Our Number Theory Textbook

Math 311: Fall 2015

December, 2015

Contents

1 Divisibility **2**
M. Gonsalves, L. Lewis . . . 2
1.1 Introduction . . . 2
1.2 Glossary of Terms . . . 2
1.3 Theorems . . . 3
1.4 Examples . . . 8

2 Primes **10**
A. Gorman, T. Maleski . . . 10
2.1 Introduction . . . 10
2.2 Glossary of Terms . . . 10
2.3 Theorems . . . 11
2.4 Examples . . . 14

3 Modularity **16**
M. Farrow and M. Harry . . . 16
3.1 Introduction . . . 16
3.2 Glossary of Terms . . . 17
3.3 Theorems . . . 17
3.4 Examples . . . 21

4 Order of a Natural Number **22**
B. Franjione, J. Matuk, A. Wobrak . . . 22
4.1 Introduction . . . 22
4.2 Glossary of Terms . . . 23
4.3 Theorems . . . 23
4.4 Examples . . . 28

5 Primitive Roots **30**
J. Pinaroc, A. Waldo, A. Cunningham . . . 30
5.1 Introduction . . . 30
5.2 Glossary of Terms . . . 30
5.3 Theorems . . . 30
5.4 Examples . . . 35

1 Divisibility

Marina Gonsalves, Lisa Lewis

1.1 Introduction

This chapter starts off with an introduction into some basic operations on integers as well as definitions that will be used throughout the entire book. The operations used in this chapter center around the definitions of divides, greatest common divisor (*gcd*), and relatively prime. The chapter starts off with defining divides as well as how to use the division algorithm. This definition is then used to establish proofs to conjectures 1.1 through 1.3. The use of the division algorithm is helpful in establishing the existence of quotients and remainders. Through understanding quotients, remainders, and the definition of divides, conjectures 1.4 and 1.5 are proved. An example at the end of the chapter uses the division algorithm to find integer solutions to a linear diophantine equation. The chapter proceeds next by defining greatest common divisor and relatively prime and how it can be useful in determining how integers relate and the existence of linear combinations of integers. Previously proven theorem 1.5 is used to establish a general procedure to find the greatest common divisor (*gcd*) of two integers. This procedure is known as the Euclidean algorithm. This algorithm can be used to find the *gcd* of the provided integers in example 2 in this chapter. Using our established procedure, we are able to work through and provide proofs to theorems involving the *gcd* of two integers. Previous theorems 1.1 through 1.6 involving the definition of divides are used to look at the linear combination of two integers and how they relate to the *gcd*. To conclude Chapter 1, proof to conjecture 1.13 is provided. This proof is crucial in determining all integer solutions to a linear diophantine equation.

1.2 Glossary of Terms

- An *axiom* is a universally accepted statement whose veracity does not require justification.
- A *theorem* is a unique statement whose veracity must be justified through a series of logical steps.
- A *series* is a series of logical steps by which a statement's truth value is verified.
- $\mathbb{Z}$ is the set of all integers, i.e. (...-1,0,1,2,...)
- $\mathbb{N}$ is the set of all natural numbers, i.e. (1,2,3,...)
- For any integer a,b, where b is nonzero, b *divides* a if there exists an integer c such that $a = c.b$, we denote this $b \mid a$.
- The *greatest common divisor* is the largest natural number that divides any two integers, a and b, denoted by $gcd(a, b)$ or sometimes (a, b) .

- *Relatively Prime* is when two nonzero integers are relatively prime if the greatest common divisor is 1.
- *The Euclidean Algorithm* is an algorithm used for finding the greatest common divisor of two numbers. There exist unique integers $a, b, n_1 and r_1$ where $gcd(a, b) = r_m$

1.3 Theorems

Theorem 1.1. *Let a, b and c be integers. If* $a \mid b$ *and* $a \mid c$ *then* $a \mid (b + c)$

Proof. Assume a, b and c are integers as well as $a \mid b$ and $a \mid c$. We will show that $a \mid (b + c)$. By definition of divides, $b = a.p$ and $c = a.q$ where $q, n \in \mathbb{Z}$. Therefore,

$$b + c = (ap) + (aq)$$

$$b + c = a(p + q)$$

By the closure properties of integers, $b + c = an$ where $n \in \mathbb{Z}$. Thus be the definition of divides, $a \mid (b + c)$ □

Theorem 1.2. *Let a, b and c be integers. If* $a \mid b$ *and* $a \mid c$*, then* $a \mid (b - c)$

Proof. Suppose a ,b and c are integers and $a \mid b$ and $a \mid c$. We will show that $a \mid (b-c)$. By definition of divides $b = ap$ and $c = aq$ where $p, q \in \mathbb{Z}$. Therefore,

$$b - c = (ap) - (aq)$$

$$b - c = a(p - q)$$

By the closure properties of integers, $b-c = an$ where $n \in \mathbb{Z}$. Thus by definition of divides, $a \mid (b - c)$ □

Theorem 1.3. *Let a, b and c be integers. If* $a \mid b$ *and* $a \mid c$*, then* $a \mid bc$

Proof. Let $a, band c \in \mathbb{Z}$. Assume $a \mid b$ and $a \mid c$. By definition there exists $p, q \in \mathbb{Z}$ such that $b = pa$ and $c = qa$. Consider

$$bc = pa.qa$$

$$bc = (pqa).a$$

By the closure properties of integers, $bc = an$ where $n \in \mathbb{Z}$. Thus $a \mid bc$ by definition of divides. □

Theorem 1.4. *Let* a, n, b *and* r *be integers. If* $a = nb + r$ *and* $k \mid a$ *and* $k \mid b$ *then* $k \mid r$.

Proof. Let a, n, b and $r \in \mathbb{Z}$. We will assume that $a = nb+r$, $k \mid a$, $k \mid b$ and will show that $k \mid r$. First consider $k \mid a$ and $k \mid b$ and will show that $k \mid r$. Consider $k \mid a$ and $k \mid b$. By definition of divides (1) $kt = a$ where $t \in \mathbb{Z}$. Similarly, we can say that (2) $kq = b$ where $q \in \mathbb{Z}$. By substitution (1) and (2) into this equation, we obtain:

$$kt = n(kq) + r$$
$$kt - nkq = r$$
$$kz = r$$

We now have that $kz = r$ where $z \in \mathbb{Z}$, by the closure properties of integers, therefore by definition of divides, $k \mid r$. □

Theorem 1.5. *Let a, b, n_1 and r_1 be integers with a and b not both 0. If $a = n_1 b + r_1$, then $(a, b) = (b, r_1)$.*

Proof. Let a, b, n_1 and r_1 be integers where a and b are both nonzero integers. We want to prove that if (1) $a = n_1 b + r_1$ then $(a, b) = (b, r_1)$. By the definition of *divides* and *greatest common divisor* we can say there exists an integer d such that (2) $a = dx$ and $b = dy$. By substituting equations (1) and (2).

$$dx = n_1 dy + r_1$$
$$dx - n_1 dy = r_1$$
$$d(x - n_1 y) = r_1$$
$$dz = r_1$$

Now we assume there is a $gcd(b, r_1)$ such that there exists an integer d where $r_1 = dx$ and $b = dy$. By substituting these two equations

$$a = n_1(dy) + (dx)$$
$$a = d(n_1 y + X)$$
$$a = dz$$

Thus there exists z such that $kz = r$ where $z \in \mathbb{Z}$, by the closure properties of integers.

Therefore we have established that $(a, b) = (b, r_1)$. □

Theorem 1.6. *Let a and b be integers. If $gcd(a, b) = 1$, then there exist integers x and y such that $ax + by = 1$*

Proof. Let $a, b \in \mathbb{Z}$ and $gcd(a, b) = 1$. By the Euclidean Algorithm, $a = n_1 b + r_1$, $b = n_2 r_1 + r_2$, $r_1 = n_3 r_2 + r_3$ and so on until $r_{m-2} = n_m r_{m-1} + r_m$, where $r_m = 1$. Note that the equation $r_{m-2} = n_m r_{m-1} + r_m$ can be written for any $k \in \mathbb{Z}$ where $3 \leq k \leq m$. By substitution,

$$1 = r_m = r_{m-2} - n_m r_{m-1}$$
$$1 = r_{m-2} - n_m(r_{m-3} - n_{m-1} r_{m-2})$$

Until r_1 is substituted at which point the equation can be written in integer terms of a and b, i.e. $1 = ax + by$ where $x, y \in \mathbb{Z}$ □

Theorem 1.7. *Let a and b be integers. If there exists integers x and y with ax+by = 1 ,then gcd(a,b) = 1*

Proof. Let $a, b, x, y \in \mathbb{Z}$ such that $ax + by = 1$ and let $gcd(a, b) = m$ where $m \in \mathbb{Z}$. We will show that $m = 1$. By the definition of divides we see that $m \mid a$ and $m \mid b$. Equivalently $a = mk$ and $b = ml$ where $k, l \in \mathbb{Z}$. Using the given equation, we can make substitutions for a and b such that,

$$mkx + mly = 1$$

$$m(kx + ly) = 1$$

$kx + ly$ is some integer, therefore $m \mid 1$. Since the only number that can divide 1 is 1, $m = 1$. Thus $gcd(a, b) = 1$ □

Theorem 1.8. *Let a and b be integers. Then gcd(a,b) = 1, if and only if there exists integers x and y such that ax + by = 1*

Proof. Let $a, b \in \mathbb{Z}$. First assume that $gcd(a, b) = 1$. By Theorem 1.6, we know that $\exists x, y \in \mathbb{Z}$ such that $ax + by = 1$. Now assume $\exists x, y \in \mathbb{Z}$ where $ax + by = 1$. By Theorem 1.7 we know $gcd(a, b) = 1$. Therefore $gcd(a, b) = 1$ if and only if there exists $x, y \in \mathbb{Z}$ such that $ax + by = 1$ □

Lemma 1.9. *If a = gcd(a,b) . m and b = gcd(a,b) . l then the gcd(m,l) = 1*

Proof. Let $a = gcd(a, b).m$ and $b = gcd(a, b).l$ where $m, l \in \mathbb{Z}$. There exists some integer d such that $gcd(m, l) = d$. By definition $d.r = m$ and $d.k = l$ where $k, r \in \mathbb{Z}$. By substitution, $gcd(a, b).dr = a$ and $gcd(a, b).dk = b$. Thus, $gcd(a, b)d \mid a$ and $gcd(a, b)d \mid b$. By definition of gcd, $gcd(a, b)d \mid gcd(a, b)$ therefore, $d = 1$ □

Theorem 1.10. *Let a and b be integers. There exist integers x and y such that* $ax + by = gcd(a, b)$.

Proof. By the Euclidean Algorithm, $a = bq_1 + r_1$, $b = r_1q_2 + r_2$, and so on until $r_n = gcd(a, b)$. Then $r_(n-2) = r_(n-1)q_n + r_n$, which can be rewritten as $r_n = r_(n-2) - r_(n-1)q_n$. This is true for all $r_k, 3 < k < n$, since $r_3 = r_1 - r_2q_3$. By substitution, $r_n = r_(n-2) - (r_(n-3) - r_(n-2)q_(n-1))q_n$ and so on until r_1 is substitute, at which point the equation is rewritten in terms of a and b, i.e. $ax + by = r_n, x, y$ are elements of r_n □

Theorem 1.11. *Let a and b be integers. Then gcd(*$\frac{a}{gcd(a,b)}, \frac{b}{gcd(a,b)}$*)=1.*

Proof. Let a and b be integers. By theorem 1.9, there exists integers x and y such that

$$ax + by = gcd(a, b). \tag{1}$$

Thus,

$$\frac{a}{gcd(a, b)}x + \frac{b}{gcd(a, b)}y = \frac{gcd(a, b)}{gcd(a, b)} = 1. \tag{2}$$

Therefore it follows from theorem 1.7 that gcd($\frac{a}{gcd(a,b)}, \frac{b}{gcd(a,b)}$)=1. □

Theorem 1.12. *Let a, b and c be integers. If $a|bc$ and $gcd(a,b) = 1$, then a* mod *c.*

Proof. Let a, b and c be integers and assume that $a \mod bc$ and $gcd(a,b) = 1$. By theorem 1.8 it follows that if the $gcd(a,b) = 1$ then there exists integers x and y such that $ax + by = 1$. Thus, by the definition of divides, $bc = aq$ where q is an integer. It follows that

$$\begin{aligned} ax + by &= 1 \\ acx + bcy &= c; bc = aq \\ acx + aqy &= c \\ a(cx + qy) &= c. \end{aligned}$$

Thus, $cx + qy$ is an integer and $a \mod c$ □

Theorem 1.13. *Given integers a, b and c, there exist integers x and y that satisfy the equation $ax + by = c$ if and only if $gcd(a,b) \mid c$.*

Proof. We will first prove in the forward direction whereby we can assume that $ax + by = c$ and we want to show that $gcd(a,b) \mid c$. From the definition of gcd(a,b) we know $gcd(a,b) \mid a$ and also $gcd(a,b) \mid b$ therefore we have that

$$a = gcd(a,b)m$$

and

$$b = gcd(a,b)n$$

By substitution we can then obtain that

$$gcd(a,b)mx + gcd(a,b)ny = c$$

$$gcd(a,b)(mx + ny) = c$$

By closure properties of integers we can say there exist an integer k such that $gcd(a,b)k = c$ Thus this is equivalent to saying the $gcd(a,b) \mid c$ □

Theorem 1.14. *If $x_0 + y_0$ are solutions to the linear diophantine equation $ax + by = c$, then all other solutions are given by*

$$x = x_0 + (\frac{b}{gcd(a,b)})t$$

and

$$y = y_0 - (\frac{a}{gcd(a,b)})t$$

where t is an arbitrary integer.

Proof. To start the proof we need to show that the above equations have given solutions. Therefore we plug the values of integers x and y into the function $ax + by = c$

$$a(x_0 + \frac{b}{gcd(a,b)}t) + b(y_0 - \frac{a}{gcd(a,b)}t)$$

We then obtain that $ax_0 + by_0 = c$ Now we need to show that and two solutions is actually of the form in the theorem.

$$ax_1 + b_y 1 = ax_0 + by_0$$

$$a(x_1 - x_0) = b(y_0 - y_1)$$

$$\frac{a}{gcd(a,b)}(x_1 - x_0) = \frac{b}{gcd(a,b)}(y_0 - y_1)$$

Using Theorem 1.10 we can say that

$$\frac{a}{gcd(a,b)} \mid \frac{b}{gcd(a,b)}(y_0 - y_1)$$

$$and vice versa that$$

$$\frac{b}{gcd(a,b)} \mid \frac{a}{gcd(a,b)}(x_1 - x_0)$$

Using Theorem 1.11 we say that

$$\frac{a}{gcd(a,b)} \mid (y_0 - y_1)$$

and

$$\frac{b}{gcd(a,b)} \mid (x_1 - x_0)$$

By the definition of gcd,

$$y_0 - y_1 = \frac{a}{gcd(a,b)}l$$

$$y_1 = y_0 - \frac{a}{gcd(a,b)}l$$

$$x_1 - x_0 = \frac{b}{gcd(a,b)}l$$

$$x_1 = x_0 - \frac{b}{gcd(a,b)}l$$

□

1.4 Examples

Example 1. *Suppose that the sequence a_n of numbers defined by $a_1 = 1$, $a_2 = 2$, $a_3 = 3$ and $a_n = a_{n-1} + a_{n-2} + a_{n-3}$ for all $n \geq 4$. Show that $a_n < 2$*

Proof. Using mathematical induction, we will show for each natural number n, we let $P(n)$ be the function $a_n = a_{n-1} + a_{n-2} + a_{n-3}$. We will show the base case is true for $P(1)$ such that,

$$a_2 = a_1 + a_0 + a_{-1}$$

$$a_2 > a_1$$

$$2 > 1$$

Thus the base case holds true. Now for the inductive step, we prove that for all $k \in \mathbb{N}$, if $P(k)$ is true then $P(k+1)$ is also true. So by assuming $P(k)$ is true we show that,

$$a_k < 2^k$$

Also this shows that $a_k = a_{k-1} + ak - 2 + ak - 3$. Now we want to prove that $P(k+1)$ is true, such that $a_{k+1} < 2^{k+1}$. We know that $a_{k+1} = a_k + a_{k-1} + ak - 2$. Thus from our inductive step we can say that $a_{k+1} < 2^k + a_{k-1} + a_{k-2}$. From our solution in our inductive step we know that $a_k = a_{k-1} + ak - 2 + ak - 3$. Using algebra,

$$a_k - a_{k-3} = a_{k-1} + a_{k-2}$$

Now by substitution we can say that

$$a_{k+1} < 2^k + a^k - a^{k-3}$$

Equivalently this is $a_{k+1} < 2^k + 2^k$. Using algebra $a_{k+1} < 2(2^k)$ thus $a_{k+1} < 2^{k+1}$. This proves that if $P(k)$ is true then $P(k+1)$ is true. Our inductive step has been established and so by the Principle of Mathematical induction, $a_n < 2^n$

□

Example 2. *Use the Euclidean algorithm to find the gcd(175,24).*

$$175 = 24n + r \tag{3}$$

$$24 = 7n_2 + r_2 \tag{4}$$

$$7 = 3n_3 + r_3 \tag{5}$$

$$3 = 1n_4 + r_4 \tag{6}$$

Note that for (3), the quotient n=7 and remainder r=7 so these values must be plugged back in and result in equation (4). The remainder r=3 in (4) so the process must be repeated until the remainder r=0. Hence equation (6). The

gcd(175,24) equals the quotient in the equation where the remainder is zero. Thus gcd(175,24)=1. Now find the gcd(256,10).

$$\begin{aligned} 256 &= 10n + r && (7)\\ 10 &= 6n_2 + r_2 && (8)\\ 6 &= 4n_3 + r_3 && (9)\\ 4 &= 2n_4 + r_4 && (10) \end{aligned}$$

Because n=2 and r=0 in equation (10), gcd(256,10)=2.

Example 3. *Find integers x and y such that 175x + 24y = 1.*

$$\begin{aligned} 175 &= (24)7 + 7\ ;\ 7 = 175 - 7(24) && (11)\\ 24 &= (7)3 + 3\ ;\ 3 = 24 - 3(7) && (12)\\ 7 &= (3)2 + 1\ ;\ 1 = 7 - 2(3) && (13) \end{aligned}$$

From the above equations integers x and y can be derived using substitution.

$$\begin{aligned} 1 &= 175 - 7(24) - 2(24 - 3(7)) && (14)\\ 1 &= 175 - 9(24) + 6(7) && (15)\\ 1 &= 175 - 9(24) + 6(175 - 7(24)) && (16)\\ 1 &= 7(175) - 51(24) && (17) \end{aligned}$$

Thus the solutions are x=7 and y=-51.

2 Primes

Ashleigh Gorman, Taryn Maleski

2.1 Introduction

This chapter introduces the concepts of prime numbers and how prime numbers exhibits different characteristics than composite numbers. In this chapter, we will define what a prime is in additional to composite, prime factorization, arithmetic progression, and factorial. These new definitions will allow us to explore different ideas and problems in number theory that are specific to the prime numbers. We will notice that throughout this chapter that the theorems are building blocks for one another in the sense that theorem 2.2 will be proven true based upon the result from theorem 2.1. It is crucial to be able to recall the definitions and results from Chapter 1 as they will also be used as a foundation to the 12 proofs in this chapter. Throughout Chapter 2, we will continue to rely on the definition of divides and greatest common divisors in order to conclude the results. These proofs explore how primes can be utilized in number theory with the biggest result being that there are infinitely many primes. Using previous theorems from this chapter, we can show that there are infinitely many prime numbers in two lines. In this chapter, we will utilize various techniques like proof by cases and contradiction. For example, conjecture 2.1 will be proved using proof by cases with case one being p does not divide a, and then the second case explaining if p does divide a. Contradiction can be used in theorem 2.9. We can assume that a does divide $b + 1$ and reach a false statement at the end. Most importantly, we are able to use the results from theorem 2.11 to show that there are infinitely many prime numbers. We can also prove there are infinitely many primes in specific forms say $4k + 3$ that we will prove in the examples. Later, we will be able to recall this information in future chapters in order to prove the veracity of other problems.

2.2 Glossary of Terms

- A *prime* is a natural number greater than 1 whose divisors are itself and 1.
- A *composite* is an integer other than 1 which is not prime.
- A *prime factorization* of a natural number, n, is n written as a product of primes.
- Given two integers a and b, an *arithmetic progression* is given by

$$a, a + b, a + 2b, a + 3b, ...$$

.

- Given a natural number, n, its *factorial* denoted $n!$ is

$$n! = n(n-1)(n-2)...3 \cdot 2 \cdot 1$$

given integers a, b and a natural number m, we say a is *congruent* to b modulo m if m divides $a - b$, denoted

$$a \equiv b \mod n$$

.

2.3 Theorems

Theorem 2.1. *If p is a prime number and $p|ab$ then $p|a$ or $p|b$.*

Proof. We will assume that p is a prime number and $p \mid ab$ to show that $p \mid a$ or $p \mid b$. First, we will suppose that $p \mid ab$ and $p \nmid a$, that means we must show $p \mid d$. Since $p \nmid a$, $gcd(p, a) = 1$. By theorem 1.11, we know that $p \mid b$. On the other hand, suppose that $p \mid a$. Then we are done. □

Theorem 2.2. *If p is a prime number and $p|a_1 \cdots a_k$ then $p|a_i$ for some $1 \leq i \leq k$.*

Proof. Assume that $p \mid a_i \cdots a_k$ where p is a prime number. We want to show that $p \mid a_i$ for some $1 \leq i \leq k$. By theorem 2.1, $p \mid a_1$ or $p \mid a_2 \cdots a_k$. If $p \mid a$, we are done, otherwise $p \mid a_2 \cdots a_k$ where the $gcd(p, a) = 1$ and we repeat this process until $p \mid a_k$. This shows that there exists and elementa_k that is divisible by p.By the commutative property of multiplication, $a_k = a_i$ for $1 \leq i \leq k$. □

Theorem 2.3. *If $p, q_1, ..., q_k$ are prime numbers and $p|q_1 \cdots q_k$ then $p = q_i$ for some $1 \leq i \leq k$.*

Proof. Let $p, q_1, ..., q_k$ be prime, and assume that $p \mid q_1 \cdots q_k$. By theorem 2.2, $p \mid q_i$ for some $1 \leq i \leq k$. Because q_i is prime, it's only divisors are 1 and itself. Because p is prime, $p \neq 1$. Thus $p = q_i$ for some $1 \leq i \leq k$. □

Theorem 2.4. *A natural number n is prime if an only if for all primes $p \leq \sqrt{n}$, p does not divide n.*

Proof. Let $n \in \mathbb{N}$ and p be an arbitrary prime integer. First, we will show that if n is prime, then $p \leq \sqrt{n}$ and $p \nmid n$. Since we know n is prime, then by definition of a prime number, it's only divisors are 1 and itself. Thus we are done and have proved this direction of the statement.

Now we must prove the other direction. If for an arbitrary prime $p \leq \sqrt{n}$ and $p \nmid n$, then n is prime. To do so, we will prove the contrapositive of this statement. Now the statement reads, if n is composite, then there exists some $p \leq \sqrt{n}$ and $p \mid n$. By the Fundamental Theorem of Arithmetic, we know that n

is a prime factorization. This means that $n = p_1 \cdots p_k$. By way of contradiction, assume that all $p > \sqrt{n}$. Thus,

$$\begin{aligned} p_1 &> \sqrt{n} \\ p_1 \cdot p_2 &> n \\ p_1 \cdots p_k &> n. \end{aligned}$$

We have reached a contradiction. We stated through the fundamental theorem of arithmetic that $n = p_1 \cdots p_k$ and that $p_i > \sqrt{n}$. So, through contradiction, we have proven the contrapositive. Thus n is prime. □

Theorem 2.5. *Let a and b be natural numbers greater than 1 and let $p_1^{r_1} p_2^{r_2} \cdot \cdot p_m^{r_m}$ be the unique prime factorization of a and let $q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$ be the unique prime factorization of b. Then $a|b$ if and only if for all $i \leq m$ there exists a $j \leq s$ such that $p_1 = q_j$ and $r_i \leq t_j$.*

Proof. Let $a, b \in \mathbb{N}$ with $a, b \leq 1$. Let $p_1^{r_1} \cdots p_m^{r_m}$ be the unique prime factorization of a and let $q_1^{t_1} \cdots q_s^{t_s}$ be the unique prime factorization of b. Assume that $a \mid b$. By definition, $(p_1^{r_1} \cdots p_m^{r_m})n = q_1^{t_1} \cdots q_s^{t_s}$.By factoring q_n from the left hand side, it follows that $p_i \mid q_1^{t_1} \cdots q_s^{t_s}$. It follows for all p_i, there exists a q such that $p_i = q_j$ by theorem 2.3. By way of contradiction, assume that $r_i > t_j$. Thus $p_i^{r_i} > q_j^{t_j}$. By a harmless reordering of terms we know that this leads us to $p_1^{r_1} \cdots p_m^{r_m} > q_1^{t_1} \cdots q_k^{t_k}$ for some $k \leq s$. Thus $r_i \leq t_j$. Conversely, assume for all $i \leq m$ there exists $j \leq s$ such that $p_i = q_j$ where $r_i \leq t_j$. If follows that $p_i^{r_1} \leq q_j^{t_j}$ for all $i \leq m$. Moreover, $p_1^{r_1} \cdots p_m^{r_m} \leq q_1^{t_1} \cdots q_m^{t_m}$. Thus, there exists l such that $(p_1^{r_1} \cdots p_m^{r_m})l = q_1^{t_1} \cdots q_k^{t_k}$. Let $n = q_k^{t_k} \cdots q_s^{t_s}$. It follows that $a(ln) = b$. Thus we can conclude that $a \mid b$ □

Theorem 2.6. *If a, b and n are natural numbers and $a^n|b^n$ then $a|b$.*

Proof. We know that $a^n \mid b^n$ such that a, b, and $n \in \mathbb{N}$. We want to prove that $a \mid b$. By the fundamental theorem of Arithmetic, we will write a and b as a product of primes such that,

$$a = p_1^{a_1} ... p_k^{a_k} \qquad\qquad b = q_1^{B_1} ... q_r^{B_r}.$$

for $1 \leq i \leq k$ and $1 \leq j \leq r$. So,

$$a^n = p_1^{na_1} ... p_k^{na_k} \qquad\qquad b^n = q_1^{nB_1} ... q_1^{nB_r}.$$

Since $a^n \mid b^n$, then $p_1 = q_i$ where $1 \leq i \leq k$ and $1 \leq j \leq r$ by theorem 2.5. Thus $na_i \leq nB_j$. So $a_i \leq B_j$. Using theorem 2.5, since $a_i \leq B_j$ and $p_1 = q_i$, then $a \mid b$. □

Theorem 2.7. *Let a, b and c be integers. If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$ then $\gcd(a, bc) = 1$.*

Proof. Given that a, b, $c \in \mathbb{Z}$, we will assume that $gcd(a,b) = 1$, $gcd(a,c) = 1$, and show that $gcd(a,bc) = 1$. By theorem 1.6, we can say that $ax_by = 1$ and that $ax_1 + cy_1 = 1$, where x,y,x_1 $y_1 \in \mathbb{Z}$. By multiplying both sides of the equation by each other, we obtain

$$\begin{aligned}(ax + by)(ax_1 + cy_1) &= 1^2\\ a^2xx_1 + axcy_1 + abxy + bcyy_1 &= 1\\ a(axx_1 + xcy_1 + bxy) + bcyy_1 &= 1.\end{aligned}$$

Therefore, by theorem 1.7, $gcd(a,bc) = 1$. □

Theorem 2.8. *Let a, b, u and v be integers. If* $\gcd(a,b) = 1$ *and $u|a$ and $v|b$ then* $\gcd(u,v) = 1$.

Proof. Let a, b, u, $v \in \mathbb{Z}$. By definition of divides, we know that $a = u \cdot m$ and $b = v \cdot n$ where m, $n \in \mathbb{Z}$. Also, by theorem 1.6, when the $gcd(a,b) = 1$, we can say that $ax + by = 1$ where x, $y \in \mathbb{Z}$. Now we will substitute in for a and b like so,

$$\begin{aligned}u \cdot m \cdot x + v \cdot n \cdot y &= 1\\ u \cdot (mx) + v \cdot (ny) &= 1.\end{aligned}$$

Since this equation is now in the form of $ax + by = 1$, by theorem 1.7 we can conclude that $gcd(u,v) = 1$.

□

Theorem 2.9. *Let a and b be integers where $a \neq 1$. If $a|b$ then $a \nmid b + 1$.*

Proof. We will assume $a \mid b$ where a, $b \in \mathbb{Z}$ and $a \neq 1$ to show that $a \nmid b + 1$. By way of contradiction, assume $a \mid b + 1$. If $a \mid b$ and $a \mid b + 1$, the $b = aq$ and $b = ak - 1$ where a, $k \in \mathbb{Z}$. If we set the equations equal to each other, we have

$$\begin{aligned}aq &= ak - 1\\ 1 &= a(k - q).\end{aligned}$$

This shows $a \mid 1$, so $a = 1$. Thus we have reached a contradiction. Therefore $a \nmid b + 1$. □

Theorem 2.10. *Let k be a natural number. Then there exists a natural number n which is not divisible by any natural number between k and 1.*

Proof. Let $k \in \mathbb{N}$. Look at $k! = 1 \cdot 2 \cdot 3 \cdots k$. We know that any number between 1 and k divides $k!$. According to theorem 2.9, if all numbers between 1 and k divide $k!$ divide $k! + 1$. Thus, there exists a natural number $n = k! + 1$ which is not divisible by any number between k and 1. □

Theorem 2.11. *Let k be a natural number. Then there exists a prime larger than k.*

Proof. Let $k \in \mathbb{N}$. We will show that there exists a prime N such that $n > k$. By theorem 2.10, there exits and element in the natural numbers which is not divisible by any number between k and 1. Let $n = k! + 1$. This means that every natural number between k and 1 does not divide n. By the fundamental theorem of arithmetic, either n is prime, or it can be written as a finite product of primes. If n is prime, we are done because $n = K! + 1 > k$. If n is not prime, this means a prime number m divides n where $m > k$ since all numbers between k and 1, specifically all primes, do not divide n. Therefore, there exists a prime number greater than k. □

Theorem 2.12. *There are infinitely many prime numbers.*

Proof. By theorem 2.11, for any $k \in \mathbb{N}$ there exists a prime larger than k. Therefore, there are infinitely many prime numbers. □

2.4 Examples

Example 4. *Find the* $\gcd(61^{88} \cdot 13^5 \cdot 3^{12} \cdot 19^5, 13^3 \cdot 11^4 \cdot 7^2 \cdot 19^{97})$. *Is it better to use the division algorithm or another method?*

For this example, we are given the prime factorization of two numbers and are asked to determine the greatest common divisors of the two natural numbers. Since the natural numbers are represented as a product of prime numbers, we do not need to utilize the division algorithm. Notice that there the values 13 and 19 are both values in the prime factorization of these values. Thus, both 13 and 19 will divide both of these values. Since 19 is greater than 13, the $\gcd(61^{88} \cdot 13^5 \cdot 3^{12} \cdot 19^5, 13^3 \cdot 11^4 \cdot 7^2 \cdot 19^{97}) = 19$.

Example 5. *Use a prime factorization method to find the factors of the following numbers:*

(a) 28

(b) 425

(c) 612

(d) 877

Determine which of the above values are prime and which are composite.

The way we find numbers in elementary school is through a prime factorization tree. There is another way that we can go about these items through the use of writing them out as equations.

(a) 28

$$28 = 14 \cdot \mathbf{2}$$
$$14 = \mathbf{7} \cdot \mathbf{2}$$

Thus the prime factorization of 28 is $2^2 \cdot 7$.

(b) 425

$$425 = 85 \cdot \mathbf{5}$$
$$85 = \mathbf{17} \cdot \mathbf{5}$$

Thus the prime factorization of 425 is $5^2 \cdot 17$.

(c) 612

$$612 = 306 \cdot \mathbf{2}$$
$$306 = 153 \cdot \mathbf{2}$$
$$153 = 51 \cdot \mathbf{3}$$
$$51 = \mathbf{17} \cdot \mathbf{3}$$

Thus the prime factorization of 612 is $2^2 \cdot 3^2 \cdot 17$.

(d) 877

$$877 = \mathbf{877} \cdot \mathbf{1}$$

Thus the prime factorization of 877 is $877 \cdot 1$.

The composite numbers are 28, 425, and 612 because these natural numbers can be written as a product of prime numbers. The only prime number in this set is 877. 877 is prime because its only factors are itself and 1.

Example 6. *Prove that there are infinitely many primes in the form* $4k + 3$.

By way of contradiction, assume there are a finite number of primes, $q_1, ..., q_n$ in the form of $4k+3$ where $k \in \mathbb{Z}$. Let $r_1 = 4q_1+3$, $r_2 = 4q_2+3, ..., r_m = 4q_n+3$ where $r_1, ..., r_m = 4k + 3$ and $r_1, ...r_m \in \mathbb{Z}$. If $r_1, ..., r_m$ are all prime, we are done. If $r_1, ..., r_m$ are not prime, then every r has at least one prime factor. Since all primes, other than 2, are odd, only primes in the form $4k + 1$ can divide the $r_1, ...r_m$. But the product of 2 or more prime sin this form would be in the form $4z + 1$ where $z \in \mathbb{Z}$. Therefore $r_1, ..., r_m$ can not be a product of only prime factors in the form of $4k + 1$. We have reached a conclusion. Thus there are infinitely many primes in the form of $4k + 3$.

3 Modularity

Maggi Farrow and Michelle Harry

3.1 Introduction

Really difficult divisibility problems can be simplified and solved using modular arithmetic. Many important results come from simply using the definition of congruence modulo m and are discussed in the following section. Theorems 3.1 through 3.6 in particular rely heavily on the definition of congruence modulo m as well as the definition of divides to prove many interesting facts and properties that can be applied when dealing with congruence and modular arithmetic. Theorem 3.7 gives us an interesting result that is examined in the proofs that follow from it. When examining the result of Theorem 3.9 further, a specific set of numbers can now be defined from 0 to n to be the canonical residue system modulo n. After working through some examples it becomes possible to produce a definition of *residue system* which is a boarder version of the *canonical residue system*. Theorems 3.8 and 3.9 contain more important results which aid in reducing congruences in modular arithmetic. Then with Theorem 3.10, an important result is established that can be used as a tool in knowing whether or not there exists a solution to a congruence. Going along with Theorem 3.10, the remaining Theorems discussed in this chapter deal with the existence of solutions to congruences. In order to prove the remaining Theorems, 3.11 through 3.14, results from Chapters 1 and 2 were heavily utilized. In addition to the results proved in this section, the very important result of the *Chinese Remainder Theorem* must be examined.

The Chinese Remainder Theorem Let $n_1, n_2, ..., n_r$ be postive integers such that $(n_i, n_j) = 1$ for $i \neq j$. Then the system of congruences

$$\begin{aligned} x &\equiv a_1 \mod n_1 \\ x &\equiv a_2 \mod n_2 \\ &\vdots \\ x &\equiv a_r \mod n_r. \end{aligned}$$

has a simultaneous solution, which is unique modulo to the integer $n_1 \cdot n_2 \cdot ... \cdot n_r$.

Proof of The Chinese Remainder Theorem required the following Lemmas to be established and proven as well.

Lemma 3.1. *If $a \mid b$ and $c \mid b$ and $gcd(a, c) = 1$ then $ac \mid b$.*

Lemma 3.2. *if $a_i \mid b$ for $i = 1, .., n$ and the $gcd(a_i, a_j) = 1$ for all $i \neq j$, then $a_1 \cdots a_n \mid b$.*

This chapter examines and discovers how to prove hard divisibility problems in just a few steps. From the various results, it is now possible to discover if there is in fact a solution to a congruence as well as gain more insight on the nature of congruences.

3.2 Glossary of Terms

- For a natural number n, the ***canonical residue system*** modulo n is given by $\{0, ..., n-1\}$.
- For a natural number n, a ***residue system*** modulo n is a list $\{a_1, ..., a_n\}$ such that each integer t is congruent to exactly one a_i.
- Given integers a and b and a natural number m, we say a is ***congruent to b modulo m***, denoted $a \equiv b \bmod m$, if m divides $a - b$.

3.3 Theorems

Theorem 3.3. *$a \equiv a$ mod n for any integer a.*

Proof. We know that any integer $n \mid 0$. So, $n \mid a - a$ for any integer a. By definition, $a \equiv a \bmod n$. □

Theorem 3.4. *If $a \equiv b$ mod n, then $b \equiv a$ mod n.*

Proof. Assume $a \equiv b \bmod n$. By definition, $n \mid (a-b)$. By definition of divides, there exists an integer k such that

$$\begin{aligned} nk &= a - b \\ (-1)(nk) &= (-1)(a - b) \\ n(-k) &= b - a. \end{aligned}$$

Thus by definition of divides, $n \mid (b-a)$ and by definition of congruence modulo n, $b \equiv a \bmod n$. □

Theorem 3.5. *If $a \equiv b$ mod n, and $b \equiv c$ mod n, then $a \equiv c$ mod n.*

Proof. Let $a \equiv b \bmod n$, and $b \equiv c \bmod n$. By definition $n \mid (a - b)$ and $n \mid (b - c)$. By definition of divides there exists $x, y \in \mathbb{Z}$ such that $nx = a - b$ and $ny = b - c$. We can rewrite these as $b = a - nx$ and $b = ny + c$. Setting these equations equal we have

$$\begin{aligned} a - nx &= ny + c \\ a - c &= ny + nx \\ a - c &= n(y + x) \end{aligned}$$

Since, $y + x$ is an integer, $n \mid (a - c)$ so by definition $a \equiv c \bmod n$. □

Theorem 3.6. *If $a \equiv b \ mod \ n$ and $c \equiv d \ mod \ n$, then $a + c \equiv b + d \ mod \ n$ and $ac \equiv bd \ mod \ n$.*

Proof. Let $a \equiv b \bmod n$ and $c \equiv d \bmod n$. By definition $n \mid (a - b)$ and $n \mid (d - c)$. By definition of divides there exists $x, y \in \mathbb{Z}$ such that $nx = a - b$ and $ny = d - c$. We can rewrite these as $a = b + nx$ and $c = d + ny$. Thus,

$$\begin{aligned} a + c &= b + nx + d + ny \\ a + c &= b + d + n(x + y) \\ (a + c) - (b + d) &= n(x + y). \end{aligned}$$

By definition of divides $n \mid (a + c) - (b + d)$ so $a + c \equiv b + d \bmod n$.
Using the equations above for a and c we have

$$\begin{aligned} ac &= (b + nx)(d + ny) \\ ac &= bd + nxd + nyb + n^2xy \\ ac - bd &= n(xd + yb + nxy). \end{aligned}$$

Thus, since $(xd + yb + nxy) \in \mathbb{Z}$, $n \mid (ac - bd)$ and hence $ac \equiv bd \bmod n$. □

Theorem 3.7. *If $a \equiv b \ mod \ n$, then $a + c \equiv b + c \ mod \ n$ and $ac \equiv bc \ mod \ n$.*

Proof. Let $a \equiv b \bmod n$. Thus, by definition $n|a - b$. By definition of divides, $a - b = nx$ where $n \in Z$. We can add $0 = c - c$ to the left side of this equation and get

$$\begin{aligned} a + c - b - c &= nx \\ (a + c) - (b + c) &= nx. \end{aligned}$$

From this we can say that $n|(a + c) - (b + c)$ and so by definition, $a + c \equiv b + c \bmod n$. Now, we can multiply both sides of $a - b = nx$ by c and obtain

$$\begin{aligned} (c)(a - b) &= (nx)(c) \\ ac - bc &= n(xc). \end{aligned}$$

where $xc \in Z$. This tells us that $n|ac - bc$. So by definition, we can conclude that $ac \equiv bc \bmod n$. □

Theorem 3.8. *If $a \equiv b \ mod \ n$, then $a^k \equiv b^k \ mod \ n$ for any positive integer k.*

Proof. Assume $a \equiv b \bmod n$. Proceed by induction. When $k = 1$, $a^k \equiv b^k \bmod n$ becomes $a \equiv b \bmod n$ which is true by assumption and thus the base case holds. Now, assume that $a^k \equiv b^k \bmod n$ is true fro all natural numbers, k. Consider

$$\begin{aligned} a^{k+1} &= a^k a^1 \\ &= (b^k \ mod \ n)(b \ mod \ n) \\ &= b^k b \qquad (By \ Theorem \ 3.1) \\ &= b^{k+1} \\ &= b^{k+1} \ mod \ n \qquad (By \ Theorem \ 3.1). \end{aligned}$$

Thus, $a^k \equiv b^k \bmod n$ for any positive integer k. □

Theorem 3.9. *Given any integer a and any natural number n, there exists a unique integer t in the set $\{0, 1, 2, ..., n-1\}$ such that $a \equiv t \bmod n$.*

Proof. Let a be an integer and n be a natural number. Using the division algorithm we can say, $a = nk + t$ where $t, k \in Z$, $0 \leq t \leq n$, and t is unique. This equation can be rewritten as $a - t = nk$ showing us that $n|a - t$. By definition, $a \equiv t \bmod n$. Therefore we can conclude there exists a unique integer t in the set $\{0, 1, 2, ..., n-1\}$ such that $a \equiv t \bmod n$. □

Theorem 3.10. *If $ca \equiv cb \bmod n$, then $a \equiv b \bmod (n/d)$, where $d = gcd(c, n)$.*

Proof. Let $ca \equiv cb \bmod n$, and $d = gcd(c, n)$. By defintion, $n \mid ca - cb$. By definition of divides

$$\begin{aligned} nk &= ca - cb \\ nk &= c(a - b) \\ \frac{nk}{d} &= \frac{c(a-b)}{d} \\ (\frac{n}{d})k &= \frac{c}{d}(a - b). \end{aligned}$$

Thus, by definition of divides, $\frac{n}{d} \mid \frac{c}{d}(a-b)$. Also, since $d = gcd(c, n)$, $\gcd(\frac{n}{d}, \frac{c}{d}) = 1$ by Theorem 1.10. Hence, by Theorem 1.11, $\frac{n}{d} \mid (a - b)$ and by definition of congruence, $a \equiv b \bmod (n/d)$. □

Theorem 3.11. *If $ca \equiv cb \bmod n$ and $gcd(c, n) = 1$, then If $a \equiv b \bmod n$.*

Proof. Let $ca \equiv cb \bmod n$ and $\gcd(c, n) = 1$. By Theorem 3.8, $a \equiv b \bmod (n/gcd(c, n))$. Since $\gcd(c, n) = 1$, $a \equiv b \bmod (n/1)$ or $a \equiv b \bmod n$. □

Theorem 3.12. *Let a, b, and n be integers with $n > 0$. Show that $ax \equiv b \bmod n$ has a solution if and only if there exist integers x and y such that $ax + ny = b$.*

Proof. Let a, b, and n be integers with $n > 0$. Assume $ax \equiv b \bmod n$. Thus, by definition $n \mid ax - b$. So, there exists an integer y such that

$$\begin{aligned} ny &= ax - b \\ ny - ax &= -b \\ ax - ny &= b \\ ax + n(-y) &= b. \end{aligned}$$

Thus there exist integers x and y such that $ax + ny = b$.
Now assume there are integers x and y such that $ax + ny = b$. So, $ax - b = ny$ and by definition of divides $n \mid ax - b$. By definition of congruence modulo n, $ax \equiv b \bmod n$. Conclude that $ax \equiv b \bmod n$ has a solution if and only if there exist integers x and y such that $ax + ny = b$.

□

Theorem 3.13. *Let a, b, and n be integers with $n > 0$. The equation $ax \equiv b$ mod n has a solution if and only if $gcd(a, n) \mid b$.*

Proof. Assume there exists an integer x such that $ax \equiv b \bmod n$. By Theorem 3.10 $ax + ny = b$ where $x, y \in \mathbb{Z}$. By Theorem 1.12, $\gcd(a, n) \mid b$.
Now we will assume $\gcd(a, n) \mid b$. By Theorem 1.12, there are integers x and y such that $ax + ny = b$. Therefore by Theorem 3.10, $ax \equiv b \bmod n$. Conclude that the equation $ax \equiv b \bmod n$ has a solution if and only if $\gcd(a, n) \mid b$. □

Theorem 3.14. *Let a, b, and n be integers with $n > 0$. Suppose that x_0 is a solution to the congruence $ax \equiv b$ mod n, then all solutions are given by*

$$x_0 + \frac{n}{gcd(a, n)} \cdot t$$

where $t \in \mathbb{Z}$.

Proof. Let a, b, and n be integers with $n > 0$. Assume that x_0 is a solution to the congruence $ax \equiv b \bmod n$. By definition of congruence modulo n, $n \mid ax_0 - b$ and further $ax_0 - b = ny$ for some $y \in \mathbb{Z}$. So, $ax_0 + n(-y) = b$ and by Theorem 1.13 all other solutions of x will be given by

$$x_0 + \frac{n}{gcd(a, n)} \cdot t$$

where t is an arbitrary integer. □

Theorem 3.15. *Let a, b, and n be integers with $n > 0$, let $d = gcd(a, n)$. Then the congruence $ax \equiv b$ mod n has either no solutions or precisely d mutually incongruent solutions modulo n, given by*

$$x_0 + \frac{n}{d} \cdot t$$

where $t \in \{0, ..., d - 1\}$.

Proof. Let a, b, and n be integers with $n > 0$. Let $d = gcd(a, n)$.
Case 1: Assume $ax \equiv b \bmod n$ has no solutions. Then we are done.
Case 2: Assume $ax \equiv b \bmod n$ has a solution x_0. By Theorem 3.12, we know all other solutions to this congruence will be of the form

$$x_0 + \frac{n}{gcd(a, n)} \cdot t \qquad or \qquad x_0 + \frac{n}{d} \cdot t$$

Proceed by way of contradiction. Assume that of the solutions which occur when $t = \{0, 1, 2, ..., d - 1\}$, two are mutually congruent modulo n. Then, choosing

any two distinct solutions we have,

$$\begin{aligned}
x_0 + \frac{n}{d} \cdot t_1 &\equiv x_0 + \frac{n}{d} \cdot t_2 \ mod\ n \\
\frac{n}{d} t_1 &\equiv \frac{n}{d} t_2 \ mod\ n \\
t_1 &\equiv t_2 \ mod(\frac{n}{gcd(n, n/d)}) \qquad by\ Theorem\ 3.8 \\
t_1 &\equiv t_2 \ mod(\frac{n}{n/d}) \qquad since\ gcd(n, nd) = n/d \\
t_1 &\equiv t_2 \ mod\ d.
\end{aligned}$$

By definition, this shows that $d|t_1 - t_2$. Which would mean $t_1 = t_2$. Thus, we can conclude that there are d mutually incongruent solutions modulo n to the congruence $ax \equiv b \bmod n$ which are given by

$$x_0 + \frac{n}{d} \cdot t$$

when $t = \{0, 1, 2, ..., d-1\}$.

□

3.4 Examples

Example 7. *Using theorems 3.1-3.6, show that* $2^{20} - 1$.

Example 8. *Find all solutions in the appropriate canonical residue system for* $26x \equiv 14 \mod 3$ *and* $4x \equiv 7 \mod 8$. *How did you do that?*

Example 9. *For each of the congruences* $ax + b = 0$ *mod* n *below, find all its solutions mod* n*:*

(a) $3x + 7 = 0$ *mod* 11,
(b) $4x + 22 = 0$ *mod* 12,
(c) $382x + 121 = 0$ *mod* 563,
(d) $55x - 3000 = 0$ *mod* 121.

4 Order of a Natural Number

Bradley Franjione, James Matuk, Autumn Wobrak

4.1 Introduction

This chapter focusses on the order of a natural number, a modulo n, and applications. The definition of the order of a is the smallest positive natural number k such that $a^k \equiv 1 \mod n$. Before studying the results of this definition, the first concern is the existence of an order for a natural number. In order to gain some intuition about this topic, it helps to do some elementary examples. These examples will illuminate conditions necessary for the order of a number to exist modulo n. Precisely, the $gcd(a, n) = 1$, otherwise, the order of a will not be defined. The concern of the existence of an order is addressed in theorem 4.4. This result follows from the previous theorems in chapter 4 and applications of theorems in chapter 3, as well as previous topics like greatest common divisor, and congruence modulo n. Following this result, the properties of the order of a natural number and applications will be studied.

Properties of the order of a natural number modulo n are noted in theorems 4.5 and 4.6. These results hinged upon the definition of order. By the results of previous theorems, one can establish a residue system described by the order of a natural number. A natural number raised to any power is congruent modulo n to an element in the residue system of the number raised to positive integer power less than the order. This interesting fact lead to a series of theorems that allowed us to prove Fermats Little Theorem in theorem 4.10. This theorem allows one to compute modulo congruencies very efficiently. Following Fermats Little Theorem, we expand upon the order properties of a natural number modulo n while not working with our typical framework.

Rather than working on the set of natural numbers, we started to consider different sets, such as $\mathbb{Z}_n$, the canonical residue system, and $\mathbb{Z}_n^\times$ which is called the reduced residue system and is formally defined in the glossary of terms for this chapter. Essentially, this is the elements of $\mathbb{Z}_n$ that are also relatively prime to n. These definitions give the framework to prove more conjectures regarding modulo arithmetic. Another important result of the order of a natural number is the multiplicative inverse of a natural number modulo n. An inverse of a natural number a is the number $b \in Z_n$ such that $ab \equiv 1 \mod n$. As a corollary to one of the theorems in chapter 4, it can be shown that the inverse of a natural number is unique, and as a result of many of the theorems proved in this chapter, one can show the veracity of Eulers Theorem. Although this theorem disobeys Stiglers law of Eponymy, its consequences are still interesting. As long as $a, n \in \mathbb{Z}$ with $gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \mod n$, where $\phi(n)$ is the Euler ϕ-function defined in the terminology section. This result allows for easier computation of the order of natural numbers.

4.2 Glossary of Terms

- Given natural numbers a and n, with $gcd(a, n) = 1$, the *order of a modulo* n denoted $ord_n(a)$ is the minimal natural number k for which $a^k \equiv 1 \mod n$.
- For a natural number n, $\mathbb{Z}_n = \{0, ..., n-1\}$ i.e., the canonical residue system modulo n.
- For a natural number n, $\mathbb{Z}_n^\times$ is the set of elements in $\mathbb{Z}_n$ which are relatively prime to n. Alternatively, $\mathbb{Z}_n^\times$ is the set of invertable elements in $\mathbb{Z}_n$.
- For a natural number n, the *Euler ϕ - function* is the number of natural numbers that are relatively prime to n and less than n.
- For a natural number n and an integer a, *the inverse of a modulo* n is the number $b \in \mathbb{Z}$ for which $ab \equiv 1 \mod n$.

4.3 Theorems

Theorem 4.1. *Let a and n be natural numbers with $gcd(a, n) = 1$, then $gcd(a^j, n) = 1$ for any natural number j*

Proof. Let a and n be natural numbers with $gcd(a, n) = 1$. Proceed by induction. When $j = 1$, then $gcd(a^1, n) = 1$ follows immediately from the assumption, and note that it follows $az + nm = 1$ for some $z, m \in \mathbb{Z}$ by theorem 1.8. For the inductive step, assume $gcd(a, n) = 1$. By theorem 1.8, $a^k x + ny = 1$ for some $x, y \in \mathbb{Z}$. Multiplying $a^k x + ny = 1$ by $az + nm = 1$ yeilds,

$$\begin{aligned} 1 &= a^{k+1}xz + a^k xnm + azny + n^2 ym \\ &= a^{k+1}(xz) + n(a^k xm + azy + nym) \end{aligned}$$

Thus by theorem 1.8, $gcd(a^{k+1}, n) = 1$ □

Theorem 4.2. *Let a, b and n be natural numbers $n > 0$ and $gcd(a, n) = 1$. If $a \equiv b \mod n$ then $gcd(b, n) = 1$.*

Proof. Let a, b and n be natural numbers with $n > 0$ and $gcd(a, n) = 1$. Assume $a \equiv b \mod n$. It follows by definition of congruence, $n \mid a - b$ and $nk = a - b$ for some $k \in \mathbb{Z}$. Further, $a = nk + b$.. Because $gcd(a, n) = 1$, by theorem 1.8, $ax + ny = 1$.
By substitution,

$$\begin{aligned} 1 &= (nk + b)x + ny \\ &= nkx + bx + ny \\ &= b(x) + n(kx + y) \end{aligned}$$

Hence, by theorem 1.8, $gcd(b, n = 1)$. □

Theorem 4.3. *Let a and n be natural numbers. Then there exists a natural number i and j with $i \neq j$ such that $a^i \equiv a^j \mod n$.*

Proof. Let a and n be natural numbers. By theorem 3.7, all a^i's have a unique $t \in \{0, ..., n-1\}$ such that $a^i \equiv t \mod n$ for $i \in \mathbb{N}$. There are n many elements in $\{0, ..., n-1\}$ and more than $n+1$ many a^i's. So there must be at least two a^i's where $a^i \equiv a^j \mod n$ and $i \neq j$. □

Theorem 4.4. *Let a and n be natural numbers with $gcd(a, n) = 1$. Then there exists a natural number k such that $a^k \equiv 1 \mod n$.*

Proof. Let a and n be natural numbers with $gcd(a, n) = 1$. By theorem 4.3, it follows

$$a^i \equiv a^j \mod n$$

where $i, j \in \mathbb{N}$ and $i \neq j$. Without loss of generality, assume $i > j$. By theorem 4.1 and 3.9, $a^{i-j} \equiv 1 \mod n$. By closure, $i - j = k \in \mathbb{N}$. Hence, $a^k \equiv 1 \mod n$, where $k \in \mathbb{N}$. □

Theorem 4.5. *Let a and n be natural numbers with $gcd(a, n) = 1$ and let $k = ord_n(a)$. Then the natural numbers numbers $a^1, a^2, \ldots, a^k$ are pairwise incongruent modulo n.*

Proof. Let $a, n \in \mathbb{N}$ with $gcd(a, n) = 1$ and $k = ord_n(a)$. Let $a^i, a^j \in \{a^1, a^2, \ldots, a^k\}$. By way of contradiction, let

$$a^i \equiv a^j \mod n,$$

where $i \neq j$. Without loss of generality assume $i > j$. By theorem 3.9,

$$a^{i-j} \equiv 1 \mod n.$$

Thus we have found an integer smaller than k such that $a^{i-j} \equiv 1 \mod n$. This is a contradiction. Hence, the natural numbers numbers $a^1, a^2, \ldots, a^k$ are pairwise incongruent modulo n. □

Theorem 4.6. *Let a and n be natural numbers with $gcd(a, n) = 1$ and let $k = ord_n(a)$. For any natural number m, a^m is congruent modulo n to one of the numbers $a^1, a^2, \ldots, a^k$ with $1 \leq i, j \leq k$.*

Proof. Let $a, n \in \mathbb{N}$ so that $gcd(a, n) = 1$ and let $ord_n(a) = k$. Let $m \in \mathbb{N}$. If $m \leq k$ then $a^m \in \{a^1, a^2, \ldots, a^k\}$, and is congruent modulo n to itself in this set by theorem 3.1. If $m > k$, then by the division algorithm there exists unique integers q, r such that $m = qk + r$, where $0 \leq r < k$. It follows,

$$\begin{aligned} a^m &= a^{qk+r} \\ &= a^{qk} \cdot a^r \end{aligned}$$

Note, by the definition of order, 1 $1 \equiv a^k \mod n$. Thus,

$$\begin{aligned} a^m &\equiv 1^q \cdot a^r mod n \\ &= a^r \mod n \end{aligned}$$

Because $0 \leq r < k$ and $a^0 \equiv a^k mod n$, we conclude a^m is congruent modulo n to one of the numbers $a^1, a^2, \ldots, a^k$. □

Theorem 4.7. *Let a and n be natural numbers with $gcd(a, n) = 1$ and let m be a ntural number. Then, $a^m \equiv 1 \mod n$ if an only if $\text{ord}_n(a) \mid m$.*

Proof. Let a, m, n be natural numbers and $\gcd(a, n) = 1$. Assign $\text{ord}_n(a) = k$ where k is an integer. We will begin by assuming that $a^m \equiv 1 \mod n$. By the division algorithim, $m = kq + r$ where $0 < r < k$. Then it follows that,

$$\begin{aligned} a^m &\equiv a^{kq+r} \mod n \\ a^m &\equiv (a^k)^q \cdot a^r \mod n \\ a^m &\equiv 1^q \cdot a^r \mod n \\ a^m &\equiv a^r \mod n \end{aligned}$$

Thus r can only be 0. When $r = 0$ it follows that $m = kq$. Therefore, $\text{ord}_n(a) \mid m$ becasue $k \mid m$.

Now we will assume that $\text{ord}_n(a) \mid m$. It follows that,

$$\begin{aligned} a^m &\equiv a^{kq} \mod n \\ a^m &\equiv (a^k)^q \mod n \\ a^m &\equiv 1^q \mod n \\ a^m &\equiv 1 \mod n \end{aligned}$$

Thus we have come to our conclusion. □

Theorem 4.8. *Let p be a prime. If a is an integer and p does not divide a then $\{a, 2a, ..., pa\}$ is a residue system modulo p.*

Proof. Let p be a prime and a be an integer not divisible by p. Consider $\{a, 2a, ..., pa\} = C$. Also, note that the $\gcd(a, p) = 1$. To show that the are distinct modulo p we will assume that $an \equiv am \mod p$. By Theorem 3.8, we know that $n \equiv m \mod p$. Thus, the elements of C are distinct modulo p. By Theorem 3.7, since there are p distinct elements in C, each element is congruent to one element in the canonical residue system. Thus, C is a residue system modulo p. □

Theorem 4.9. *Let p be a prime and a be an integer not divisible by p. Then,*

$$a \cdot 2a \cdot 3a \cdot ... \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \mod p.$$

Proof. Let p be a prime and a be an integer not divisible by p. By Theorem 4.8, we know that $\{a, 2a, ..., pa\}$ is a residue system modulo p. Notcie, since p divides pa, that $pa \equiv 0 \mod p$. Then, every other element in the residue system maps to one remaining element in the canonical residue system. So, by Theorem 3.4, we have

$$a \cdot 2a \cdot 3a \cdot ... \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \mod p,$$

in some order. □

Theorem 4.10. *If p is a prime, then $a^p \equiv a \mod p$ for any integer a.*

Proof. Let p be a prime and a be an arbitrary integer. By Theorem 4.9 we know that,

$$a \cdot 2a \cdot 3a \cdot ... \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \mod p.$$

By algebra,

$$\begin{aligned} a^{p-1}(p-1)! &\equiv (p-1)! \mod p \\ a^{p-1} &\equiv 1 \mod p \\ a^{p-1} \cdot a &\equiv a \mod p \\ a^p &\equiv a \mod p \end{aligned}$$

Thus, we are done. □

Theorem 4.11. *If p and q are distinct primes with $a^p \equiv a \mod q$ and $a^q \equiv a \mod p$, then $a^p q \equiv a \mod pq$.*

Proof. Let p, q be prime where $p \neq q$. Assume $a^p \equiv a \mod q$ and $a^q \equiv a \mod p$. By Theorem 4.10, we know that $a^p \equiv a \mod p$ and $a^q \equiv a \mod q$. By algebra,

$$\begin{aligned} a^p &\equiv a \mod p \\ a^{pq} &\equiv aq \mod p \\ a^{pq} &\equiv a \mod p \end{aligned}$$

This means that $p \mid a^{pq} - a$. Also,

$$\begin{aligned} a^q &\equiv a \mod q \\ a^{qp} &\equiv ap \mod p \\ a^{qp} &\equiv a \mod p \end{aligned}$$

This means that $q \mid a^{qp} - a$. By lemma 1, since we know that $p \mid a^{pq} - a$ and $q \mid a^{qp} - a$, we have that $pq \mid a^{pq} - a$. Thus, by definition on congruence, $a^p q \equiv a \mod pq$. □

Theorem 4.12. *Suppose that gcd$(a, n) = 1$. Then there exists $b \in \mathbb{Z}_n^\times$, such that $a \cdot b \equiv 1 \mod n$.*

Proof. We will begin by assuming that $\gcd(a, n) = 1$. In other words, $\gcd(a, n) \mid 1$. By Theorem 3.11, we have that if $\gcd(a, n) \mid 1$, then $a \cdot t \equiv 1 \mod n$, where t is an integer. By Theorem 3.7, we know that there exists and element $b \in \mathbb{Z}_n$, such that $b \equiv t \mod n$. Thus, $ab \equiv 1 \mod n$. Now, we must show that b is in $\mathbb{Z}_n^\times$, meaning that $\gcd(b, n) = 1$. Since $ab \equiv 1 \mod n$, it is true that $n \mid ab - 1$. By the definition of divides, $ab - 1 = nk$, where k is an integer. Thus, we obtain,

$$\begin{aligned} ab - nk &= 1 \\ b(a) + n(-k) &= 1 \end{aligned}$$

Thus, $\gcd(b, n) = 1$. Hence, there exists $b \in \mathbb{Z}_n^\times$, such that $a \cdot b \equiv 1 \mod n$. □

Theorem 4.13. *If p is a prime, then every non-zero element in $\mathbb{Z}_p$ has an inverse in $\mathbb{Z}_p$.*

Proof. Let p be prime. By definition, $\mathbb{Z}_p = \{0, ..., p-1\}$ and $\mathbb{Z}_p^\times = \{1, ..., p-1\}$. Note that $\mathbb{Z}_p^\times$ contains every non-zero element in $\mathbb{Z}_p$. By definition, $\gcd(a, p) = 1$ for any $a \in \mathbb{Z}_p^\times$. By theorem 4.12, there exists some $b \in \mathbb{Z}_p^\times$ such that $ab \equiv 1$ *mod* n. Thus, by definition of an inverse, every non-zero element in $\mathbb{Z}_p$, or every element in $\mathbb{Z}_p^\times$, has an inverse $b \in \mathbb{Z}_p$. □

Theorem 4.14. *If p is a prime larger than 2, then $2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1$ mod p.*

Proof. Let p be a prime larger than 2. We want to show that $2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1 \bmod p$. From 4.13, we know that every non-zero element in $\mathbb{Z}_p$ has an inverse. Also from 4.13, we know that the inverse of all elements can be found in $\mathbb{Z}_p$. Note that zero is never an inverse, since $0 \cdot a \equiv 0 \bmod p$ for any $a \in \mathbb{Z}_p$. We do not know how they are paired, but if we can show that 1 is its own inverse and $p-1$ is its own inverse, then certainly $2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1 \bmod p$. Since $1 \cdot 1 \equiv 1 \bmod p$, we can conclude that 1 is its own inverse. Additionally, $(p-1)(p-1) = p^2 - 2p + 1 \equiv 1 \bmod p$ since $p^2 \equiv 0 \bmod p$ and $-2p \equiv 0 \bmod p$, so $p-1$ is its own inverse. Therefore, we can safely conclude that $2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1 \bmod p$. □

Theorem 4.15. *($Wilson's Theorem$) If p is prime, then $(p-1)! \equiv -1$ mod p.*

Proof. By theorem 4.14, we know that $2 \cdot 3 \cdot 4 \cdots (p-2) \equiv 1 \bmod p$. By multiplying each side of the congruence by $p-1$, we have that $(p-1)! \equiv p-1 \bmod p$. But since $p \equiv 0 \bmod p$, then we can conclude that $(p-1)! \equiv -1 \bmod p$. □

Theorem 4.16. *Suppose that $x_i, x_j \in \mathbb{Z}_n^\times$ and gcd(a, n) = 1. If $ax_i \equiv ax_j$ mod n, then $x_i = x_j$.*

Proof. We will assume that $x_i, x_j \in \mathbb{Z}_n^\times$ and that $\gcd(a, n) = 1$. Given that $ax_i \equiv ax_j \bmod n$, we will show that $x_i = x_j$. By theorem 3.9, we can say that $x_i \equiv x_j \bmod n$. Without loss of generality, assume $x_i \geq x_j$. By definition of congruence, we know that $n \mid x_i - x_j$. By definition of $\mathbb{Z}_n^\times$, x_i can be at most $n-1$, and
$1 \leq x_j \leq n-1$. Therefore, $x_i - x_j$ will yield a result of a non negative integer less than n, so n cannot divide it unless $x_i = x_j$. □

Corollary 4.17. *All inverses are unique modulo n.*

Proof. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}_n^\times$. Assume that $ab \equiv 1 \bmod n$ and $ac \equiv 1 \bmod n$, where $b, c \in \mathbb{Z}_n^\times$. We will show that $b = c$. Using our above congruencies, we can conclude that $ab \equiv ac \bmod n$. By theorem 4.16,
$b = c$. Therefore, all inverses are unique modulo n. □

Theorem 4.18. *Suppose that $x_i \in \mathbb{Z}_n^\times$ and gcd(a, n) = 1. Then there exists $x_j \in \mathbb{Z}_n^\times$ such that $ax_i \equiv x_j$ mod n.*

Proof. Let $x_i \in \mathbb{Z}_n^\times$ and $\gcd(a,\, n) = 1$. Consider ax_i. By theorem 3.7, $ax_i \equiv x_j \bmod n$ where $x_j \in \mathbb{Z}_n$. Note that $a \neq 0$ and $x_i \neq 0$, so $ax_i \neq 0$. Thus, $x_j \in \mathbb{Z}_n \setminus \{0\}$. Because $\gcd(a,\, n) = 1$ and $\gcd(x_i,\, n) = 1$ by definition of $\mathbb{Z}_n^\times$, then $\gcd(ax_i,\, n) = 1$ by theorem 2.7. By theorem 4.2, $\gcd(x_j,\, n) = 1$. Hence, $x_j \in \mathbb{Z}_n^\times$. Therefore, there exists an $x_j \in \mathbb{Z}_n^\times$ such that $ax_i \equiv x_j \bmod n$. □

Theorem 4.19. *If gcd(a, n) = 1, then*

$$ax_1 \cdot ax_2 \cdots ax_{\phi(n)} \equiv x_1 \cdot x_2 \cdots x_{\phi(n)} \ mod\ n.$$

Proof. Let $\gcd(a,\, n) = 1$ and $\mathbb{Z}_n^\times = \{x_1, ..., x_{\phi(n)}\}$. Since $\gcd(a,\, n) = 1$, we know that $n \nmid a$. By theorem 4.17, $ax_i \equiv x_j \bmod n$ where $x_i, x_j \in \mathbb{Z}_n^\times$. Assume $ax_i \equiv x_k \bmod n$ where $x_k \in \mathbb{Z}_n^\times$. Then by transitivity, $x_j \equiv x_k \bmod n$. Since x_j and x_k are both in $\mathbb{Z}_n^\times$, they are both clearly less than n. By definition of congruence, $n \mid x_j - x_k$, so $x_j = x_k$, otherwise $x_j - x_k$ results in a non-negative integer less than n, which means n cannot divide it. Since each ax_i must be congruent to a unique x_j in $\mathbb{Z}_n^\times$, then

$$ax_1 \cdot ax_2 \cdots ax_{\phi(n)} \equiv x_1 \cdot x_2 \cdots x_{\phi(n)} \bmod n.$$

□

Theorem 4.20. (*Euler'sTheorem*) *If a and n are integers, $n > 0$ and gcd(a, n) = 1, then*

$$a^{\phi(n)} \equiv 1\ mod\ n.$$

Proof. Let $a, n \in \mathbb{Z}$ such that $\gcd(a,\, n) = 1$. Consider $\mathbb{Z}_n^\times = \{x_1, x_2, ..., x_{\phi(n)}\}$. Note that by theorem 2.7, $\gcd(x_1 \cdot x_2 \cdots x_{\phi(n)}\ ,\ n) = 1$. By theorem 4.18, $ax_1 \cdot ax_2 \cdots ax_{\phi(n)} \equiv x_1 \cdot x_2 \cdots x_{\phi(n)} \bmod n$. It then follows that $a^{\phi(n)} \cdot (x_1 \cdot x_2 \cdots x_{\phi(n)}) \equiv x_1 \cdot x_2 \cdots x_{\phi(n)} \bmod n$. Then by theorem 3.8, $a^{\phi(n)} \equiv 1 \bmod n$. □

4.4 Examples

Example 10. *Compute $ord_3(5)$ and $ord_5(2)$. What happens if you try to compute $ord_4(2)$?*

To compute some $ord_n(a)$, we want to find the smallest natural number k such that $a^k \equiv 1\ mod\ n$.

To compute $ord_3(5)$, we are trying to find the smallest natural number k such that $5^k \equiv 1\ mod\ 3$. In this example, $ord_3(5) = 2$ since $k = 2$ is the smallest natural number such that $5^k \equiv 1\ mod\ 3$.

To compute $ord_5(2)$, we are trying to find the smallest natural number k such that $2^k \equiv 1\ mod\ 5$. In this example, $ord_5(2) = 4$ since $k = 4$ is the smallest natural number such that $2^k \equiv 1\ mod\ 5$.

T compute $ord_4(2)$*, we would be trying to find the smallest natural number* k *such that* $2^k \equiv 1 \ mod \ 4$*. But in this example, there is no* k *that makes this congruence true. If we look back to the previous 2 examples, you will notice that the gcd(a, n) = 1, while in this example, the gcd(a, n)* $\neq$ *1. Therefore, in order for some* $ord_n(a)$ *to exist, we must have that the gcd(a, n) = 1.*

Example 11. *Compute the inverses of 2, 3, and 4 modulo 7.*

To compute the inverse of some natural number a modulo n, we want to find some $b \in \mathbb{Z}_n$ *such that*
$ab \equiv 1 \ mod \ n$*.*

To find the inverse of 2 modulo 7, we want to find some $b \in \mathbb{Z}_n$ *such that* $2b \equiv 1 \ mod \ 7$*. In this case, our inverse of 2 modulo 7 would be 4 since* $4 \in \mathbb{Z}_n$ *and* $2 \cdot 4 = 8 \equiv 1 \ mod \ 7$*.*

To find the inverse of 3 modulo 7, we want to find some $b \in \mathbb{Z}_n$ *such that* $3b \equiv 1 \ mod \ 7$*. In this case, our inverse of 3 modulo 7 would be 5 since* $5 \in \mathbb{Z}_n$ *and* $3 \cdot 5 = 15 \equiv 1 \ mod \ 7$*.*

To find the inverse of 4 modulo 7, we want to find some $b \in \mathbb{Z}_n$ *such that* $4b \equiv 1 \ mod \ 7$*. In this case, our inverse of 4 modulo 7 would be 2 since* $2 \in \mathbb{Z}_n$ *and* $4 \cdot 2 = 8 \equiv 1 \ mod \ 7$*.*

Example 12. *Find* $\mathbb{Z}_n$*,* $\mathbb{Z}_n^\times$*, and* $\phi(n)$ *for* $n = 8$*.*

$\mathbb{Z}_n = \{1, 2, 3, 4, 5, 6, 7\}$*, since* $\mathbb{Z}_n$ *contains all non-negative integers up to and including* $n-1$*. In this example, our n is 8, and so* $\mathbb{Z}_n$ *contains all non-negative integers between 0 and 7 inclusive.*

$\mathbb{Z}_n^\times = \{1, 3, 5, 7\}$*, since* $\mathbb{Z}_n^\times$ *contains all natural numbers in* $\mathbb{Z}_n$ *that are relatively prime to n, which is 8 in this example.*

$\phi(n) = 4$*, since* $\phi(n)$ *simply tells us how many elements are in* $\mathbb{Z}_n^\times$*. Since there are 4 elements in* $\mathbb{Z}_n^\times$*, specifically 1, 3, 5, and 7, then* $\phi(n) = 4$*.*

5 Primitive Roots

Joshua Pinaroc, Allison Waldo, Alexander Cunningham

5.1 Introduction

In this chapter we are going to be looking at Primitive Roots Modulo n. With the theorems from this chapter we are going to be building up to the proof that Primitive Roots exist. However, primitive roots are quite hard to find due to the way that they are defined. After we show that primitive roots exist, we have several ways to test to see if a number is a primitive root modulo n.

5.2 Glossary of Terms

- *Primitive Roots Modulo n:* A primitive root modulo n, is a number of order $\phi(n)$ which is relatively prime to n.

5.3 Theorems

Theorem 5.1. *If a is a primitive root modulo n, then $\{a, a^2, ..., a^{\phi(n)}\}$ forms a reduced residue system modulo n.*

Proof. Let a be a primitive root modulo n. Thus, by definition $gcd(a, n) = 1$. By Theorem 4.5, $a, ..., a^{\phi}(n)$ are all pairwise incongruent modulo n. Also, by Theorem 4.1 if $gcd(a, n) = 1$, then $gcd(a^j, n) = 1$ for any natural number j. Thus,, $gcd(a^j, n) = 1$ for $j = 1, ..., \phi(n)$. Thus, $\{a, a^2, ..., a^{\phi}(n)\}$ forms a reduced residue system modulo n. □

Theorem 5.2. *If p is prime and a is a primitive root modulo p, then $\{0, a, ..., a^{p-1}\}$.*

Proof. Note that $\phi(p) = p - 1$. So, by Theorem 5.1, $\{a, a^2, ..., a^{p-1}\}$ forms a reduced residue system modulo p. Since $\{0\} \cup \mathbb{Z}_p^{\times}$ is $\mathbb{Z}_p$ for p prime, it follows that $\{0, a, ..., a^{p-1}\}$ is a residue system modulo p. □

Theorem 5.3. *Let $f(x)$ be a polynomial of degree n. Then r is a root of $f(x)$ if and only if*

$$f(x) = (x - r) \cdot g(x)$$

where $g(x)$ is a polynomial of degree $n - 1$.

Proof. Let $f(x)$ be a polynomial of degree n. Let r be a root of $f(x)$. Proceed by strong induction. Base case is $f(x) = k \cdot (x - r)$ where $k \in \mathbb{Z}$. Inductive step is assume $f(x) = (x - r) \cdot g(x) + q(x)$. Since r is a root of $f(x)$, $f(r) = 0$ and thus,

$$\begin{aligned} 0 &= (r - r) \cdot g(r) + q(r) \\ 0 &= q(r) \end{aligned}$$

So $q(x) = (x - r) \cdot h(x)$ where $q(x)$ has a degree less than $f(x)$. From our inductive step,

$$\begin{aligned} f(x) &= (x - r) \cdot g(x) + q(r) \\ &= (x - r) \cdot g(x) + (x - r) \cdot h(x) \\ &= (x - r)[g(x) + h(x)] \end{aligned}$$

where $g(x)$ has degree $n - 1$ and $h(x)$ has degree less than $g(x)$. Now assume $f(x) = (x - r) \cdot g(x)$ where $g(x)$ is of degree $n - 1$. Then,

$$\begin{aligned} f(r) &= (r - r) \cdot g(x) \\ &= 0 \cdot g(x) \\ &= 0 \end{aligned}$$

Thus we have come to our conclusion. □

Theorem 5.4. *Let $f(x)$ be a polynomial of degree n, let p be a prime, and let r be an integer. Then $f(r) \equiv 0 \mod p$, if and only if,*

$$f(x) \equiv (x - r) \cdot g(x) \mod p$$

where $g(x)$ is a polynomial of degree $n - 1$.

Proof. First, let $f(r) \equiv 0 \mod p$. By definition of congruence, $f(r) = kp$ for some $k \in \mathbb{Z}$. Define $h(x) = f(x) - kp$. Then, $h(r) = f(r) - kp = 0$, so r is a root of $h(x)$. By theorem 6.3, $h(x) = (x - r) \cdot g(x)$ where $g(x)$ is a polynomial of degree $n - 1$. Then,

$$\begin{aligned} f(x) - kp &= (x - r) \cdot g(x) \\ f(x) &= (x - r) \cdot g(x) + kp. \end{aligned}$$

By definition of congruence modulo p,

$$f(x) \equiv (x - r) \cdot g(x) \mod p.$$

Now, let $f(x) \equiv (x - r) \cdot g(x) mod p$. Then,

$$f(r) \equiv (r - r) \cdot g(x) \equiv 0 \mod p.$$

□

Theorem 5.5. *Let $f(x)$ be a polynomial of degree n, and let p be a prime. Then*

$$f(x) \equiv 0 \mod p$$

has at most n incongruent solutions.

Proof. We will proceed by mathematical induction. Base case is let $f(x)$ be of degree 1. Since it is of degree 1, there is only at most 1 solution, therefore it is incongruent. Inductive step is assume $f(x)$ is a polynomial of degree $n-1$ such that

$$f(x) \equiv 0 \mod p$$

has at most $n-1$ incongruent solutions. Either it has no roots or it has at least 1 root say "r". If we have no solutions, then we're done. Otherwise, we will show that $f(x)$ of degree n with p prime,

$$f(x) \equiv 0 \mod p$$

has at most n incongruent solutions. By Theorem 6.4, we can write $f(x)$ as,

$$f(x) \equiv (x-r) \cdot g(x) \mod p$$

where $g(x)$ is a polynomial of degree $n-1$. By our inductive hypothesis, we know $g(x)$ has at most $n-1$ incongruent solutions. By our base case, $x-r$ has at most 1 solution because it is of degree 1. Thus, $f(x)$ has at most n incongruent solutions because $(n-1)+1 = n$. □

Theorem 5.6. *Let p be prime. For any $d \mid p-1$, the congruence $x^d - 1 \equiv 0 \mod p$ has exactly d incongruent solutions.*

Proof. By Theorem 5.5, we know $x^d - 1 \equiv 0 \mod p$ has at most d incongruent solutions. By Fermat's Little Theorem, $x^{p-1} - 1 \equiv 0 \mod p$ has $p-1$ solutions, they are $\{1, 2, ..., p-1\}$. But, $d \mid p-1$, meaning $p-1 = dk$ for $k \in \mathbb{Z}$. So,

$$x^{p-1} - 1 = (x^d - 1) \cdot g(x),$$

where $g(x)$ has degree $p-1-d$. By 6.5, we know $g(x)$ has at most $p-1-d$ roots. But, since $x^{p-1}-1$ has $p-1$ roots, and since any root of $x^{p-1}-1$ is either a root of x^d-1 or a root of $g(x)$, we know x^d-1 has at least $(p-1)-(p-1-d) = d$ roots. Thus, x^{d-1} has exactly d solutions.

□

Theorem 5.7. *Let p be prime, then $\sum_{d|p} \phi(d) = p$.*

Proof. If p prime and $d \mid p$, then p has only 2 divisors, 1 and itself. Thus, $\sum_{d|p} \phi(d) = \phi(1) + \phi(p) = 1 + p - 1 = p$. □

Theorem 5.8. *Let p be prime and k a positive integer, then $\sum_{d|p^k} \phi(d) = p^k$.*

Proof. Let p be a prime and k a positive integer. Note the divisors of p^k are $1, p, ..., p^{k-1}, p^k$. Thus,

$$\begin{aligned}\sum_{d|p^k} \phi(d) &= \phi(1) + \phi(p) + \phi(p^2) + ... + \phi(p^k) \\ &= 1 + (p-1) + p(p-1) + ... + p^{k-1}(p-1).\end{aligned}$$

Note this is a telescoping sum. Hence, $\sum_{d|p^k} \phi(d) = p^k$. □

Theorem 5.9. *If p and q are two different primes, then $\sum_{d|pq} \phi(d) = pq$.*

Proof. Observe that since p and q are distinct primes and $\gcd(p, q) = 1$, only $1 \mid pq$, $p \mid pq$, $q \mid pq$, and $pq \mid pq$. Then

$$\begin{aligned}\sum_{d|pq} \phi(d) &= \phi(1) + \phi(p) + \phi(q) + \phi(pq) \\ &= \phi(1) + \phi(p) + \phi(q) + \phi(p)\phi(q) \\ &= 1 + (p-1) + (q-1) + (p-1)(q-1) \\ &= 1 + (p-1) + (q-1) + pq - p - q + 1 \\ &= pq.\end{aligned}$$

□

Theorem 5.10. *If m and n are two relatively prime positive integers, then $\sum_{d|m} \phi(d) \cdot \sum_{d|n} \phi(d) = \sum_{d|mn} \phi(d)$.*

Proof. Let $a_1, ..., a_q$ be the divisors of m and $b_1, ..., b_r$ be the divisors of n. Then $\{a_s b_t \mid 1 \le s \le q, 1 \le r \le t\}$ is the set of all divisors of mn. Since $\gcd(m, n) = 1$, $a_q \neq b_r$ for all q and r, hence every $a_q b_r$ is unique. Hence

$$\begin{aligned}\sum_{d|m} \phi(d) \cdot \sum_{d|n} \phi(d) &= (\phi(a_1) + \cdots + \phi(a_q))(\phi(b_1) + \cdots + \phi(b_r)) \\ &= \phi(a_1)\phi(b_1) + \phi(a_1)\phi(b_2) + \cdots \phi(a_q)\phi(b_{r-1}) + \phi(a_q)\phi(b_r) \\ &= \phi(a_1 b_1) + \phi(a_1 b_2) + \cdots \phi(a_q b_{r-1}) + \phi(a_q b_r) \\ &= \sum_{d|mn} \phi(d)\end{aligned}$$

□

Lemma 5.11. *For p prime and an integer k, $\phi(p^k) = p^{k-1}(p-1)$.*

Proof. By definition, $\phi(p^k)$ counts the natural numbers that are in $\mathbb{Z}_{p^k}$ but not in $\mathbb{Z}_{p^k}^{\times}$. Note that only $1 \mid p^k, p \mid p^k, ..., p^{k-1} \mid p^k, p^k \mid p^k$. Thus for a natural number $n \le p^k, \gcd(n, p^k) \neq 1$ implies $\gcd(n, p) \neq 1$. Since only $1 \mid p$ and $p \mid p$, we have that $\gcd(n, p) = p$, thus $n = ap$ for some natural number a. Since $n \le p^k$, by substitution, $ap \le p^k$ i.e. $a \le p^{k-1}$. Hence there are p^{k-1} such n that are in $\mathbb{Z}_{p^k}$ but not in $\mathbb{Z}_{p^k}^{\times}$. Thus $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$. □

Theorem 5.12. *For any natural number n, we have $\sum_{d|n} \phi(d) = n$.*

Proof. Either n is prime, in which case the statement is automatic from Theorem 5.7, or n can be written as a unique product of prime factors, namely $p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$. Since $\gcd(p_1^{a_1}, p_2^{a_2} \cdots p_k^{a_k}) = 1$, by Theorem 6.10,

$$\sum_{d|n} \phi(d) = \sum_{d|p_1^{a_1}} \phi(d) \cdot \sum_{d|p_2^{a_2} \cdots p_k^{a_k}} \phi(d)$$

and so on until

$$\sum_{d|n} \phi(d) = \sum_{d|p_1^{a_1}} \phi(d) \cdots \sum_{d|p_k^{a_k}} \phi(d).$$

By Theorem 6.8, $\sum_{d|p_i^{a_i}} \phi(d) = p_i^{a_i}$ for all $1 \leq i \leq k$. Hence

$$\sum_{d|n} \phi(d) = p_1^{a_1} \cdots p_k^{a_k} = n.$$

□

Theorem 5.13. *Let p be prime and a be an integer relatively prime to p with $\text{ord}_p(a) = d$. Then $\text{ord}_p(a^k) = d$ ifa and only if $\gcd(a, k) = 1$.*

Proof. First suppose $\text{ord}_p(a^k) = d$. By definition, d is the smallest natural number such that $(a^k)^d \equiv 1 \mod p$. Let $\gcd(d, k) = m$ where $m \in \mathbb{N}$. So $m \mid d$, hence $\frac{d}{m} \in \mathbb{N}$. By Theorem 3.6,

$$\begin{aligned}(a^k)^{\frac{d}{m}} &= a^{\frac{kd}{m}} mod p \\ &= (a^d)^{\frac{k}{m}} \\ &\equiv 1^{\frac{k}{m}} \mod p \\ &\equiv 1 \mod p.\end{aligned}$$

Hence $\frac{d}{m} \geq d$ which is only true for $m = 1$. Thus $\gcd(d, k) = 1$.
Next suppose $\gcd(d, k) = 1$. Since $a^d \equiv 1 \mod p$, we have $(a^k)^d \equiv 1 \mod p$. Let $\text{ord}_p(a^k) = m$. By Theorem 4.7, $m \mid d$ and $d \mid km$, but because $\gcd(d, k) = 1$, we have $d \mid m$. Hence $d = m$, i.e. $\text{ord}_p(a^k) = d$. □

Theorem 5.14. *Let p be prime. For any $d \mid p-1$, there are exactly $\phi(d)$ many incongruent integers having order d modulo p.*

Theorem 5.15. *For p prime, there are exactly $\phi(p-1)$ incongruent primitive roots modulo p.*

Proof. Observe $p - 1 \mid p - 1$, so by Theorem 5.14, there are exactly $\phi(p-1)$ many incongruent integers having order $p - 1$ modulo p, which is simply the definition of a primitive root modulo p. □

Theorem 5.16. *Let p be prime. Then a is a primitive root modulo p if and only if for all factors f of p-1 not including 1, $a^{\frac{p-1}{f}} \not\equiv 1 \mod p$.*

Proof. First, let a be a primitive root modulo p. Then $\phi(p) = p - 1$ is the smallest $n \in \mathbb{N}$ such that $a^n \equiv 1 \mod p$. Hence for all $f > 1$ such that $f \mid p-1$, $\frac{p-1}{f} < p - 1$, so by definition, $a^{\frac{p-1}{f}} \not\equiv 1 \mod p$.
Next, assume for all factors $f > 1$ of $p-1$, $a^{\frac{p-1}{f}} \not\equiv 1 \mod p$. By Theorem 4.10, $a^{p-1} \not\equiv 1 \mod p$. By Theorem 4.7, $\text{ord}_p(a) \mid p - 1$. By definition of divides, $p - 1 = \text{ord}_p(a) \cdot f$ for some $f \in \mathbb{N}$, i.e. $\frac{p-1}{f} = \text{ord}_p(a)$. Then $a^{\frac{p-1}{f}} \equiv 1 \mod p$, but by the assumption, $f = 1$. Hence $\text{ord}_p(a) = p-1 = \phi(p)$, so a is a primitive root modulo p. □

5.4 Examples

- 1 Does $3, 4$ or 5 have primitive roots?
  - Primitive Roots modulo 3.

$$\begin{aligned} n = 3, \phi(3) &= 2 \\ 2^1 &\equiv 2 \mod 3 \\ 2^2 &\equiv 1 \mod 3 \end{aligned}$$

    2 is a primitive root modulo 3.
  - Primitive Roots modulo 4.

$$\begin{aligned} n = 4, \phi(4) &= 2 \\ 3^1 &\equiv 3 \mod 4 \\ 3^2 &\equiv 1 \mod 4 \end{aligned}$$

    3 is a primitive root modulo 4.
  - Primitve Roots modulo 5

$$\begin{aligned} n = 5, \phi(5) &= 4 \\ 2^1 &\equiv 2 \mod 5 \\ 2^2 &\equiv 4 \mod 5 \\ 2^3 &\equiv 3 \mod 5 \\ 2^4 &\equiv 1 \mod 5 \end{aligned}$$

    2 is a primitive Root Modulo 5.

$$\begin{aligned} 3^1 &\equiv 3 \mod 5 \\ 3^2 &\equiv 4 \mod 5 \\ 3^3 &\equiv 2 \mod 5 \\ 3^4 &\equiv 1 \mod 5 \end{aligned}$$

    3 is a Primitive Root Modulo 5.

$$\begin{aligned} 4^1 &\equiv 4 \mod 5 \\ 4^2 &\equiv 1 \mod 5 \end{aligned}$$

    4 is not a primitive root modulo 5 because it does not have order 4.

- 2 Compute $(\sum_{d|8} \phi(d))$ and $(\sum_{d|12} \phi(d))$.
  - $\sum_{d|8} \phi(d)$

$$\begin{aligned} & \sum_{d|8} \phi(d) \\ &= \phi(1) + \phi(2) + \phi(4) + \phi(8) \\ &= 1 + 1 + 2 + 4 = 8 \end{aligned}$$

  - $\sum_{d|12} \phi(d)$

$$\begin{aligned} & \sum_{d|12} \phi(d) \\ &= \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) \\ &= 1 + 1 + 2 + 2 + 2 + 4 = 12 \end{aligned}$$