, namely 12 o’clock. If you add that to any time, you get the same exact time back.
- For each time \( x \) o’clock, there exists a time \( y \) o’clock such that if you add those two clocks you get 12 o’clock. Each \( x \) has an inverse!
Addition versus Multiplication?

**QUESTION:** Is it the multiplication that makes it not work? Hmmm. . . in the case of the 12 clocks, we only had a nice structure when we used addition. But consider the world where there are only 6 clocks, and the times are 1 o’clock thru 6 o’clock, and we are living in the modulo 7 world. Here is the multiplication table.

![Multiplication Table]

**QUESTION:** Is everything fine here? Is there an identity? Do inverses exist? Well the answer is yes. Because what you are looking at is essentially the following:

\[ \text{the multiplicative cyclic group of units in the group } (\mathbb{Z}_7, \oplus) \]
9.2 The Groups \((\mathbb{Z}_n, \oplus)\) and \((\mathbb{U}(n), \cdot)\)

Though this course does not assume one knows abstract algebra, the concept of a group is useful in number theory since a good deal of it involves the additive group \((\mathbb{Z}_n, \oplus)\) and its unit group \((\mathbb{U}(n), \cdot)\), both to be defined shortly.

**Definition 9.1.** A binary operation \(*\) on a set \(S\) is a function that associates to each ordered pair \((a, b)\) in the Cartesian product \(S \times S\) an element of \(S\) which we call \(a * b\).

**Note:** The definition of a Cartesian product of two sets \(A\) and \(B\) is
\[
A \times B := \{(a, b) \mid a \in A \text{ and } b \in B\}.
\]

**What is meant by the term “closed under *”**

**Remark 9.2.** Since we know that the “product” \(a * b\) lies in \(S\) for \(a, b \in S\), we say that the binary operation is closed under \(*\). Hence EVERY binary operation is closed by definition! However, when defining a binary operation, we must always verify that closure holds!

**Definition 9.3.** A set \(G\) with binary operation \(*\) is called a group if it satisfies the four properties.

- **[Closure]** \(\forall a, b \in G, \text{ we have } a * b \in G.\)
- **[Associativity]** \(\forall a, b, c \in G, \text{ we have } (a * b) * c = a * (b * c).\)
- **[Identity]** \(\exists e \in G \text{ such that } a * e = e * a \ \forall a \in A.\)
- **[Inverse]** \(\forall a \in G, \exists a^{-1} \in G \text{ such that } a * a^{-1} = e = a^{-1} * a.\)

We denote the group \(G\) with binary operation \(*\) by the tuple notation \((G, *)\).

**NOTE:** We can show that for each \((G, *)\), the identity \(e\) is unique. Also, for each \(a \in G\), its inverse \(a^{-1}\) is also unique.
Example 9.4. We determine if the following sets are groups.

(i) \((\mathbb{Z}, +)\) is a group. [Why?]

- \(a, b \in \mathbb{Z} \implies a + b \in \mathbb{Z}\).
- \(a, b, c \in \mathbb{Z} \implies a + (b + c) = (a + b) + c\).
- There exists a unique identity element \(0 \in \mathbb{Z}\) such that \(a + 0 = 0 + a\) for all \(a \in \mathbb{Z}\).
- \(a \in \mathbb{Z} \implies -a\) exists and is unique.

(ii) \((\mathbb{Z}, \cdot)\) is not a group.

- [Is the operation closed?] Yes.
- [Is the operation associative?] Yes.
- [Is there an identity?] Yes, 0 is the identity.
- [Do inverses exist?] No, because 7 has no inverse in \(\mathbb{Z}\) since \(\frac{1}{7} \notin \mathbb{Z}\).

(iii) Even integers under addition \((2\mathbb{Z}, +)\) is a group. [ELFS]

(iv) Odd integers under addition \((2\mathbb{Z} + 1, +)\) is a not a group.

- [Is the operation closed?] No since \(1 + 1 = 2 \notin 2\mathbb{Z} + 1\).
- [Is the operation associative?] Yes.
- [Is there an identity?] No. It would be 0 but 0 \(\notin 2\mathbb{Z} + 1\).
- [Do inverses exist?] No, because 7 has no inverse in \(\mathbb{Z}\) since \(\frac{1}{7} \notin \mathbb{Z}\).
- **BOTTOMLINE:** This is EXTREMELY not a group.

(v) \((\mathbb{R}, +)\) is a group. [ELFS]

(vi) \((\mathbb{R}, \cdot)\) is not a group. [Why?] 0 has no inverse in \(\mathbb{R}\).

(vii) \((\mathbb{R} - \{0\}, \cdot)\) is a group. [What is the identity?] 1

(viii) Is \(\mathbb{R} - \{1\}\) under the operation \(a \ast b = a + b - ab\) a group? [This is HW.]

(ix) Let \(G\) be the set of all real-valued functions \(f\) on \(\mathbb{R}\) such that \(f(x) \neq 0\) for all \(x \in \mathbb{R}\). For \(f, g \in G\), define a binary operation \(\ast\) on \(G\) as follows: \((f \ast g)(x) = f(x) \cdot g(x)\) for all \(x \in \mathbb{R}\). Prove \((G, \ast)\) is a group. [This is HW.]
Definition 9.5. A relation $\sim$ on a set $S$ is a subset of the Cartesian product $S \times S$. If $(a, b) \in \sim$, then we write $a \sim b$. We say

- $\sim$ is **reflexive** if $a \sim a$ $\forall a \in S$.
- $\sim$ is **symmetric** if $\forall a, b \in S$, we have $a \sim b$ implies $b \sim a$.
- $\sim$ is **transitive** if $\forall a, b, c \in S$, we have $a \sim b$ and $b \sim c$ implies $a \sim c$.

If a relation $\sim$ is reflexive, symmetric, and transitive, then we say $\sim$ is an **equivalence relation**.

Example 9.6. Let $n \in \mathbb{Z}^+$. Define $a \sim b$ on $\mathbb{Z}$ by $a \equiv b \pmod{n}$. Show that $\sim$ is an equivalence relation.

**Proof.** It suffices to prove properties (i), (ii), and (iii) of Theorem 6.7.

**We leave this problem as a HW exercise.**

Q.E.D.

Definition 9.7. If $\sim$ is an equivalence relation on a set $S$ and $a \in S$, then the set $\bar{a} = \{x \in S \mid x \sim a\}$ is called the **equivalence class** of $a$. Elements of the same class are called **equivalent**.

Recall Definition 1.36 where we spoke about the set theory of collections of sets. In particular, review a **set partition**.

Definition 9.8. An equivalence relation $\sim$ on a set $S$ partitions $S$ into disjoint pieces $S_i$ such that $S = S_1 \bigsqcup S_2 \bigsqcup \cdots$. Each $S_i$ is an equivalence class. Below are two pictorial views via the **peanut view**.
The following peanut below illustrates a set $S$ partitioned into exactly two equivalence classes:

The following peanut below illustrates a set $S$ partitioned into an arbitrary number of equivalence classes:

We can pick any member of each class to be a representative of the class $S_i$. We denote this class by square brackets or over bar. In the “Peanut” case above

- $S_1$ is $[x_1]$ or $\overline{x_1}$.
- $S_2$ is $[x_2]$ or $\overline{x_2}$.

**Example 9.9.** Consider the equivalence relation $a \sim b$ on $\mathbb{Z}$ by $a \equiv b \pmod{n}$ for some fixed $n \in \mathbb{Z}^+$.

- **Exercise 1:** If $n = 2$, describe the distinct equivalence classes.

$$\overline{0} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$$

$$\overline{1} = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$$

Note: $\overline{0}$ and $\overline{1}$ are famously called even and odd integers, respectively.

- **Exercise 2:** If $n = 3$, describe the distinct equivalence classes.

$$\overline{0} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

$$\overline{1} = \{\ldots, -8, -5, -2, 1, 4, 7, 10 \ldots\}$$

$$\overline{2} = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}$$
The group \((\mathbb{Z}_n, \oplus)\) of integers modulo \(n\)

**Definition 9.10.** If \(a \in \mathbb{Z}\), then its equivalence class \(\bar{a}\) with respect to congruence modulo \(n\) is called its **residue class modulo \(n\):**

\[
\bar{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\}.
\]

**Definition 9.11.** The **set of integers modulo \(n\)** is a group under the binary operation \(\oplus\) defined by \(\bar{a} \oplus \bar{b} = a + b\). We denote this group \((\mathbb{Z}_n, \oplus)\).

A **complete residue system** of \(\mathbb{Z}_n\) is any set of \(n\) pairwise-distinct residue classes. A **least residue system** of \(\mathbb{Z}_n\) is the set \(\{0, 1, \ldots, n-1\}\). [Why?]

**Example 9.12.** The least residue class of \((\mathbb{Z}_5, \oplus)\) is

\[
\{0, 1, 2, 3, 4\}.
\]

Another complete residue class of \((\mathbb{Z}_5, \oplus)\) is

\[
\{-43, 19, -10, -64, 8\}.
\]

[Why?] Because \(-43 = 2, 19 = 4, -10 = 0, -64 = 1,\) and \(8 = 3\).

Obviously the least residue system is a prettier set than the latter. ☺

⊕ is a well-defined

**Remark 9.13.** The binary operation \(\oplus\) is a **well-defined operation** on \(\mathbb{Z}_n\). That is, it does not depend on the choice of residue class representative. For example, in \(\mathbb{Z}_5\) we have \(-43 = 2\) and \(8 = 3\), so [You Do!]

\[
2 \oplus 3 = 5 = 0 \\
-43 \oplus 8 = -35 = 0
\]

We give a formal proof that \(\oplus\) is well-defined in Theorem 9.16.
**Definition 9.14.** Multiplication in $\mathbb{Z}_n$ is defined by $\overline{a} \odot \overline{b} = \overline{ab}$.

**Note:** multiplication, like addition, is also well-defined. [This is HW.]

Verify that in $\mathbb{Z}_5$ we have $\overline{-43} \odot \overline{8}$ equals $\overline{2} \odot \overline{3}$. [You do!]

\[
\overline{-43} \odot \overline{8} = \overline{-344} = \overline{1}, \text{ and } \\
\overline{2} \odot \overline{3} = \overline{6} = \overline{1}.
\]

**A criterion for two classes in $\mathbb{Z}_n$ to coincide**

**Remark 9.15.** Given $n \geq 2$ and $a, b \in \mathbb{Z}$, we have

\[
\overline{a} = \overline{b} \text{ in } \mathbb{Z}_n \iff a \equiv b \pmod{n}.
\]

**Proof.** Routine. \(\text{Q.E.D.}\)

**Theorem 9.16.** Addition in $\mathbb{Z}_n$ given by $\overline{a} \oplus \overline{b} = \overline{a + b}$ is well-defined. That is, if $\overline{a_1} = \overline{a_2}$ and $\overline{b_1} = \overline{b_2}$ in $\mathbb{Z}_n$, then $\overline{a_1 + b_1} = \overline{a_2 + b_2}$.

**Proof.** [You Do!] Let $\overline{a_1} = \overline{a_2}$ and $\overline{b_1} = \overline{b_2}$ in $\mathbb{Z}_n$.

Observe that

\[
\overline{a_1} = \overline{a_2} \implies a_1 - a_2 = nk \text{ for some } k \in \mathbb{Z} \quad [\text{WHY?}] \quad (10) \\
\overline{b_1} = \overline{b_2} \implies b_1 - b_2 = nj \text{ for some } j \in \mathbb{Z} \quad [\text{WHY?}] \quad (11)
\]

Adding (1) and (2), we get $(a_1 - a_2) + (b_1 - b_2) = nk + nj$ and hence

\[
(a_1 + b_1) - (a_2 + b_2) = n(k + j) \implies a_1 + b_1 \equiv a_2 + b_2 \pmod{n} \\
\implies \overline{a_1 + b_1} = \overline{a_2 + b_2}.
\]

\(\text{Q.E.D.}\)
The group \((\mathbb{U}(n), \circ)\) of units of \((\mathbb{Z}_n, \oplus)\)

**Definition 9.17.** A unit in \(\mathbb{Z}_n\) is an element \(\bar{a}\) that has a multiplicative inverse. That is, there exists an element \(\bar{b} \in \mathbb{Z}_n\) such that \(\bar{a} \circ \bar{b} = \overline{1}\).

**Definition 9.18.** (The group of units in \(\mathbb{Z}_n\)) Let \(\mathbb{U}(n)\) be the set of elements in \((\mathbb{Z}_n, \oplus)\) which have a multiplicative inverse. That is,
\[
\mathbb{U}(n) = \{\bar{a} \in \mathbb{Z}_n \mid \bar{a} \circ \bar{b} = \overline{1} \text{ for some } \bar{b} \in \mathbb{Z}_n\}.
\]
Under the multiplication operation \(\circ\), the set \(\mathbb{U}(n)\) forms a group.

**Example 9.19.** For \(n = 4, 5, 6, 7\) find \(\mathbb{U}(n)\).
\[
\begin{align*}
\mathbb{U}(4) &= \{\overline{1}, \overline{3}\} \\
\mathbb{U}(5) &= \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\} \\
\mathbb{U}(6) &= \{\overline{1}, \overline{5}\} \\
\mathbb{U}(7) &= \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}
\end{align*}
\]

When does \(\bar{a}\) have a multiplicative inverse in \(\mathbb{Z}_n\)?

It is helpful to recall Theorem 6.12 which states the following:

**Theorem.** The linear congruence \(ax \equiv b \pmod{n}\) has a solution if and only if \(d \mid b\) where \(d = \gcd(a, n)\).

An immediate corollary is the following. [Why?]

**Corollary 9.20.** The linear congruence \(ax \equiv 1 \pmod{n}\) has a solution if and only if \(\gcd(a, n) = 1\).
Using Corollary 9.20, we can prove the following necessary and sufficient condition for \( \overline{a} \) to have an inverse in \( \mathbb{Z}_n \).

**Theorem 9.21.** The class \( \overline{a} \) in \( \mathbb{Z}_n \) has a multiplicative inverse if and only if \( \gcd(a, n) = 1 \).

**Proof.**

\((\Longrightarrow)\) Assume the class \( \overline{a} \) in \( \mathbb{Z}_n \) has a multiplicative inverse. \([\text{You Finish!}]\)

**WWTS:** \( \gcd(a, n) = 1 \).

Let \( \overline{b} \) be the inverse for \( \overline{a} \) in \( \mathbb{Z}_n \). Then \( \overline{a} \circ \overline{b} = 1 \) and so \( \overline{ab} = 1 \). But that implies \( ab \equiv 1 \pmod{n} \) [WHY?]. By the corollary, we have \( \gcd(a, n) = 1 \).

\((\Longleftarrow)\) Assume that \( \gcd(a, n) = 1 \). \([\text{You Finish!}]\)

**WWTS:** \( \overline{a} \) in \( \mathbb{Z}_n \) has a multiplicative inverse.

By the corollary, since \( \gcd(a, n) = 1 \) then the linear congruence \( ax \equiv 1 \pmod{n} \) has a solution. Call this solution \( x = b \) for some \( b \in \mathbb{Z} \). Thus \( ab \equiv 1 \pmod{n} \) which implies \( \overline{ab} = 1 \). And hence \( \overline{a} \circ \overline{b} = 1 \). Thus \( \overline{a} \) in \( \mathbb{Z}_n \) has a multiplicative inverse.

Q.E.D.

**Corollary 9.22.** The set \( (\mathbb{Z}_n - \{0\}, \circ) \) with operation multiplication forms a group whenever \( n \) is prime.

**Proof.** Assume \( n \) is prime. The set \( \mathbb{Z}_n - \{0\} \) is \( \{1, 2, \ldots, n - 1\} \). Since \( n \) is prime, then \( \gcd(a, n) = 1 \) for all \( 1 \leq a \leq n - 1 \). Thus all the elements of \( \mathbb{Z}_n - \{0\} \) are units. The claim follows.

Q.E.D.
A Practical Method to Find Units in $\mathbb{Z}_n$

Recall in Diophantine Exercise 1, we used the Euclidean algorithm to complete

$$\text{gcd}(15, 49) = 1$$

and then we reversed our steps in the algorithm to verify Bézout’s identity that there exists $x, y \in \mathbb{Z}$ such that $\text{gcd}(15, 49) = 15x + 49y$ and we find

$$1 = 15(-13) + 49(4) \tag{12}$$

**EXERCISE:** Use Equation (12) to find the multiplicative inverse of 15 in $\mathbb{Z}_{49}$ and the multiplicative inverse of 49 in $\mathbb{Z}_{15}$.

**ANSWER:** [You Do!]

To find the inverse of $15$ in $\mathbb{Z}_{49}$, observe that

$$1 = 15(-13) + 49(4) \implies 1 - 15(-13) = 49(4) \implies 1 \equiv 15(-13) \pmod{49} \implies 15 \odot -13 = 1 \text{ in } \mathbb{Z}_{49}.$$  

But $-13 = 36$, so 36 is the inverse of 15 in $\mathbb{Z}_{49}$. ✓

To find the inverse of 49 in $\mathbb{Z}_{15}$, observe that

$$1 = 15(-13) + 49(4) \implies 1 - 49(4) = 15(-13) \implies 1 \equiv 49(4) \pmod{15} \implies 49 \odot 4 = 1 \text{ in } \mathbb{Z}_{15}.$$  

So 4 is the inverse of 49 in $\mathbb{Z}_{15}$. ✓

---

**An EASIER WAY to find the inverse of 49 in $\mathbb{Z}_{15}$?**

[You Do!] Since 49 equals 4 in $\mathbb{Z}_{15}$, then the inverse of 49 is the same as the inverse of 4. By inspection $4 \times 4 = 16$, so we’re done. ☺
9.3 Group Homomorphisms and Isomorphisms

Definition 9.23. A group homomorphism between two groups $(G, *_G)$ and $(H, *_H)$ is a map $\phi : G \rightarrow H$ such that for all $g_1, g_2 \in G$, we have

$$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2).$$

This property is called “$\phi$ preserves the group operations”.

Example 9.24. Let $G = (\mathbb{R}, +)$ and $H = (\mathbb{R}\setminus\{0\}, \cdot)$. Consider the exponential map $\phi : G \rightarrow H$ by $\phi(x) = e^x$ for all $x \in \mathbb{R}$. Prove that $\phi$ is a homomorphism.

[You Do!] Let $x, y \in \mathbb{R}$.

WWTS: $\phi(x + y) = \phi(x) \cdot \phi(y)$.

Observe that

$$\phi(x + y) = e^{x+y}$$
$$= e^x \cdot e^y$$
$$= \phi(x) \cdot \phi(y).$$

Thus $\phi$ is a homomorphism.

Q.E.D.

Definition 9.25. Let $\phi : G \rightarrow H$ be a map from group $G$ to group $H$. Then we say

- $\phi$ is injective if $\phi(g_1) = \phi(g_2)$ implies $g_1 = g_2$ for all $g_1, g_2 \in G$.
- $\phi$ is surjective if for each $h$ in the codomain $H$, there exists a $g$ in the domain $G$ such that $\phi(g) = h$.
- $\phi$ is bijective if $\phi$ is injective and surjective.
Question 9.26. Is the map $\phi : \mathbb{R} \to \mathbb{R}$ by $\phi(x) = x^2$ injective?

Answer: No since $\phi(3) = 9 = \phi(-3)$ for instance, but $3 \neq -3$.

Question 9.27. Is the map $\phi : \mathbb{R} \to \mathbb{R}$ by $\phi(x) = x^3$ surjective?

Answer: Let $y \in \mathbb{R}$. Set $x := \sqrt[3]{y}$. Observe that $\phi(x) = (\sqrt[3]{y})^3 = y$. Hence $\phi$ is surjective.

Definition 9.28. A group isomorphism between two groups $(G, *_G)$ and $(H, *_H)$ is a map $\phi : G \to H$ which is a homomorphism and bijective. If so we denote this isomorphism as $G \cong H$.

EXERCISE: Show that $(\mathbb{Z}_4, \oplus)$ is isomorphic to $\{\{1, -1, i, -i\}, \cdot\}$ as groups.

NOTE: The group $\{\{1, -1, i, -i\}, \cdot\}$ is called the 4th roots of unity; that is, the four distinct roots in $\mathbb{C}$ of the polynomial $x^4 - 1$. This group is denoted $U_4$. In general, the roots of $x^n - 1$ form the group $U_n$ called the $n$th roots of unity.

ANSWER: [You Do!] Define $\phi : \mathbb{Z}_4 \to U_4$ by $\phi : \overline{1} \mapsto i$. We claim that this alone defines the isomorphism. Since $\phi(\overline{1}) = i$, this forces

$$\phi(\overline{2}) = \phi(\overline{1} \oplus \overline{1}) = \phi(\overline{1}) \cdot \phi(\overline{1}) = i \cdot i = -1.$$  

Similarly, $\phi(\overline{3}) = i^3 = -i$ and $\phi(\overline{4}) = i^4 = 1$. So $\phi$ is clearly bijective. Moreover $\phi$ is the map that sends $\overline{a}$ to $i^a$. It is a homomorphism since for $\overline{a}, \overline{b} \in \mathbb{Z}_4$, we have

$$\phi(\overline{a} \oplus \overline{b}) = \phi(\overline{a+b}) = i^{a+b} = i^a \cdot i^b = \phi(\overline{a}) \cdot \phi(\overline{b}).$$

Q.E.D.
Bijective Poetry Break

The following poem was written by aBa during his undergrad days at Sonoma State University. It is simply called The Bijection Function Poem.

And it clearly follows that the function is bijective
Let’s take a closer look and make this more objective
It bears a certain quality – that which we call injective
A lovin’ love affair, Indeed, a one-to-one perspective.

Injection is the stuff that bonds one range to one domain
For Mr. X in the domain, only Ms. Y can take his name
But if some other domain fool should try to get Ms. Y’s affection,
The Horizontal Line Police are here to check for one-to-one Injection.

Observe though, that injection does not alone grant one bijection
A function of this kind must bear Injection AND Surjection
Surjection!? What is that? Another math word gone surreal?
Its just a simple concept we call “Onto”. Here’s the deal:

If for EVERY lady y who walks the Codomain of f
There’s at least one x in the Domain who fancies her as his sweet best.
So hear the song that Onto sings – a simple mathful melody:

“There ain’t a Y in Codomain not imaged by some X, you see!”

So there you have it two conditions that define a quality.
If it’s injective and surjective, then it’s bijective, by golly!

Now if you’re paying close attention to my math-poetic verse
I reckon that you’ve noticed implications of Inverse
Inverse functions blow the same tune – They biject oh so happily
By sheer existence, inverse functions mimic Onto qualities
And per uniqueness of solution, another inverse golden rule
By gosh, that’s One-to-One and Onto straight up out the Biject School!

A video of aBa singing this to his students when he was a PhD student at the University of Iowa is available by clicking on this:

https://www.youtube.com/watch?v=_cMOQGSowfU
**Bijection Exercise**

**PROVE:** If \( f : \mathbb{R} \rightarrow \mathbb{R} \) is a map defined by \( f(x,y) = (x+y,x-y) \), then \( f \) is bijective.

*Proof.* First we show \( f \) is injective and then we show \( f \) is surjective.

**SHOW INJECTIVE:** Suppose that \( f(x_1,y_1) = f(x_2,y_2) \). \[\text{WWTS: } (x_1,y_1) = (x_2,y_2).\]

Since \( f(x_1,y_1) = f(x_2,y_2) \), then we know
\[
(x_1 + y_1, x_1 - y_1) = (x_2 + y_2, x_2 - y_2).
\]

And hence we have the following sequence of equalities:
\[
\begin{align*}
x_1 + y_1 &= x_2 + y_2 \\
x_1 - y_1 &= x_2 - y_2
\end{align*}
\]

Adding the two equalities we get 
\[
(x_1 + y_1) + (x_1 - y_1) = (x_2 + y_2) + (x_2 - y_2) \implies 2x_1 = 2x_2 \implies x_1 = x_2.
\]

Moreover, subtracting the two equalities we get
\[
(x_1 + y_1) - (x_1 - y_1) = (x_2 + y_2) - (x_2 - y_2) \implies 2y_1 = 2y_2 \implies y_1 = y_2.
\]

Thus \((x_1, y_1) = (x_2, y_2)\) as desired. Hence the map \( f \) is injective.

**Q.E.D.**

**SHOW SURJECTIVE:** Let \((a,b)\) be in the codomain of \( f \).

**WWTS:** \( \exists (x,y) \in \mathbb{R}^2 \text{ such that } f(x,y) = (a,b). \)

We leave this problem as a HW exercise.
9.4 The Order of an Element in a Group and Primitive Roots

First let us recall an important arithmetic function we encountered in Section 7, called Euler’s phi function.

For a positive integer \( n \), we define \( \phi(n) \) to be the number of positive integers that are less than or equal to \( n \) that are relatively prime to \( n \). That is,
\[
\phi(n) = |\{k \in \mathbb{N} : \gcd(k, n) = 1 \text{ and } k \leq n\}|.
\]

Clearly, this can be used to compute the size of the group \((\mathbb{U}(n), \circ)\). [Why?]

Example 9.29. Since 11 is prime, then \( \phi(11) = 10 \). So the elements in \((\mathbb{U}(11), \circ)\) are all the nonzero elements in \( \mathbb{Z}_{11} \). Below we give a table of the powers of each element. NOTE: We are suppressing the bar notation for now.

<table>
<thead>
<tr>
<th>( a )</th>
<th>( a^2 )</th>
<th>( a^3 )</th>
<th>( a^4 )</th>
<th>( a^5 )</th>
<th>( a^6 )</th>
<th>( a^7 )</th>
<th>( a^8 )</th>
<th>( a^9 )</th>
<th>( a^{10} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>9</td>
<td>5</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>9</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>9</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>7</td>
<td>9</td>
<td>10</td>
<td>5</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>10</td>
<td>4</td>
<td>6</td>
<td>9</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>6</td>
<td>4</td>
<td>10</td>
<td>3</td>
<td>2</td>
<td>5</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>6</td>
<td>5</td>
<td>1</td>
<td>9</td>
<td>4</td>
<td>3</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>10</td>
<td>1</td>
<td>10</td>
<td>1</td>
<td>10</td>
<td>1</td>
<td>10</td>
<td>1</td>
</tr>
</tbody>
</table>

QUESTION: What observations do you make from this table? [You Do!]

- \( a^{10} = 1 \) for all \( a \) since FLT says \( a^{p-1} \equiv 1 \pmod{p} \) if \( \gcd(a, p) = 1 \).
- For \( a = 2, 6, 7, 8 \), the powers of \( a \) give the complete set \( \{1, 2, \ldots, 10\} \).
- For \( a = 3, 4, 5, 9 \), the powers of \( a \) give the set \( \{1, 3, 4, 5, 9\} \).
- The powers of \( a = 10 \) give the set \( \{1, 10\} \).
Example 9.30. Since $\phi$ is a multiplicative function, then $\phi(15)$ equals

$$\phi(3) \cdot \phi(5) = 2 \cdot 4 = 8.$$ 

So there are 8 elements in $(\mathbb{U}(15), \odot)$. Below we give a table of the powers of each element. **NOTE:** Again, we are suppressing the bar notation for now.

<table>
<thead>
<tr>
<th>$a$</th>
<th>$a^2$</th>
<th>$a^3$</th>
<th>$a^4$</th>
<th>$a^5$</th>
<th>$a^6$</th>
<th>$a^7$</th>
<th>$a^8$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>8</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>13</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>11</td>
<td>1</td>
<td>11</td>
<td>1</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>4</td>
<td>7</td>
<td>1</td>
<td>13</td>
<td>4</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>1</td>
<td>14</td>
<td>1</td>
<td>14</td>
<td>1</td>
<td>14</td>
<td>1</td>
</tr>
</tbody>
</table>

**QUESTION:** What observations do you make from this table? **[You Do!]**

- $a^8 = 1$ for all $a$ since Euler’s Theorem says $a^{\phi(n)} \equiv 1 \pmod{n}$ if $\gcd(a, n) = 1$.
- For $a = 2, 4$, the powers of $a$ give the set $\{1, 2, 4, 8\}$.
- For $a = 7, 13$, the powers of $a$ give the set $\{1, 4, 7, 13\}$.
- The powers of $a = 4$ give the set $\{1, 4\}$.
- The powers of $a = 11$ give the set $\{1, 11\}$.
- The powers of $a = 14$ give the set $\{1, 14\}$.
- The powers of NO $a$ give the complete set $\mathbb{U}(15)$. 
Definition 9.31. The **order of an element** \(a\) modulo \(n\) is the smallest positive integer \(k\) such that \(a^k \equiv 1 \pmod{n}\).

Definition 9.32. The **order of a group** \((G,\ast)\) is the number of elements in the group.

**QUESTION**: What were the possible orders in the group \(\mathbb{U}(11)\)? [You Do!]

\[1, 2, 5, \text{ and } 10.\]

**QUESTION**: What were the possible orders in the group \(\mathbb{U}(15)\)? [You Do!]

\[1, 2, \text{ and } 4.\]

**CONJECTURE TIME!!! YAY!**: What do you conjecture about the relationship between the order of the elements and the order of the group? [You Do!]

**YOUR CONJECTURE**: The order of each element divides the order of the group.
A Quick Tour of Subgroups and Lagrange

**Definition 9.33.** Given a group \((G, \ast)\), a subset \(H\) of \(G\) is called a **subgroup** of \(G\) if \(H\) also forms a group under the operation \(\ast\). This is usually denoted \(H \leq G\).

**Example 9.34.** Justify the following examples and non-examples. [You Do!]

- \(2\mathbb{Z}\) is a subgroup of \((\mathbb{Z}, +)\). [Why?]
- \(2\mathbb{Z} + 1\) is not a subgroup of \((\mathbb{Z}, +)\). [Why?]
- \(\{1, -1\}\) is a subgroup of \((\{1, -1, i, -i\}, \cdot)\). [Why?]
- \(\{1, i\}\) is not a subgroup of \((\{1, -1, i, -i\}, \cdot)\). [Why?]
- \(\{1, 4, 7, 13\}\) is a subgroup of \((\mathbb{U}(15), \cdot)\). [Why?]

That last example in the list above brings up a very important subgroup that every group has, namely cyclic subgroups.

**Definition 9.35.** Let \((G, \ast)\) be a group. Let \(g \in G\). Then the “powers\(^{38}\)” of \(g\) generate a subgroup of \(G\) called a **cyclic subgroup**. Using multiplicative notation, we write

\[
\langle g \rangle := \{g^k \mid k \in \mathbb{Z}\} = \{\ldots, g^{-3}, g^{-2}, g^{-1}, “1”, g^1, g^2, g^3, \ldots\}.
\]

Using additive notation, we write

\[
\langle g \rangle := \{kg \mid k \in \mathbb{Z}\} = \{\ldots, -g, -g, -g, -g, “0”, g, g + g, g + g + g, \ldots\}.
\]

Moreover a group \(G\) that can be generated by one element in \(G\) is called a **cyclic group**.

---

\(^{38}\)We put “powers” in quotes because multiplication is not always the operation of a group. So we use this word rather loosely to mean taking successive application of the operation on an element.
The following theorem is such a fundamental and important result in Group Theory so we place it inside the “SPECIAL BOX”!

**Lagrange’s Theorem**

Given a finite group \( G \), the order of every subgroup \( H \) of \( G \) divides the order of \( G \).

*Proof.* Beyond the scope of this course. But do consider taking an abstract algebra course some day!

Q.E.D.

**Corollary 9.36.** The order of an element \( g \) in a finite group \( G \) divides the order of the group \( G \).

*Proof.* [You Do!] Let \( G \) be a finite group and let \( g \in G \).

Consider the the cyclic subgroup \( \langle g \rangle \) of \( G \). Then clearly \( \langle g \rangle \) is finite since \( G \) is. By Lagrange’s Theorem the order of \( \langle g \rangle \) divides the order of \( G \).

The claim holds if we can show that \( |g| = |\langle g \rangle| \). Suppose \( |g| = n \) for some \( n \in \mathbb{N} \). Consider the elements \( 1, g, g^2, \ldots, g^{n-1} \). These \( n \) elements are distinct, for otherwise if \( g^k = g^j \) for some \( 0 \leq j < k < n \), then \( g^{k-j} = g^0 = 1 \), contradicting the fact that \( n \) is the smallest power for which \( g^n = 1 \). Thus \( \langle g \rangle \) has at least \( n \) elements.

It suffices to show that these \( n \) elements are all of them. Consider \( g^t \) for some \( t \in \mathbb{Z} \). Then by the division algorithm, we have \( t = qn + r \) for some \( q, r \in \mathbb{Z} \) such that \( 0 \leq r < n \). It follows that

\[
g^t = g^{qn+r} = (g^n)^q \cdot g^r = 1^q \cdot g^r = g^r \in \{1, g, g^2, \ldots, g^{n-1}\}
\]

as desired. Thus \( |g| = |\langle g \rangle| \). So the order of every element in a finite group \( G \) divides the order of \( G \).

Q.E.D.
**Primitive Roots**

**Definition 9.37.** A number $g$ is called a **primitive root modulo** $n$ if for every number coprime to $n$ is congruent to a power of $g$ modulo $n$.

That is, for every $a$ such that $\gcd(a, n) = 1$, we have $a \equiv g^k$ for some $k \in \mathbb{Z}$.

**EXERCISE:** Show that 3 is a primitive root modulo 7 but not a primitive root modulo 11.

**SOLUTION:**
Modulo 7, the powers of 3 are as follows:

$$3^0 \equiv 1, \ 3^1 \equiv 3, \ 3^2 \equiv 2, \ 3^3 \equiv 6, \ 3^4 \equiv 4, \ 3^5 \equiv 5, \ 3^6 \equiv 1 \pmod{7}.$$

However modulo 11, the powers of 3 are as follows:

$$3^0 \equiv 1, \ 3^1 \equiv 3, \ 3^2 \equiv 9, \ 3^3 \equiv 5, \ 3^4 \equiv 4, \ 3^5 \equiv 1 \pmod{11}.$$

There is an equivalent definition of primitive roots which goes as follows.

**Definition 9.38.** A number $g$ is called a **primitive root modulo** $n$ if $\gcd(g, n) = 1$ and $g$ has order $\phi(n)$.

**EXERCISE:** Use this definition to show that 3 is a primitive root modulo 7 but not a primitive root modulo 11.

**SOLUTION:**
Since the order of 3 modulo 7 is 6 and $\phi(7) = 6$, then 3 is a primitive root modulo 7. Whereas the order of 3 modulo 11 is 5 and $\phi(11) = 10$, so we conclude that 3 is not a primitive root modulo 11.
Recall the powers of each \( a \) in \( \mathbb{U}(11) \):

<table>
<thead>
<tr>
<th>( a )</th>
<th>( a^2 )</th>
<th>( a^3 )</th>
<th>( a^4 )</th>
<th>( a^5 )</th>
<th>( a^6 )</th>
<th>( a^7 )</th>
<th>( a^8 )</th>
<th>( a^9 )</th>
<th>( a^{10} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>9</td>
<td>5</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>9</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td>9</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>7</td>
<td>9</td>
<td>10</td>
<td>5</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>10</td>
<td>4</td>
<td>6</td>
<td>9</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>9</td>
<td>6</td>
<td>4</td>
<td>10</td>
<td>3</td>
<td>2</td>
<td>5</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>3</td>
<td>5</td>
<td>1</td>
<td>9</td>
<td>4</td>
<td>3</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>10</td>
<td>1</td>
<td>10</td>
<td>1</td>
<td>10</td>
<td>1</td>
<td>10</td>
<td>1</td>
</tr>
</tbody>
</table>

**QUESTION:** Which elements are primitive roots?

**SOLUTION:**
The values 2, 6, 7, and 8 are primitive roots modulo 11.

Recall the powers of each \( a \) in \( \mathbb{U}(15) \):

<table>
<thead>
<tr>
<th>( a )</th>
<th>( a^2 )</th>
<th>( a^3 )</th>
<th>( a^4 )</th>
<th>( a^5 )</th>
<th>( a^6 )</th>
<th>( a^7 )</th>
<th>( a^8 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>8</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>4</td>
<td>13</td>
<td>1</td>
<td>7</td>
<td>4</td>
<td>13</td>
<td>1</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>8</td>
<td>4</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>11</td>
<td>1</td>
<td>11</td>
<td>1</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>13</td>
<td>4</td>
<td>7</td>
<td>1</td>
<td>13</td>
<td>4</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>1</td>
<td>14</td>
<td>1</td>
<td>14</td>
<td>1</td>
<td>14</td>
<td>1</td>
</tr>
</tbody>
</table>

**QUESTION:** Which elements are primitive roots?

**SOLUTION:**
There are no primitive roots.
Deer Hunting? Nope, Just Primitive Root Hunting!

An equivalent THIRD DEFINITION of primitive roots is cast in the group theory setting.

**Definition 9.39.** The group $\mathbb{U}(n)$ has a **primitive root** if $\mathbb{U}(n)$ is cyclic.

**QUESTION:** For what $n$ is the group $\mathbb{U}(n)$ cyclic? So begins the “Hunt for Primitive Roots Modulo $n$”!!

**HINT:** One of these two hunters succeeded and one failed. Who are they?

**SOLUTION:** On the left is Euler. He gave an incomplete proof in 1773 for the existence of primitive roots if $n$ is prime. But the guy on the right is Gauss and he proved the following:

**Theorem 9.40.** [Gauss, 1801] The group $\mathbb{U}(n)$ is cyclic if and only if $n = 1, 2, 4, p^k,$ or $2p^k$ where $p$ is an odd prime.
Chinese Remainder Theorem (revisited)

**QUESTION:** What is the unique integer \( x \in \{0, 1, 2, \ldots, 104\} \) that solves the system of linear congruences:

\[
\begin{align*}
  x &\equiv 2 \pmod{3} \\
  x &\equiv 3 \pmod{5} \\
  x &\equiv 2 \pmod{7}
\end{align*}
\]

If this looks familiar, then you have a good memory of Sun-Tsu problem given in Question 6.15.

**ANSWER:** [You Do!] Recall that we found that \( x = 23 \) is the unique solution modulo \( 3 \times 5 \times 7 = 105 \). [VERIFY!]

---

**GROUP THEORY SETTING**

It is known that \( \mathbb{Z}_{105} \) is isomorphic to the Cartesian product \( \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \). That is, there exists a bijective homomorphism

\[
\phi : \mathbb{Z}_{105} \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7.
\]

**CONSEQUENCES:**

- Since \( \mathbb{Z}_{105} \) is cyclic, then \( \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \) is cyclic too.
- Each element in \( \mathbb{Z}_{105} \) corresponds to one and only one tuple \((\overline{a}, \overline{b}, \overline{c})\) in \( \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \).
- The corresponding unit groups are isomorphic. That is,

\[
\mathbb{U}(105) \cong \mathbb{U}(3) \times \mathbb{U}(5) \times \mathbb{U}(7).
\]

**QUESTION:** What is the unique tuple \((\overline{a}, \overline{b}, \overline{c})\) \( \in \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \) that corresponds to the element \( \overline{23} \in \mathbb{Z}_{105} \)?

**ANSWER:** [You Do!] \((\overline{2}, \overline{3}, \overline{2})\) [VERIFY!]
Towards the Isomorphism $\mathbb{U}(mn) \cong \mathbb{U}(m) \times \mathbb{U}(n)$ given that $\gcd(m, n) = 1$

Example 9.41. Exhibit the isomorphism $\mathbb{U}(15) \cong \mathbb{U}(3) \times \mathbb{U}(5)$. [You Do!]

<table>
<thead>
<tr>
<th>$\bar{g} \in \mathbb{U}(15)$</th>
<th>$(\bar{a}, \bar{b}) \in \mathbb{U}(3) \times \mathbb{U}(5)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(1, 1)</td>
</tr>
<tr>
<td>2</td>
<td>(2, 2)</td>
</tr>
<tr>
<td>4</td>
<td>(4, 4) = (1, 4)</td>
</tr>
<tr>
<td>7</td>
<td>(7, 7) = (1, 2)</td>
</tr>
<tr>
<td>8</td>
<td>(8, 8) = (2, 3)</td>
</tr>
<tr>
<td>11</td>
<td>(11, 11) = (2, 1)</td>
</tr>
<tr>
<td>13</td>
<td>(13, 13) = (1, 3)</td>
</tr>
<tr>
<td>14</td>
<td>(14, 14) = (2, 4)</td>
</tr>
</tbody>
</table>

Corollary 9.42. If $\gcd(m, n) = 1$ implies $\mathbb{U}(mn) \cong \mathbb{U}(m) \times \mathbb{U}(n)$, then we have

- The isomorphism implies another proof that $\phi$ is multiplicative. That is, if $\gcd(m, n) = 1$ then $\phi(mn) = \phi(m) \cdot \phi(n)$. [Why?]

$$|\mathbb{U}(mn)| = |\mathbb{U}(m)| \cdot |\mathbb{U}(n)|$$

- If $n$ has prime factorization $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ where the $p_i$ are distinct primes and $n_i \geq 1$, then

$$\mathbb{U}(n) \cong \mathbb{U}(p_1^{n_1}) \times \mathbb{U}(p_2^{n_2}) \times \cdots \times \mathbb{U}(p_r^{n_r}).$$ [Why?] □ Induction

- Recall by Theorem 7.24 that $\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$

- The VERY COOL formula follows: $\phi(n) = n \cdot \prod_{p_i \mid n} \left(1 - \frac{1}{p_i}\right)$. [Why?]

$$\phi(n) = \phi(p_1^{n_1}) \phi(p_2^{n_2}) \cdots \phi(p_r^{n_r}) = \prod_{i=1}^{n_1} \left(1 - \frac{1}{p_1}\right) \prod_{i=2}^{n_2} \left(1 - \frac{1}{p_2}\right) \cdots \prod_{i=r}^{n_r} \left(1 - \frac{1}{p_r}\right)$$
Corollary 9.42 is a consequence of the theorem below. Let us now prove it.

**Theorem 9.43.** Let \(m, n \in \mathbb{N}\) such that \(\text{gcd}(m, n) = 1\). Then we have an isomorphism of groups

\[
\mathbb{U}(mn) \cong \mathbb{U}(m) \times \mathbb{U}(n).
\]

**Proof.** Let \(m, n \in \mathbb{N}\) such that \(\text{gcd}(m, n) = 1\). Define a map 
\[f : \mathbb{U}(mn) \rightarrow \mathbb{U}(m) \times \mathbb{U}(n)\]
by \(f(c) = (\overline{c}, \overline{c})\). More specifically,

\[f(c \pmod{mn}) = (c \pmod{m}, c \pmod{n}).\]

**WWTS:** \(f\) is a bijective homomorphism.

The map \(f\) is a homomorphism since

\[
f(ab) = f(ab) = (\overline{ab}, \overline{ab}) = (\overline{a}, \overline{a}) \cdot (\overline{b}, \overline{b}) = f(a) \cdot f(b).
\]

To show that \(f\) is injective, suppose that \(f(k) = f(l)\). It suffices to show \(k = l\) in \(\mathbb{Z}_{mn}\) or equivalently that \(mn\) divides \(k - l\). Since \(f(k) = f(l)\) implies \((k, k) = (l, l)\) in \(\mathbb{U}(m) \times \mathbb{U}(n)\), then \(k = l\) in \(\mathbb{Z}_m\) and \(k = l\) in \(\mathbb{Z}_n\). Thus \(m \mid k - l\) and \(n \mid k - l\). But \(\text{gcd}(m, n) = 1\) and hence \(mn \mid k - l\) as desired.

To show \(f\) is surjective, let \((\overline{a}, \overline{b}) \in \mathbb{U}(m) \times \mathbb{U}(n)\). We want to find an \(x \in \mathbb{Z}_{mn}\) such that \(f(x) = (\overline{a}, \overline{b})\). By the Chinese Remainder Theorem, this \(x\) is guaranteed to exist. BUT we need to check it is in \(\mathbb{U}(mn)\). Since \(f(x) = (\overline{a}, \overline{b})\) implies \((x, x) = (\overline{a}, \overline{b})\), we have

\[
\begin{align*}
\bar{x} &= \overline{a} \text{ in } \mathbb{U}(m) \implies \text{gcd}(x, m) = 1, \text{ and} \\
\bar{x} &= \overline{b} \text{ in } \mathbb{U}(n) \implies \text{gcd}(x, n) = 1.
\end{align*}
\]

Hence \(\text{gcd}(x, mn) = 1\) so \(x \in \mathbb{U}(mn)\) so \(f\) is surjective.

Q.E.D.
10 Quadratic Reciprocity

10.1 Motivation

In Subsection 6.3, we learned how to solve linear congruences of the form

\[ ax \equiv b \pmod{n}. \]

These were INTIMATELY connected to Diophantine equations and their corresponding “Diophantine lines” in the following sense: [You Do!]

\[ a x \equiv b \pmod{n} \implies b \equiv a x \pmod{n} \]
\[ \implies b - ax = ny \]
\[ \implies ax + ny = b \quad \text{the Diophantine equation} \]
\[ \implies y = -\frac{a}{n}x + \frac{b}{n} \quad \text{the Diophantine line} \]

Recall that in Example 5.30, we found all solutions to the Diophantine equation

\[ 15x + 49y = 8. \]

We drew the graph of the corresponding Diophantine line \( y = -\frac{15}{49}x + \frac{8}{49} \)

\[ (-104, 32), (-55, 17), (-6, 2), (43, -13), (92, -28) \]

So equivalently, the solutions to the linear congruence \( 15x \equiv 8 \pmod{49} \) are all the points \( x = -6 + 49t \) for each \( t \in \mathbb{Z} \).

**REMINDER:** We don’t care about the \( y \)-value solutions of \( ax + ny = b \) if all we care about is solving \( ax \equiv b \pmod{n} \).

**BOTTOMLINE:** The \( x \)-solutions of the linear congruence \( ax \equiv b \pmod{n} \) have an INTIMATE connection to the \( x \)-values of the integer-lattice points that the Diophantine line goes through.
Is there an Analogous Graphical Idea in the Quadratic Setting?

Consider the quadratic congruence equation

\[ ax^2 + bx + c \equiv d \pmod{n}. \]

Is there an analogous “Diophantine quadratic” for which we can just find the integer lattice points that the quadratic passes through?

**Example 10.1.** Find all solutions to the following quadratic congruence

\[ 5x^2 + 6x + 1 \equiv 0 \pmod{23}. \]  

(13)

**QUESTION:** How might you go about solving this if it was just a “regular ole quadratic” equation \( 5x^2 + 6x + 1 = 0 \)? [You Do!]

You would try to factor it, or perhaps use the quadratic formula:

\[ x = \frac{-6 \pm \sqrt{6^2 - 4(5)(1)}}{2(5)} = \frac{-6 \pm \sqrt{16}}{10} = \frac{-6 \pm 4}{10} - 1. \]

So there are two real roots to the quadratic, namely \(-1\) and \(-\frac{1}{5}\).

**QUESTION:** What can be said about the integral root with respect to the quadratic congruence in Equation (13)? [You Do!]

The integral root \(-1\) is clearly a solution to \( 5x^2 + 6x + 1 \equiv 0 \pmod{n} \) for any \( n \in \mathbb{N} \) and in particular for \( n = 23 \).

**QUESTION:** What can be said about the non-integral root with respect to the quadratic congruence in Equation (13)? Any idea on how we might “interpret”/“translate” it as a root of the congruence equation? [You Do!]

Since \(-\frac{1}{5}\) is not an integer, then it is meaningless to speak of it a root of the congruence equation. HOWEVER, maybe we can interpret it as the negative inverse of 5 modulo 23.
The $5x^2 + 6x + 1 \equiv 0 \pmod{23}$ Example (continued)

How to convert $-\frac{1}{5}$ into an integer modulo 23?

Two steps:

- **STEP 1:** Find the inverse of 5 modulo 23.
- **STEP 2:** Take the negative of the inverse you just found modulo 23.

**STEP 1:** Find the inverse of 5 modulo 23. [You Do!]

First use the Euclidean algorithm to find the gcd(23, 5):

\[
\begin{align*}
23 &= 4 \cdot 5 + 3 \\
5 &= 1 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1
\end{align*}
\]

Hence gcd(23, 5) = 1. Now we run the algorithm backwards to produce Bézout’s identity:

\[
\begin{align*}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (5 - 1 \cdot 3) \\
&= 3 - 1 \cdot 5 + 1 \cdot 3 \\
&= 2 \cdot 3 - 1 \cdot 5 \\
&= 2 \cdot (23 - 4 \cdot 5) - 1 \cdot 5 \\
&= 2 \cdot 23 - 9 \cdot 5
\end{align*}
\]

Thus it follows that

\[
1 = 2 \cdot 23 + (-9) \cdot 5 \implies 1 - (-9) \cdot 5 = 2 \cdot 23 \implies 1 \equiv -9 \cdot 5 \pmod{23},
\]

and hence $-9$ is “the” inverse of 5 modulo 23. But $-9 \equiv 14 \pmod{23}$.

Therefore, the inverse of 5 modulo 23 is $14$.
The $5x^2 + 6x + 1 \equiv 0 \pmod{23}$ Example (continued)

**STEP 2:** Take the negative of the inverse you just found modulo 23. [You Do!]

Since the inverse of 5 modulo 23 is 14, and $-14 \equiv 9 \pmod{23}$.

Therefore, $-\frac{1}{5}$ can be interpreted modulo 23 as $9$.

---

**Question 10.2.** Is the value above another solution to the quadratic congruence in Equation (13)? [You Verify!]

Plugging in $x = 9$ into the congruence, we get

\[
5 \cdot 9^2 + 6 \cdot 9 + 1 \equiv 405 + 54 + 1 \pmod{23} \\
\equiv 460 \pmod{23} \\
\equiv 0 \pmod{23}.
\]

And yes, 9 is a root of the quadratic congruence.

Below are three copies of the graph of $5x^2 + 6x + 1$ each shifted by 23 units on the $x$-axis. Place six dots (two on each graph) which represent the $(x, y)$ values of solutions to the congruence. [You Do!]

---

**BOTTOMLINE:** The method we just used to find two solutions to the congruence $5x^2 + 6x + 1 \equiv 0 \pmod{23}$ was TERRIBLY inconvenient. There has got to be an easier way. Carl Friedrich Gauss paved this road long ago, and it is called Quadratic Reciprocity!
10.2 The Many Masks of Quadratic Reciprocity (QR)

**Definition 10.3.** Let $p$ be an odd prime and $\gcd(a, p) = 1$. If the quadratic congruence $x^2 \equiv a \pmod{p}$ has a solution, then $a$ is said to be a **quadratic residue of** $p$. Otherwise, $a$ is called a **quadratic nonresidue of** $p$.

Equivalently, if $a$ is a solution to $x^2 \equiv a \pmod{p}$, then we say $a$ is a **square modulo** $p$ and otherwise called a **nonsquare modulo** $p$.

---

A Brief History Sketch of QR

1. **(Mid 1600s)** Fermat states that $-1$ is a square modulo an odd prime $p$ if and only if $p \equiv 1 \pmod{4}$.

2. **(1744)** Euler made conjectures equivalent to QR Laws. However, he was unable to prove most of them.

3. **(Late 1700s)** Legendre makes an attempt at proving QR Laws, but although incomplete, gives valuable progress—especially, with the powerful notation now called the Legendre symbol $(\frac{a}{b})$.

4. **(1797)** Gauss gives the first (of many of his) proofs of QR Laws.

5. **(1797 and onward)** At least 196 proofs of QR have been published as shown in the bibliography of a 2000 text by Lemmermeyer.$^h$

---

**QUESTION:** For which primes $p$ is the element $\overline{a} \in \mathbb{U}(p)$ a perfect square?

**THE SURPRISING ANSWER:** We will eventually see that the answer depends only on the reduction of $p$ modulo $4a$. 

---

10.3 Solving Quadratic Congruences

10.4 Euler’s Criterion

Euler came up with a simple criterion for deciding whether an integer $a$ is a quadratic residue of a given prime $p$.

**Theorem 10.4** (Euler’s criterion). Let $p$ be an odd prime and $\gcd(a, p) = 1$. Then $a$ is a quadratic residue of $p$ if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

[Still to do!]

While Euler’s criterion can be used in deciding whether an integer $a$ is a quadratic residue of a given prime $p$, it is only practical if the modulus is small because of the calculations. In the next few sections, we will lead up to a more effective method of computation for finding solutions to quadratic congruences.

10.5 The Legendre Symbol and Its Properties

**Question 10.5.** Who is Legendre?

- Adrien-Marie Legendre (1752 – 1833), France
- For two centuries until the year 2005, the image on the left of the French politician Louis Legendre has been cited in books, articles, etc. to be that of the mathematician Legendre! There is no known image however of Legendre.
- He conjectured the famous quadratic reciprocity law which was later to be proven by Gauss.
- The Legendre symbol $\left(\frac{a}{p}\right)$ is named after him.
- He has a crater on the moon also named after him!

$aBa$: Mention that the Legendre symbol is an example of a completely multiplicative function in its top argument. That is

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$
aBa will give this Section 10 later in the semester!
Index

A
absolute pseudoprime, 208
abundant number, 178
additive function, 182
algebraic number, 25
arithmetic function, 170
asymptotic functions, 96

B
Bézout, Étienne (1730–1783), 131
Bellhegor’s prime, 100
bijective map, 235
binary operation, 226
binomial coefficients, 82
Brocard’s Conjecture, 22
Brocard’s Problem, 22

C
cardinality, 64
Carmichael number, 208
Cartesian product, 67, 226
Chinese Remainder Theorem, 153, 156
Cole, Frank Nelson (1861–1926), 102
complement of a set, 66
complement rule, 91
complete residue system, 230
completely additive function, 182
completely multiplicative function, 191, 256
composite number, 95
congruence modulo  n, 142
correlation, 39
contradiction, 40
contrapositive statement, 42
converse statement, 42
cyclic group, 242
cyclic subgroup, 242

D
da Vinci, Leonardo (1452–1519), 14
De Morgan’s laws for logic, 40
De Morgan’s laws for sets, 67
decimal representation, 124
deficient number, 178
density of primes, 95
Diophantine equation, 134
Diophantine line, 136, 251
Diophantus of Alexandria (fl. A.D. 250), 134
disjoint sets, 67
disjoint union, 67
disjunction, 39
divisible, 120
division algorithm, 126
domain of a predicate, 46

E
element of a set, 64
equivalence class, 228
equivalence relation, 228
Erdős-Straus Conjecture, 22
Euclid (fl. 300 B.C.), 129
Euclid’s Lemma, 106
Euclid-Euler Theorem, 179
Euler’s Criterion, 256
Euler’s phi function, 183, 214, 239
Euler’s Theorem, 214
Euler, Leonhard (1707–1783), 183
Eulerian logarithmic integral, 97
existence proof, 31
existential quantifier, 47
existential statement, 47
expressionless people, 11

F
factorial, 82
Fermat number, 104
Fermat prime, 104
Fermat’s Last Theorem, 23
Fermat’s Little Theorem, 207, 211
Fermat, Pierre de (1601–1665), 206
Fundamental Theorem of Arithmetic, 106

G
Gauss, Carl Friedrich (1777–1855), 32, 142
Germain, Sophie (1776–1831), 105
Goldbach Conjecture, 112
Goldbach, Christian (1690–1764), 112
greatest common divisor, 111, 127
group, 226
group (U(n), ⊕) of units modulo  n, 232
group (Zn, ⊕) of integers modulo  n, 230
group \((U_n, \cdot)\) of \(n\)th roots of unity, 236

group homomorphism, 235

group isomorphism, 236

H

Halmos, Paul (1916–2006), 6

Hardy, Godfrey Harold (1877–1947), 12

Hasan Ibn al-Haytham (c. A.D. 965–1040), 179

Hippasus (fl. 500 B.C.), 61

Hui, Yang (1238–1298), 83

I

implication, 39

induction, 74

injective map, 235

intersection, 66

inverse statement, 43

L

Landau’s problems, 20

Landau, Edmund (1877–1938), 20

least common multiple, 111, 127

least residue system, 230

Legendre symbol, 191

Legendre, Adrien-Marie (1752–1833), 96, 256

Lehmer, Derrick (1905–1991), 103

logarithmic integral, 97

logically equivalent, 40

Lucas, Édouard (1842–1891), 102

M

Mahaviracharya (c. 850), 119, 139

Mersenne factor theorem, 102

Mersenne prime, 101

Mersenne, Marin (1588–1648), 101

Mona Lisa painting, 14

multiplicative function, 176

Möbius function, 188

Möbius Inversion Formula, 192

Möbius, August Ferdinand (1790–1868), 188

N

negation, 38

Nicomachus of Gerasa (c. A.D. 60–120), 35, 179

nullset, 64

number theory, 12

O

Omega function, 182

omega function, 182

order of a group, 241

order of an element, 241

P

palindromic prime, 99

partition of a set, 67, 228

Pascal, Blaise (1623–1662), 83

peanut view of equivalence classes, 228

perfect number, 178

pigeonhole principle, 29

Powers, Ralph Ernest (1875–1952), 103

predicate, 46

Prevushin, Ivan (1827–1900), 102

prime counting function, 95

Prime Factorization Theorem, 106

prime number, 17, 95

prime number theorem, 95

primitive root, 246

primitive root modulo \(n\), 244

proof by cases, 57

proof by contradiction, 58

proof by contrapositive, 58

proof by exhaustion, 48

proof, direct method, 57

proper divisor, 120

pseudoprime, 208

pseudoprime to the base \(a\), 208

public key cryptography, 13

pure mathematics, 12

Pythagoras (c. 570–495 B.C.), 35, 61

Pythagorean triples, 17

Q

quadratic nonresidue of \(p\), 255

quadratic residue of \(p\), 255

quantifier, 46

quotient, 126

R

Ramanujan, Srinivasa (1887–1920), 15, 33

rearrangement property, 209

reflexive relation, 228

relation, 228

relatively prime, 127

remainder, 126
residue class modulo $n$, 230
Riemann Hypothesis, 22

S
safe prime, 105
set, 64
set of integers modulo $n$, 230
sigma function, 171
Sophie Germain prime, 105
stars and bars method, 140
statement, 38
subgroup, 242
surjective map, 235
symmetric relation, 228

T
tau function, 171
tautology, 40
transcendental number, 25
transitive relation, 228
triangular number, 75
truth table, 38
twin primes, 17

U
union, 66
unit in $\mathbb{Z}_n$, 232
universal conditional statement, 49
universal quantifier, 47
universal set, 66
universal statement, 47

V
vacuously true statement, 39

W
well-defined operation, 230
Well-Ordering Principle, 106, 132
Wilson’s Theorem, 212
Wilson, John (1741–1793), 212
WWTS bubble, 11