Contents

Notation for Math 506 5

Chapter 1. Divisibility, Congruences and Induction 7
  1.1. Introduction 7
  1.2. A brief look at the Axioms sheet 9
  1.3. Divisibility Properties of \( \mathbb{Z} \) 10
  1.4. Greatest common divisors and least common multiples 11
  1.5. The Euclidean algorithm 11
  1.6. Euclidean Algorithm 12
  1.7. Linear Combinations and the GCDLC theorem. 12
  1.8. Euclid’s Lemma 15
  1.9. Linear Equations in two variables 15
  1.10. Introduction to Congruences 16
  1.11. Principle of Induction 18

Chapter 2. Primes and Unique Factorization 19
  2.1. Fundamental Theorem of Arithmetic 19
  2.2. Gaussian Integers 20
  2.3. Distribution of primes 22

Chapter 3. Arithmetic Functions 23
  3.1. Multiplicative Functions 23
  3.2. Perfect, Deficient and Abundant Numbers 25
  3.3. Properties of multiplicative functions. 27
  3.4. The Möbius Function 29

Chapter 4. More on Congruences 33
  4.1. Counting Solutions of Congruences 33
  4.2. Linear Congruences 33
  4.3. Multiplicative inverses (mod \( m \)) 34
  4.4. Chinese Remainder Theorem 35
  4.5. Fermat’s Little Theorem and Euler’s Theorem 35
  4.6. Orders of elements (mod \( m \)) 36
  4.7. Decimal Expansions 37
  4.8. Primality Testing 38
  4.9. Public-Key Cryptography 39

Chapter 5. Polynomial Congruences 41
  5.1. Lifting solutions from (mod \( p \)) to (mod \( p^e \)) 41
  5.2. Counting Solutions of congruences 43
  5.3. Solving congruences (mod \( p \)) 44
## CONTENTS

5.4. Quadratic Residues and the Legendre Symbol 45  
5.5. Quadratic Reciprocity 47  
5.6. Representing primes as sums of two squares 48  

Appendix A. Axioms for the set of Integers $\mathbb{Z}$ 51  
Appendix B. A Little Bit of Logic for Math 506 55
Notation for Math 506

\[ \mathbb{N} = \{1, 2, 3, 4, 5, \ldots\} = \text{Natural numbers} \]
\[ \mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\} = \text{Integers} \]
\[ \mathbb{E} = \{0, \pm 2, \pm 4, \pm 6, \ldots\} = \text{Even integers} \]
\[ \mathbb{O} = \{\pm 1, \pm 3, \pm 5, \ldots\} = \text{Odd integers} \]
\[ \mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\} = \text{Rational numbers} \]
\[ \mathbb{R} = \text{Real numbers} \]
\[ \mathbb{C} = \text{Complex numbers} \]
\[ \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\} = \text{Gaussian integers} \]
\[ \mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \ldots\} = \text{Primes} \]

\[ a \equiv b \pmod{m} \text{ means } a \text{ is congruent to } b \text{ mod } m, \text{ that is, } m|(b-a) \]
\[ [a]_m = \{a + mk : k \in \mathbb{Z}\} = \text{Residue class of } a \text{ mod } m \]
\[ \mathbb{Z}_m = \{[0]_m, \ldots, [m-1]_m\} = \text{Ring of integers mod } m \]
\[ a^{-1} \pmod{m} = \text{multiplicative inverse of } a \pmod{m} \]
\[ \phi(m) = \text{Euler phi-function} \]
\[ (a, b) = \text{gcd}(a, b) = \text{greatest common divisor of } a \text{ and } b \]
\[ [a, b] = \text{lcm}[a, b] = \text{least common multiple of } a \text{ and } b \]
\[ a|b \text{ means } a \text{ divides } b \]
\[ p^c|m \text{ means } p^c \text{ is the largest power of } p \text{ dividing } m \]

\[ \pi(x) = \text{the number of primes less than or equal to } x. \]
\[ \tau(n) = d(n) = \text{number of positive divisors of } n \]
\[ \sigma(n) = \text{sum of the positive divisors of } n \]
\[ \phi(n) = \text{Euler phi-function} = \text{number of positive } a < n \text{ with } (a, n) = 1 \]
\[ \mu(n) = \text{Möbius function} \]
\[ \left(\frac{a}{p}\right) = \text{Legendre symbol} \]

\[ |S| = \text{order or cardinality of a set } S; \text{ the number of elements in } S \]
<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>∩</td>
<td>intersection</td>
</tr>
<tr>
<td>∅</td>
<td>empty set</td>
</tr>
<tr>
<td>∈</td>
<td>element of</td>
</tr>
<tr>
<td>∀</td>
<td>for all</td>
</tr>
<tr>
<td>∃</td>
<td>there exists</td>
</tr>
<tr>
<td>∃!</td>
<td>there exists a unique</td>
</tr>
<tr>
<td>⇒</td>
<td>implies</td>
</tr>
<tr>
<td>⇔</td>
<td>equivalent to</td>
</tr>
<tr>
<td>≡</td>
<td>congruent to</td>
</tr>
<tr>
<td>∪</td>
<td>union</td>
</tr>
<tr>
<td>⊆</td>
<td>subset</td>
</tr>
<tr>
<td>iff</td>
<td>if and only if</td>
</tr>
</tbody>
</table>

**Example:**

If $A$ and $B$ are sets, then $A \cap B$ represents the intersection of $A$ and $B$, and $A \cup B$ represents the union of $A$ and $B$. The empty set is denoted by $\emptyset$. The symbol $\exists$ indicates that there exists a set, and $\exists!$ indicates that there exists a unique set.
CHAPTER 1

Divisibility, Congruences and Induction

1.1. Introduction

\( \mathbb{N} = \text{Natural Numbers: } 1, 2, 3, 4, 5, 6, \ldots \)

Kronecker: “God created the natural numbers. Everything else is man’s handiwork.”

Gauss: “Mathematics is the queen of sciences— and number theory is the queen of mathematics.”

Number Theory: The study of the natural numbers.

Questions: It is very easy to ask questions about the natural numbers. Let’s ask a few about the set of primes \( \mathcal{P} = \{2, 3, 5, 7, 11, 13, \ldots \} \).

Q1. Are there infinitely many primes?
Q2. How many primes are there up to a given value \( x \)?
Q3. Are there infinitely many twin primes? (3,5), (5,7), (11,13), (17,19), etc.
Q4. Which primes can be expressed as a sum of two squares? 5 = 1\(^2\) + 2\(^2\), 13 = 2\(^2\) + 3\(^2\), etc.

Which of these problems are easy to solve and which are hard?

Q1: We can answer this question affirmatively at the beginning of this semester. The proof goes back to Euclid.
Q2: This is a difficult problem, but there are now excellent estimates for the number of primes up to \( x \). See Example 1.1.11.
Q3: This is still an open problem, but exciting progress has been made in the past couple years. We now know that there are infinitely many consecutive primes \( p_n, p_{n+1} \) with \( p_{n+1} - p_n \leq 246 \).
Q4: This is a problem that you can investigate right now. Make a table with primes up to 43 and test them. What conjecture do you make? We will be able to answer this question fully by the end of the semester.

2. Puzzles, Patterns and Games: Amateur mathematicians of all ages enjoy these problems. This is important in early school education to get children interested in mathematics and in thinking. People enjoy mathematical puzzles more than is generally believed. Chess, Checkers, Tic-Tac-Toe, Card Games, Cross Word Puzzles, etc. all involve elements of mathematical reasoning and are valuable skills.
1. DIVISIBILITY, CONGRUENCES AND INDUCTION

Example 1.1.1. Theory. Triangular numbers: $1, 3, 6, 10, 15, 21, 28, 36, 45, \ldots, n(n+1)/2$. Squares: $1, 4, 9, 16, 25, 36, \ldots, n^2$. Pentagonal numbers: $1, 5, 12, 22, 35, \ldots, n(3n-1)/2$. Fermat (1640) Polygonal number conjecture: Every whole number is a sum of at most three triangular numbers, at most 4 squares, at most 5 pentagonal numbers, 6 hexagonal numbers, etc. Lagrange proved squares. Gauss proved triangular numbers. Cauchy proved general case.

The next few examples are patterns and puzzles.

Example 1.1.2. Squaring numbers that end in 5. Make a conjecture and prove it.

Example 1.1.3. $816^2 + 357^2 + 492^2 = 618^2 + 753^2 + 294^2$.

Example 1.1.4. Euler conjectured that a sum of three fourth powers could never be a fourth power. Elkies (1988) proved there are infinitely many counterexamples. $422481^4 = 95800^4 + 217519^4 + 414560^4$.

Example 1.1.5. Collatz conjecture. Open problem today. Start with any positive integer. If it is even divide it by 2. If odd, multiply by 3 and add 1. After a finite number of steps one eventually ends up with 1.

Example 1.1.6. N. Elkies and I. Kaplansky. Every integer $n$ can be expressed as a sum of a cube and two squares. Note that $n$ may be negative, as also may be the cube. For example, if $n$ is odd, say $n = 2k + 1$, then

$$n = 2k + 1 = (2k - k^2)^3 + (k^3 - 3k^2 + k)^2 + (k^2 - k - 1)^2$$

Example 1.1.7. There are just five numbers which are the sums of the cubes of their digits. $1 = 1^3$. $153 = 1^3 + 5^3 + 3^3$, $370 = 3^3 + 7^3 + 0^3$, $371 = 3^3 + 7^3 + 1^3$, $407 = 4^3 + 0^3 + 7^3$. This is an amusing fact, although challenging to prove. (extra credit).

Example 1.1.8. Start with any four digit number, say 2512 (with not all the same digits). Rearrange the digits and subtract the smaller from the larger. Repeat. What happens?

Example 1.1.9. Consider the six digit number $x = 142857$. Note that $2x = 285714$, $3x = 428571$, $4x = 571428$, $5x = 714285$, $6x = 857142$. Is this just a coincidence? Are there any other six digit numbers with such a cyclical property? Have you ever seen the digits 142857 before? (There’s a little bit of theory going on in this problem. The result can be generalized).

Note that the first three examples depend on the base 10 representation of natural numbers. The important properties of the natural numbers are those that are intrinsic, that is, that do not depend on the manner in which the number is represented.

Example 1.1.10. $1^3 + 2^3 = 9 = (1 + 2)^2$. $1^3 + 2^3 + 3^3 = 36 = (1 + 2 + 3)^2$. $1^3 + 2^3 + 3^3 + 4^3 = 100 = (1 + 2 + 3 + 4)^2$. Maybe we’ve discovered a general formula. Let’s see, is it always true that $(x^3 + y^3) = (x + y)^2$. No. But we suspect that $1^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$. We shall use induction to prove results of this nature.
1.2. A brief look at the Axioms sheet

Example 1.1.11. Prime Numbers. 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43,\ldots The prime numbers are the building blocks of the whole numbers, in the sense that every whole number is a product of primes. Do they just pop up at random? How many primes are there? Are there infinitely many twin primes? How many primes are there up to $N$? Gauss, using a table of primes up to 100000, at the age of 15 made a table comparing the number of primes up to $N$ with the function $li(x) = \int_2^x \frac{dt}{\ln t}$.

$$\begin{array}{c|c|c}
N & \pi(N) & li(N) \\
\hline
10^3 & 168 & 178 \\
10^4 & 1229 & 1246 \\
10^5 & 9592 & 9630 \\
10^6 & 78498 & 78628 \\
10^7 & 664579 & 664918 \\
10^8 & 5761455 & 5762209 \\
10^9 & 50847534 & 50849235 \\
10^{10} & 455052512 & 455055614 \\
\end{array}$$

The ratio of these two quantities approaches 1 as $N$ goes to infinity. This can be proved, (although Gauss wasn’t able to prove it. But he was instrumental in the development of Complex numbers, which are an essential tool for proving this result). Its called the prime number theorem, one of the jewels of mathematics. It was proven by J. Hadamard and C. de la Vallee Pousin (1896). Look briefly at the axiom sheet. In particular, the associative law.

1.2. A brief look at the Axioms sheet

Look at the axiom sheet. The first page are axioms shared by the real number system. What distinguishes the integers is their discreteness property. There are three equivalent ways of expressing this property.

Well-Ordering Axiom of the Integers. Any nonempty subset $S$ of positive integers contains a minimum element. That is, there is a minimal element $m$ in $S$ having the property that $m \leq x$ for all $x \in S$.

Note 1.2.1. (i) The rationals and reals do not have such a property. Consider for example the set of real numbers on the interval $(0, 1)$.

(ii) It is this property that assures us that there is no integer hiding somewhere between 0 and 1, in other words that 1 is the smallest positive integer. For if such an integer $a < 1$ existed we could construct an infinite descending chain of positive integers $a, a^2, a^3, \ldots$, with no minimal element.

Axiom of Induction. If $S$ is a nonempty subset of $\mathbb{N}$ containing 1 and having the property that if $n \in S$ then $n + 1 \in S$ then $S = \mathbb{N}$.

Note 1.2.2. It is from this axiom that we obtain the Principle of Induction, which is the basis for induction proofs.

Note: We say that a set of integers $S$ is bounded above if there is some number $L$ say, such that $x < L$ for all $x \in S$.

Maximum Element Property of the integers. Any nonempty set $S$ of integers bounded above contains a maximum element, that is, there is an element $M \in S$ such that $x \leq M$ for all $x \in S$. 
Note the use of the word “has”: If we say a set $S$ has an upper bound, this does not mean the upper bound is in $S$. If we say a set $S$ has a maximum element, this does mean the maximum element is in $S$.

### 1.3. Divisibility Properties of $\mathbb{Z}$

**Definition 1.3.1.** Let $a, b \in \mathbb{Z}$, with $a \neq 0$. We say that $a$ divides $b$, written $a \mid b$, if there is an integer $x$ such that $ax = b$.

Equivalently: $a \mid b$ iff $b/a$ is an integer. This formulation assumes that we have already constructed the set of rational numbers. Our textbook uses this as a definition. In this class I want you to be able to write proofs about integers just using the axioms for the integers (so avoid using the rationals).

Terminology: The definition above is mathematical wording “$a$ divides $b$”. This is not a common usage of the word divides, it sounds like the number $a$ is doing something to $b$. Note the difference between $3 \mid 6$ and $3 \nmid 6$.

Other variations of $3 \mid 6$: We can say $3$ divides $6$, $3$ is a divisor of $6$, $3$ is a factor of $6$, $6$ is divisible by $3$, $6$ is a multiple of $3$.

**Example 1.3.1.** $3 \mid 15, 5 \mid 15$, but $7 \nmid 15$. What is wrong with saying $7 \mid 15$ because $7 \times 15/7 = 15$.

**Example 1.3.2.** List all divisors of $12$. What numbers divide $0$? What numbers are divisible by $0$?

**Example 1.3.3.** Find all positive $n$ such that $5 \mid n$ and $n \mid 60$. $5 \mid n$ so $n = 5k$ for some integer $k$. $5k \mid 60$ so $5kx = 60$ for some integers $k, x$. Thus $kx = 12$ for some $k, x$. Thus $k$ is a divisor of $12$ so can let $k = 1, 2, 3, 4, 6, 12, n = 5, 10, 15, 20, 30, 60$.

**Theorem 1.3.1.** **Transitive property of divisibility.** If $a \mid b$ and $b \mid c$ then $a \mid c$.

**Proof.** You should be able to write a rigorous proof starting from the definition of divisibility. Note the use of the associative law. □

**Example 1.3.4.** $7 \mid 42, 42 \mid 420$ therefore, $7 \mid 420$.

**Theorem 1.3.2.** **Additive property of divisibility.** Let $a, b, c$ be integers such that $c \mid a$ and $c \mid b$. Then (i) $c \mid (a + b)$, (ii) $c \mid (a - b)$ and (iii) For any integers $x, y$, $c \mid (ax + by)$.

**Proof.** Again, this is a basic proof. □

**Example 1.3.5.** Note that the additive property of divisibility can be reworded: If $a$ and $b$ are multiples of $c$ then so is $a + b$. Thus, a sum of two evens is even, or a sum of two multiples of 5 is a multiple of 5.

**Example 1.3.6.** $3 \mid 21, 3 \mid 15$. Therefore $3 \mid (21 - 15)$, i.e. $3 \mid 6$, and $3 \mid (2 \cdot 21 + 15)$, i.e. $3 \mid 57$. 

1.4. Greatest common divisors and least common multiples

**Definition 1.4.1.** Let $a, b$ be integers, not both 0.

1) An integer $d$ is called the greatest common divisor (gcd) of $a$ and $b$, denoted $gcd(a, b)$ or $(a, b)$, if (i) $d$ is a divisor of both $a$ and $b$, and (ii) $d$ is the greatest common divisor, that is, if $e | a$ and $e | b$ then $d ≥ e$.

2) An integer $m$ is called the least common multiple (lcm) of $a, b$ denoted $lcm[a, b]$ or $[a, b]$, if (i) $m > 0$, (ii) $m$ is a common multiple and (iii) $m$ is the least common multiple.

Note: (i) If $a, b$ are not both 0, then $(a, b)$ exists and is unique. Proof. Let $S$ be the set of common divisors of $a$ and $b$. Note, $S$ is nonempty since $1 ∈ S$. Also, $S$ is bounded above by $|a|$, that is, if $x ∈ S$ then $x ≤ |a|$. Thus by the Maximum element principle $S$ contains a maximum element.

(ii) For any $a, b$, not both zero, $gcd(a, b) ≥ 1$. Why? 1 is always a common divisor, and 1 is the smallest positive integer.

(iii) $(0, 0)$ is not defined?

(iv) $gcd(0, a) = |a|$ for any nonzero $a$.

(v) $lcm[a, 0]$ does not exist.

**Example 1.4.1.** $(6, −2) = 2$, $(0, 17) = 17$, $[6, −2] = 6$, $[6, 10] = 30$.

There are three ways of computing GCD’s: (i) Brute force. (ii) Factoring method. (iii) Euclidean Algorithm. For large numbers, the Euclidean algorithm is much faster. A PC can handle GCD’s of numbers with thousands of digits using the Euclidean algorithm in “no time”. But the fastest known algorithms cannot factor a 200 digit numbers (in general), given any amount of time.

**Example 1.4.2.** Factoring Method. Find gcd$(240, 108)$ given the factorizations $240 = 2^4 · 3 · 5$, $108 = 2^2 · 3^3$. Find lcm$[240, 108]$. This method is a little out of order, because we have not proven the fundamental theorem of arithmetic yet, but this is a procedure you likely saw back in grade school.

**Example 1.4.3.** Find gcd$(1127, 1129)$. Consider the three different methods listed above.

1.5. The Euclidean algorithm

The Euclidean algorithm is based on the following lemma.

**Lemma 1.5.1. gcd subtraction lemma.** Let $a, b$ be integers, not both 0. Then for any integer $k$, $(a, b) = (a − kb, b)$.

**Proof.** Let $S$ be the set of common divisors of $a, b$ and $T$ the set of common divisors of $a − kb, b$. Claim $S = T$, and so $S$ and $T$ have the same maximal element. □

**Example 1.5.1.** (Euclidean Algorithm.) Show gcd$(234, 182) = 26$

**Example 1.5.2.** $(108, 48) = (108 − 96, 48) = (12, 48) = 12$. What we are actually doing is computing $108/48 = 2 + 12/48$.

In order to implement the Euclidean algorithm we use the Division algorithm.
Then there exist unique integers \( q, r \) the quotient, and \( r \) the remainder. Equivalently, we can write \( \frac{a}{b} = q + \frac{r}{b} \).

**Proof.** Existence: Let \( S = \{ x \in \mathbb{Z} : xb \leq a \} \). Then \( S \) is bounded above by \( a/b \) and so it contains a maximum element, say \( q \). Define \( r = a - qb \). Then \( a = qb + r \). By maximality of \( q \) we have \( qb \leq a < (q + 1)b \), and so \( 0 \leq r < b \).

Uniqueness: Suppose that \( a = q'b + r' \), with \( 0 \leq r' < b \). Then \( b|q - q'| = |r' - r| < b \). Since the LHS is a multiple of \( b \) this is only possible if \( q = q' \). It follows that \( r = r' \). \( \square \)

**Example 1.5.3.** Find \( q, r \) when \(-392\) is divided by \(15\). We first observe that \(392/15 = 26 + 2/15\), so that \(392 = 15 \cdot 26 + 2 \) and so \(-392 = (-27)15 + 13\).

### 1.6. Euclidean Algorithm

The Euclidean Algorithm is a procedure for calculating gcd’s by using successive applications of the division algorithm. There are two versions of it that we will look at.

I) Traditional Euclidean Algorithm: In this version a positive remainder is always chosen. Let \( a \geq b > 0 \) be positive integers. Then, by the division algorithm and gcd subtraction lemma, we have

\[
\begin{align*}
(1.1) & \quad a = bq_1 + r_1, \quad 0 \leq r_1 < b, \quad (a, b) = (r_1, b) \\
(1.2) & \quad b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1, \quad (a, b) = (r_1, r_2) \\
(1.3) & \quad \ldots \\
(1.4) & \quad r_{k-3} = r_{k-2}q_{k-1} + r_{k-1}, \quad (a, b) = (r_{k-1}, r_{k-2}) \\
(1.5) & \quad r_{k-2} = r_{k-1}q_k, \quad (a, b) = r_{k-1}.
\end{align*}
\]

Since \( r_1 > r_2 > \cdots > r_{k-1} \) we are guaranteed that this process will stop in a finite number of steps.

II) Fast Euclidean Algorithm: In your homework you prove the following version of division algorithm. Given integers \( a > b > 0 \) with \( a > 0 \) there exist integers \( q \) and \( r \) such that \( a = qb + r \) with \( |r| \leq b/2 \). Thus if we allow ourselves to work with negative remainders we can assume that the remainder in absolute value is cut by a factor of 2 at each step of the algorithm. Thus \( |r_1| \leq b/2, |r_2| \leq |r_1|/2 \leq b/4, \ldots, |r_i| \leq b/2^i \). The algorithm terminates when \( |r_i| < 1 \), for this would imply that \( r_i = 0 \). Thus it suffices to have \( b < 2^i \) and so the algorithm terminates in at most \( \lfloor \log_2 b \rfloor + 1 \) steps; here \( \lfloor x \rfloor \) denotes the greatest integer less than or equal to \( x \), called the floor function or greatest integer function.

**Example 1.6.1.** Find \( \gcd(150, 51) \) both ways.

### 1.7. Linear Combinations and the GCDLC theorem.

**Definition 1.7.1.** A linear combination of two integers \( a, b \) is an integer of the form \( ax + by \), with \( x, y \in \mathbb{Z} \). Thus, we say that an integer \( d \) is a linear combination of \( a \) and \( b \) if there exist integers \( x, y \) such that \( d = ax + by \).
1.7. LINEAR COMBINATIONS AND THE GCDLC THEOREM

**Example 1.7.1.** Find all linear combinations of 9 and 15. Try to get the smallest possible.

<table>
<thead>
<tr>
<th>x</th>
<th>y</th>
<th>9x + 15y</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>24</td>
</tr>
<tr>
<td>2</td>
<td>−1</td>
<td>3</td>
</tr>
</tbody>
</table>

Note that every linear combination is a multiple of 3, the greatest common divisor of 9, 15.

Recall: We saw earlier that if \( d \) is a common divisor of \( a, b \) then \( d \mid ax + by \) for any \( x, y \in \mathbb{Z} \). In particular this holds for the greatest common divisor of \( a, b \).

**Claim:** If \( d = \gcd(a, b) \) then \( d \) can be expressed as a linear combination of \( a \) and \( b \).

**Example 1.7.2.** \( \gcd(20, 8) = 4 \). By trial and error, \( 4 = 1 \cdot 20 + (-2)8 \).
\( \gcd(21, 15) = 3 \). By trial and error, \( 3 = 3 \cdot 21 - 4 \cdot 15 \).

To prove the claim in general we again use the Euclidean Algorithm, together with the method of back substitution.

**Example 1.7.3.** Find \( d = \gcd(126, 49) \).

\[
\begin{align*}
(1) \quad 126 &= 2 \cdot 49 + 28, \quad d = \gcd(28, 49) \\
(2) \quad 49 &= 28 + 21, \quad d = \gcd(28, 21) \\
(3) \quad 28 &= 21 + 7, \quad d = \gcd(7, 21) \\
(4) \quad 21 &= 3 \cdot 7, \quad d = \gcd(7, 0) = 7, \text{STOP}
\end{align*}
\]

**Back Substitution:** A method of solving the equation \( d = ax + by \) (with \( d = \gcd(a, b) \)) by working backwards through the steps of the Euclidean algorithm.

**Example 1.7.4.** Use example above for \( \gcd(126, 49) \) to express 7 as a linear combination of 126 and 49 by using the method of back substitution. Start with equation (3): \( 7 = 28 - 21 \). By (2) we have \( 21 = 49 - 28 \). Substituting this into previous equation yields \( 7 = 28 - (49 - 28) = 2 \cdot 28 - 49 \). By (1) we have \( 28 = 126 - 2 \cdot 49 \). Substituting this into previous equation yields \( 7 = 2 \cdot (126 - 2 \cdot 49) - 49 = 2 \cdot 126 - 5 \cdot 49 \), QED.

**Theorem 1.7.1. GCDLC Theorem.**

The greatest common divisor of two integers \( a, b \) (not both zero) can be expressed as a linear combination of \( a, b \).

**Proof.** (Optional Reading) A constructive proof can be given by following the Euclidean Algorithm together with the method of back substitution. The notation is rather cumbersome however. We shall give here instead a non-constructive proof. Let \( S = \{ax + by : x, y \in \mathbb{Z}\} \), the set of all linear combinations of \( a \) and \( b \). This set clearly contains positive integers, so let \( e \) be the smallest positive integer in the set (\( e \) exists by well ordering). Say \( e = ax_0 + by_0 \), for some \( x_0, y_0 \in \mathbb{Z} \). We claim that \( e = d \). Since \( d \mid a \) and \( d \mid b \), we know \( d \mid e \), by a basic divisibility property. In particular, \( d \leq e \). Thus, it suffices to show that \( e \) is a common divisor of \( a \) and \( b \), for this would imply that \( e \leq d \), the greatest common divisor of \( a \) and \( b \).
Let's show that \( e \mid a \). To do this, we shall compute \( a \div e \) and show that the remainder is 0. By the division algorithm, \( a = qe + r \), for some \( q,r \in \mathbb{Z} \) with \( 0 \leq r < e \). Thus \( a = (ax_0 + by_0) + r \), so \( r = a(1 - qx_0) - by_0 \) a linear combination of \( a \) and \( b \). Since \( r < e \) we must have \( r = 0 \) by the minimality of \( e \) in \( S \). Therefore \( e \mid a \). In the same manner we obtain \( e \mid b \). QED □

**Theorem 1.7.2. GCDLC Corollary** Let \( a,b \) be integers, not both zero, and \( d = (a,b) \).

(i) Every linear combination of \( a,b \) is a multiple of \( d \) and conversely every multiple of \( d \) is a linear combination of \( a,b \).

(ii) In particular, \( d \) is the smallest positive linear combination of \( a \) and \( b \).

**Proof.** The first part of (i) is just a special case of the additive property of divisibility. For the second part of (ii) let \( d = (a,b) \). Then we can write \( d = ax + by \) for some integers \( x,y \). Suppose that \( kd \) is an arbitrary multiple of \( d \). Then \( kd = (kx)a + (ky)b \) and so \( kd \) is a linear combination of \( a,b \). Part (ii) is obvious from (i) since every positive multiple of \( d \) is \( \geq d \).

**Example 1.7.5.** Suppose I tell you that \( a,b \) are whole numbers such that \( 45a + 37b = 1 \). What is \( (a,b) \)?

**Example 1.7.6.** Describe all positive integers that can be expressed as a linear combination of 45 and 37.

**Array Method.** A more efficient method than back substitution for expressing the greatest common divisor of two integers as a linear combination of them.

**Example 1.7.7.** We shall redo a previous example using the array method. Find \( \text{gcd}(49,126) \) and express it as a linear combination of 49 and 126. To begin, set up an array with the first three columns initialized as shown below. For a given choice of \( x \) and \( y \) the linear combination \( 126x + 49y \) is given in the first row. Now, perform the Euclidean Algorithm on the numbers in top row, but do the corresponding column operations on the entire array. Let \( C_1 \) be the column with top entry 126, \( C_2 \) the column with top entry 49, etc.. The first step in the Euclidean algorithm is to subtract 2 times 49 from 126, so we let the next column \( C_3 \) be given by \( C_3 = C_1 - 2C_2 \). Then \( C_4 = C_2 - C_3 \), \( C_5 = C_3 - C_4 \). The Euclidean algorithm stops on the next step, but there is no need to include an extra column with zero at the top.

<table>
<thead>
<tr>
<th>126x + 49y</th>
<th>126</th>
<th>49</th>
<th>28</th>
<th>21</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>2</td>
</tr>
<tr>
<td>y</td>
<td>0</td>
<td>1</td>
<td>-2</td>
<td>3</td>
<td>-5</td>
</tr>
</tbody>
</table>

Thus we have discovered that \( 7 = \text{gcd}(49,126) \) and that \( 7 = 2 \cdot 126 - 5 \cdot 49 \).

**Example 1.7.8.** Find \( \text{gcd}(83,17) \) and express it as a LC of 83 and 17.

<table>
<thead>
<tr>
<th>83x + 17y</th>
<th>83</th>
<th>17</th>
<th>15</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>1</td>
</tr>
<tr>
<td>y</td>
<td>0</td>
<td>1</td>
<td>-4</td>
<td>5</td>
<td>-39</td>
</tr>
</tbody>
</table>

Thus \( \text{gcd}(83,17) = 1 \) and \( 1 = 8 \cdot 83 - 39 \cdot 17 \).
Example 1.7.9. Solve the equation $15x + 21y + 35z = 1$, that is express 1 as a LC of 15, 21, and 35, using the array method. Just start subtracting multiples of one column from another any way you like, with the goal of producing a smaller entry in the top row. (There are many ways to produce a 1 in this manner. The first three columns are initialized as before, then I did $C_2 - C_1$, $C_3 - C_2$, $C_1 - C_5$).

\[
\begin{array}{rrr|rrr}
15 & 21 & 35 & 15 & 21 & 35 \\
x & 1 & 0 & 0 & -1 & 0 & 1 \\
y & 0 & 1 & 0 & 1 & -1 & 1 \\
z & 0 & 0 & 1 & 0 & 1 & -1 \\
\end{array}
\]

thus $15 + 21 - 35 = 1$.

### 1.8. Euclid's Lemma

**Definition 1.8.1.** We say two integers $a, b$ are relatively prime if $\gcd(a, b) = 1$, that is $a, b$ have no common factor other than $\pm 1$.

**Theorem 1.8.1.** Let $a, b \in \mathbb{Z}$ (not both zero) with $(a, b) = d$. Then $(\frac{a}{d}, \frac{b}{d}) = 1$. (Note the two fractions are integers.)

**Proof.** Proof 1: (This proof doesn’t require GCDLC.) Suppose that $k$ is a common positive divisor of $\frac{a}{d}$ and $\frac{b}{d}$, so that $kx = \frac{a}{d}$, $ky = \frac{b}{d}$, for some integers $x, y$. Then $(kx)d = a$ and $(ky)d = b$, that is, $(kd)x = a$ and $(kd)y = b$. Thus $kd$ is a common divisor of $a, b$. Since $d$ is the greatest common divisor of $a$ and $b$, $0 < kd \leq d$ and so $k = 1$. This means $(\frac{a}{d}, \frac{b}{d}) = 1$.

Proof 2: By GCDLC we have $ax + by = d$ for some integers $x, y$. Dividing by $d$ gives $\frac{a}{d}x + \frac{b}{d}y = 1$. Thus $(\frac{a}{d}, \frac{b}{d})$ is a divisor of 1, and therefore must equal 1.

□

**Lemma 1.8.1.** Euclid’s Lemma. If $d|ab$ and $\gcd(d, a) = 1$ then $d|b$.

**Proof.** Since $d|ab$ we have $dz = ab$ for some integer $z$. Since $\gcd(d, a) = 1$, by GCDLC Theorem, there exist integers $x, y$ with $dx + ay = 1$. Multiplying by $b$ we obtain

\[
b = b(dx + ay) = d(bx) + (ab)y = d(bx) + (dz)y = d(bx + zy),
\]

and so $d|b$ since $bx + zy$ is an integer.

□

**Note 1.8.1.** In general, if $a|bc$ can we conclude that $a|b$ or $a|c$? No.

**Note 1.8.2.** Further applications of GCDLC theorem, in homework.

i) Every common divisor of $a$ and $b$ is a divisor of $\gcd(a, b)$.

ii) Every common multiple of $a$ and $b$ is a multiple of $\text{lcm}[a, b]$.

### 1.9. Linear Equations in two variables

For integers $a, b, c$ consider solving the linear equations

\[ax + by = c \quad (NH)\]

and

\[ax + by = 0 \quad (H)\]

in integers $x, y$. (NH) is called a nonhomogeneous equation and (H) a homogeneous equation. Geometrically, we are looking for integer points on a line in the plane.
The GCDLC theorem immediately yields a simple criterion for when (NH) has a solution.

**Corollary 1.9.1. Solvability of a Linear Equation.** Let \( a, b, c \in \mathbb{Z} \) with \( d = (a,b) \). The linear equation \( ax + by = c \) has a solution in integers \( x, y \) if and only if \( d|c \).

**Proof.** The equation is solvable if and only if \( c \) is a linear combination of \( a \) and \( b \). But the corollary to the GCDLC theorem states that this is possible if and only if \( d|c \). \( \square \)

To find all solutions of (NH) we use principle that you are familiar with from differential equations, namely that the general solution to (NH) is obtained by finding a particular solution of (NH) and adding to it any solution of (H). This works because the equation is linear.

Suppose that \((x_0, y_0)\) is a particular solution of (NH). Let \((x, y)\) be any solution of (H). Then \((x_0 + x, y_0 + y)\) is also a solution of (NH). Conversely, if \((x_1, y_1)\) is any solution of (NH) then we can write \((x_1, y_1) = (x_0, y_0) + (x_1 - x_0, y_1 - y_0)\) where the latter is a solution of (H).

Focus on solving (H): Let \( d = (a,b) \).

\[ ax = by \Rightarrow \frac{a}{d}x = \frac{b}{d}y \Rightarrow \frac{a}{d}|y \]

the last implication following from Euclid’s Lemma. Say \( \frac{a}{d}t = y \), with \( t \in \mathbb{Z} \). Then, since \( x = by/a \), we also get \( x = \frac{-b}{a}t \). Conversely for any integer \( t \), these values of \( x, y \) yield a solution of (NH). Thus we have

**Theorem 1.9.1.** Let \( d = (a,b) \). Then the equation (NH) above has a solution iff \( d|c \). Suppose \( d|c \) and that \((x_0, y_0)\) is a particular solution. Then the general solution is given by \( x = x_0 - \frac{b}{d}t, y = y_0 + \frac{a}{d}t, \) with \( t \) any integer. (Draw picture).

In applications we may wish to restrict the variables to positive values.

**Example 1.9.1.** A person has a collection of 17 and 25 cent stamps, but fewer than 30 25 cent stamps. How can he mail a parcel costing $8.00.

**Example 1.9.2.** In baseball a few years ago the American league had 2 divisions with 7 teams each. Say that teams play \( x \) games against each team in their own division and \( y \) games against each team in the other division. Find possible solutions for \( x, y \) assuming there are 162 games in a season? Which solution do think was used?

### 1.10. Introduction to Congruences

Let \( m \) be a fixed positive integer, referred to as the “modulus”.

**Definition 1.10.1.** We say that two integers \( a, b \) are congruent \( \mod m \) and write

\[ a \equiv b \pmod{m} \]

if \( m|a - b \). Equivalently \( a \equiv b \pmod{m} \) iff \( a = b + km \) for some integer \( k \).

**Example 1.10.1.** Clock Arithmetic. \( m = 12 \). The set of integers congruent to 3 \( \mod 12 \) is

\[ \{3 + 12k : k \in \mathbb{Z}\} \]
Example 1.10.2. \(23 \equiv 18 \equiv 13 \equiv 8 \equiv 3 \equiv -2 \pmod{5}\). The values 18, 13, etc. are called residues of 23 \(\pmod{5}\), and the number 3 is called the least residue of 23 \(\pmod{5}\).

Definition 1.10.2. The least residue \(lr\) of \(a \pmod{m}\) is the smallest non-negative integer that \(a\) is congruent to \(\pmod{m}\). It is a value between 0 and \(m - 1\) (inclusive).

Lemma 1.10.1. Let \(a \in \mathbb{Z}\). The least residue of \(a \pmod{m}\) is the remainder in dividing \(a\) by \(m\).

Proof. Use division algorithm. \(\square\)

Example 1.10.3. What is the least residue of 800 \(\pmod{7}\)?

Theorem 1.10.1. **Congruence is an Equivalence Relationship**, that is, it satisfies the following three properties for any integers \(a, b, c\).

(i) Reflexive: \(a \equiv a \pmod{m}\)

(ii) Symmetric: If \(a \equiv b \pmod{m}\) then \(b \equiv a \pmod{m}\).

(iii) Transitive: If \(a \equiv b \pmod{m}\) and \(b \equiv c \pmod{m}\), then \(a \equiv c \pmod{m}\).

Thus, congruence \(\pmod{m}\) partitions \(\mathbb{Z}\) into equivalence classes of the form \([a]_m = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\}\), called congruence classes or residue classes. That is,

\[\mathbb{Z} = [0]_m \cup [1]_m \cup \cdots \cup [m-1]_m.\]

Theorem 1.10.2. **Substitution Properties of Congruences.** Let \(a, b, c, d\) be integers with \(a \equiv b \pmod{m}\) and \(c \equiv d \pmod{m}\). Then

(i) \(a + c \equiv b + d \pmod{m}\).

(ii) \(ac \equiv bd \pmod{m}\).

(iii) For any positive integer \(n\), \(a^n \equiv b^n \pmod{m}\).

Example 1.10.4. Find \(2004 \cdot 123 \cdot 77 \pmod{20}\). What is the remainder on dividing \(3^{298}\) by 7? Find \(799^4 \pmod{8}\).

Theorem 1.10.3. **Standard Algebraic properties of congruences.** For any integers \(a, b, c\) we have

(i) \(a + b \equiv b + a \pmod{m}\) (commutative law)

(ii) \(ab \equiv ba \pmod{m}\) (commutative law)

(iii) \(a + (b + c) \equiv (a + b) + c \pmod{m}\) (associative law)

(iv) \((ab)c \equiv a(bc) \pmod{m}\) (associative law)

(v) \(a(b + c) \equiv ab + ac \pmod{m}\) (distributive law)

Example 1.10.5. What day of the week will it be 10 years from today?

Note: \(a\) is divisible by \(d\) iff \(a \equiv 0 \pmod{d}\).

Example 1.10.6. Prove that a number is divisible by 9 iff the sum of its digits (base 10) is divisible by 9. Similarly for 11.

Example 1.10.7. Can 2013 be expressed as a sum of two squares? Suppose that \(a \equiv 3 \pmod{4}\). Can \(a\) be expressed as a sum of two squares of integers. Try 3, 7, 11, 15, etc.
1.11. Principle of Induction

Example 1.11.1. Example Notice the pattern for the sum of the first \(k\) odd numbers. Now prove by induction a formula.

Example 1.11.2. Fibonacci sequence 1,1,2,3,5,8,13,21,... Find a formula for 
\[f_1 + f_2 + f_3 + f_4 + \cdots + f_k\]

To prove formulas that hold for positive integers, induction is a very powerful technique. Recall,

**Axiom of Induction**: Suppose that \(S\) is a subset of the natural numbers such that (i) 1 \(\in\) \(S\) and (ii) If \(n \in S\) then \(n + 1 \in S\). Then \(S = \mathbb{N}\).

**Principle of Induction**: Let \(P(n)\) be a statement involving the natural number \(n\). Suppose that (i) \(P(1)\) is true and (ii) If \(P(n)\) is true for a given \(n\) then \(P(n+1)\) is true. Then \(P(n)\) is true for all natural numbers \(n\).

The connection of course is just to let \(S\) be the set of all natural numbers for which the statement \(P(n)\) is true.

Example 1.11.3. On first HW you conjecture: 
\[\sum_{k=1}^{n} k^3 = (1 + 2 + \cdots n)^2 = \left[\frac{n(n+1)}{2}\right]^2\]. Prove.

Note the two ways to conclude an induction proof. 1) “Therefore, by the principle of induction, the statement is true for all natural numbers.” 2) “QED” = Quod Erat Demonstrandum. Thus we have established what we wished to demonstrate.

One might object to this method by saying that we are assuming what we wish to prove. Is this a valid objection?

Example 1.11.4. Prove that \(16^n \equiv 1 - 10n \pmod{25}\) for any \(n \in \mathbb{N}\).

Example 1.11.5. Show that \(16^n | (6n)!\) for all \(n \in \mathbb{N}\).

Example 1.11.6. Prove that everyone has the same name. Let \(P(n)\) be the statement that in any set of \(n\) people, everyone has the same name. \(P(1)\) is trivially true.

**Strong Form of Induction.** Let \(P(n)\) be a statement involving \(n\). Suppose (i) \(P(1)\) is true and (ii) If \(P(1), P(2), \ldots P(n)\) are all true for a given \(n\), then so is \(P(n+1)\). Then \(P(n)\) is true for all natural numbers \(n\).

The induction assumption is stronger, and so this allows us to prove more.
CHAPTER 2

Primes and Unique Factorization

2.1. Fundamental Theorem of Arithmetic

There are three types of natural numbers:
1) 1, multiplicative identity or unity element.
2) primes. \( P = \{2, 3, 5, 7, \ldots \} \).
3) Composites.

Definition 2.1.1. A natural number \( n > 1 \) is called a prime if its only positive divisors are 1 and itself. Otherwise it is called a composite. Thus \( n \) is composite if \( n = ab \) for some natural numbers \( a, b \) with \( 1 < a < n, 1 < b < n \).

Note 2.1.1. 1 is not called a prime for a couple reasons. The main reason is that if 1 is a prime, then we would not have unique factorization, for example we could factor 6 as follows: \( 6 = 2 \cdot 3 = 2 \cdot 3 \cdot 1 = 2 \cdot 3 \cdot 1 \cdot 1, \ldots \). Each would be a different factorization of 6 into primes. A second reason is that 1 has a single positive divisor, whereas every prime has exactly 2 positive divisors.

Example 2.1.1. i) Everyone factor 120 using a factor tree. Compare. Note that everyone gets the same factorization.

   ii) Do the same thing, but only use even numbers. What do you discover? Note the set of even numbers \( E = \{2n : n \in \mathbb{Z}\} \) is closed under + and \( \cdot \), and enjoys all the usual axioms as \( \mathbb{Z} \) (with one exception).

Theorem 2.1.1. Fundamental Theorem of Arithmetic. Any natural number \( n > 1 \) can be expressed uniquely as a product of primes.

Note 2.1.2. It is understood that if \( n \) is a prime then it trivially is a product of primes.

Proof. Existence. Strong form of induction. For uniqueness we need following lemma.

Lemma 2.1.1. (i) If \( p \) is a prime and \( p|ab \), then \( p|a \) or \( p|b \).
(ii) More generally, if \( p|a_1 \cdots a_k \) then \( p|a_i \) for some \( i \).

Proof. Use Euclid to prove (i) and induction to prove (ii).

Proof. Uniqueness of FTA.

Example 2.1.2. Factor 60.

Note 2.1.3. Every positive integer \( n \) has a unique prime power factorization of the form \( n = p_1^{e_1} \cdots p_k^{e_k} \), with the \( p_i \) distinct primes and the \( e_i \) positive integers.

Definition 2.1.2. Let \( p \) be a prime \( n \in \mathbb{Z} \). We write \( p^e \| n \) if \( p^e | n \) but \( p^{e+1} \nmid n \). \( e \) is called the multiplicity of \( p \) dividing \( n \).
Example 2.1.3. \(2000 = 2^4\cdot5^3\), so \(2^4|2000\) and \(5^3|2000\).

Example 2.1.4. Find the multiplicity of 2 dividing \(2^1\cdot5^3 - 2^3\cdot5^7\). Answer = 3.

Theorem 2.1.2. Let \(n > 1\) have prime power factorization \(n = p_1^{e_1}\cdots p_k^{e_k}\), and let \(d \in \mathbb{N}\). Then \(d|n\) iff \(d = p_1^{f_1}\cdots p_k^{f_k}\) for some nonnegative integers \(f_i \leq e_i\), \(1 \leq i \leq k\).

Note 2.1.4. Useful trick: We can use the same set of prime factors for factoring any two integers provided that we allow zero in the exponent position. We will use this trick for proving the preceding theorem.

Proof. Suppose that \(d\) is a positive integer dividing \(n\), say \(dx = n\) for some integer \(x\). Say \(d = \prod_{i=1}^l p_i^{l_i}\), \(x = \prod_{i=1}^l p_i^{g_i}\), \(n = \prod_{i=1}^l p_i^{e_i}\), where for \(i > k\), \(e_i = 0\), and all exponents are nonnegative. Then \(dx = \prod_{i=1}^l p_i^{f_i+g_i}\). By uniqueness of factorization we deduce that \(e_i = f_i + g_i\), \(1 \leq i \leq l\). If \(i > k\) then \(f_i + g_i = e_i = 0\), and so \(f_i = g_i = 0\). If \(i \leq k\), then \(f_i = e_i - g_i \leq e_i\). □

2.1.1. The factoring method for finding GCDs and LCMs.

Theorem 2.1.3. Formula for GCD and LCM. Let \(a, b\) be positive integers with prime power factorizations, \(a = p_1^{e_1}\cdots p_k^{e_k}\), \(b = p_1^{f_1}\cdots p_k^{f_k}\) where the \(e_i, f_i\) are nonnegative integers. Then

\begin{align*}
\text{i)} & \quad (a, b) = p_1^{\min(e_1,f_1)}\cdots p_k^{\min(e_k,f_k)}.
\text{ii)} & \quad [a, b] = p_1^{\max(e_1,f_1)}\cdots p_k^{\max(e_k,f_k)}.
\end{align*}

Proof. Use FTA, the trick for representing \(a, b\) using the same primes, and the preceding theorem. □

Example 2.1.5. Let \(a = 2^5\cdot3^7\cdot15\), \(b = 2^2\cdot3^6\cdot5^4\). Find gcd and lcm.

Corollary 2.1.1. For any nonzero integers \(a, b\) we have \((a, b)[a, b] = |ab|\).

Proof. Just use preceding theorem and one simple idea, the proof of which we leave to the reader. For any integers \(e, f\)

\[\text{max}(e, f) + \text{min}(e, f) = e + f.\]

Note 2.1.5. An elementary proof of the corollary can be given based on just the definitions of gcd and lcm, but it is not as transparent as the preceding proof.

2.2. Gaussian Integers

Definition 2.2.1. The Gaussian integers is the set \(\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}\). Note that \(\mathbb{Z}[i]\) satisfies the ring axioms.

Definition 2.2.2. The absolute value or modulus of a complex number \(z = a + bi\) is given by \(|z| = \sqrt{a^2 + b^2}\).

Recall the properties \(|zw| = |z||w|\), \(|z/w| = |z|/|w|\).

Definition 2.2.3. Let \(z, w\) be Gaussian integers, \(z \neq 0\). We say that \(z\) divides \(w\), written \(z|w\) if \(zu = w\) for some \(u \in \mathbb{Z}[i]\).

Example 2.2.1. \((1 + 2i)|5\) because \((1 + 2i)(1 - 2i) = 5.\)
2.2. Gaussian Integers

Definition 2.2.4. A Gaussian integer \( z = a + bi \) is called a unit if it has a multiplicative inverse in \( \mathbb{Z}[i] \).

Note 2.2.1. i) The units in \( \mathbb{Z}[i] \) are \{±1, ±i\}. Why? Suppose \( z \) is a unit, say \( zw = 1 \). Then \( |z||w| = 1 \) so \( |z| = 1 \). The only Gaussian integers on the unit circle are the four listed here.

ii) Units are divisors of every Gaussian integer.

Definition 2.2.5. i) A nonzero Gaussian integer \( z \) is called composite if \( z = uv \) for some non-unit Gaussian integers \( u, v \).

ii) A nonzero Gaussian integer \( z \) is called a prime if \( z \) is not composite and not a unit.

Example 2.2.2. i) 2, 5 are composites, because 2 = (1 + i)(1 − i), 5 = (1 + 2i)(1 − 2i), and the factors 1 ± i, 1 ± 2i are not units. ii) 1 + i is a prime because if 1 + i = uv for some \( u, v \in \mathbb{Z}[i] \), then 2 = |1 + i|² = |u|²|v|² and so either |u| = 1 or |v| = 1, that is, \( u \) or \( v \) is a unit.

Definition 2.2.6. The gcd of two Gaussian integers \( z, w \) is the Gaussian integer \( u \) of largest modulus dividing both \( z \) and \( w \). It is unique up to unit multiples.

Our convention is to choose the representative in the first quadrant (including the positive real axis but not the imaginary axis.)

Theorem 2.2.1. Division Algorithm. Let \( z, w \in \mathbb{Z}[i], w \neq 0 \). Then there exist Gaussian integers \( q, r \) such that
\[
z = qw + r \quad \text{and} \quad 0 \leq |r| < |w|.
\]

Proof. We want \( z/w = q + r/w \) with \( |r/w| < 1 \). Define \( q \) to be the Gaussian integer closest to \( z/w \). Certainly \(|\frac{z}{w} - q| < 1\). \( \square \)

Example 2.2.3. a) Find the quotient and remainder for \( 12 + 5i \div 1 + 2i \).
\( q = 4 - 4i, r = i \).

b) Find gcd(12 + 5i, 1 + 2i) = (12 + 5i − q(1 + 2i), 1 + 2i) = (i, 1 + 2i) = 1, using convention up choosing rep in 1st quadrant.

What are the primes in \( \mathbb{Z}[i] \)? There are three types (we will prove this later):

(i) Odd integer primes \( p \) with \( p \equiv 3 \pmod{4} \): 3,7,11,19,...

(ii) The factors of integer primes \( p \) with \( p \equiv 1 \pmod{4} \): 5 = (1 + 2i)(1 − 2i), 13 = (2 + 3i)(2 − 3i), ...

(iii) 1 + i, 1 − i, the factors of 2.

Now that we have a division algorithm, we can proceed as we did with \( \mathbb{Z} \) to prove uniqueness of factorization:
Division algorithm ⇒ Euclidean algorithm ⇒ GCDLC ⇒ Euclid’s Lemma ⇒ Unique Factorization.

Theorem 2.2.2. Every Gaussian integer can be uniquely expressed as a product of primes, up to the order of the primes and unit multiples.

Example 2.2.4. i) Factor 5. We have 5 = (1 + 2i)(1 − 2i), 5 = (2 + i)(2 − i).
These are the same factorization, since \((1 + 2i)(−i) = 2 − i, (1 − 2i)i = 2 + i\).

ii) Factor 30. 30 = 2 · 3 · 5 = (1 + i)(1 − i)3(1 + 2i)(1 − 2i).
2.3. Distribution of primes

**Theorem 2.3.1.** There are infinitely many primes in \( \mathbb{N} \).

**Proof.** Euclid. Proof by contradiction. Suppose that there are finitely many primes, say \( p_1, \ldots, p_k \). Let \( N = p_1 \cdots p_k + 1 \). Then, by FTA, \( N \) has a prime factor, say \( p_i \). Then we have \( p_i | N \) and \( p_i | (p_1 \cdots p_k) \). Thus \( p_i | (N - p_1 \cdots p_k) \), that is, \( p_i | 1 \), a contradiction. Therefore, there must be infinitely many primes. \( \square \)

**Theorem 2.3.2.** There exist arbitrarily large gaps between consecutive primes.

**Proof.** Let \( n \in \mathbb{N} \). Consider the sequence of consecutive integers \( n! + 2, n! + 3, \ldots, n! + n \). For \( 2 \leq k \leq n \) we have \( k | n! \) and \( k | k \) and so \( k | (n! + k) \), and moreover it is a proper divisor. Thus \( n! + k \) is composite. Therefore we have a sequence of \( n - 1 \) consecutive composite numbers, and so if we let \( p \) be the largest prime less than \( n! + 2 \), the gap between \( p \) and the next prime must be at least \( n \). \( \square \)

**Note 2.3.1.** Some open problems: 1) Are there infinitely many twin primes. 2) Given any even number, is there a pair of consecutive primes with gap \( n \) between them? Are there infinitely many pairs with gap \( n \) between them? 3) Goldbach: Given any even number, can we express \( n \) as a sum of two primes.

### 2.3.1. Sieve of Eratosthenes

An elementary algorithm for finding the set of primes on an interval by sieving out multiples of small primes.

**Example 2.3.1.** Find all primes between 200 and 220.

**Theorem 2.3.3. Basic primality test.** If \( n \) is a positive integer having no prime divisor \( p \leq \sqrt{n} \), then \( n \) is a prime.

**Proof.** Proof by contradiction. Suppose that \( n \) is composite, say \( n = ab \) with \( 1 < a < n \), \( 1 < b < n \). We claim that either \( a \leq \sqrt{n} \) or \( b \leq \sqrt{n} \), else \( ab > \sqrt{n} \sqrt{n} = n = ab \), a contradiction. Say \( a \leq \sqrt{n} \). Let \( p \) be any prime divisor of \( a \). Then \( p \leq a \leq \sqrt{n} \), and, since \( p \nmid a \) and \( a | n \) we have \( p | n \). But this contradicts assumption that \( n \) has no prime divisor \( p \leq \sqrt{n} \). Therefore \( n \) is a prime. \( \square \)

### 2.3.2. Estimating \( \pi(x) \)

Pick a positive integer at random from 1 to \( x \). What is the probability that it is a prime? Let \( P_q \) be the probability that \( n \) is not divisible by \( q \): \( P_q = 1 - \frac{1}{q} \). Let \( p_1, \ldots, p_k \) be the primes up to \( x \). Thus prob that \( n \) is a prime roughly equals the prob that \( n \) is not divisible by 2, 3, \ldots, \( p_k \), which (assuming the events are independent) is given by

\[
P = \prod_{i=1}^{k} \left( 1 - \frac{1}{p_i} \right) = \prod_{p < x} \left( 1 - \frac{1}{p} \right).
\]

Now

\[
P^{-1} = \prod_{p < x} \left( 1 - \frac{1}{p} \right)^{-1} = \sum_{p < x} \frac{1}{p} \approx \sum_{n \leq x} \frac{1}{n} \approx \ln x,
\]

where \( \sum_{n} \) is a sum over all \( n \) such that all prime factors of \( n \) are \( \leq x \). Thus \( P \approx \frac{1}{\ln x} \), and \( \pi(x) \approx \frac{x}{\ln x} \).

**Theorem 2.3.4. Prime Number Theorem.** \( \lim_{x \to \infty} \frac{\pi(x)}{x/\ln(x)} = 1 \).

Conjectured by Gauss and proved by J. Hadamard and C. de la Vallee Poussin (1896).
CHAPTER 3

Arithmetic Functions

3.1. Multiplicative Functions

Definition 3.1.1. Let \( f : \mathbb{N} \to \mathbb{N} \) be a function defined on \( \mathbb{N} \). Such functions are called arithmetic.

1) We say that \( f \) is multiplicative if for any two natural numbers \( a, b \) with \( \gcd(a, b) = 1 \) we have \( f(ab) = f(a)f(b) \).

2) We say that \( f \) is totally multiplicative if for any two natural numbers \( a, b \), \( f(ab) = f(a)f(b) \).

Example 3.1.1. \( f(n) = n, f(n) = n^k, f(n) \equiv 1 \), are all multiplicative, in fact, they are totally multiplicative.

Note 3.1.1. If \( f \) is a multiplicative function that is not identically 0, then \( f(1) = 1 \).

Example 3.1.2. Suppose \( f \) is a multiplicative function such that \( f(p) = 2p \) for odd prime \( p \), \( f(p^j) = 3 \) for odd \( p \) and \( j > 1 \), \( f(2) = 4, f(4) = 5, f(8) = 6 \), \( f(2^k) = 0 \) for \( k > 3 \). Evaluate \( f(13), f(100), f(80) \).

Theorem 3.1.1. a) If \( f \) is a multiplicative function and \( n \) is a positive integer with prime factorization \( n = p_1^{c_1} \cdots p_k^{c_k} \) then

\[
f(n) = f(p_1^{c_1}) \cdots f(p_k^{c_k}).
\]

b) Conversely, if \( f \) is an arithmetic function satisfying (3.1), then \( f \) is multiplicative.

Proof. a) The proof is by induction on \( k \). The case \( k = 1 \) is trivial. Suppose statement is true for a given \( k \), and now consider \( k + 1 \). Let \( n = p_1^{c_1} \cdots p_k^{c_k + 1} \). Then

\[
f(n) = f((p_1^{c_1} \cdots p_k^{c_k})p_{k+1}^{c_{k+1}}) = f(p_1^{c_1} \cdots p_k^{c_k})f(p_{k+1}^{c_{k+1}}),
\]

since \( f \) is multiplicative. Then, by the induction assumption, we conclude that

\[
f(n) = f(p_1^{c_1}) \cdots f(p_k^{c_k})f(p_{k+1}^{c_{k+1}}),
\]

QED.

b) Let \( a, b \) be positive relatively prime integers, with factorizations \( a = p_1^{c_1} \cdots p_k^{c_k} \), \( b = q_1^{d_1} \cdots q_l^{d_l} \) where the \( p_i, q_j \) are all distinct primes. Then

\[
f(ab) = f(p_1^{c_1} \cdots p_k^{c_k}q_1^{d_1} \cdots q_l^{d_l}) = \prod_{i=1}^{k} f(p_i^{c_i}) \prod_{j=1}^{l} f(q_j^{d_j}) = f(a)f(b).
\]

Thus, multiplicative functions are determined by their values at prime powers.
Theorem 3.1.2. If \(f\) and \(g\) are multiplicative functions then so are \(fg\), \(f/g\) and \(f^n\) for any \(n \in \mathbb{N}\).

Proof. Immediate from definition. For example, to show \(fg\) is multiplicative, let \(a\), \(b\) be positive integers with \((a, b) = 1\) then \(fg(ab) = f(ab)g(ab) = f(a)f(b)g(a)g(b) = f(a)g(a)\)\(f(b)g(b) = fg(a)fg(b)\). \(\square\)

Definition 3.1.2. For any positive integer \(n\) we let \(\tau(n)\) (or \(d(n)\)) denote the number of positive divisors of \(n\), and \(\sigma(n)\) denote the sum of the positive divisors of \(n\).

Example 3.1.3. \(\tau(1) = 1\). \(\tau(2) = 2\). For prime \(p\), \(\tau(p) = 2\), \(\tau(p^k) = k + 1\). For distinct primes \(p, q\), \(\tau(pq) = 4\). \(\sigma(1) = 1\), \(\sigma(2) = 3\), \(\sigma(p) = p + 1\), \(\sigma(p^k) = 1 + p + \cdots + p^k\).

We claim that \(\tau(n)\) and \(\sigma(n)\) are multiplicative. To prove this we need.

Theorem 3.1.3. Correspondence Theorem for divisors. Let \(a, b\) be relatively prime positive integers. Then every divisor of \(ab\) can be uniquely expressed in the form \(de\), where \(d|a\) and \(e|b\). Moreover, any number of the form \(de\) where \(d|a\) and \(e|b\) is a divisor of \(ab\).

Proof. Let \(a = p_1^{e_1} \cdots p_k^{e_k}\), \(b = q_1^{f_1} \cdots q_l^{f_l}\) with the \(p, q\) all distinct primes. Then \(ab = p_1^{e_1} \cdots p_k^{e_k} q_1^{f_1} \cdots q_l^{f_l}\). By an earlier theorem, any divisor \(s\) of \(ab\) is of the form \(s = p_1^{g_1} \cdots p_k^{g_k} q_1^{h_1} \cdots q_l^{h_l}\) for some integers \(g, h\) with \(0 \leq g_i \leq e_i\) and \(0 \leq h_i \leq f_i\). Let \(d = p_1^{g_1} \cdots p_k^{g_k}\), \(e = q_1^{h_1} \cdots q_l^{h_l}\). Then \(s = de\), \(d|a\) and \(e|b\). Conversely, if we start with \(d\) and \(e\) as defined above, plainly \(de\) is a divisor of \(ab\). The expression is unique by FTA. \(\square\)

Equivalent Statement: Let \(D_a, D_b, D_{ab}\) denote the sets of positive divisors of \(a, b, ab\) respectively and let \(D_a \times D_b\) denote the set of all ordered pairs. Then there is a 1-to-1 correspondence between \(D_{ab}\) and \(D_a \times D_b\) given by the mapping \(D_a \times D_b \to D_{ab}\) given by \((d, e) \to de\).

Proof. (i) Note the mapping goes into \(D_{ab}\). (ii) The mapping is one-to-one: \(d_1 e_1 = d_2 e_2 \to d_1 | d_2 e_2 \to d_1 | d_2\) since \((d_1, e_2) = 1\). Similarly \(d_2 | d_1\) and so \(d_1 = d_2\), \(e_1 = e_2\). (iii) The mapping is onto. Let \(f|ab\). Put \(d = (f, a)\), \(e = (f, b)\). Then \(f = (f, ab) = (f, a)(f, b) = de\).

One can also use prime power decomposition to prove the result: A typical divisor of \(a\) is of the form, \(d = \prod p_i^{g_i}, g_i \leq e_i\). A typical divisor of \(b\) is of form \(e = \prod q_i^{h_i}, h_i \leq f_i\). Then \(de = \prod p_i^{g_i} \prod q_i^{h_i}\), which is a typical divisor of \(ab\). \(\square\)

Example 3.1.4. Make an array to illustrate the correspondence for \(a = 28, b = 15\).

Theorem 3.1.4. \(\tau(n)\) and \(\sigma(n)\) are multiplicative functions.

Proof. Suppose \((a, b) = 1\). let \(D_a = \{d_1, \ldots, d_k\}, D_b = \{e_1, \ldots, e_l\}\). Then, by correspondence theorem \(D_{ab} = \{d_i e_j : 1 \leq i \leq k, 1 \leq j \leq l\}\). In particular \(\tau(ab) = |D_{ab}| = kl = \tau(a)\tau(b)\). Also

\[
\sigma(ab) = \sum_{i=1}^{k} \sum_{j=1}^{l} d_i e_j = (d_1 + d_2 + \cdots + d_k)(e_1 + e_2 + \cdots + e_l) = \sigma(a)\sigma(b),
\]

by the distributive law. \(\square\)
Now for prime powers we easily see:
\[
\tau(p^e) = e + 1,
\]
\[
\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \frac{p^{e+1} - 1}{p - 1}.
\]
Thus, since \(\tau(n)\) and \(\sigma(n)\) are multiplicative, we obtain

**Theorem 3.1.5. Formulas for \(\tau(n)\) and \(\sigma(n)\).** Let \(n = p_1^{e_1} \cdots p_k^{e_k}\). Then

i) \(\tau(n) = \prod_{i=1}^{k} (e_i + 1)\).

ii) \(\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{e_i+1} - 1}{p_i - 1}\).

### 3.2. Perfect, Deficient and Abundant Numbers

**Definition 3.2.1.** We say that a positive integer \(n\) is

i) Deficient if \(\sigma(n) < 2n\),

ii) Abundant if \(\sigma(n) > 2n\), and

iii) Perfect, if \(\sigma(n) = 2n\).

Another way to think about it. A number is perfect if it equals the sum of its proper divisors.

**Example 3.2.1.** i) 6, 28 are perfect.

ii) Any prime power is deficient. Any product of two odd prime powers is deficient.

iii) Any multiple of a perfect number (greater than the perfect number) is abundant.

**Example 3.2.2.** The following numbers were known to be perfect to the ancients. Let’s look at their factorizations to see if a pattern can be discerned.

\[
\begin{align*}
6 &= 2 \cdot 3, \\
28 &= 4 \cdot 7 = 2^2 \cdot 7, \\
496 &= 16 \cdot 31 = 2^4 \cdot 31, \\
8128 &= 64 \cdot 127 = 2^6 \cdot 127 
\end{align*}
\]

What about \(8 \cdot 15\)? This is abundant.

**Conjecture:** \(n\) is perfect if \(n = 2^k(2^{k+1} - 1)\) and \(2^{k+1} - 1\) is a prime.

**Proof.** We have \(\sigma(n) = \sigma(2^k(2^{k+1} - 1)) = \sigma(2^k)\sigma(2^{k+1} - 1)\). Now \(\sigma(2^k) = 2^{k+1} - 1\) and since \(2^{k+1} - 1\) is a prime, \(\sigma(2^{k+1} - 1) = 2^{k+1}\). Thus \(\sigma(n) = (2^{k+1} - 1)2^{k+1} = 2n\).

**Questions:** Are these the only perfect numbers? Are there any odd perfect numbers? When is \(2^{k+1} - 1\) a prime?

These are all open questions. It is known that if \(n\) is an odd perfect number, then \(n > 10^{300}\), \(n\) must have a prime divisor > 100000 and it must have at least 11 distinct prime factors. However, for even perfect numbers we have

**Theorem 3.2.1. Euler’s characterization of even perfect numbers.** An even number is perfect if and only if it is of the form \(2^k(2^{k+1} - 1)\) with \(2^{k+1} - 1\) a prime.
Proof. Already shown one way. Suppose now that \( n = 2^k a \) with \( a \) odd. Then \( \sigma(n) = 2n \) iff \((2^{k+1} - 1)\sigma(a) = 2^{k+1}a\). Let \( \sigma(a) = a + b \). The above holds iff \( a = b(2^{k+1} - 1) \). In particular \( b|a \) and \( b < a \). If \( b \neq 1 \) then \( a, b, 1 \) are distinct divisors of \( a \) and so \( \sigma(a) \geq a + b + 1 \) a contradiction. Thus \( b = 1 \) and \( a = 2^{k+1} - 1 \) and \( \sigma(a) = a + 1 \). It follows that \( a \) must be an odd prime of the desired form. \( \square \)

### 3.2.1. Mersenne Primes.

**Definition 3.2.2.** Any prime of the form \( M_k = 2^k - 1 \) is called a Mersenne prime. (In general, numbers of the form \( M_k \) are called Mersenne numbers.)

**Theorem 3.2.2.** (i) If \( d|k \) then \( 2^d - 1|2^k - 1 \).

(ii) Thus if \( 2^k - 1 \) is a prime then \( k \) must be a prime.

**Proof.** (i) Immediate from the factoring formula \( X^n - 1 = (X - 1)(X^{n-1} + \cdots + 1) \). Say \( k = dn \) for some \( n \in \mathbb{N} \), and put \( X = 2^d \). (ii) Immediate from part (i). \( \square \)

**Example 3.2.3.** \( k = 2, 3, 5, 7 \) yield Mersenne primes 3, 7, 31, 127. However, \( k = 11 \), gives \( 2047 = 2^2 \cdot 23 \cdot 31 \), a composite. Thus we do not always get a Mersenne prime when \( k \) is prime.

**Example 3.2.4.** Factors of Mersenne numbers with composite \( k \). If \( k = 2^m \cdot n \), then \( 2^{2^m} - 1 \) is a factor and we see \( M_9 = 511 = 7 \cdot 73 \). If \( k = 10 \), then \( 2^2 - 1 = 3 \) and \( 2^5 - 1 = 31 \) are factors and we see \( M_{10} = 1023 = 3 \cdot 11 \cdot 31 \).

### 3.2.2. GIMPS, Great Internet Mersenne Prime Search.

It was popular for many years to test the speed of new computers by seeing if they can find the largest known prime number using standard algorithms. All of the largest known primes are Mersenne primes. In 1876 Lucas had the record \( k = 127 \). He discovered a clever algorithm in order to deal with numbers of this size by hand. In 1985 a Cray X-MP obtained \( k = 216,091 \) a 65000 digit number, in 3 hours. In 2008 the 45th Mersenne prime was discovered at UCLA, \( 2^{43,112,609} - 1 \) a number with 12,978,189 digits, earning the finders $100000. Check GIMPS on the internet if you wish to participate in this search. You will also find there a list of all known Mersenne primes and when they were discovered.

Open Problem: Are there infinitely many Mersenne primes?

**3.2.3. Fermat primes.**

**Definition 3.2.3.** Any prime of the form \( F_k = 2^k + 1 \) is called a Fermat prime. (In general, numbers of the form \( F_k \) are called Fermat numbers.)

Make table with \( 2^k + 1 \), \( k = 1 \) to 8. Discover that it is prime iff \( k \) is a power of 2. Fermat conjectured that every number of the form \( 2^{2^k} + 1 \) is a prime. This is true for \( k = 0, 1, 2, 3, 4 \), \( (3,5,17,257,65537) \), but false for \( 2^{2^5} + 1 \). Euler was able to factor the latter. Here’s one way.

\[
2^{32} + 1 = (2^9 + 2^7 + 1)(2^{23} - 2^{21} + 2^{19} - 2^{17} + 2^{14} - 2^9 - 2^7 + 1)
\]

\( 4,294,967,297 = 641 \cdot 6700417 \).

How might one discover that 641 is a divisor of \( 2^{32} + 1 \) without a lot of trial and error? Using properties of congruences (Fermat’s Little Theorem, orders of
3.3. Properties of multiplicative functions.

Recall definition of multiplicative function.

Let \( f(n) \) be a given multiplicative function. Define

\[
F(n) := \sum_{d|n} f(d),
\]

the sum being over all positive divisors of \( n \). We claim that \( F \) is multiplicative.

**Example 3.3.1.** Let \( f \equiv 1 \). Then \( F(n) = \tau(n) \). Let \( f(n) = \tau(n) \) then

\[
F(n) = \sigma(n).
\]

Let \( f(n) = n^2 \) then \( F(n) = \sigma_2(n) \) the sum of the squares of the divisors of \( n \). etc.

**Theorem 3.3.1.** Suppose that \( f \) is a multiplicative function. Then so is the function \( F \) defined by \( F(n) = \sum_{d|n} f(d) \).

**Proof.** Same as for \( \sigma \). Suppose that \( (a, b) = 1 \). By the correspondence theorem, any divisor \( d \) of \( ab \) can be expressed uniquely in the manner \( d = ce \), where \( c|a \) and \( e|b \). Thus we have

\[
F(ab) = \sum_{d|ab} f(d) = \sum_{c|a} \sum_{e|b} f(ce)
\]

\[
= \sum_{c|a} \sum_{e|b} f(c)f(e) = \sum_{c|a} f(c) \sum_{e|b} f(e) = F(a)F(b).
\]

**Example 3.3.2.** Let \( F(n) = \sum_{d|n} \tau(d) \). Find a formula for \( F(n) \) and evaluate \( F(8000) \). First we evaluate \( F(p^e) \) for any prime power \( p^e \).

\[
F(p^e) = \tau(1) + \tau(p) + \tau(p^2) + \cdots + \tau(p^e) = 1 + 2 + 3 + \cdots + e + 1 = \frac{(e+1)(e+2)}{2}.
\]
Next we observe that since \( \tau \) is multiplicative, so is \( F \) by preceding theorem. Thus, if \( n = p_1^{e_1} \cdots p_k^{e_k} \), then
\[
F(n) = \prod_{i=1}^{k} F(p_i^{e_i}) = \prod_{i=1}^{k} \frac{(e_i + 1)(e_i + 2)}{2}.
\]

If \( n = 8000 = 2^3 \cdot 1000 = 2^6 \cdot 5^3 \), then \( F(n) = \frac{(6+1)(6+2)}{2} \frac{(3+1)(3+2)}{2} = 28 \cdot 10 = 280 \).

**Example 3.3.3.** Let \( \sigma^{-1}(n) = \sum_{d|n} \frac{1}{d} \). Show that \( \sigma^{-1}(n) = \frac{\sigma(n)}{n} \).

### 3.3.1. The Euler Phi Function.

**Definition 3.3.1.** For any positive integer \( n \) we define \( \phi(n) \) to be the number of positive integers less than or equal to \( n \) that are relatively prime to \( n \).

**Example 3.3.4.** Find \( \phi(10) \).

**Example 3.3.5.** \( \phi(p) = p - 1 \), for prime \( p \). \( \phi(p^k) = p^k - p^{k-1} \) for prime power \( p^k \).

Suppose \( n \) is a positive integer with factorization \( p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \). How do we find \( \phi(n) \)? For any divisor \( d \) of \( n \), let
\[
S_d = \{ k : 1 \leq k \leq n, d|k \}.
\]

Note \( |S_d| = n/d \). By the inclusion-exclusion principle, to find the number of values for 1 to \( n \) relatively prime to \( n \), we need to count how many points are not in \( S_{p_1} \), \( S_{p_2} \), ..., or \( S_{p_k} \).

\[
\phi(n) = n - |S_{p_1}| - |S_{p_2}| - \cdots - |S_{p_k}| + |S_{p_1p_2}| + |S_{p_1p_3}| + \cdots + (-1)^k |S_{p_1 \cdots p_k}|
\]

\[
= n \left( 1 - \frac{1}{p_1} - \cdots - \frac{1}{p_k} + \cdots + (-1)^k \frac{1}{p_1 \cdots p_k} \right)
\]

\[
= n \prod_{i=1}^{k} \left( 1 - \frac{1}{p_i} \right).
\]

Thus we have established the following theorem.

**Theorem 3.3.2.** Let \( n \) have prime power factorization \( n = p_1^{e_1} \cdots p_k^{e_k} \). Then
\[
\phi(n) = \prod_{i=1}^{k} \phi(p_i^{e_i}) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1).
\]

**Corollary 3.3.1.** The Euler phi-function is multiplicative.

**Proof.** Follows from Theorem 3.1 (b). \( \square \)

We will see two more ways of showing that the Euler phi-function is multiplicative, one making use of the identity \( \sum_{d|n} \phi(d) = n \), and the other involving the Chinese Remainder Theorem.

Here is another interesting property of the Euler phi-function.

**Theorem 3.3.3.** For any natural number \( n \) we have \( \sum_{d|n} \phi(d) = n \).

**Proof.** Let \( F(n) = \sum_{d|n} \phi(d) \). First note that since \( \phi \) is multiplicative, so is \( F \). Next, for any prime power \( p^e \) we have
\[
F(p^e) = \phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^e) = 1 + (p-1) + (p^2 - p) + \cdots + (p^e - p^{e-1}) = p^e,
\]

where we have used the fact that \( \phi(p^e) = p^e - p^{e-1} \). Therefore,
\[
F(n) = \sum_{d|n} F(d) = \sum_{d|n} \sum_{p^e|d} \phi(p^e) = \sum_{p^e|n} \phi(p^e) \sum_{p^e|d} = \sum_{p^e|n} p^e = n.
\]

\( \square \)
since the last sum is telescoping. Thus if \( n \) is any integer, with prime factorization \( n = p_1^{c_1} \cdots p_k^{c_k} \), then we have
\[
F(n) = F(p_1^{c_1}) \cdots F(p_k^{c_k}) = p_1^{c_1} \cdots p_k^{c_k} = n.
\]

A direct proof of this theorem, that does not appeal to the multiplicative property of \( \phi \) can be given as follows. A complex number \( w \) is called a primitive \( n \)-th root of unity if \( w^n = 1 \) but \( w^d \neq 1 \) for all \( d < n \). There are \( \phi(n) \) primitive \( n \)-th roots of unity. Now every \( n \)-th root of unity is a primitive \( d \)-th root of unity for some (unique) \( d \mid n \). Thus since there are \( n \), \( n \)-th roots of unity, and \( \phi(d) \) primitive \( d \)-th roots of unity for each \( d \mid n \), we see that \( n = \sum_{d \mid n} \phi(d) \).

3.4. The Möbius Function

**Definition 3.4.1.** The Möbius function \( \mu \) is defined by
\[
\mu(n) = \begin{cases} 
1 & \text{if } n = 1; \\
(-1)^k & \text{if } n = p_1 p_2 \cdots p_k, \text{ a product of distinct primes;} \\
0 & \text{if } p^2 \mid n \text{ for some prime } p.
\end{cases}
\]

Make table illustrating random behavior of \( \mu(n) \). Is it statistically random in some sense? If so then \( \sum_{n \leq x} \mu(n) \ll \sqrt{x} \), but this is an open problem.

**Theorem 3.4.1.** \( \mu(n) \) is a multiplicative function.

**Proof.** Let \( a, b \) be positive integers with \( (a, b) = 1 \). If \( a \) or \( b \) equals 1, say wlog \( a = 1 \) then \( \mu(ab) = \mu(b) \) while \( \mu(a) \mu(b) = \mu(1) \mu(b) = 1 \cdot \mu(b) = \mu(b) \) and so \( \mu(ab) = \mu(a) \mu(b) \). Next, suppose that either \( a \) or \( b \) is divisible by \( p^2 \) for some prime \( p \), say wlog \( a \). Then so is \( ab \), and so \( \mu(ab) = 0 \), while \( \mu(a) \mu(b) = 0 \cdot \mu(b) = 0 \), so again \( \mu(ab) = \mu(a) \mu(b) \). Finally, suppose that \( a, b \) are products of distinct primes, say \( a = p_1 \cdots p_k, b = q_1 \cdots q_l \). The \( p_i, q_j \) must all be distinct since \( (a, b) = 1 \). Thus \( ab \) is a product of \( k + l \) distinct primes, and we have \( \mu(ab) = (-1)^{k+l} = (-1)^k(-1)^l = \mu(a) \mu(b) \).

**Theorem 3.4.2.** For any natural number \( n \)
\[
\sum_{d \mid n} \mu(d) = \begin{cases} 
1 & \text{if } n = 1; \\
0 & \text{if } n > 1.
\end{cases}
\]

**Proof.** Let \( F(n) = \sum_{d \mid n} \mu(d) \). For any prime power \( p^r \) we have
\[
F(p^r) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^r) = 1 - 1 + 0 + \cdots + 0 = 0,
\]
Thus if \( n > 1 \) with prime factorization \( n = p_1^{c_1} \cdots p_k^{c_k} \) \( (k \geq 1) \), then \( F(n) = F(p_1^{c_1}) \cdots F(p_k^{c_k}) = 0 \cdots 0 = 0 \). Trivially, \( F(1) = 1 \).

**Example 3.4.1.** Calculate sum for \( n = 10 \).

**Definition 3.4.2.** The indicator function (or characteristic function) for a singleton point set \( \{n\} \) is defined by
\[
\delta_n(x) = \begin{cases} 
1 & \text{if } x = n, \\
0 & \text{if } x \neq n.
\end{cases}
\]
Thus the previous theorem can be restated: \( \sum_{d \mid n} \mu(d) = \delta_1(n) \).

**Corollary 3.4.1.** Let \( n \in \mathbb{N} \). For any divisor \( d \) of \( n \) we have, \( \delta_n(d) = \sum_{e \mid \frac{n}{d}} \mu(e) \).

**Proof.** Since \( d \mid n \) we have \( \delta_n(d) = \delta_1(n/d) = \sum_{e \mid \frac{n}{d}} \mu(e) \). \( \square \)

Suppose that \( f \) is an arithmetic function and we define \( F \) by \( F(n) = \sum_{d \mid n} f(d) \).

How can we invert this equation, and solve for \( f(n) \) in terms of \( F(n) \)? Letting \( \delta \) be the indicator function for the point set \( \{ n \} \), we have

\[
f(n) = \sum_{d \mid n} f(d) \delta_n(d) = \sum_{d \mid n} f(d) \left( \sum_{e \mid \frac{n}{d}} \mu(e) \right)
= \sum_{e \mid n} \mu(e) \left( \sum_{d \mid \frac{n}{e}} f(d) \right) = \sum_{e \mid n} \mu(e)F\left(\frac{n}{e}\right).
\]

**Theorem 3.4.3.** Möbius inversion formula. Let \( f \) be any arithmetic function and \( F(n) = \sum_{d \mid n} f(d) \). Then for any \( n \in \mathbb{N} \) we have

\[
f(n) = \sum_{d \mid n} F(d) \mu(n/d) = \sum_{d \mid n} F\left(\frac{n}{d}\right) \mu(d).
\]

Think of it as a sum over the divisor pairs \( d, \frac{n}{d} \) of \( n \).

**Proof.** A proof was given above that actually derives the formula. Lets give a second proof (that assumes such a formula has already been conjectured). By the definition of \( F \), we have

\[
\sum_{d\mid n} F\left(\frac{n}{d}\right) \mu(d) = \sum_{d\mid n} \mu(d) \left( \sum_{e\mid \frac{n}{d}} f(e) \right)
= \sum_{e\mid n} f(e) \sum_{d\mid \frac{n}{e}} \mu(d)
= \sum_{e\mid n} f(e) \delta_1(n/e) = f(n).
\]

**Example 3.4.2.** \( \sigma(n) = \sum_{d\mid n} d \) and so \( n = \sum_{d\mid n} \sigma(d) \mu(n/d) \).

**Theorem 3.4.4.** Let \( f, g \) be multiplicative functions and define \( F(n) = \sum_{d\mid n} f(d)g(n/d) \). Then \( F \) is multiplicative.
Proof. Follows from correspondence theorem. Let \((a, b) = 1\). Then

\[
F(ab) = \sum_{l \mid ab} f(l)g\left(\frac{ab}{l}\right) \\
= \sum_{d \mid a} \sum_{e \mid b} f(de)g\left(\frac{a}{d}\right)g\left(\frac{b}{e}\right) \\
= \sum_{d \mid a} \sum_{e \mid b} f(d)f(e)g\left(\frac{a}{d}\right)g\left(\frac{b}{e}\right) \\
= \sum_{d \mid a} f(d)g\left(\frac{a}{d}\right) \sum_{e \mid b} f(e)g\left(\frac{b}{e}\right) = F(a)F(b).
\]

\[\square\]

Corollary 3.4.2. Let \(f\) be any arithmetic function and \(F\) be defined by \(F(n) = \sum_{d \mid n} f(d)\). Then \(F\) is multiplicative if and only if \(f\) is multiplicative.

Proof. One direction is just Theorem 3.3.1. For the converse, suppose that \(F\) is multiplicative. Then by the Möbius inversion formula we have \(f(n) = \sum_{d \mid n} \mu(d)F(n/d)\), which is multiplicative by the preceding theorem. \[\square\]

Example 3.4.3. Suppose we start with the formula \(n = \sum_{d \mid n} \phi(d)\), in Theorem 3.3.3. By the preceding corollary we deduce that \(\phi\) is multiplicative. In fact, by the Möbius inversion formula we obtain

\[
\phi(n) = \sum_{d \mid n} \mu(d) \frac{n}{d} = n \sum_{d \mid n} \frac{\mu(d)}{d}.
\]
CHAPTER 4

More on Congruences

DEFINITION 4.0.3. A complete residue system \((\mod m)\) is a set of \(m\) distinct integers \((\mod m)\), \(\{x_1, \ldots, x_m\}\). Thus, every integer is congruent to exactly one of the \(x_i\) \((\mod m)\).

EXAMPLE 4.0.4. For \(m = 5\), the following are all examples of complete residue systems \((\mod 5)\): \(\{0, 1, 2, 3, 4\}\), \(\{5, 6, 7, 8, 9\}\), \(\{5, 1, 22, -27, 94\}\).

4.1. Counting Solutions of Congruences

Let \(f(x)\) be a polynomial with integer coefficients and \(m\) be a positive integer. We wish to solve the congruence

(4.1) \[ f(x) \equiv 0 \pmod{m}. \]

EXAMPLE 4.1.1. Solve \(x^2 \equiv 1 \pmod{8}\). By testing values from 0 to 7, we see that the solution set is all \(x\) with \(x \equiv 1, 3, 5, 7 \pmod{8}\). Thus \(\{1, 3, 5, 7\}\) is called a complete set of solutions of the congruence \(x^2 \equiv 1 \pmod{8}\). Thus this congruence has 4 distinct solutions \((\mod 8)\).

DEFINITION 4.1.1. (i) A set of integers \(\{x_1, \ldots, x_k\}\) is called a complete set of solutions of the congruence (4.1) if the values \(x_1, \ldots, x_k\) are distinct residues \((\mod m)\), and every solution of (4.1) is congruent to one of these values \((\mod m)\).

(ii) A complete set of solutions is called the “least” complete set of solutions if the \(x_i\) are least residues (that is, \(0 \leq x_i \leq m-1\)).

(iii) If \(\{x_1, \ldots, x_k\}\) is a complete set of solutions of (4.1), then we say (4.1) has \(k\) distinct solutions \((\mod m)\).

4.2. Linear Congruences

Consider the linear congruence

(4.2) \[ ax \equiv b \pmod{m}, \]

where \(a, b \in \mathbb{Z}\). Note, this is equivalent to solving the linear equation \(ax = b + my\), that is \(ax - my = b\), and we did this earlier. Putting \(d = (a, m)\), we saw that this was solvable iff \(d|b\), in which case the general solution was given by \(x = x_0 + \frac{m}{d}t\), \(y = y_0 - \frac{a}{d}t\), with \(t\) any integer and \((x_0, y_0)\) any particular solution.

THEOREM 4.2.1. Let \(d = (a, m)\). The linear congruence (4.2) has a solution if and only if \(d|b\), in which case a complete set of solutions is given by

\[ x = x_0 + t\frac{m}{d}, \quad 0 \leq t \leq d - 1, \]

where \(x_0\) is any particular solution of (4.2). Thus, if a solution exists, then there are \(d\) distinct solutions \((\mod m)\).
Note that we stop at \( t = d - 1 \) in order to avoid repetition of solutions.

**Example 4.2.1.** Solve \( 7x \equiv 2 \pmod{11} \). \( d = (7, 11) = 1 \) and \( 1|2 \) so a unique solution exists. To solve, we solve linear equation \( 7x - 11y = 2 \) using array method. \( x \equiv 5 \pmod{11} \).

A useful trick for solving linear congruence: If you notice that \( a, b, m \) all have a common factor \( d \), then it can be divided out. That is,

\[
ax \equiv b \pmod{m}, \quad \text{iff} \quad \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}.
\]

**Example 4.2.2.** Solve \( 3x \equiv 6 \pmod{18} \), implies \( x \equiv 2 \pmod{6} \). Thus \( x \equiv 2, 8, 14 \pmod{18} \).

### 4.3. Multiplicative inverses \( \pmod{m} \)

**Definition 4.3.1.** Let \( a \in \mathbb{Z} \). An integer \( x \) is called a multiplicative inverse of \( a \pmod{m} \) if \( ax \equiv 1 \pmod{m} \). In this case we write \( x \equiv a^{-1} \pmod{m} \).

**Example 4.3.1.** Find a mult inverse of 3 \( \pmod{10} \). Find mult inverse of 2 \( \pmod{10} \). Can’t do the latter because \( (2, 10) > 1 \)

**Theorem 4.3.1.** An integer \( a \) has a multiplicative inverse \( \pmod{m} \) if and only if \( (a, m) = 1 \). In this case, the mult inverse is unique.

**Example 4.3.2.** Use the mult inverse of 3 \( \pmod{10} \) to solve the congruence \( 3x \equiv 7 \pmod{10} \).

**Note 4.3.1.** By definition, there are \( \phi(n) \) integers between 1 and \( n \) that are relatively prime to \( n \). These are the values that have multiplicative inverses.

**Definition 4.3.2.** A reduced residue system \( \pmod{m} \) is a set of integers \( \{a_1, \ldots, a_{\phi(m)}\} \) that are distinct \( \pmod{m} \), and relatively prime to \( m \).

Note: The values in a reduced residue system \( \pmod{m} \) are all invertible \( \pmod{m} \).

**Example 4.3.3.** \( m = 10 \). \( \{1, 3, 7, 9\} \) is a reduced residue system \( \pmod{10} \). So is \( \{11, 33, 17, 9\} \).

**Theorem 4.3.2.** **Cancellation Law.** If \( (a, m) = 1 \) and \( ax \equiv ay \pmod{m} \), then \( x \equiv y \pmod{m} \).

**Proof.** Since \( (a, m) = 1 \), \( a \) has a mult inverse \( \pmod{m} \) and so we can multiply both sides of the congruence \( ax \equiv ay \pmod{m} \) by \( a^{-1} \pmod{m} \), to get \( x \equiv y \pmod{m} \).

**Theorem 4.3.3.** **Wilson’s Theorem** For any prime \( p \), \( (p-1)! \equiv -1 \pmod{p} \).

**Proof.** The statement is trivial for \( p = 2 \), so assume that \( p \) is odd. Note that the only solutions of the congruence \( x^2 \equiv 1 \pmod{p} \) are \( x \equiv \pm 1 \pmod{p} \). Thus if \( x \not\equiv \pm 1 \pmod{p} \) then \( x^{-1} \not\equiv x \pmod{p} \), and so we can form pairs \( (x, x^{-1}) \), and obtain

\[
\{1, 2, \ldots, p-1\} \equiv \{1, -1, x_1, x_1^{-1}, x_2, x_2^{-1}, \ldots, x_k, x_k^{-1}\} \pmod{p}.
\]

Thus taking the product of all of the elements in each set we see,

\[
(p-1)! \equiv 1(-1)x_1x_1^{-1}\cdots x_kx_k^{-1} \equiv -1 \pmod{p}.
\]
4.4. Chinese Remainder Theorem

Example 4.4.1. Find a whole number \( n \) such that the remainder is 3 when \( n \) is divided by 7, 5 when divided by 11. This is equivalent to the system \( x \equiv 3 \pmod{7} \), \( x \equiv 5 \pmod{11} \). Set \( x = 3 + 7t \), \( 3 + 7t \equiv 5 \pmod{11} \), \( t \equiv 5 \pmod{11} \). Thus \( x \equiv 38 \pmod{77} \).

Theorem 4.4.1. Chinese Remainder Theorem. Let \( a, b \) be positive integers with \( (a, b) = 1 \). Let \( h, k \) be any integers. Then the system
\[
\begin{align*}
x &\equiv h \pmod{a} \\
x &\equiv k \pmod{b} 
\end{align*}
\]
has a unique solution \( \pmod{ab} \).

Proof. Set \( x = h + at \), substitute to get \( at \equiv k - h \pmod{b} \). By previous theorem this system has solution \( t = t_0 + bs \), \( s \in \mathbb{Z} \). Substituting gives \( x \equiv h + at_0 \pmod{ab} \) is the unique solution. \( \square \)

Example 4.4.2. Historical example used by the ancient Chinese. Suppose we wish to determine the exact number of people in a large crowd of about 500 people. Have the crowd break into groups of 7, 8 and 9 people, with 2, 4, 6 people left over in the three cases. Thus we must solve \( x \equiv 2 \pmod{7} \), \( x \equiv 4 \pmod{8} \), \( x \equiv 6 \pmod{9} \). To solve, start with the biggest modulus, that is set \( x = 6 + 9t \), \( t \in \mathbb{Z} \). Substitute to get \( t \equiv 6 \pmod{8} \) and consequently \( x \equiv 60 \pmod{7} \). Say \( x = 60 + 72s \). Substitute again to get \( s \equiv 6 \pmod{7} \) and \( x \equiv 492 \pmod{5} \). Thus there are 492 people.

Definition 4.4.1. We say a set of integers \( \{a_1, a_2, \ldots, a_k\} \) are pairwise relatively prime if \( (a_i, a_j) = 1 \) for all \( i, j \) with \( 1 \leq i < j \leq k \).

Example 4.4.3. The integers 6, 11, 15 are not pairwise relatively prime, even though \( \gcd(6, 11, 15) = 1 \).

Theorem 4.4.2. CRT with more than 2 congruences Let \( m_1, \ldots, m_n \) be pairwise relatively prime positive integers, and \( h_1, \ldots, h_n \) be any integers. Then the system
\[
\begin{align*}
x &\equiv h_i \pmod{m_i}, & 1 \leq i \leq n,
\end{align*}
\]
has a unique solution \( \pmod{m_1m_2 \cdots m_n} \).

4.5. Fermat’s Little Theorem and Euler’s Theorem

Theorem 4.5.1. Fermat’s Little Theorem FLT. Let \( p \) be a prime and \( a \) be an integer with \( p \nmid a \). Then \( a^{p-1} \equiv 1 \pmod{p} \).

Proof. Special case of Euler’s Theorem, coming next. Just set \( m = p \) and note \( \phi(p) = p - 1 \). \( \square \)

An equivalent version of Fermat’s Little Theorem is the following: For any prime \( p \) and integer \( a \) we have \( a^p \equiv a \pmod{p} \). Note, if \( p \mid a \) then this statement is trivially true (both sides are 0) while if \( p \nmid a \) then we can divide both sides by \( a \) to obtain the original statement.

Theorem 4.5.2. Euler’s Theorem. Let \( m \in \mathbb{N} \) and \( a \in \mathbb{Z} \) with \( (a, m) = 1 \). Then \( a^{\phi(m)} \equiv 1 \pmod{m} \).

Note: Euler’s theorem fails if \( (a, m) > 1 \).
Example 4.5.1. Find the value of $17^{1802} \pmod{27}$. Note $\phi(27) = 18$ and $(17, 27) = 1$, so $17^{18} \equiv 1 \pmod{27}$. Thus $17^{1802} = (17^{18})^{100}17^2 \equiv 289 \equiv 19 \pmod{27}$.

Lemma 4.5.1. Permutation Lemma. Let $m \in \mathbb{N}$ and $a$ be an integer with $(a, m) = 1$ and $k = \phi(m)$. Let $\{x_1, x_2, \ldots, x_k\}$ be a reduced residue system (mod $m$). Then the set $\{ax_1, ax_2, \ldots, ax_k\}$ is also a reduced residue system (mod $m$).

Example 4.5.2. $m = 10$, $\{1, 3, 7, 9\}$ is a reduced residue system. Let $a = 3, 7, 9$ to obtain new reduced residue systems, and note that they are just permutations of the original.

Proof of Permutation Lemma. By the cancelation law, the values $ax_1, \ldots, ax_k$ are all distinct (mod $p$). Since there are $k$ distinct values, this must be a reduced residue system.

Proof of Euler’s Theorem. Let $a \in \mathbb{Z}$ with $(a, m) = 1$ and $\{x_1, \ldots, x_k\}$ be a reduced residue system (mod $m$), where $k = \phi(m)$. By the permutation lemma, $\{ax_1, \ldots, ax_k\} = \{[x_1]_m, \ldots, [x_k]_m\}$. Thus the product of all of the elements in each of these sets must be equal (mod $m$), that is,

$$(ax_1)(ax_2)\cdots(ax_k) \equiv x_1x_2\cdots x_k \pmod{m}.$$ 

By the cancelation law we obtain $a^k \equiv 1 \pmod{m}$, which is the statement of the theorem.

Example 4.5.3. Find the last 3 digits of $17^{801}$. That is, find $\text{lr}$ of $17^{801} \pmod{1000}$. Note $\phi(1000) = 400$, so by Euler, $17^{400} \equiv 1 \pmod{1000}$. Thus $17^{1801} \equiv 17 \pmod{1000}$. So last three digits are 017.

4.5.1. Applications of Euler’s Theorem and Fermat’s Little Theorem. We will see five applications. (i) Computing powers of integers (mod $m$). (Already done.) (ii) Finding orders of elements (mod $m$). (iii) Finding the length of the repeating pattern in the decimal expansion of a rational number. (iv) Primality testing. (iv) RSA cryptography. We look at these applications in the next few sections.

4.6. Orders of elements (mod $m$)

Definition 4.6.1. Let $m$ be a positive integer and $a$ be any integer with $(a, m) = 1$. The order of $a$ (mod $m$), written $\text{ord}_m(a)$ is the smallest positive integer $k$ such that $a^k \equiv 1 \pmod{m}$.

Example 4.6.1. $\text{ord}_7(2) = 3$, $\text{ord}_5(2) = 4$.

Note 4.6.1. i) If $(a, m) = 1$ then $\text{ord}_m(a)$ exists. Why? Consider the values $a, a^2, \ldots, \pmod{m}$ Eventually there must be repetition, that is, $a^i \equiv a^j \pmod{m}$ for some $i > j$. But then $a^{i-j} \equiv 1 \pmod{m}$. Thus there exists some $k$ such that $a^k \equiv 1 \pmod{m}$, and therefore a minimal such $k$ must exist by well ordering.

ii) If $(a, m) > 1$ then there is no $k$ with $a^k \equiv 1 \pmod{m}$ and so $\text{ord}_m(a)$ doesn’t exist.

iii) If $k = \text{ord}_m(a)$ then $a^{-1} \equiv a^{k-1} \pmod{m}$.
Theorem 4.6.1. Powers of $a \pmod{m}$. Let $(a, m) = 1$ and $k = \text{ord}_m(a)$. 

i) The values $1, a, a^2, \ldots, a^{k-1}$ are distinct $\pmod{m}$.

ii) Every power of $a$ is congruent to exactly one of these values. To be precise if $n \in \mathbb{Z}$ and $r$ is the remainder in dividing $n$ by $k$ then $a^n \equiv a^r \pmod{m}$. 

iii) $a^n \equiv 1 \pmod{m}$ if and only if $k|n$.

Proof. i) Proof by contradiction. Suppose that $a^i \equiv a^j \pmod{m}$ for some $0 \leq i < j < k$. Then by cancelation law $a^{j-i} \equiv 1 \pmod{m}$, but since $0 < j-i < k$ this contradicts the minimality of $k$.

ii) By division algorithm, $n = qk + r$, with $0 \leq r < k$. Thus $a^n \equiv a^r \pmod{m}$. 

iii) $a^n \equiv 1 \pmod{m}$ iff $a^r \equiv 1 \pmod{m}$ iff $r = 0$ (by minimality of $k$) iff $k|n$. \hfill \Box

Theorem 4.6.2. Orders of elements. Let $m \in \mathbb{N}$, $a \in \mathbb{Z}$ with $(a, m) = 1$. Then $\text{ord}_m(a)|\phi(m)$.

Proof. Let $k = \text{ord}_m(a)$. By Theorem 4.6.1. $a^n \equiv 1 \pmod{m}$ iff $k|n$. Since $a^{\phi(m)} \equiv 1 \pmod{m}$ (by Euler’s Theorem), we must have $k|\phi(m)$. \hfill \Box

Example 4.6.2. a) Find $k = \text{ord}_{18}(7)$. $\phi(18) = 6$. Thus $k|6$, that is, $k = 1, 2, 3$ or $6$. Plainly $k \neq 1$ (1 is the only element of order 1 for any modulus). $7^2 \equiv 13 \pmod{18}$ and $7^3 \equiv 13 \cdot 7 = 91 \equiv 1 \pmod{18}$, so $k = 3$.

b) Next lets find $k = \text{ord}_{18}(5)$. Note $5^2 \equiv 7 \pmod{18}$, $5^3 \equiv -1 \pmod{18}$. Thus $k = 6$.

For composite moduli, the next theorem is convenient for calculating orders.

Theorem 4.6.3. Suppose $m = m_1m_2$ with $(m_1, m_2) = 1$ and $(a, m) = 1$. Then $\text{ord}_{m_1m_2}(a) = [\text{ord}_{m_1}(a), \text{ord}_{m_2}(a)]$.

Proof. Just note that $a^k \equiv 1 \pmod{m_1m_2}$ is equivalent to the system, $a^k \equiv 1 \pmod{m_1}$ and $a^k \equiv 1 \pmod{m_2}$. Any $k$ satisfying the first is a multiple of $\text{ord}_{m_1}(a)$ while any $k$ satisfying the second is a multiple of $\text{ord}_{m_2}(a)$. Thus the minimal such $k$ is the least common multiple of these two orders. \hfill \Box

Example 4.6.3. Find $\text{ord}_{21}(10)$. We must find the minimal $k$ such that $10^k \equiv 1 \pmod{21}$, that is, $10^k \equiv 1 \pmod{3}$ and $10^k \equiv 1 \pmod{7}$. The first congruence is $1^k \equiv 1 \pmod{3}$ which holds for any $k$, while the second $3^k \equiv 1 \pmod{7}$ requires $6|k$. Thus $k = 6$ is the minimal value.

4.7. Decimal Expansions

$\frac{1}{7} = 0.\overline{142857}$. In your first homework you discovered that the length of the repeating cycle in the decimal expansion of $1/p$ where $p$ is a prime, is a divisor of $p-1$. Lets see how we can predict the length of the cycle without ever finding the decimal expansion.

Theorem 4.7.1 (Decimal Expansions). Let $a/b$ be a fraction with $0 < a < b$ and $(a, b) = 1$. Say $b = 2^e5^f m$ with $(m, 10) = 1$, and that $a/b$ has a decimal expansion of the form

$$a/b = .a_1a_2 \ldots a_i\overline{c_1c_2 \ldots c_k},$$

with $i, k$ minimal, that is, $k$ is the (minimal) length of the repeating cycle, and the repeating cycle does not start earlier. Then $i = \max(e, f)$, and $k = \text{ord}_m(10)$.
Note: The decimal expansion is called purely periodic if \( i = 0 \). By the theorem, this will occur iff \( \left( b, 10 \right) = 1 \).

**Corollary 4.7.1.** If \( a/b \) is a fraction as given in Theorem 4.7.1 then \( k | \phi(m) \).

**Proof.** Let \( k = \text{ord}_m(10) \). By Theorem 4.6.2 we have \( k | \phi(m) \). \( \square \)

**Example 4.7.1.** Consider \( \frac{1}{7} \). Let \( k = \text{ord}_7(10) = \text{ord}_7(3) \), \( k | 6 \), so \( k = 2, 3 \) or 6, and one easily finds \( k = 6 \). Thus \( 1/7 \) is purely periodic with cycle of length 6.

**Example 4.7.2.** Consider \( \frac{125}{336} \). Note \( 125 = 5^3 \), \( 336 = 2^4 \cdot 3 \cdot 7 \). Thus \( m = 21 \), \( k = \text{ord}_{21}(10) = \left[ \text{ord}_3(10) \cdot \text{ord}_7(10) \right] = \left[ \text{ord}_3(1), \text{ord}_7(3) \right] = [1, 6] = 6 \). Thus \( i = \max(e, f) = 4 \), \( k = 6 \). One finds on a calculator \( \frac{125}{336} = 0.3720238095 \). Having done the calculation of \( i \) and \( k \) ahead of time we are assured that the answer on calculator is exact.

**Proof of Theorem 4.7.1.** Let \( \frac{a}{b} \) have a decimal expansion as given in the theorem with \( i, k \) minimal.

\[
10^{-i} \frac{a}{b} = a_1 \ldots a_i \overline{x_1 \ldots x_k}.
\]

and

\[
10^{-i+k} \frac{a}{b} = a_1 \ldots a_i c_1 \ldots c_k \overline{x_1 \ldots x_k}.
\]

Subtracting, we get \( 10^{-i} (10^k - 1) \in \mathbb{Z} \). Thus \( b | 10^i a (10^k - 1) \). Since \( (b, a) = 1 \) this is equivalent to \( b | 10^i (10^k - 1) \), that is, \( 2^i 5^i | 10^i (10^k - 1) \). Thus, by Euclid’s lemma, \( 2^i 5^i | 10^i \) and, since \( (m, 10) = 1 \), \( m | (10^k - 1) \). Moreover any \( i, k \) satisfying the last two conditions gives rise to such a decimal expansion. Thus, \( i \) is the minimal integer satisfying \( 2^i 5^i | 10^i \) and \( k \) is the minimal integer satisfying \( m | 10^k - 1 \). Plainly, \( i = \max(e, f) \) and \( k = \text{ord}_m(10) \). \( \square \)

**4.8. Primality Testing**

How can we efficiently test whether a given 100 digit number is a prime? We need the following facts:

i) Fermat’s Little Theorem: If \( p \) is a prime and \( \nmid a \) then \( a^{p-1} \equiv 1 \pmod{p} \).

ii) If \( p \) is a prime and \( x^2 \equiv 1 \pmod{p} \) then \( x \equiv \pm 1 \pmod{p} \).

iii) If \( p \) is an odd prime and \( \nmid a \) then \( a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \).

**Proof.** (i) Done. (ii) \( p | (x^2 - 1) \) if \( p | (x - 1)(x + 1) \) if \( p | (x - 1) \) or \( p | (x + 1) \) if \( x \equiv \pm 1 \pmod{p} \). (iii) Let \( x \equiv a^{\frac{p-1}{2}} \pmod{p} \). Then by FLT \( x^2 \equiv 1 \pmod{p} \) and so by (ii), \( x \equiv \pm 1 \pmod{p} \). \( \square \)

**Theorem 4.8.1** (Composite Number Test). Let \( m \) be a positive integer (we wish to test for primality) and \( b \) be any integer with \( (b, m) = 1 \). If \( b^{m-1} \not\equiv 1 \pmod{m} \), then \( m \) is composite.

**Proof.** Proof by contradiction. Suppose that \( m \) is a prime. Since \( (b, m) = 1 \) we would then have by FLT that \( b^{m-1} \equiv 1 \pmod{m} \), a contradiction. \( \square \)

**Definition 4.8.1.** (i) A composite number \( m \) is called a pseudoprime to the base \( b \) if \( b^{m-1} \equiv 1 \pmod{m} \) (that is, \( b \) satisfies the criterion in FLT).

(ii) A composite number \( m \) is called a Carmichael number if \( m \) is a pseudoprime to every base \( b \) relatively prime to \( m \).
4.8.1. The Strong Pseudoprime Test for Primality. Let \( m \) be a given odd number we wish to test for primality. Start with base 2, and calculate \( x \equiv 2^{m-1} \pmod{m} \). There are four options: If \( x \not\equiv \pm 1 \pmod{m} \) then \( m \) is composite. If \( x \equiv -1 \pmod{m} \), pause and change base. If \( x \equiv 1 \pmod{m} \) and \( 4 \nmid m-1 \) then change base. If \( x \equiv 1 \pmod{m} \) and \( 4 \mid (m-1) \) then calculate \( y \equiv 2^{m-1} \pmod{m} \). Note \( y^2 \equiv 1 \pmod{m} \) so if \( m \) is a prime we should have \( y \equiv \pm 1 \pmod{m} \), and repeat the four options. The number of possible repetitions for a given base is at most the multiplicity of 2 dividing \( m-1 \). The next base we test is 3, then 5, 7, 11, 13, ... running through the primes.

By just using bases 2 and 3 we can test any number up to one million and arrive at a definitive conclusion as to whether it is a prime or not. Using bases 2, 3, 5, 7, 11 we can test any number up to \( 2 \cdot 10^{12} \). This algorithm runs extremely fast (microsecond) on a computer.

4.9. Public-Key Cryptography


1. First we need a way of changing words into numbers. This can be public and as simple as \( A = 01, B = 02, \ldots, Z = 26, \) space = 00, etc. Thus the word “Hello” would become 0805121215, which we think of as the nine-digit number 805121215. Sentences are broken into pieces such that each piece becomes a number less than the modulus we are working with.

2. Each person selects two distinct primes \( p \) and \( q \) each with say 200 digits, and multiplies them to create their public modulus \( m = pq \) (with 400 digits). Each person also selects an encoding exponent \( e \) relatively prime to the value \( L \) calculated in step 3. A public phone book is made listing Name, modulus \( m \) and encoding exponent \( e \). The individual primes \( p \) and \( q \) are kept secret.

3. Each person \( P \) also calculates two secret values: (i) \( L := [p-1,q-1] \). This value can be calculated since \( P \) knows the individual values \( p,q \). (ii) The decoding exponent \( d \) is chosen so that \( de \equiv 1 \pmod{L} \), that is, \( d \equiv e^{-1} \pmod{L} \). \( d \) exists since \( e \) was selected relatively prime to \( L \).

4. Encoding the message: Suppose that person \( P \) wishes to send a message to person \( Q \). Person \( P \) looks in the phone book for person \( Q \)'s \( m \) and \( e \), and then chops his/her message into pieces smaller than \( m \) and relatively prime to \( m \). Let \( M \) be one such piece. Person \( P \) then calculates the least least residue \( M_e \) of \( M^e \pmod{m} \), that is,

\[
M_e \equiv M^e \pmod{m}, \quad 0 < M_e < m.
\]

\( M_e \) is called the encoded message.

5. The encoded message is delivered to person \( Q \) in a public manner. Anyone is free to look at \( M_e \), but it is undecipherable to anyone not having the decoding exponent \( d \).

6. Person \( Q \) receives the message and calculates the least residue \( M_d \) of \( M_e^d \pmod{m} \), that is,

\[
M_d \equiv M_e^d \pmod{m}, \quad 0 < M_d < m.
\]
We claim that $M_d = M$, that is, person $Q$ has recovered the original message!

**Proof.** Since $M_d$ and $M$ are less than $m$ it suffices to show that $M_d \equiv M \pmod{m}$. Claim: $M^L \equiv 1 \pmod{m}$. This is equivalent to $M^L \equiv 1 \pmod{p}$ and $M^L \equiv 1 \pmod{q}$. Since $L$ is a multiple of $p - 1$ we have, by FLT, $M^L \equiv 1 \pmod{p}$, and since $L$ is a multiple of $q - 1$ we have $M^L \equiv 1 \pmod{q}$, completing the proof of the claim.

Now, since $ed \equiv 1 \pmod{L}$, we have $ed = 1 + kL$ for some integer $k$. Thus

$$M_d \equiv M_e^d \equiv (M^e)^d \equiv M^{1+kL} = M \cdot (M^L)^k \equiv M \pmod{m},$$

by the claim. QED.

**Example 4.9.1.** Let $p = 31$, $q = 37$, $m = pq = 1147$. $L = [p - 1, q - 1] = [30, 36] = 180$. Let $e = 7$. Note that $(e, L) = 1$. Select $d \equiv e^{-1} \pmod{L}$, so $d = 103$. Let's send the message $M = 805$. $M_e \equiv 805^7 \equiv 650 \pmod{m}$. $M_d \equiv 650^{103} \equiv 805 \pmod{m}$.

**4.9.1. Computing powers** $(\pmod{m})$. An efficient way to compute powers $(\pmod{m})$ is to use the binary expansion of the power. Most computing software that handles modular arithmetic uses this method. Let's illustrate the method with an example.

**Example 4.9.2.** Find $2^{149} \pmod{m}$. The binary expansion of 149 is given by

$$128 + 0 \cdot 64 + 0 \cdot 32 + 16 + 0 \cdot 8 + 4 + 0 \cdot 2 + 1 = 10010101_2.$$

By successive squaring we calculate $2^2 \pmod{m}$, $2^4 \pmod{m}$, $2^8 \pmod{m}$, $2^{16} \pmod{m}$, . . . , $2^{128} \pmod{m}$. Start with $x = 1$. If a digit 1 appears in the binary expansion then we replace $x$ with $x$ times the corresponding power of 2, as we go along. Thus, altogether we will have computed

$$1 \cdot 2^1 \cdot 2^4 \cdot 2^{16} \cdot 2^{128} \equiv 2^{1+4+16+128} = 2^{149} \pmod{m}.$$
CHAPTER 5

Polynomial Congruences

We wish to solve the congruence

\[
 f(x) \equiv 0 \pmod{m},
\]

where \( f(x) \) is a polynomial with integer coefficients.

**The three step process:** Let \( m = p_1^{e_1} \cdots p_k^{e_k} \).

(i) Solve the congruence \( f(x) \equiv 0 \pmod{p_i} \) for each prime \( p_i \).

(ii) Lift the solutions in (i) from \( \pmod{p_i} \) to solutions \( \pmod{p_i^{e_i}} \).

(iii) Use CRT to find all possible solutions \( \pmod{m} \) using the info from (ii).

**Example 5.0.3.** Solve \( 26x^3 + x^2 - 13x + 5 \equiv 0 \pmod{35} \). Note this is equivalent to solving the congruence \( \pmod{7} \) and \( \pmod{5} \).

(i) Solve \( \pmod{5} \).

\[
 26x^3 + x^2 - 13x + 5 \equiv x^3 + x^2 + 2x = x(x^2 + x + 2) \pmod{5}.
\]

The quadratic has no zero \( \pmod{5} \) (as seen by testing 0,1,2,3,4). Thus the only solution \( \pmod{5} \) is \( x \equiv 0 \pmod{5} \).

(ii) Next solve \( \pmod{7} \). First note that

\[
 26x^3 + x^2 - 13x + 5 \equiv 5x^3 + x^2 + x + 5 = 5(x^3 + 1) + x(x + 1)
\]

\[
 = (x + 1)(5x^2 - x + 1) + x = (x + 1)(5x^2 - 4x + 5) \pmod{7}.
\]

The quadratic is again seen to have no solution \( \pmod{7} \), and so the unique solution is \( x \equiv -1 \pmod{7} \). By CRT we then find that the unique solution to the original congruence is \( x \equiv 20 \pmod{35} \).

**5.1. Lifting solutions from \( \pmod{p} \) to \( \pmod{p^e} \)**

Let \( p \) be a prime and \( f(x) \) a polynomial with integer coefficients. Suppose that we wish to solve \( f(x) \equiv 0 \pmod{p^2} \). Any solution must already be a solution \( \pmod{p} \). Let \( x_1 \) be an integer solution of the congruence

\[
 f(x) \equiv 0 \pmod{p}.
\]

We shall attempt to lift the solution \( x_1 \) to a solution \( \pmod{p^2} \), that is find a point \( x_2 \) such that,

\[
 x_2 \equiv x_1 \pmod{p} \quad \text{and} \quad f(x_2) \equiv 0 \pmod{p^2}.
\]

Say \( x_2 = x_1 + tp \) for some \( t \in \mathbb{Z} \). Can we choose \( t \) so that this is a solution \( \pmod{p^2} \).

Recall from Calc II the Taylor expansion,

\[
 f(a + y) = f(a) + f'(a)y + \frac{f''(a)}{2!}y^2 + \cdots + \frac{f^{(n)}(a)}{n!}y^n,
\]
Clearly, the second solution (obtained by lifting $-f$ is 1) is a singular solution, while for option (iii), that is, the lifting congruence is 0
t, Congruence is 4, nonsingular if $f$ and so again we have three possibilities.

(5.3) **Lifting Congruence:** $f'(x_1)t \equiv -\frac{f(x_1)}{p} \pmod{p}$.

**The three possibilities:**

(i) If $f'(x_1) \not\equiv 0 \pmod{p}$, then there is a unique solution $t$ of (5.3) and hence a unique solution $x_2$ of (5.2) (mod $p^2$).

(ii) If $f'(x_1) \equiv 0 \pmod{p}$ and $f(x_1) \not\equiv 0 \pmod{p^2}$ then there is no solution of (5.3) and hence no solution of (5.2).

(iii) If $f(x_1) \equiv 0 \pmod{p}$ and $f(x_1) \equiv 0 \pmod{p^2}$, then any value of $t$ is a solution of (5.3), and hence there are $p$ distinct solutions of (5.2) (mod $p^3$).

Suppose that we have constructed by induction a sequence of integers $x_1, x_2, \ldots, x_n$ such that

$$x_{i+1} \equiv x_i \pmod{p^r} \quad \text{and} \quad f(x_i) \equiv 0 \pmod{p^r},$$

for $i = 1, 2, \ldots, n$. To continue we wish to find an $x_{n+1} = x_n + p^nt$ such that

$f(x_n + p^nt) \equiv 0 \pmod{p^{n+1}}$. This amounts to solving

$$f(x_n) + f'(x_n)p^nt \equiv 0 \pmod{p^{n+1}},$$

or equivalently (noting that $f'(x_1) \equiv f'(x_n) \pmod{p}$)

$$f'(x_1)t \equiv -\frac{f(x_n)}{p^n} \pmod{p}$$

and so again we have three possibilities.

**Definition 5.1.1.** A solution $x_1$ of the congruence $f(x) \equiv 0 \pmod{p}$ is called nonsingular if $f'(x_1) \not\equiv 0 \pmod{p}$ and singular if $f'(x_1) \equiv 0 \pmod{p}$.

**Theorem 5.1.1.** If $x_1$ is a nonsingular solution of the congruence $f(x) \equiv 0 \pmod{p}$ then for any positive integer $n$ there is a unique solution $x_n \pmod{p^n}$ of the congruence $f(x) \equiv 0 \pmod{p^n}$ such that $x_n \equiv x_1 \pmod{p}$.

**Example 5.1.1.** Solve the congruence $x^2 \equiv -1 \pmod{125}$. Start with $x^2 \equiv -1 \pmod{5}$ which has solutions $\pm2$. First lets lift 2. Set $x = 2 + 5t$. $f(x) = x^2 + 1, f(2) = 5, f'(2) = 4$, and so Lifting Congruence is $4t \equiv -1 \pmod{5}$, which gives $t \equiv 1 \pmod{5}$, $x \equiv 7 \pmod{25}$. Next lift 7. Set $x = 7 + 25t$. $f(7) = 50$. The Lifting Congruence is $4t \equiv -50/25 \pmod{5}$, so $t \equiv 2 \pmod{5}$ and $x \equiv 57 \pmod{125}$. Clearly, the second solution (obtained by lifting $-2$) is $x \equiv -57 \pmod{125}$.

**Example 5.1.2.** Solve $x^3 + x^2 + 23 \equiv 0 \pmod{5^3}$.

(i) Take $x_1 = 1$. Put $x = 1 + 5t$. Note that $f'(1) = 5 \equiv 0 \pmod{5}$, that is 1 is a singular solution, while $f(1)/5 = 5 \equiv 0 \pmod{5}$. Thus we have have option (iii), that is, the lifting congruence is $0t \equiv 0 \pmod{5}$, so $t$ is arbitrary and

for any $a, y \in \mathbb{Z}$. Note that since the coefficients on the left are all integers, so are the coefficients on the right. Inserting $a = x_1, y = pt$ we obtain

$$f(x_1 + tp) = f(x_1) + f'(x_1)tp + \frac{f''(x_1)}{2}(tp)^2 + \cdots \equiv f(x_1) + f'(x_1)tp \pmod{p^2},$$

since all of the other coefficients are divisible by $p^2$. Thus we need to solve the congruence

(5.3) Lifting Congruence: $f'(x_1)t \equiv -\frac{f(x_1)}{p} \pmod{p}$.
we get \( x_2 = 1 + 5t = 1, 6, 11, 16, 21 \). Now \( f(1 + 5t)/25 = 4t^2 + t + 1 \), and we see \( f(1 + 5t)/25 \equiv 0 \pmod{5} \) iff \( t = 3 \). Thus for \( x_2 = 16 \) we have option (iii) and get five liftings to solution \((\mod{125})\), namely
\[
\begin{align*}
x &\equiv 16, 41, 66, 91, 116 \pmod{125}.
\end{align*}
\]

If one continues this to \((\mod{5^2})\) one discovers that all of the solutions \((\mod{5^2})\) lift. Thus there are 25 solutions \((\mod{625})\) all living above \( x_1 = 1 \).

(ii) Since \( x_1 = 2 \) is a nonsingular solution, there is a unique lifting each time. We obtain \( x_2 \equiv 17 \pmod{25} \) and \( x_3 \equiv 42 \pmod{125} \), and (if we continue one more level) \( x_4 \equiv 417 \pmod{625} \).

This information can be displayed in a tree graph with vertices 1 and 2 at the top and branches below for the \((\mod{25}), (\mod{125}), (\mod{625})\) liftings.

**Example 5.1.3.** Solve the congruence \( f(x) = x^3 + 7x^2 + x = x(x-1)^2 \equiv 0 \pmod{3^2} \).

### 5.2. Counting Solutions of congruences

**Example 5.2.1.** Suppose that we wish to count the number of solutions of \( f(x) \equiv 0 \pmod{35} \), where \( f(x) \) is a polynomial over \( \mathbb{Z} \). We start by solving the congruences \( f(x) \equiv 0 \pmod{5} \) and \( f(x) \equiv 0 \pmod{7} \). Say \( a_1, a_2, \ldots, a_r \) are the solutions of the former, and \( b_1, \ldots, b_s \) the solutions of the latter. By CRT, for any choice of \( i, j \) there is a unique \( x \pmod{35} \) with
\[
\begin{align*}
x &\equiv a_i \pmod{5}, \\
x &\equiv b_j \pmod{7}.
\end{align*}
\]

By the substitution principle, \( f(x) \equiv f(a_i) \equiv 0 \pmod{5} \) and \( f(x) \equiv f(b_j) \equiv 0 \pmod{7} \), and so \( f(x) \equiv 0 \pmod{35} \). Thus, altogether, we obtain \( rs \) solutions \((\mod{35})\).

The content of this example is given in the following theorem.

**Theorem 5.2.1.** Let \( f(x) \) be a polynomial with integer coefficients and \( m \) a positive integer with factorization \( m = p_1^{e_1} \cdots p_k^{e_k} \). Then
\[(5.4)\]
\[
f(x) \equiv 0 \pmod{m}
\]
if and only if \( x \) satisfies the system of congruences
\[
(5.5) \quad f(x) \equiv 0 \pmod{p_i^{e_i}}, \quad 1 \leq i \leq k.
\]

(ii) Letting \( N(m) \) denote the number of solutions of \((\mod{m})\) and \( N(p_i^{e_i}) \) denote the number of solutions of \((\mod{p_i^{e_i}})\), we have \( N(m) = \prod_{i=1}^k N(p_i^{e_i}) \).

**Proof.** (i) \( m|f(x) \Leftrightarrow p_i^{e_i}|f(x), 1 \leq i \leq k \).

(ii) We claim that the CRT gives us a one-to-one correspondence between the \( k \)-tuples \((x_1, \ldots, x_k) \in \mathbb{Z}/(p_1^{e_1}) \times \cdots \times \mathbb{Z}/(p_k^{e_k}) \) with \( x_i \) a solution of \((5.5)\) for \( 1 \leq i \leq k \) and the solutions \( x \) of \((5.4)\). Indeed, suppose that \( x_i \) is a solution of \((5.5)\) for \( 1 \leq i \leq k \), and let \( x \pmod{m} \) be the unique value with \( x \equiv x_i \pmod{p_i^{e_i}} \), \( 1 \leq i \leq k \). Such an \( x \) satisfies \( f(x) \equiv f(x_i) \equiv 0 \pmod{p_i^{e_i}} \) for all \( i \), and so \( f(x) \equiv 0 \pmod{m} \).
5.3. Solving congruences \((\text{mod } p)\)

As we saw above, in order to solve a polynomial congruence \((\text{mod } m)\), one starts by solving congruences \((\text{mod } p)\) where \(p\) is a prime. For small \(p\) this is generally done by trial and error. Another tool that can be useful is the factor theorem for congruences.

**Theorem 5.3.1. Factor Theorem** Suppose that \(p\) is a prime, \(f(x)\) is a polynomial of degree \(d\) over \(\mathbb{Z}\), and that \(a\) is a solution of the polynomial congruence \(f(x) \equiv 0 \pmod{p}\). Then \(f(x) \equiv (x-a)g(x) \pmod{p}\), for some polynomial \(g(x)\) over \(\mathbb{Z}\) of degree \(d-1\).

Note: To say two polynomials are congruent \((\text{mod } p)\) means that all of the corresponding coefficients are congruent \((\text{mod } p)\).

**Proof.** We are given that \(f(a) \equiv 0 \pmod{p}\). Thus \(f(a) = kp\) for some \(k \in \mathbb{Z}\). Let \(h(x) = f(x) - kp\). Then \(a\) is a zero of \(h(x)\) and so by the factor theorem for \(\mathbb{Z}\), \((x-a)\) is a factor of \(h(x)\), that is, \(h(x) = (x-a)g(x)\) for some polynomial \(g(x)\) over \(\mathbb{Z}\) of degree \(d-1\). Clearly \(\deg(g) = d-1\) and \(f(x) = (x-a)g(x) + pk\), that is, \(f(x) \equiv (x-a)g(x) \pmod{p}\).

**Definition 5.3.1.** (i) We say that \(a\) is a zero of a polynomial \(f(x) \pmod{p}\), if \(f(a) \equiv 0 \pmod{p}\). In this case \((x-a)\) is a factor of \(f(x) \pmod{p}\).

(ii) We say that \(a\) is a zero of \(f(x) \pmod{p}\) of multiplicity \(k\), if \((x-a)^k\) is a factor of \(f(x) \pmod{p}\), that is, \(f(x) \equiv (x-a)^kg(x) \pmod{p}\) for some polynomial \(g(x)\), but \((x-a)^{k+1}\) is not a factor.

**Example 5.3.1.** (i) Let \(f(x) = x^p - 1\). Since \(p|\left(\frac{x}{x}\right)\) for \(1 \leq k \leq p-1\) we have \(x^p - 1 \equiv (x-1)^p \pmod{p}\), and so \(1\) is a zero of \(f(x) \pmod{p}\) of multiplicity \(p\).

(ii) Let \(f(x) = x^{p-1} - 1\). By FLT, \(1, 2, \ldots, p-1\) are all zeros of \(f(x) \pmod{p}\), and so

\[x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-(p-1)) \pmod{p}\]

In particular, matching the constant terms on the RHS and LHS, we obtain Wilson’s Theorem, \((p-1)! \equiv -1 \pmod{p}\).

**Theorem 5.3.2. Lagrange’s Theorem** Let \(f(x)\) be a polynomial of degree \(d\) over \(\mathbb{Z}\), and \(p\) a prime. Then the congruence \(f(x) \equiv 0 \pmod{p}\) has at most \(d\) distinct solutions \((\text{mod } p)\).

**Proof.** The proof is by induction on \(d\). When \(d = 1\) the statement is trivial. Indeed, a linear congruence has either no solution or 1 solution \((\text{mod } p)\). Suppose the statement is true for \(d\) and now let \(f\) be a polynomial of degree \(d+1\). If \(f\) has no zero \((\text{mod } p)\) we are done. Otherwise, let \(a\) be a zero of \(f \pmod{p}\). Then, by the factor theorem \(f(x) \equiv (x-a)g(x) \pmod{p}\) for some polynomial \(g(x)\) of degree \(d\). By the induction assumption \(g(x) \) has at most \(d\) zeros \((\text{mod } p)\), counted with multiplicity. Thus \(f(x)\) has at most \(d+1\) zeros, since if \(f(x) \equiv 0 \pmod{p}\) then either \(x-a \equiv 0 \pmod{p}\), or \(g(x) \equiv 0 \pmod{p}\) (since \(p\) is a prime.) Thus either \(x \equiv a \pmod{p}\), or \(x\) is one of the zeros of \(g(x) \pmod{p}\).

**Note 5.3.1.** Lagrange’s Theorem fails for composite moduli. For example if \(f(x) = x^2 - 1\) and \(m = p_1 \cdot \ldots \cdot p_k\), a product of \(k\) distinct primes, then \(f(x) \equiv 0 \pmod{m}\) has \(2^k\) distinct solutions \((\text{mod } m)\), even though \(f(x)\) is just of degree 2.
Example 5.3.2. Solve \( x^3 + x + 1 \equiv \pmod{11} \). Plainly \( x = 2 \) is a solution, and so \( (x - 2) \) is a factor. By long division we obtain \( x^3 + x + 1 \equiv (x - 2)(x^2 + 2x + 5) \pmod{11} \). By trial and error one can check that the quadratic has no solution. Thus \( x = 2 \) is the only solution.

Example 5.3.3. Solve the congruence \( x^3 + x + 1 \pmod{31^2} \). Hint: Note that \( 3 \) is a solution \( \pmod{31} \). Use factor theorem and quadratic formula to obtain others.

Example 5.3.4. Solve the congruence \( x^{495} - x^{24} + 3 \equiv 0 \pmod{7} \). Hint: Use Fermat’s Little Theorem to make life easier.

5.4. Quadratic Residues and the Legendre Symbol

Definition 5.4.1. Let \( p \) be a prime, \( a \in \mathbb{Z} \), with \( p \nmid a \). \( a \) is called a quadratic residue \( \pmod{p} \) if \( a \equiv x^2 \pmod{p} \) for some integer \( x \). Otherwise \( a \) is called a quadratic non-residue \( \pmod{p} \).

Example 5.4.1. \( 5 \) is a quadratic residue \( \pmod{11} \) since \( 7^2 = 49 \equiv 5 \pmod{11} \).

Theorem 5.4.1. Exactly \( \frac{p-1}{2} \) values \( \pmod{p} \) are quadratic residues and \( \frac{p-1}{2} \) are not.

Proof. The quadratic residues are \( 1^2, 2^2, \ldots, (p - 1)^2 \pmod{p} \). Note \( x^2 \equiv y^2 \pmod{p} \) iff \( x \equiv \pm y \pmod{p} \). Thus the valued \( 1^2, 2^2, \ldots, \left( \frac{p-1}{2} \right)^2 \pmod{p} \) are the distinct quadratic residues.

Example 5.4.2. Find all quadratic residues \( \pmod{11} \). \( 1^2, 2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 5, 5^2 \equiv 3 \pmod{11} \).

Definition 5.4.2. Let \( p \) be a prime, \( a \in \mathbb{Z} \), with \( p \nmid a \). The Legendre symbol is defined by

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue } \pmod{p}; \\
-1 & \text{if } a \text{ is a quadratic non-residue } \pmod{p}.
\end{cases}
\]

Example 5.4.3. \( \left( \frac{3}{13} \right) = 1, \left( \frac{2}{3} \right) = -1 \).

Theorem 5.4.2. Euler’s Criterion. Let \( p \) be an odd prime and \( a \in \mathbb{Z} \) with \( p \nmid a \). Then

\[
\left( \frac{a}{p} \right) \equiv a^{\frac{p-1}{2}} \pmod{p}.
\]

Proof. We’ve already seen that the RHS is equiv \( \pm 1 \pmod{p} \) (by FLT). Suppose that \( a \) is a quadratic residue, so that \( a \equiv x^2 \pmod{p} \) for some integer \( x \). Then \( a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p} \), and so both sides of (5.6) are 1. Thus all \( \frac{p-1}{2} \) quadratic residues are solutions of the congruence \( x^{\frac{p-1}{2}} \equiv 1 \pmod{p} \). Since this is a polynomial of degree \( \frac{p-1}{2} \) it cannot have any other solutions by Lagrange’s theorem. Thus for any quadratic nonresidue \( \pmod{p} \) the RHS must be -1, agreeing with the LHS.

Example 5.4.4. \( \left( \frac{3}{13} \right) \equiv 3^6 \equiv (3^3)^2 \equiv 1 \pmod{13} \) so 3 is a quadratic residue. Indeed \( 4^2 \equiv 3 \pmod{13} \).
THEOREM 5.4.3. Multiplicative property of Legendre symbol. Suppose that $p$ is a prime and that $a, b \in \mathbb{Z}$ with $p \nmid ab$. Then
\[
\left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \left( \frac{b}{p} \right).
\]

PROOF. Trivial for $p = 2$. Suppose $p$ is odd. By Euler criterion we have
\[
\left( \frac{ab}{p} \right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left( \frac{a}{p} \right) \left( \frac{b}{p} \right) \quad \text{(mod } p).\]
Since the LHS and RHS are both $\pm 1$ we see that equality (as integers) follows. □

THEOREM 5.4.4. Trivial Properties of Legendre symbol. Suppose that $p$ is a prime.

(i) For any integer $a$ with $p \nmid a$, we have $\left( \frac{a^2}{p} \right) = 1$.

(ii) For any integers $a, b$ with $a \equiv b \pmod{p}$, we have $\left( \frac{a}{p} \right) = \left( \frac{b}{p} \right)$.

THEOREM 5.4.5. Legendre symbol for $-1$ and $2$.

a) For any odd prime $p$ we have
\[
\left( \frac{-1}{p} \right) = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{4}; \\
-1 & \text{if } p \equiv 3 \pmod{4}.
\end{cases}
\]

b) For any odd prime $p$ we have
\[
\left( \frac{2}{p} \right) = \begin{cases} 
1 & \text{if } p \equiv \pm 1 \pmod{8}; \\
-1 & \text{if } p \equiv \pm 3 \pmod{8}.
\end{cases}
\]

PROOF. a) Suppose $p \equiv 1 \pmod{4}$, say $p = 1 + 4k, k \in \mathbb{N}$. Then $(-1)^{(p-1)/2} = (-1)^{2k} = 1$ and so by Euler’s criterion, $-1$ is a quadratic residue (mod $p$). If $p \equiv 3 \pmod{4}$, say $p = 3 + 4k$, then $(-1)^{(p-1)/2} = (-1)^{2k+1} = -1$, so $-1$ is a quadratic non-residue.

b) Suppose that $p \equiv 1 \pmod{4}$, and so $p \equiv 1$ or $5 \pmod{8}$. We calculate $2^{(p-1)/2}$ (mod $p$) two different ways. Set
\[
Q = 2 \cdot 4 \cdot 6 \cdots (p - 1).
\]
First note that $Q = 2^{(p-1)/2}((p-1)/2)!$. Also, noting that $\frac{p-1}{2}$ is even, we have
\[
Q = \left( \frac{2 \cdot 4 \cdots p - 1}{2} \right) \left( \frac{p+3}{2} \cdots (p-1) \right) \\
\equiv \left( \frac{2 \cdot 4 \cdots p - 1}{2} \right) \left( \frac{-(p-3)}{2} \cdots (-5)(-3)(-1) \right) \quad \text{(mod } p) \\
\equiv (-1)^{\frac{p-1}{4}} \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdots \left( \frac{p-3}{2} \right) \left( \frac{p-1}{2} \right) \quad \text{(mod } p).
\]
Equating the two expressions for $Q$ and canceling the $((p-1)/2)!$ we obtain
\[
2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \quad \text{(mod } p).
\]
If $p \equiv 1 \pmod{8}$ then the RHS = 1, while if $p \equiv 5 \pmod{8}$ then RHS = -1. The formula for $\left( \frac{2}{p} \right)$ then follows from Euler’s criterion.
Next, suppose that \( p \equiv 3 \mod 4 \), so that \( \frac{p-3}{2} \) is even. Then
\[
Q = \left( 2 \cdot 4 \ldots \frac{p-3}{2} \right) \left( \frac{p+1}{2} \ldots (p-1) \right) \\
\equiv \left( 2 \cdot 4 \ldots \frac{p-3}{2} \right) \left( -\frac{(p-1)}{2} \ldots (-5)(-3)(-1) \right) \pmod{p} \\
\equiv (-1)^{\frac{p+1}{2}} \left( \frac{p-1}{2} \right)! \pmod{p}
\]
and so
\[
2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.
\]
If \( p \equiv 3 \mod 8 \) then RHS = -1, while if \( p \equiv 7 \mod 8 \) then RHS = 1, completing the proof.

\[\square\]

### 5.5. Quadratic Reciprocity

Consider the two congruences \( x^2 \equiv 3 \mod 1009 \) and \( x^2 \equiv 1009 \mod 3 \).

Which one is easier to solve? Since \( 1009 \equiv 1 \mod 3 \), the second congruence is just \( x^2 \equiv 1 \mod 3 \) which has solutions \( x \equiv \pm 1 \mod 3 \). Does knowledge of this give me any information about the first congruence, which cannot be simplified? Is there any relationship between these two congruences? To address the solvability of the first congruence we must calculate \( \left( \frac{3}{1009} \right) \). We’ve already shown that \( \left( \frac{1009}{3} \right) = 1 \), but does this reveal any information about \( \left( \frac{3}{1009} \right) \)? Euler and Lagrange observed a beautiful relationship between these two quantities, called the law of quadratic reciprocity. It says that if \( p, q \) are distinct odd primes then
\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}
\]
unless \( p \equiv q \equiv 3 \mod 4 \), in which case \( \left( \frac{p}{q} \right) = -\left( \frac{q}{p} \right) \). Thus, for our example above we conclude that \( \left( \frac{3}{1009} \right) = 1 \).

**Example 5.5.1.** Let’s investigate the relationship between \( \left( \frac{p}{q} \right) \) and \( \left( \frac{q}{p} \right) \) for various primes \( p \). As noted above, calculating \( \left( \frac{p}{q} \right) \) is easy. To calculate \( \left( \frac{3}{p} \right) \) we use Euler’s criterion (part (i) of the preceding theorem) and a calculator.

\[
\begin{array}{cccccccccccc}
 p & 5 & 7 & 11 & 13 & 17 & 19 & 23 & 29 & 31 & 37 & 41 & 43 \\
\left( \frac{p}{5} \right) & -1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\
\left( \frac{5}{p} \right) & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1
\end{array}
\]

Note that if \( p \equiv 1 \mod 4 \) then the two values are equal while if \( p \equiv 3 \mod 4 \) they have opposite signs.

**Example 5.5.2.** Let’s do the same thing for \( \left( \frac{q}{p} \right) \) and \( \left( \frac{p}{q} \right) \) for various primes \( p \).

\[
\begin{array}{cccccccccccc}
 p & 3 & 7 & 11 & 13 & 17 & 19 & 23 & 29 & 31 & 37 & 41 & 43 \\
\left( \frac{3}{p} \right) & -1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 \\
\left( \frac{p}{3} \right) & -1 & -1 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1
\end{array}
\]

We see that the values are identical in this case!
By studying further examples of this type you will discover that whenever we start with a prime \( q \) of the form \( q \equiv 3 \) (mod 4) we get the behavior of the first example (where \( q = 3 \)), and whenever it is of the form \( q \equiv 1 \) (mod 4), we get identical values as in the second example (where \( q = 5 \)). This leads us to formulate the Law of Quadratic Reciprocity.

**Theorem 5.5.1.** Law of Quadratic Reciprocity. For any odd primes \( p, q \), \((\frac{p}{q}) = (\frac{q}{p})\) unless \( p \equiv q \equiv 3 \) (mod 4), in which case \((\frac{p}{q}) = - (\frac{q}{p})\). Equivalently, \((\frac{p}{q}) = (\frac{q}{p}) (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}\).

There are many proofs of quadratic reciprocity. Gauss was the first to prove it, and over his life he published six different proofs. I will let you read the proof of theorem in the textbook if you are interested. It is considerably more involved than any proof we have done this semester. Our interest here is in using the law for evaluating Legendre symbols.

**Example 5.5.3.** Find \((\frac{7}{1009})\). Since \( 1009 \equiv 1 \) (mod 4) we have \((\frac{7}{1009}) = 1\).

**Example 5.5.4.** Find \((\frac{227}{137})\), noting that \( 137 \) is a prime and that \( 137 \equiv 1 \) (mod 8),
\[
(\frac{227}{137}) = (\frac{90}{137}) = (\frac{9}{137}) (\frac{10}{137}) = (\frac{10}{137}) = (\frac{2}{137}) (\frac{5}{137}) = (\frac{5}{137}) = (\frac{137}{5}) = (\frac{2}{5}) = -1.
\]

**Corollary 5.5.1.** The Legendre symbol for 3. For any odd prime \( p \) we have \((\frac{3}{p}) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{12}; \\ -1, & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}\)

**Proof.** Suppose that \( p \equiv 1 \) (mod 4). Then by quadratic reciprocity \((\frac{3}{p}) = (\frac{p}{3})\). Since 1 is the unique quadratic residue (mod 3), we see that if \( p \equiv 1 \) (mod 3), \((\frac{3}{p}) = 1\) and if \( p \equiv 2 \) (mod 3) then \((\frac{3}{p}) = -1\). Now by CRT, if \( p \equiv 1 \) (mod 4) and \( p \equiv 1 \) (mod 3) then \( p \equiv 1 \) (mod 12), while if \( p \equiv 1 \) (mod 4) and \( p \equiv 2 \) (mod 3) then \( p \equiv 5 \) (mod 12).

Next, suppose that \( p \equiv 3 \) (mod 4). Then by quadratic reciprocity \((\frac{3}{p}) = -(\frac{p}{3})\) which equals -1 if \( p \equiv 1 \) (mod 3), and 1 if \( p \equiv 2 \) (mod 3). Now, by CRT if \( p \equiv 3 \) (mod 4) and \( p \equiv 1 \) (mod 3) then \( p \equiv 7 \) (mod 12), while if \( p \equiv 3 \) (mod 4) and \( p \equiv 2 \) (mod 3) then \( p \equiv 11 \) (mod 12).

**5.6. Representing primes as sums of two squares**

When can a prime \( p \) be expressed as a sum of two squares. It is easy to see that if \( p \) is odd and \( p = a^2 + b^2 \), then since \( a^2 \equiv 0 \) or 1 (mod 4), we must have \( p \equiv 1 \) (mod 4). Test such \( p \): 5 = 1\(^2 + 2\(^2\), 13 = 2\(^2 + 3\(^2\), 17 = 1\(^2 + 4\(^2\), 29 = 5\(^2 + 2\(^2\),\,

It is reasonable to conjecture the following result

**Theorem 5.6.1.** Let \( p \) be an odd prime. Then \( p \) is a sum of two squares if and only if \( p \equiv 1 \) (mod 4).
Proof. Suppose that \( p \equiv 1 \pmod{4} \). Then \( \left( \frac{-1}{p} \right) = 1 \), so there exists a \( u \in \mathbb{Z} \) with \( u^2 \equiv -1 \pmod{p} \). Consider the set of integers of the form \( x + uy \) with \( x, y \in [0, \sqrt{p}] \cap \mathbb{Z} \). Since there are \((\sqrt{p} + 1)^2 > p \) choices for \((x, y)\), there must exist, by the pigeonhole principle, distinct \((x_1, y_1) \neq (x_2, y_2)\) with

\[
x_1 + uy_1 \equiv x_2 + uy_2 \pmod{p}, \text{ that is, } (x_1 - x_2) \equiv u(y_2 - y_1) \pmod{p}.
\]

Set \( a = x_1 - x_2 \), \( b = y_1 - y_2 \). Then \(|a| < \sqrt{p}, |b| < \sqrt{p} \) and \( a \equiv ub \pmod{p} \). Therefore \( a^2 + b^2 \equiv (1 + u^2)b^2 \equiv 0 \pmod{p} \) and \( a^2 + b^2 < 2p \). Furthermore, since \((x_1, y_1) \neq (x_2, y_2)\), \( a^2 + b^2 > 0 \). Thus \( a^2 + b^2 = p \). \( \square \)
Axioms for the set of Integers $\mathbb{Z}$

We shall assume the following properties as axioms for the set of integers.

1] **Addition Properties.** There is a binary operation $+$, called addition, on $\mathbb{Z}$ satisfying

- **Addition is well defined.** That is, given any two integers $a, b$, $a + b$ is uniquely defined. Thus, if $a = b$ and $c = d$ then $a + c = b + d$, $c + a = d + b$, $a + d = b + c$, $d + a = c + b$. In particular, if $a = b$ then $a + c = b + c$ and $c + a = c + b$ for any integer $c$. (We sometimes call this the substitution law.)

- **The set of integers is closed under addition.** For any $a, b \in \mathbb{Z}$, $a + b \in \mathbb{Z}$.
  - a) **Addition is commutative.** For any $a, b \in \mathbb{Z}$, $a + b = b + a$.
  - b) **Addition is associative.** For any $a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$.
  - c) **There is a zero element** $0 \in \mathbb{Z}$, satisfying $0 + a = a = a + 0$ for any $a \in \mathbb{Z}$.
  - d) **For any** $a \in \mathbb{Z}$, **there exists an additive inverse** $-a \in \mathbb{Z}$ satisfying $a + (-a) = 0 = (-a) + a$.

Note: Axioms $\alpha$ and $\beta$ are actually part of the definition of a binary operation and so they often are not included in the list of axioms. A binary operation on $\mathbb{Z}$ is just a function from the set of ordered pairs of integers into $\mathbb{Z}$.

Definition: Subtraction in $\mathbb{Z}$ is defined by $a - b = a + (-b)$ for $a, b \in \mathbb{Z}$.

2] **Multiplication Properties.** There is an operation $\cdot$ (or $\times$) on $\mathbb{Z}$ satisfying,

- **Multiplication is well defined.** That is, given any two integers $a, b$, $a \cdot b$ is uniquely defined. Thus, if $a = b$ then $ac = bc$ and $ca = cb$ for any integer $c$. (Also, if $a = b$ and $c = d$ then $ac = bd$, $ca = db$, $ad = bc$, $da = cb$. This is also sometimes called the substitution law.)

- **$\mathbb{Z}$ is closed under multiplication.** For any $a, b \in \mathbb{Z}$, $a \cdot b \in \mathbb{Z}$.
  - a) **Multiplication is commutative.** For any $a, b \in \mathbb{Z}$, $ab = ba$.
  - b) **Multiplication is associative.** For any $a, b, c \in \mathbb{Z}$, $(ab)c = a(bc)$.
  - c) **There is an identity element** $1 \in \mathbb{Z}$ satisfying $1 \cdot a = a = a \cdot 1$ for any $a \in \mathbb{Z}$.

3] **Distributive property.** This is the one property that combines both addition and multiplication. For any $a, b, c \in \mathbb{Z}$, $a(b + c) = ab + ac$. One can deduce the additional distributive laws, $(a + b)c = ac + bc$, $a(b - c) = ab - ac$ and $(a - b)c = ac - bc$ from the other axioms.

4] **Trichotomy Principle.** The set of integers can be partitioned into three disjoint sets, $\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}$, where
\[ N = \{1, 2, 3, \ldots \} = \text{Natural Numbers} = \text{Positive Integers}, \]
\[-N = \{-1, -2, -3, \ldots \} = \text{Negative Integers}. \]
One then defines the inequalities > and < by saying \(a > b\) if \(a - b \in N\) and \(a < b\) if \(a - b \in -N\). Thus we get the Law of Trichotomy which states that for any two integers \(a, b\) exactly one of the following holds: \(a < b\), \(a = b\) or \(a > b\), (that is \(a - b \in -N, a - b = 0\) or \(a - b \in N\).)

5) **Positivity Axiom.** The sum of two positive integers is positive. The product of two positive integers is positive.

6) Discreteness Properties.
   a) **Well Ordering Property of \(N\).** Any nonempty subset of \(N\) has a smallest element. That is, given any nonempty subset \(S\) of natural numbers, there exists an element \(m \in S\) such that \(m \leq x\) for all \(x \in S\).

   b) **Principle of Induction.** Let \(S\) be a subset of \(N\) such that
   \[(i) \ 1 \in S \quad \text{and} \quad (ii) \ n \in S \implies n + 1 \in S.\]
Then \(S = N\).

   c) **Maximum Element Principle.** If \(S\) is a nonempty subset of integers bounded above, then \(S\) has a maximum element. (Note, we say a set of integers \(S\) is bounded above if there exists an integer \(M\), not necessarily in \(S\), such that \(x \leq M\) for all \(x \in S\).)
Further Properties of $\mathbb{Z}$.

The properties below can all be deduced from the axioms above. You may assume them whenever needed.

7] Cancellation law for addition: If $a + x = a + y$ then $x = y$.

Cancellation law for multiplication: If $ax = ay$ and $a \neq 0$ then $x = y$.

8] Additive inverses are unique, that is, if $a, b, c$ are integers such that $a + b = 0$ and $a + c = 0$ then $b = c$.

9] Zero multiplication property: $a \cdot 0 = 0$ for any $a \in \mathbb{Z}$.

10] Zero divisor property, (or integral domain property): If $ab = 0$ then $a = 0$ or $b = 0$.

11] Properties of negatives: $(-a)b = -(ab) = a(-b)$, $(-a)(-b) = ab$.

12] The product of two negative integers is positive.

13] “FOIL” Law (and all similar distributive laws): For any integers $a, b, c, d,$

$$(a + b)(c + d) = ac + ad + bc + bd.$$  

14] Genassocomm Law: General Associative-Commutative Law:

a) Addition: When adding a collection of $n$ integers $a_1 + a_2 + \cdots + a_n$, the numbers may be grouped in any way and added in any order. In particular, the sum $a_1 + a_2 + \cdots + a_n$ is well defined, that is, no parentheses are necessary to specify the order of operations.

b) Multiplication: When multiplying a collection of $n$ integers $a_1 a_2 \cdots a_n$, the numbers may be grouped in any way and multiplied in any order. In particular, the product $a_1 a_2 \cdots a_n$ is well defined, that is, no parentheses are necessary to specify the order of operations.

15] Binomial Expansion: For any integers $a, b$ and positive integer $n$ we have

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \cdots + b^n,$$

where $\binom{n}{k}$ is the binomial coefficient, $\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}$. In particular,

$$(a + b)^2 = a^2 + 2ab + b^2$$

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3.$$  

16] Standard Factoring formulas, such as $a^2 - b^2 = (a - b)(a + b),$ $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$ or

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}),$$

$$a^k + b^k = (a + b)(a^{k-1} - a^{k-2}b + \cdots - ab^{k-2} + b^{k-1}),$$

for any $k \in \mathbb{N}, k > 1$ for any odd $k \in \mathbb{N}$. 


APPENDIX B

A Little Bit of Logic for Math 506

\[ \exists \ \text{there exists} \quad \exists! \ \text{there exists a unique} \]
\[ \forall \ \text{for all} \quad \Rightarrow \ \text{implies} \]
\[ \Leftrightarrow \ \text{equivalent to} \quad \text{iff if and only if} \]

Let \( P, Q \) be statements and \( \sim P, \sim Q \) denote their negations (called “not \( P \)” and “not \( Q \)”.) For example, if \( P \) = “\( x \) is an integer” and \( Q \) = “\( x \) is a real number”. Then \( \sim P \) = “\( x \) is not an integer”, \( \sim Q \) = “\( x \) is not a real number”.

\( Q \Rightarrow P \) is called the converse of \( P \Rightarrow Q \).
\( \sim Q \Rightarrow \sim P \) is called the contrapositive of \( P \Rightarrow Q \).

The following are equivalent: (Consider the above example.)
\[ P \Rightarrow Q \quad (P \ \text{is true implies } Q \ \text{is true.}) \]
If \( P \) then \( Q \)  
(If \( P \) is true then \( Q \) is true.)
\[ P \ \text{only if } Q \quad (P \ \text{is true only if } Q \ \text{is true.}) \]
\[ P \ \text{is sufficient for } Q \]
\[ Q \ \text{is necessary for } P \]
\[ \sim Q \Rightarrow \sim P \quad (Q \ \text{false implies that } P \ \text{is false.}) \]
If \( \sim Q \) then \( \sim P \),  
(If \( Q \) is false then \( P \) is false.)

Proof by Contradiction. In order to prove \( P \Rightarrow Q \) one proves the equivalent statement \( \sim Q \Rightarrow \sim P \). Thus the proof starts by assuming \( Q \) is false, and ends with the conclusion that \( P \) is false.

The following are equivalent: (For example, let \( P = \{x^2 = 1\}, Q = \{x = \pm 1\} \).)
\[ P \Leftrightarrow Q \]
\[ P \ \text{if and only if } Q \]
\[ P \ \text{iff } Q \]
\[ P \ \text{is necessary and sufficient for } Q \]
\[ \sim P \Leftrightarrow \sim Q \]