This small text is an online, preliminary edition which was written for Mathematics 313 (Number Theory) offered at Philadelphia University, Jordan. It has now been superseded by the book *Theory of Numbers*, published by BookSurge, 2008. Although this book may continue to be used by students of relevant courses, be aware that the author has ceased any efforts toward further revision, correction, or update of the contents herein. Nevertheless, comments and suggestions are still welcome and may be addressed to awitno@gmail.com.

Last edited,
March 2007

© 2007 Amin Witno
http://www.witno.com
## Contents

1 Divisibility 1  
1.1 Divisibility and Residues 1  
1.2 Greatest Common Divisors 4  
1.3 Linear Diophantine Equations 8  
1.4 Project: Blankinship Algorithm 10  

2 Primes 11  
2.1 Primes and Divisibility 11  
2.2 Factorization into Primes 13  
2.3 The Infinitude of Primes 15  
2.4 Project: Fermat Factorization 18  

3 Congruences 19  
3.1 Congruences and Residue Classes 19  
3.2 Linear Congruences 22  
3.3 Chinese Remainder Theorem 24  
3.4 Project: Divisibility Tests 27  

4 Modular Exponentiation 29  
4.1 Fermat’s Theorem and Euler’s Function 29  
4.2 Computing Powers and Roots 33  
4.3 The RSA Cryptosystem 37  
4.4 Project: RSA Cycling Attack 39  

5 Primitive Roots 41  
5.1 Orders and Primitive Roots 41  
5.2 The Existence of Primitive Roots 44  
5.3 Discrete Logarithm Problems 46  
5.4 Project: Secret Key Exchange 48  


6 Quadratic Residues
   6.1 Quadratic Residues and the Legendre Symbol .... 49
   6.2 The Jacobi Symbol ................................ 54
   6.3 Computing Square Roots ............................ 56
   6.4 Project: Electronic Coin Tossing ................. 58

A To Learn More ........................................ 59

B Answers & Hints ...................................... 61

C Primes < 10,000 ...................................... 65
Chapter 1

Divisibility

The counting numbers 1, 2, 3, . . . together with their negatives and zero make up the set of integers. Number Theory is the study of integers, so every number represented throughout this book will be understood an integer unless otherwise stated.

1.1 Divisibility and Residues

It is reasonable to claim without proof that addition and multiplication of integers will yield another integer. Dividing an integer by another, however, does not always return an integer value, and that is exactly where we begin our study of numbers.

Definition. The number $d$ divides $m$, or $m$ is divisible by $d$, if the operation $m \div d$ produces an integer. Such a relation may be written $d \mid m$, or $d \not\mid m$ if it is not true. When $d \mid m$ then we say that $d$ is a divisor or factor of $m$, and $m$ a multiple of $d$.

Example. Let us illustrate this idea with a few examples.

1. The number 3 divides 18 since $18/3 = 6$, an integer. We write $3 \mid 18$.

2. We have $5 \not\mid 18$ because $18/5 = 3.6$, not an integer. Hence 5 is not a divisor of 18.

3. Both the numbers 28 and 42 have a common factor 7. We can see this by writing $28 = 7 \cdot 4$ and $42 = 7 \cdot 6$.

4. Multiples of 2 are integers of the form $2k$. These are the numbers $0, \pm 2, \pm 4, \pm 6, \ldots$ which we call the even numbers. The odd numbers, on the other hand, are those not divisible by 2 such as 1, $-5, 17, \text{etc.}$
Exercise 1.1. Does 3 divide 250313?1

Note that 0 cannot divide any number for division by 0 is not allowed. However, you may check that 0 is always divisible by other integers! This and some other elementary facts about divisibility are listed in the next proposition.

Proposition 1.1. The following statements hold.

1) The number 1 divides all integers.
2) \(d | 0\) and \(d | d\) for any integer \(d \neq 0\).
3) If \(d | m\) and \(m | n\) then \(d | n\).
4) If \(d | m\) and \(d | n\) then \(d | (am + bn)\) for any integers \(a\) and \(b\).

Proof. The first two statements follow immediately from the definition of divisibility. For (3) simply observe that if \(m/d\) and \(n/m\) are integers then so is \(n/d = n/m \times m/d\). Similarly for (4), the number \((am + bn)/d = a(m/d) + b(n/d)\) is an integer when \(d | m\) and \(d | n\). □

Any sum of multiples of \(m\) and \(n\), that is \(am + bn\), is what we call a linear combination of \(m\) and \(n\). In other fields of mathematics we say integral linear combination when \(a\) and \(b\) have to be integers, but for us there will be no ambiguity omitting the word integral. Proposition 1.1(4) states, in other words, that a common divisor of two numbers must divide their linear combinations too.

Exercise 1.2. Investigate true or false.

a) If \(d | m\) then \(d \leq m\).
b) If \(m | n\) and \(n | m\) then \(m = n\).
c) If \(c | m\) and \(d | n\) then \(cd | mn\).
d) If \(d | mn\) then either \(d | m\) or \(d | n\).
e) If \(dn | mn\) then \(d | m\).

Definition. For a real number \(x\), the notation \(\lfloor x \rfloor\) denotes the greatest integer \(\leq x\). For example \(\lfloor 3.14 \rfloor = 3\) and \(\lfloor 2 \rfloor = 2\). The integer-valued function \(f(x) = \lfloor x \rfloor\) is known as the floor function and so the symbol \(\lfloor x \rfloor\) is read “the floor of \(x\)”. It is useful to note the inequalities \(\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1\).

Exercise 1.3. What is \(\lfloor 250313/3 \rfloor\)?

---

1250313 is the course code for Number Theory at Philadelphia University, Jordan, where the author has first taught it.
1.1. DIVISIBILITY AND RESIDUES

Definition. With \( n > 0 \) we now define the residue of \( m \mod n \) by

\[
\text{ } m \mod n = m - \left\lfloor \frac{m}{n} \right\rfloor \cdot n
\]

Here the symbol \( \mod \) is to be read “mod”. For example to compute \( 18 \mod 5 \) we first see, since \( 18 / 5 = 3.6 \), that \( \left\lfloor 18 / 5 \right\rfloor = 3 \), therefore \( 18 \mod 5 = 18 - 3 \cdot 5 = 3 \).

Similarly we have \( 18 \mod 3 = 18 - 6 \cdot 3 = 0 \).

Exercise 1.4. Find these residues.

a) \( 369 \mod 5 \)
b) \( 24 \mod 8 \)
c) \( 123456789 \mod 10 \)
d) \( 250313 \mod 3 \)
e) \( 7 \mod 11 \)

Exercise 1.5. Suppose the time is now 11 o’clock in the morning. What time will it be after 100 hours? How does this problem relate to residues?

Note that \( m \mod n \) is really the remainder upon dividing \( m \) by \( n \) using the “long division” technique and that it lies in the range \( 0 \leq m \mod n \leq n - 1 \). In particular \( m \mod n = 0 \) if and only if \( n | m \). These claims, though seemingly obvious, need to be stated and proved carefully as follow.

Theorem 1.2. Suppose \( m, n \) are integers with \( n > 0 \). Then

1) \( 0 \leq m \mod n \leq n - 1 \).
2) \( m \mod n = 0 \) if and only if \( n | m \).
3) if \( m = q \cdot n + r \) with \( 0 \leq r \leq n - 1 \) then \( q = \left\lfloor m/n \right\rfloor \) and \( r = m \mod n \).

Proof. Let \( Q = \left\lfloor m/n \right\rfloor \) and \( R = m \mod n \).

1) By definition we have \( Q \leq m/n \) hence \( R = m - Qn \geq m - (m/n)n = 0 \).
But we also have \( Q + 1 > m/n \) hence \( R = m - Qn < m - (m/n - 1)n = n \).
We have shown that \( 0 \leq R < n \) and the claim follows.

2) If \( m/n \) is an integer then clearly \( R = m - (m/n)n = 0 \). Conversely if \( 0 = R = m - Qn \) then \( Q = m/n \) and thus, \( Q \) being integer, \( n | m \).

3) Suppose \( m = q \cdot n + r \) with \( 0 \leq r \leq n - 1 \). We then have \( m/n = q + r/n \) with \( 0 \leq r/n < 1 \). It can only mean that \( \left\lfloor m/n \right\rfloor = q \). Hence \( q = Q \) and \( r = m - Qn = R \).
Example. Let \( n = 2 \). Since \( m \% 2 = 0 \) or \( 1 \), we find that the integers can be partitioned in two groups: the even numbers in the form \( 2k \) and the odd numbers in the form \( 2k + 1 \). Similarly with \( n = 3 \) there are three classes of integers, those in the forms \( 3k \), \( 3k + 1 \), and \( 3k + 2 \).

Exercise 1.6. Prove that \( n^2 + 2 \) is not divisible by 4 for any integer \( n \).

We conclude this section with a simple yet useful fact which can be proved using the concept of residues.

Proposition 1.3. One in every \( k \) consecutive integers is divisible by \( k \).

Proof. Let \( m \) be the first integer and let \( r = m \% k \). If \( r = 0 \) then \( k \mid m \).
Otherwise \( 1 \leq r \leq k - 1 \) and our consecutive integers can be written

\[
m = \lfloor m/k \rfloor k + r, \lfloor m/k \rfloor k + (r + 1), \lfloor m/k \rfloor k + (r + 2), \ldots, \lfloor m/k \rfloor k + (r + k - 1)
\]

with \( r + k - 1 \geq k \). Then one of these numbers is \( \lfloor m/k \rfloor k + k = (\lfloor m/k \rfloor + 1)k \), that is a multiple of \( k \).

Exercise 1.7. Prove the following statements.

a) A number in the form \( n^2 \pm n \) is always even.

b) A number in the form \( n^3 - n \) is divisible by 3.

c) The number \( n^2 - 1 \) is divisible by 8 when \( n \) is odd.

d) The number \( n^5 - n \) is a multiple of 5 for every integer \( n \).

1.2 Greatest Common Divisors

Given two integers \( m, n \) there always exists a number dividing both, for instance \( d = 1 \). Moreover for each non-zero integer there is only a finite number of divisors, since \( d \mid m \) implies \( |d| \leq |m| \). We are then interested in finding the greatest of all common divisors of \( m \) and \( n \).

Definition. The greatest common divisor of two integers \( m \) and \( n \), not both zero, is the largest integer which divides both. This number is denoted by \( \gcd(m, n) \). For example \( \gcd(18, 24) = 6 \) because 6 is the largest integer with the property \( 6 \mid 18 \) and \( 6 \mid 24 \).

Exercise 1.8. Evaluate \( \gcd(m, n) \).

a) \( \gcd(28, 42) \)

b) \( \gcd(36, -48) \)

c) \( \gcd(24, 0) \)

d) \( \gcd(1, 99) \)

e) \( \gcd(123, 100) \)
Exercise 1.9. Find all integers \( n \) from 1 to 12 such that \( \gcd(n, 12) = 1 \).

Exercise 1.10. Investigate true or false.

a) \( \gcd(m, n) > 0 \)
b) \( \gcd(m, n) = \gcd(m - n, n) \)
c) \( \gcd(m, mn) = m \)
d) \( \gcd(m, m + 1) = 1 \)
e) \( \gcd(m, m + 2) = 2 \)

The good news is there exists an algorithm to evaluate \( \gcd(m, n) \) which is very time-efficient even for large values of \( m \) and \( n \). The name is Euclidean Algorithm, which is essentially an iterative application of the following theorem.

**Theorem 1.4.** For any integers \( m \) and \( n > 0 \) we have

\[
\gcd(m, n) = \gcd(n, m \mod n)
\]

**Proof.** It suffices to show that the two pairs \( \{m, n\} \) and \( \{n, m \mod n\} \) have identical sets of common divisors. This is achieved entirely using Proposition 1.1(4) upon observing that, from its definition, \( m \mod n \) is a linear combination of \( m \) and \( n \), and so is \( m \) of \( n \) and \( m \mod n \).

\[\square\]

**Example** (Euclidean Algorithm). Suppose we wish to evaluate \( \gcd(486, 171) \). First note that \( \left\lfloor \frac{486}{171} \right\rfloor = 2 \) and so \( 486 \mod 171 = 486 - 2 \cdot 171 = 144 \). Theorem 1.4 implies that \( \gcd(486, 171) = \gcd(171, 144) \), for which we may then iterate this process another time and so on. Here is the complete work.

\[
\begin{align*}
486 &= 2 \cdot 171 + 144 \\
171 &= 1 \cdot 144 + 27 \\
144 &= 5 \cdot 27 + 9 \\
27 &= 3 \cdot 9 + 0
\end{align*}
\]

\[
\gcd(486, 171) = \gcd(171, 144) = \gcd(144, 27) = \gcd(27, 9) = \gcd(9, 0)
\]

We arrive in the end at the result \( \gcd(486, 171) = \gcd(9, 0) = 9 \), which is the last non-zero residue in the computations shown on the left.

**Exercise 1.11.** Use Euclidean Algorithm to evaluate \( \gcd(m, n) \).

a) \( \gcd(456, 144) \)
b) \( \gcd(999, 503) \)
c) \( \gcd(1000, 725) \)
d) \( \gcd(12345, 67890) \)
e) \( \gcd(12345, 54321) \)
Now an extremely important property about greatest common divisors is that they are actually a linear combination.²

**Theorem 1.5** (Bezout’s Lemma). For any integers \( m, n \) we have

\[
\gcd(m, n) = am + bn
\]

for some integers \( a \) and \( b \).

**Proof.** Without loss of generality we may assume that \( n > 0 \). Now the sequence of residues in applying the Euclidean Algorithm consists of strictly decreasing positive integers, as a result of Theorem 1.2(1).

\[
gcd(m, n) = gcd(n, m \mod n) = gcd(m \mod n, n \mod (m \mod n)) = \cdots
\]

Hence this algorithm always terminates with a zero residue, say \( \gcd(m, n) = \cdots = \gcd(d, 0) = d \). Since each of these residues is a linear combination of the previous pair of integers, we may by a finite number of steps express \( d \) as a linear combination of \( m \) and \( n \).

\( \Box \)

**Exercise 1.12.** Prove that if \( d \mid m \) and \( d \mid n \) then \( d \mid \gcd(m, n) \).

The algorithm involved in actually finding the integers \( a \) and \( b \) in Bezout’s Lemma is called the *Extended Euclidean Algorithm*, illustrated in the next example. There is also a somewhat cleaner version of this method, known by the name of *Blankinship Algorithm*, which will be given at the end of this chapter as a project assignment.

**Example** (Extended Euclidean Algorithm). Let us find integers \( a, b \) such that \( \gcd(486, 171) = 486a + 171b \). We refer back to the Euclidean Algorithm example whereby we obtain \( \gcd(486, 171) = 9 \) but this time we will solve each equation for the residue.

\[
\begin{align*}
486 &= 2 \cdot 171 + 144, & 144 &= 486(1) + 171(-2) \\
171 &= 1 \cdot 144 + 27 & 27 &= 171(1) + 144(-1) \\
&= 171(1) + \{486(1) + 171(-2)\}(-1) & = 486(-1) + 171(3) \\
144 &= 5 \cdot 27 + 9 & 9 &= 144(1) + 27(-5) \\
&= \{486(1) + 171(-2)\} + \{486(-1) + 171(3)\}(-5) & = 486(6) + 123(-17)
\end{align*}
\]

The very last equation displays the desired result, \( a = 6 \) and \( b = -17 \).

²Worth remembering: \( \gcd \) is a linear combination!
Exercise 1.13. Continue with Exercise 1.11 and find integers $a, b$ such that $\gcd(m, n) = am + bn$.

Bezout’s Lemma also gives a number of ready consequences which will enable us to further develop the theory of divisibility and $\gcd$ in particular.

**Proposition 1.6.** Let $L$ be the set of all linear combinations of $m$ and $n$.

1) $L$ is equal to the set of all multiples of $\gcd(m, n)$.

2) $\gcd(m, n)$ is the least\(^3\) positive element of $L$.

3) $\gcd(m, n) = 1$ if and only if $L$ contains 1, in which case $L$ is the set of all integers.

*Proof.* All multiples of $\gcd(m, n)$ belong to $L$ by Bezout’s Lemma. Conversely $\gcd(m, n)$ divides every element of $L$ according to Proposition 1.1(4). This proves the first statement, from which follows the rest. \(\Box\)

**Corollary 1.7.** If $d \mid m$ and $d \mid n$ then $\gcd(m/d, n/d) = \gcd(m, n)/d$. In particular if $d = \gcd(m, n)$ then $\gcd(m/d, n/d) = 1$.

*Proof.* By Proposition 1.6(2) $\gcd(m/d, n/d)$ is the least positive linear combination of $m/d$ and $n/d$, which is $1/d$ times the least positive linear combination of $m$ and $n$, that is $\gcd(m, n)/d$. \(\Box\)

Exercise 1.14. Prove that if $k > 0$ then $\gcd(km, kn) = k \gcd(m, n)$.

**Definition.** Two integers $m, n$ are said to be relatively prime to each other when $\gcd(m, n) = 1$. This is to say that the two have no common factor other than 1. Proposition 1.6(3) says that relatively prime pair of integers can represent any integer as their linear combination.

**Theorem 1.8.** The following statements hold.

1) If $d \mid mn$ and $\gcd(d, m) = 1$ then $d \mid n$. (Euclid’s Lemma)

2) If $c \mid m$ and $d \mid m$ with $\gcd(c, d) = 1$ then $cd \mid m$.

3) If $\gcd(m, n) = 1$ and $\gcd(m, n') = 1$ then $\gcd(m, nn') = 1$.

*Proof.* Recall that $\gcd$ is a linear combination.

1) If $\gcd(d, m) = 1$ then $1 = ad + bn$ for some integers $a$ and $b$. Multiplying this by $n/d$ yields $n/d = an + b(mn/d)$, which is an integer if $d \mid mn$.

\(^3\)So the least shall be the greatest!
2) Again \( \gcd(c, d) = 1 \) implies \( 1 = ac + bd \). This time multiply by \( m/(cd) \)
to get \( m/(cd) = a(m/d) + b(m/c) \), which is an integer if \( c \mid m \) and \( d \mid m \).

3) Write \( 1 = am + bn \) and \( 1 = a'm + b'n' \) and multiply the two together,

\[
1 = (aa'm + ab'n' + a'bn)m + bb'nm'
\]

This last equation displays \( 1 \) as a linear combination of \( m \) and \( nn' \) and hence \( \gcd(m, nn') = 1 \) by Proposition 1.6(3).

\[\nabla\]

Euclid’s Lemma, that is the name for Theorem 1.8(1), is another simple yet very useful divisibility fact. Note that the relatively prime condition \( \gcd(d, m) = 1 \) cannot be omitted, for example we have \( 6 \mid 72 = 8 \cdot 9 \) where neither \( 6 \mid 8 \) nor \( 6 \mid 9 \) is true. The same can be said for Theorem 1.8(2) where, for instance, \( 4 \mid 60 \) and \( 6 \mid 60 \) but \( 4 \cdot 6 = 24 \not\mid 60 \).

Exercise 1.15. Prove the following statements.
a) Every number in the form \( n^3 - n \) is divisible by 6.
b) If \( n \) is odd then \( 24 \mid n^3 - n \).
c) The number 30 divides \( n^5 - n \) for all integers \( n \).

### 1.3 Linear Diophantine Equations

We are now in a position to describe the general solutions of linear equations in two variables \( x, y \) in the form \( mx + ny = c \). By a solution, of course, we mean integer solution, and that is the only reason an equation is called *diophantine*.

Being a linear combination of \( m \) and \( n \), according to Proposition 1.6(1) \( c \) is required to be a multiple of \( \gcd(m, n) \) or else there can be no solution. On the other hand when \( \gcd(m, n) \mid c \), we may find an equation \( ma + nb = \gcd(m, n) \) via Extended Euclidean Algorithm and then multiply it through by \( c/\gcd(m, n) \). This will produce at least one solution for \( x \) and \( y \). We give first an example before proceeding to finding the general solution.

Example. Let us find a solution for the linear equation \( 486x + 171y = 27 \). Again we refer to the earlier example on Extended Euclidean Algorithm whereby \( \gcd(486, 171) = 9 \), which divides 27, and \( 9 = 486(6) + 171(-17) \). Now multiply through this equation by 3 to see that \( x = 18 \) and \( y = -51 \) satisfy the linear equation.

Exercise 1.16. Find a solution of \( 34x + 55y = 11 \).
1.3. LINEAR DIOPHANTINE EQUATIONS

Theorem 1.9 (Linear Equation Theorem). The linear equation \( mx + ny = c \) has a solution if and only if \( d = \gcd(m, n) \mid c \), in which case all its solutions are given by the pairs \((x, y)\) in the form

\[
(x_0 - \frac{kn}{d}, y_0 + \frac{km}{d})
\]

for any particular solution \((x_0, y_0)\) and for any integer \(k\).

Proof. The necessary and sufficient divisibility condition has already been explained. Now suppose we have a particular solution \((x_0, y_0)\) and consider first the case \(d = 1\). All solutions of the linear equation must lie on the line passing through \((x_0, y_0)\) with a slope equal \(-m/n\). Another point on this line will be given by \((x_0 - t, y_0 + tm/n)\) for any real number \(t\). If the coordinates are to be integers then by Euclid’s Lemma we must have \(t = kn\) for some integer \(k\). Thus the general solution \((x_0 - kn/d, y_0 + km/d)\).

For the case \(d > 1\), replace the linear equation by \((m/d)x + (n/d)y = c/d\) which does not alter its solution set. But then Corollary 1.7 implies that \(\gcd(m/d, n/d) = 1\) and, repeating the argument for \(d = 1\), the general solution is therefore \((x_0 - kn/d, y_0 + km/d)\).

Exercise 1.17. Prove that \(\gcd(m, n) = 1\) if and only if the linear equation \(mx + ny = 1\) has a solution.

Example. The previous example continues. The equation 486\(x\) + 171\(y\) = 27 has a particular solution \((18, -51)\). The general solution is then given by \((18 - 171k/9, -51 + 486k/9) = (18 - 19k, -51 + 54k)\) for any integer \(k\). For instance \(k = 1\) corresponds to a solution \(x = -1, y = 3\) and \(k = 2\) gives \((-20, 57)\).

Exercise 1.18. Find all the solutions, if any, for each linear equation.

a) 34\(x\) + 55\(y\) = 11
b) 12\(x\) + 25\(y\) = 1
c) 24\(x\) + 18\(y\) = 9
d) 25\(x\) + 65\(y\) = -5
e) 42\(x\) - 28\(y\) = 70

Exercise 1.19. I made two calls today using my Fastlink account, one call to another Fastlink customer for 7 piasters per minute and another call to a MobileCom number for 12 piasters per minute. The total charge was one dinar and 33 piasters. For how long did I talk in each call? \(^4\)

\(^4\)The peculiar company names in this problem are relevant only in the kingdom of Jordan, where 1 dinar is equivalent to 100 piasters.
1.4 Blankinship Algorithm [Project 1]

Let us consider, one more time, the Extended Euclidean Algorithm example given in Section 1.2. The goal was to find integers $a, b$ such that $\gcd(486, 171) = 9 = 486a + 171b$. This time we will omit writing the $m$ and $n$ in each equation and align the “coefficients” neatly in columns. For convenience we add two extra rows at the top, corresponding to the equations $486 = 486(1) + 171(0)$ and $171 = 486(0) + 171(1)$, in this order.

\[
\begin{array}{ccc}
486 &=& 486(1) + 171(0) \\ 171 &=& 486(0) + 171(1) \\ 144 &=& 486(1) + 171(-2) \\ 27 &=& 486(-1) + 171(3) \\ 9 &=& 486(6) + 123(-17)
\end{array}
\]

Now concentrate on the three columns to the right. The first column is the sequence of residues, for instance 144 is the first row (486) minus 2 times the second row (171), where 2 comes from the floor of $486/171$. But note that this relation applies to the whole rows, hence the entire procedure can be done by performing row operations!

For another illustration, consider solving the equation $\gcd(444, 78) = 444a + 78b$. Since $\lfloor 444/78 \rfloor = 5$ we begin by subtracting 5 times row (78) from row (444) and on as follow.

\[
\begin{array}{ccc}
444 &=& 1 \quad 0 \\ 78 &=& 0 \quad 1 \\ 54 &=& 1 \quad -5 \\ 24 &=& -1 \quad 6 \\ 6 &=& 3 \quad -17 \\ 0 &=& -13 \quad 74
\end{array}
\]

Since $\gcd$ is the last non-zero residue, the result is $\gcd(444, 78) = 6$ with $a = 3$ and $b = -17$.

Exercise 1.20. Redo Exercise 1.13, this time using Blankinship Algorithm.

Assignment. Repeat this exercise with $m = 180180$ and $n$ equals the number obtained from the last six digits of your University Number (or any other personal identification number having at least six digits). This is your 6-digit Personal University Number, or PUN, to be remembered and used again in subsequent projects.
Chapter 2

Primes

Definition. A prime or prime number is an integer $p > 1$ with no positive divisors except 1 and $p$ itself. An integer $n > 1$ which is not a prime number is called composite.

For example 13 and 17 are primes, but 21 is composite because it is divisible by 3. Throughout this book, from now on, we shall designate $p$ to always denote a prime number.

Exercise 2.1. Find all prime numbers up to 50.

2.1 Primes and Divisibility

We will soon see that prime numbers are the building blocks of the integers. Together with the theory of divisibility, the properties of primes are foundational elements of number theory. We begin with the following observation.

Proposition 2.1. The following statements hold.

1) Other than 2, all primes are odd numbers.\footnote{Being the only even prime, 2 is the odd one out!}

2) Every integer greater than 1 has a prime divisor.

3) A number $n > 1$ is composite if and only if it has a prime divisor $p \leq \sqrt{n}$.

Proof. 1) By definition even numbers are multiples of 2, hence they are all composite except 2 is prime.
2) Suppose, by induction, the statement is true up to $n - 1$. Either $n$ is prime, and its own prime divisor, or else it has a divisor $d$ satisfying $1 < d < n$. It follows that $d$ has a prime divisor which is also a divisor of $n$ by Proposition 1.1(3).

3) A prime has no prime divisor less than itself. For composite $n = ab$ with $a, b > 1$ either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ must hold. Whichever is true, by (2) $a$ or $b$ has a prime divisor $p$ which satisfies $p \leq \sqrt{n}$ and $p \mid n$. ▽

Proposition 2.1(2) and (3) together imply that in order to test the primality of a number $n$ it suffices to check divisibility by the primes $2, 3, 5, \ldots$ up to $\sqrt{n}$. For example $\sqrt{113} \approx 10.63$ and the only primes up to this are 2, 3, 5, and 7, none of which divides 113. Hence 113 is a prime.

Exercise 2.2. Determine prime or composite.

a) 383
b) 447
c) 799
d) 811
e) 250313

Now some divisibility properties involving primes can be presented. The simplest result is perhaps the following lemma, followed by a prime analog of Euclid’s Lemma and its natural generalization.

Lemma 2.2. Let $p$ be a prime. For any integer $m$ we have $\gcd(p, m) = p$ if $p \mid m$, otherwise $\gcd(p, m) = 1$.

Proof. The claim is justified since 1 and $p$ are the only divisors of $p$. ▽

Theorem 2.3. If a prime $p \mid mn$ then either $p \mid m$ or $p \mid n$. More generally, if $p \mid n_1 n_2 \cdots n_k$ then $p$ divides one of $n_1, n_2, \ldots, n_k$.

Proof. If $p \not\mid m$ then by Lemma 2.2 $\gcd(p, m) = 1$ and by Theorem 1.8(1) (Euclid’s Lemma) we must have $p \mid n$. Repeated use of this argument establishes the general claim. ▽

Exercise 2.3. Investigate true or false.

a) $n^2 + n + 41$ is prime for all $n \geq 0$.
b) $n^2 - 81n + 1681$ is prime for all $n \geq 1$.
c) If $p \mid n^2$ then $p \mid n$.
d) If $p \mid n^2$ then $p^2 \mid n^2$. 
2.2 Factorization into Primes

According to Proposition 2.1(2) every composite \( n \) can be expressed as a product of two numbers at least one of which is prime. But if the other factor is again composite then we break it down further as a product of a prime and another, possibly composite, and so on in this way until we have \( n \) written as a product of only prime numbers. This procedure is what we call \textit{prime factorization} of \( n \) or \textit{factorization of \( n \) into primes}.

The next theorem, which is of greatest importance in the theory of numbers, not only guarantees that factorization into primes can always be done but also assures that the end collection of prime factors is uniquely determined by \( n \), perhaps differing only in the order they are written. For example in factoring the number 5060 one may obtain \( 5060 = 2 \cdot 2 \cdot 5 \cdot 11 \cdot 23 \) and another \( 5060 = 5 \cdot 2 \cdot 23 \cdot 2 \cdot 11 \), but it would be impossible to find another prime factor outside the collection \{2, 2, 5, 11, 23\}.

\textbf{Theorem 2.4} (The Fundamental Theorem of Arithmetic). Every integer greater than 1 is a product of prime numbers in a unique way, up to reordering of the prime factors.

\textit{Proof.} We use induction to show that such integer is a product of primes. Suppose this claim is true up to \( n - 1 \). By Proposition 2.1(2), \( n \) has a prime divisor, say \( n = pn' \) with \( n' < n \). It follows that \( n' \) is a product of primes and so is \( n \).

To prove uniqueness we proceed by contradiction. Suppose we have two different multisets of primes \( p \)'s and \( q \)'s whose products both equal \( n \). Equating these products and cancelling out all common terms will result in \( p_1p_2 \cdots p_j = q_1q_2 \cdots q_k \) where none of the \( p \)'s equals any of the \( q \)'s. By Theorem 2.3, \( p_1 \) must divide one of the \( q \)'s, say \( q_i \), implying that \( p_1 = q_i \), a contradiction.

\( \square \)

\textit{Exercise 2.4}. Factor these numbers into primes.

a) 123 
b) 400 
c) 720 
d) 7575 
e) 250313

Theorem 2.4 has many essential consequences as far as divisibility is concerned. For example once the factorization of a composite is known, say \( n = 234000 = 2^4 \cdot 3^2 \cdot 5^3 \cdot 13 \), then we know that every positive divisor of \( n \)
must also factor into these same primes but with less, or equal, power for each. That is, if \( d \mid n \) then \( d = 2^h \cdot 3^i \cdot 5^j \cdot 13^k \) where \( 0 \leq h \leq 4, 0 \leq i \leq 2, 0 \leq j \leq 3, 0 \leq k \leq 1 \). There are \( 5 \cdot 3 \cdot 4 \cdot 2 = 120 \) positive divisors in all.

**Exercise 2.5.** Count how many positive divisors each number has.

a) 300  
 b) 720  
 c) 1024  
 d) 2310  
 e) 250313

**Exercise 2.6.** Find all the positive divisors of 968.

**Exercise 2.7.** Prove that if \( d^2 \mid m^2 \) then \( d \mid m \).

**Corollary 2.5.** Suppose \( m \) and \( n \) are factored into powers of distinct primes: 
\( m = \prod p_i^{j_i} \) and \( n = \prod p_i^{k_i} \) with \( j_i, k_i \geq 0 \). Then \( \gcd(m, n) = \prod p_i^{e_i} \) where \( e_i = \min\{j_i, k_i\} \).

**Proof.** By Theorem 2.4 a divisor of \( m \) must be of the form \( d = \prod p_i^{e_i} \) with \( e_i \leq j_i \). Similarly if \( d \mid n \) then \( e_i \leq k_i \) and so the greatest possible choice for \( d \) is that with \( e_i = \min\{j_i, k_i\} \).

Hence we now have another method for evaluating \( \gcd(m, n) \), totally independent of the Euclidean Algorithm. In contrast, however, factoring is generally slow and the computation time grows exponentially with the size of the integer.

**Example.** We evaluate \( \gcd(27720, 61152) \) using prime factorization:

\[
27720 = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^1 \cdot 11^1 \cdot 13^0 \\
61152 = 2^5 \cdot 3^1 \cdot 5^0 \cdot 7^2 \cdot 11^0 \cdot 13^1 \\
\gcd(27720, 61152) = 2^3 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^0 \cdot 13^0
\]

Thus \( \gcd(27720, 61152) = 2^3 \cdot 3 \cdot 7 = 168 \).

**Exercise 2.8.** Evaluate \( \gcd(m, n) \) using Corollary 2.5.

a) \( m = 400 \) and \( n = 720 \)  
 b) \( m = 514500 \) and \( n = 70560 \)  
 c) \( m = 2^3 \cdot 3^8 \cdot 5^4 \cdot 7^5 \) and \( n = 3^7 \cdot 5^2 \cdot 7^2 \)  
 d) \( m = 2^5 \cdot 5^7 \cdot 11^3 \) and \( n = 3^7 \cdot 7^2 \cdot 13^9 \)  
 e) \( m = 2^4 \cdot 5^2 \cdot 7 \cdot 11^3 \) and \( n = 2^7 \cdot 3^2 \cdot 5^2 \cdot 11 \)

**Exercise 2.9.** Show that \( \gcd(m^2, n^2) = \gcd(m, n)^2 \).
2.3. THE INFINITUDE OF PRIMES

Definition. The least common multiple of two non-zero integers is the smallest positive integer which is divisible by both. For example \( \text{lcm}(4, 6) = 12 \) because it is the smallest positive integer with the property \( 4 \mid 12 \) and \( 6 \mid 12 \).

Exercise 2.10. Let \( m, n \) be any non-zero integers.

a) Use prime factorization to find a formula for \( \text{lcm}(m, n) \).

b) Prove that if \( m \mid k \) and \( n \mid k \) then \( \text{lcm}(m, n) \mid k \).

c) Find an equation relating between \( \text{gcd}(m, n) \) and \( \text{lcm}(m, n) \).

d) Illustrate your answers using \( m = 600 \) and \( n = 630 \).

2.3 The Infinitude of Primes

One relevant question concerning primes is whether or not there exist infinitely many primes of a special form, such as \( 4n + 3 \) or \( n^2 + 1 \). This will turn to generate very difficult problems many of which are still unsolved. But first, of course, we need to be convinced that the sequence of prime numbers is indeed infinite and this fact is not hard to demonstrate.

Theorem 2.6. There are infinitely many prime numbers.

Proof. If there were only finitely many prime numbers, let \( N \) be the product of them all. Now by Proposition 2.1(2), one of these prime divisors of \( N \) must also divide \( N + 1 \), thus it would also divide \( 1 = (N + 1) - N \) according to Proposition 1.1(4). This is absurd since all primes are larger than 1. \( \square \)

What is more, we have a way to estimate the distribution of primes among the natural numbers in a given interval. Let \( \pi(x) \) denote the number of primes up to \( x \). For example, enumerating the smallest few primes \( 2, 3, 5, 7, 11, 13 \) gives us \( \pi(13) = 6 \). Similarly \( \pi(50) = 15 \) (See Exercise 2.1). Then for large values of \( x \) the function \( \pi(x) \) behaves as \( x/\log x \) where \( \log \) denotes the natural logarithm. We state this result as the next theorem, but unfortunately the prove requires techniques from complex analysis and therefore we will not provide it here.

Theorem 2.7 (The Prime Number Theorem). We have

\[
\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1
\]

Moreover it has been found that \( x/(\log x - 1) \) is a slightly better function than \( x/\log x \) in approximating \( \pi(x) \) for large values of \( x \).

No Proof. The proof is beyond the scope of elementary number theory. \( \square \)
Example. Up to 25 billions there are roughly
\[ \pi(25 \times 10^9) \approx \frac{25,000,000,000}{\log 25,000,000,000} - 1 \approx 1,089,697,743 \]
prime numbers, comparable to the actual count, which is 1,091,987,405.

Exercise 2.11. Estimate how many prime numbers there are,
a) up to one million.
b) up to ten millions.
c) between 9 millions and 10 millions.
d) among the ten-digit integers.

Now back to primes of special forms. We consider primes that come in the form \( an + b \) for given integers \( a, b \). According to Proposition 1.6(1) every number in this form is a multiple of \( \gcd(a, b) \). Hence if \( \gcd(a, b) > 1 \) then the range of \( an + b \) can contain only composites, except perhaps \( \gcd(a, b) \) itself if a prime. So to avoid triviality we need \( \gcd(a, b) = 1 \), and it turns that this condition is really sufficient to ensure the infinitude of such primes.

The theorem for this is a very advanced general result whose proof lies in the domain of analytic number theory and, again, we will not give it here considering our limitations. Instead we will supply, by way of illustration, a simple proof for the specific case \( a = 4, b = 3 \).

**Theorem 2.8** (Dirichlet’s Theorem on Primes in Arithmetic Progressions). Primes of the form \( an + b \) are infinitely many if and only if \( \gcd(a, b) = 1 \).

Partial proof for \( a = 4 \) and \( b = 3 \). First note that a prime \( p > 2 \) must have the form \( 4n + 1 \) or \( 4n + 3 \). Second, the product of two numbers in the form \( 4n + 1 \) is again of the same form, hence a number in the form \( 4n + 3 \) must have a prime divisor of the form \( 4n + 3 \).

We claim that there are infinitely many primes in the form \( 4n + 3 \). If it were not so, let \( N \) be the product of them all. As noted, one of these prime divisors of \( N \) must be a prime divisor of the number \( 4(N - 1) + 3 \) hence it would also divide \( 1 = 4N - (4(N - 1) + 3) \) and this is a contradiction. \( \nabla \)

Exercise 2.12. Prove that there are infinitely many primes in the form \( 6n+5 \).

We conclude this section with a number of quite well-known unsolved problems concerning primes in particular forms. Mathematicians sometimes have a good reason to believe that a certain result should be true although they have yet no proof of it. Rather than being called a theorem, these unproved assertions\(^2\) are named **conjectures**.

\(^2\)Of course then, they could be false after all!
Conjecture 2.9. The following claims are not supported by proofs.

1) There are infinitely many primes of the form \( n^2 + 1 \).
   The prime 101 = 10^2 + 1 is one of them.

2) There are only finitely many primes of the form \( 2^{2^n} + 1 \).
   Such primes are called Fermat primes. The first five integers in this form
   are Fermat primes but none other has been found until now.

3) There are infinitely many primes in the form \( p + 2 \), where \( p \) is prime.
   The pair \((p, p + 2)\) of primes, like 11 and 13, are called twin primes. At
   the time of this writing the largest known pair is \( 2003663613 \cdot 2^{195000} \pm 1 \),
   discovered in January 2007. They each have 58,711 decimal digits.

4) There are infinitely many primes in the form \( 2^p - 1 \).
   These are the Mersenne primes, for example the prime 31 = 2^5 - 1. Note
   that the exponent \( p \) must be a prime as a necessary, but not sufficient,
   condition for a Mersenne prime. (See Exercise 2.13) There are only
   44 Mersenne primes found so far, the latest in September 2006 is the
   9,808,358-digit prime corresponding to \( p = 32582657 \).

5) There are infinitely many primes of the form \( 2p + 1 \).
   A prime \( p \) for which \( 2p+1 \) is again prime is named Sophie Germain prime.
   An example is the prime 11 since \( 2 \cdot 11 + 1 = 23 \) is also prime. The biggest
   example to date has 51,910 digits, namely \( p = 48047305725 \cdot 2^{172403} - 1 \).

Exercise 2.13. Show that if \( k \) is composite then so is \( 2^k - 1 \).

Exercise 2.14. Find the smallest five primes of each kind.

a) Of the form \( n^2 + 1 \)
b) Fermat prime
c) Mersenne prime
d) Sophie Germain prime

Exercise 2.15. Find all pairs of twin primes below 100.

Exercise 2.16. Find all possible prime triplets, meaning a set of three primes
in the forms \( p \) and \( p \pm 2 \).

Exercise 2.17. Another famous conjecture, not related to any particular
form, is the Goldbach’s Conjecture. It claims that every even number \( n > 2 \)
is a sum of two primes. Write the following even numbers as sums of two
primes, in more than one way if possible.

a) 4
b) 28
c) 456
d) 1000
2.4 Fermat Factorization

We have already hinted that integer factorization, though theoretically trivial, is extremely slow in its practical implementation. In fact factorization remains a major area of modern research in the field of computational number theory. We present here an old, but still used in principle, factorization technique due to Fermat, thus the name.

If \( n = x^2 - y^2 \) then it factors to \( n = (x + y)(x - y) \). This fact is the simple idea behind the method of Fermat Factorization. We seek a factor of \( n \) by calculating the numbers \( y^2 = x^2 - n \) for each integer \( x \geq \sqrt{n} \) until we find a perfect square, that is, whose square root is an integer. For example with \( n = 4277 \) we first calculate \( \sqrt{4277} \approx 65.39 \) so we start with \( x = 66 \).

\[
\begin{align*}
66^2 - 4277 &= 79 \\
67^2 - 4277 &= 212 \\
68^2 - 4277 &= 347 \\
69^2 - 4277 &= 484 = 22^2 \\
\end{align*}
\]

The result is \( 4277 = 69^2 - 22^2 = (69 + 22)(69 - 22) = 91 \cdot 47 \).

Note that Fermat Factorization always works when \( n \) is odd because if \( n = ab \) with both \( a, b \) odd then \( n = x^2 - y^2 \) with \( x = (a + b)/2 \) and \( y = (a - b)/2 \). Moreover this shows that we should terminate the algorithm when we reach \( x = (n + 1)/2 \), in which case we obtain, trivially, \( n = n \cdot 1 \) and \( n \) is prime. The bad news is, for large \( n \), the iterations from \( \sqrt{n} \) to \( (n + 1)/2 \) could take too long to be computationally feasible. Hence Fermat Factorization works best only when \( n \) has at least one factor relatively close to its square root.

Exercise 2.18. Follow the above example with the following numbers for \( n \).

a) 2117  

b) 16781  

c) 65593  

d) 70027

Assignment. With the help of Fermat Factorization try to factor into primes your 6-digit PUN from Project 1.
Chapter 3

Congruences

The theory of congruences is perhaps what has made elementary number theory a modern systematic discipline as it is studied today. Congruent numbers, essentially, are those leaving the same residues upon division by a fixed integer, the modulus. Hence modular arithmetic could be another, equally proper, title for this chapter.

3.1 Congruences and Residue Classes

The following proposition will help in understanding what a congruence really involves.

**Proposition 3.1.** The following statements are all equivalent, where \( n > 0 \).

1) \( a \% n = b \% n \)

2) \( n \mid (a - b) \)

3) \( a = b + nk \) for some integer \( k \)

**Proof.** By the definition of residues mod \( n \), the first statement can be written

\[
a - \left\lfloor \frac{a}{n} \right\rfloor n = b - \left\lfloor \frac{b}{n} \right\rfloor n
\]

Since floor values are always integers, it follows that \( a - b \) is a multiple of \( n \), say \( a - b = nk \) for some integer \( k \). But then \( a \% n = (b + nk) \% n = \)

\[
b + nk - \left\lfloor \frac{b + nk}{n} \right\rfloor n = b + nk - \left( \left\lfloor \frac{b}{n} \right\rfloor + k \right) n = b - \left\lfloor \frac{b}{n} \right\rfloor n = b \% n
\]

Thus the argument has come round to complete the proof. \( \nabla \)
Definition. We now define two integers \(a, b\) to be congruent modulo \(n > 0\) if any one of the above equivalent conditions holds, in which case we write \(a \equiv b \pmod n\). Naturally we shall denote the negation by \(a \not\equiv b \pmod n\).

Example. Let us illustrate this idea with a few examples.

1) Both \(13 \% 3\) and \(4 \% 3\) equal 1. We write \(13 \equiv 4 \pmod 3\). Note that \(13 - 4 = 9\), divisible by 3.

2) We have \(7 \mid 42\), hence \(42 \equiv 0 \pmod 7\). In general \(a \equiv 0 \pmod n\) if and only if \(n \mid a\).

3) For arbitrary even numbers \(a\) and \(b\) we have \(a \equiv b \equiv 0 \pmod 2\), whereas if they were odd, \(a \equiv b \equiv 1 \pmod 2\). More generally, \(a \equiv a \% n \pmod n\) for any integer \(a\) and any modulus \(n > 0\).

4) If \(a \equiv 3 \pmod 4\) then \(a\) belongs to the set \{\ldots, -5, -1, 3, 7, 11, 15, \ldots\}. Conversely any number \(a\) of the form \(4k + 3\) satisfies the congruence.

Exercise 3.1. Show that if \(a\) is odd then \(a^2 \equiv 1 \pmod 8\).

Exercise 3.2. Prove that if a prime \(p \equiv 1 \pmod 3\) then \(p \equiv 1 \pmod 6\).

Exercise 3.3. Investigate true or false.

a) If \(a \equiv b \pmod n\) and \(d \mid n\) then \(a \equiv b \pmod d\).

b) If \(a \equiv b \pmod n\) then \(\gcd(a, n) = \gcd(b, n)\).

c) If \(a \equiv b \pmod n\) then \(ma \equiv mb \pmod {mn}\).

d) If \(ma \equiv mb \pmod {mn}\) then \(a \equiv b \pmod n\).

e) If \(ma \equiv mb \pmod n\) then \(a \equiv b \pmod n\).

Proposition 3.2. Suppose \(a \equiv b \pmod n\) and \(c \equiv d \pmod n\). Then

1) \(a + c \equiv b + d \pmod n\)

2) \(ac \equiv bd \pmod n\)

3) \(f(a) \equiv f(b) \pmod n\) for any integral polynomial \(f(x)\).

Proof. Proposition 3.1 allows us to write \(a = b + nk\) and \(c = d + nh\) for some integers \(k, h\). Then the sum \(a + c = b + d + n(k + h)\) and the product \(ac = bd + n(bh + kd + nkh)\) show, by Proposition 3.1 again, why statements (1) and (2) hold, of which the last statement is an immediate generalization. ∨

The above results show that we can perform congruence arithmetic, for a fixed modulus, similar to ordinary addition and multiplication. For division, however, an added condition is required for in general it does not apply. For instance dividing through the congruence \(6 \equiv 2 \pmod 4\) by 2 will result in a false statement \(3 \equiv 1 \pmod 4\).
3.1. CONGRUENCES AND RESIDUE CLASSES

Proposition 3.3. If \( am \equiv bm \pmod{n} \) and \( \gcd(m,n) = 1 \) then \( a \equiv b \pmod{n} \).

Proof. If \( n \mid (am - bm) = (a - b)m \) and \( \gcd(m,n) = 1 \) then \( n \mid (a - b) \) according to Euclid’s Lemma (Theorem 1.8(1)). \( \nabla \)

Exercise 3.4. Let \( d = \gcd(m,n) \). Prove that \( am \equiv bm \pmod{n} \) if and only if \( a \equiv b \pmod{n/d} \).

Definition. Let \( n > 0 \). For every integer \( b \) we define the residue class or congruence class of \( b \) modulo \( n \) to be the set of all integers \( a \) such that \( a \equiv b \pmod{n} \). We denote this class by \( [b]_n \) or simply \( [b] \) when there is no ambiguity.

By Proposition 3.1 the elements of \( [b]_n \) are precisely those of the form \( b + nk \) for any integer \( k \). For examples \( [1]_2 \) are the odd numbers and \( [3]_4 = \{ \ldots, -9, -5, -1, 3, 7, 11, 15, \ldots \} \). This concept will provide a nice algebraic structure\(^1\) to the set of integers, but for our purposes we will be content with what follow.

Proposition 3.4. For a fixed modulus \( n > 0 \), the following properties hold.

1) The residue class modulo \( n \) of each integer \( b \) is an infinite set of numbers in the form \( b + nk \). In particular \( [b] \) contains \( b \).

2) If \( b \equiv b' \pmod{n} \) then \( [b]_n = [b']_n \), whereas if \( b \not\equiv b' \pmod{n} \) then the two classes have no element in common.

3) Every integer \( a \) belongs to the residue class \( [a \% n]_n \).

4) There exist exactly \( n \) residue classes modulo \( n \), which are those represented by \( [0], [1], [2], \ldots, [n - 1] \), and they form a partition for the set of integers, meaning that every integer belongs to exactly one class.

Proof. The first claim is trivial. Next, the relation \( [b] = [b'] \) implies, since \( [b'] \) contains \( b \), that \( b \equiv b' \pmod{n} \). Conversely if \( b \% n = b' \% n \) then for any integer \( a \) we have \( a \equiv b \pmod{n} \) if and only if \( a \equiv b' \pmod{n} \), and \( [b] = [b'] \). This proves the second claim, which also implies that every integer \( a \) can belong to at most one residue class. But clearly \( a \) belongs to \( [a \% n] \) thus, since \( 0 \leq a \% n \leq n - 1 \), there can be no more than \( n \) residue classes represented by the numbers \( 0, 1, 2, \ldots, n - 1 \). And no two of these numbers are congruent modulo \( n \), for their difference would be too small to be divisible by \( n \), hence the \( n \) classes are all distinct, proving all. \( \nabla \)

\(^1\)Congruence is an equivalence relation, to start with.
Example. With $n = 2$ the integers are partitioned into two classes, the set of even numbers $[0]_2$ and the set of odd numbers $[1]_2$. Note that every integer is either even or odd but never both. We use the word *parity* to denote membership in a residue class modulo 2. For instance 3 and 10 have opposite parity, but 12 and 34 are of the same parity.

Similarly with $n = 3$ there are 3 classes of integers given by

- $[0]_3 = \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$
- $[1]_3 = \{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\}$
- $[2]_3 = \{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\}$

Note that the choice of 0 in representing $[0]_3$ is not at all unique, for instance $[3]_3 = [0]_3$. In fact, any element of a residue class can be chosen to represent the class.

Definition. A set of $n$ numbers form a complete residue system modulo $n$ if each comes from a different residue class modulo $n$. Thus a complete residue system modulo 3 can be $\{0, 1, 2\}$, or $\{1, 2, 3\}$, $\{3, 7, 11\}$, $\{-10, 6, 10\}$, etc.

Exercise 3.5. Find a complete residue system modulo $n$, with the given extra condition.

a) $n = 9$, all even numbers
b) $n = 7$, all odd numbers
c) $n = 5$, all multiples of 4
d) $n = 5$, all prime numbers
e) $n = 4$, all primes

### 3.2 Linear Congruences

It will be useful for us next to study linear congruences in the form $mx \equiv c \pmod{n}$. Note first that in any congruence $f(x) \equiv c \pmod{n}$ where $f(x)$ is an integral polynomial, $x = b$ is a solution if and only if $x = a$ is too, for any $a$ in $[b]_n$. This is essentially Proposition 3.2(3).

Hence by *distinct* or *incongruent solutions modulo* $n$ we mean solutions belonging to different residue classes. In fact in studying such a congruence it will suffice to consider only the values of $x$ in a complete residue system. Similarly by a *unique solution modulo* $n$ we mean a general solution given by a single residue class, which really contains infinitely many!

Now resuming with the linear congruence $mx \equiv c \pmod{n}$. By the definition of congruence, this problem is equivalent to that of linear equations in the form $mx = c + nk$, or in a more familiar way, $mx + ny = c$. Not surprisingly we conclude the following result about linear congruences.
3.2. LINEAR CONGRUENCES

Theorem 3.5 (Linear Congruence Theorem). The linear congruence $mx \equiv c \pmod{n}$ has a solution if and only if $d = \gcd(m, n) \mid c$, in which case it has a unique solution modulo $n/d$ given by $x \equiv x_0 \pmod{n/d}$ for any particular solution $x_0$.

Proof. The congruence is equivalent to the linear equation $mx + ny = c$ and, under the same condition, Linear Equation Theorem gives the general solution in the form $x = x_0 + k(n/d)$, that is the residue class $[x_0]_{n/d}$. ▽

Example (Linear Congruence). Consider $15x \equiv 9 \pmod{21}$. We check that $\gcd(15, 21) = 3 \mid 9$. Next we turn to Extended Euclidean Algorithm to find a particular solution. This gives us, omitting details, $15(3) + 21(-2) = 3$, hence $x_0 = 3 \cdot 3 = 9$. The general solution is therefore $x \equiv 9 \pmod{7}$, which are the integers in $[2]_7 = \{\ldots, -12, -5, 2, 9, 16, \ldots\}$.

Exercise 3.6. Solve each linear congruence.

a) $8x \equiv 5 \pmod{13}$
b) $35x \equiv 7 \pmod{49}$
c) $12x \equiv 18 \pmod{54}$
d) $27x \equiv 1 \pmod{209}$
e) $6x \equiv 9 \pmod{1023}$

One important consequence of Theorem 3.5 is in the idea of modular inverses, that is two integers whose product equals 1 modulo $n$. In ordinary arithmetic no such integers can exist, other than ±1.

Definition. Two integers $a$ and $b$ are inverses of each other modulo $n$ if $ab \equiv 1 \pmod{n}$, in which case we may write $a \equiv b^{-1} \pmod{n}$ or equivalently $b \equiv a^{-1} \pmod{n}$. For example 3 and 5 are inverses modulo 7 since $3 \cdot 5 = 15 \equiv 1 \pmod{7}$. Similarly the congruence $5^2 \equiv 1 \pmod{12}$ implies that 5 is its own inverse, or self-inverse, modulo 12.

Corollary 3.6 (Modular Inverse Theorem). The number $a$ has an inverse modulo $n$ if and only if $\gcd(a, n) = 1$, in which case its inverse is unique modulo $n$.

Proof. Simply let $m = a$ and $c = 1$ in the Linear Congruence Theorem. ▽

Exercise 3.7. Find all integers $b$, if any, such that $b \equiv a^{-1} \pmod{n}$.

a) $a = 2$ and $n = 7$
b) $a = -5$ and $n = 8$
c) $a = 7$ and $n = 12$
d) $a = 35$ and $n = 42$
e) \( a = 27 \) and \( n = 209 \)

Exercise 3.8. Which integers, from 1 to 12, have an inverse modulo 12?

We conclude the section with an interesting congruence theorem involving a prime modulus. It employs the following lemma, which is simple but perhaps more practical than the theorem itself.

**Lemma 3.7.** If \( p \) is prime then \( a^2 \equiv 1 \pmod{p} \) implies \( a \equiv \pm 1 \pmod{p} \).

**Proof.** According to Theorem 2.3, if \( p \) divides \( a^2 - 1 = (a + 1)(a - 1) \) then \( p \mid (a + 1) \) or \( p \mid (a - 1) \), hence the claim. \( \Box \)

Exercise 3.9. Prove that if \( a^2 \equiv b^2 \pmod{p} \) then \( a \equiv \pm b \pmod{p} \).

**Theorem 3.8** (Wilson’s Theorem). If \( p \) is prime then \((p-1)! \equiv -1 \pmod{p} \).

**Proof.** According to Lemma 2.2, each of the numbers \( 1, 2, \ldots, p-2 \) is relatively prime to \( p \), hence the Modular Inverse Theorem assures that they have inverses modulo \( p \). Furthermore by Lemma 3.7 none of them is self-inverse, except 1. Hence \((p-2)!\) is made up of the product of pairs of inverses modulo \( p \), so that \((p-2)! \equiv 1 \pmod{p} \). Now multiply by \( p - 1 \equiv -1 \pmod{p} \) to finish the proof. \( \Box \)

For example 101 is a prime, hence 100! \( \equiv -1 \pmod{101} \). Another way to state this result is by writing 100! \( \% 101 = 100 \). Wilson’s Theorem is always false for composite modulus, (See Exercise 3.11) for instance with \( n = 65 = 5 \cdot 13 \) we have \( 64! \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 13 \cdot \cdots \cdot 64 \equiv 0 \pmod{65} \). Thus Wilson’s Theorem is our first primality criterion, for testing whether a given integer is prime or composite. The enormous task of computing factorials, unfortunately, makes it of no practical value.

Exercise 3.10. Show that both \( 35! - 1 \) and \( 34! - 18 \) are multiples of 37.

Exercise 3.11. Prove that the converse of Wilson’s Theorem is also true.

### 3.3 Chinese Remainder Theorem

Chinese Remainder Theorem is a principle that applies to a pair of congruences with relatively prime moduli. This principle is so basic that it has appeared in many different forms and levels of generalization in abstract settings of higher algebra.\(^2\) We present the theorem in two most common forms and its generalization to a system of congruences.

\(^2\)And, evidently, it deserves a section of its own!
3.3. CHINESE REMAINDER THEOREM

**Theorem 3.9** (Chinese Remainder Theorem, First Form). If \( \gcd(m, n) = 1 \) then \( a \equiv b \pmod{mn} \) if and only if \( a \equiv b \pmod{m} \) and \( a \equiv b \pmod{n} \).

*Proof.* Necessity follows immediately from Proposition 1.1(3). To show sufficiency, note that if both \( m \) and \( n \) divide \( (a - b) \) then by Theorem 1.8(2) \( mn \mid (a - b) \), provided that \( \gcd(m, n) = 1 \).

\[ \begin{align*}
\text{Example.} & \quad \text{Consider the congruence } x \equiv 5 \pmod{12}, \text{ whose solution set is given by the class } [5]_{12} = \{ \ldots, -19, -7, 5, 17, 29, \ldots \}. \quad \text{According to Theorem 3.9 this congruence can be replaced by a system of two congruences, namely } x \equiv 5 \pmod{3} \text{ and } x \equiv 5 \pmod{4}. \quad \text{(Why?) Independently, these two congruences have their solution sets given by, respectively,} \\
[5]_3 &= \{ \ldots, -19, -16, -13, -10, -7, -4, -1, 2, 5, 8, 11, 14, 17, 20, \ldots \} \\
[5]_4 &= \{ \ldots, -23, -19, -15, -11, -7, -3, 1, 5, 9, 13, 17, 21, 25, 29, \ldots \}
\end{align*} \]

Hence \([5]_{12}\) consists of precisely the common elements of \([5]_3\) and \([5]_4\).

*Exercise* 3.12. Find the smallest positive integer \( x \) which satisfies all three congruences: \( x \equiv 6 \pmod{7} \), \( x \equiv 10 \pmod{11} \), \( x \equiv 12 \pmod{13} \).

*Exercise* 3.13. Prove that if \( a \equiv b \pmod{m} \) and \( a \equiv b \pmod{n} \) then \( a \equiv b \pmod{\text{lcm}(m, n)} \).

*Exercise* 3.14. Prove the following analog of Wilson’s Theorem for twin primes: \( p \) and \( q = p + 2 \) are primes if and only if \( 4(p - 1)! \equiv -p - 4 \pmod{pq} \).

**Theorem 3.10** (Chinese Remainder Theorem, Second Form). Suppose \( \gcd(m, n) = 1 \). The pair of congruences \( x \equiv c \pmod{m} \) and \( x \equiv d \pmod{n} \) have a unique common solution modulo \( mn \).

*Proof.* Solutions of \( x \equiv c \pmod{m} \) are of the form \( c + mk \) for any integer \( k \). We are seeking a value of \( k \) for which \( c + mk \equiv d \pmod{n} \), or \( mk \equiv d - c \pmod{n} \). By the Linear Congruence Theorem such an integer \( k \), hence a common solution, exists since \( \gcd(m, n) = 1 \). Now any two solutions \( x_1, x_2 \) must satisfy \( x_1 \equiv c \equiv x_2 \pmod{m} \) and \( x_1 \equiv d \equiv x_2 \pmod{n} \) so that \( x_1 \equiv x_2 \pmod{mn} \) by Theorem 3.9, proving uniqueness.

\[ \blacksquare \]

*Example.* Let us solve the congruences \( x \equiv 2 \pmod{3} \) and \( x \equiv 1 \pmod{4} \) simultaneously. The first of the two implies that \( x = 2 + 3k \) for any integer \( k \). Now let \( 2 + 3k \equiv 1 \pmod{4} \), or \( 3k \equiv -1 \pmod{4} \). By inspection \( k = 1 \) is a good choice, hence \( x = 5 \) is a common solution. By Theorem 3.10 the general solution is given by the residue class \([5]_{12}\). (Compare this example to the one before.)
**Exercise 3.15.** Follow the above example for these congruences.

a) \( x \equiv 1 \pmod{2} \) and \( x \equiv 2 \pmod{3} \)

b) \( x \equiv 1 \pmod{2} \) and \( x \equiv 2 \pmod{3} \) and \( x \equiv 3 \pmod{5} \)

c) \( x \equiv 7 \pmod{4} \) and \( x \equiv -2 \pmod{7} \)

d) \( x \equiv 5 \pmod{8} \) and \( x \equiv 7 \pmod{11} \)

**Exercise 3.16.** I have a little more than 3 dinars left in my mobile phone prepaid account. I could try to spend it all by sending international SMSs, for 6 piasters each, but then 1 piaster would be left. Or I could use it all for MMSs, 13 piasters each, and 5 piasters would be left. How much credits exactly do I have? Assume that 1 dinar is equivalent to 100 piasters.

**Definition.** Recall that \( m \) and \( n \) are relatively prime when \( \gcd(m, n) = 1 \).

Now three or more integers are pairwise relatively prime if they are relatively prime one to another.

An example is \( \{8, 11, 15\} \) where \( \gcd(8, 11) = \gcd(8, 15) = \gcd(11, 15) = 1 \) so the three are pairwise relatively prime. Note that it is not enough to simply have three numbers with 1 being the only common divisor for all, like 4, 6, 9, which are not pairwise relatively prime even though \( \gcd(4, 5, 6) = 1 \).

**Theorem 3.11** (Chinese Remainder Theorem, General Form). Suppose \( n_1, n_2, \ldots, n_k \) are pairwise relatively prime. Then the system of congruences \( x \equiv c_i \pmod{n_i} \) for \( i = 1, 2, \ldots, k \) has a unique solution modulo \( N = n_1 n_2 \cdots n_k \). Explicitly the solution is given by

\[
x \equiv \sum_{i=1}^{k} c_i \left( \frac{N}{n_i} \right) \left( \frac{N}{n_i} \right)^{-1} \pmod{N}
\]

where each inverse is taken modulo \( n_i \).

**Proof.** We have \( c_i \left( \frac{N}{n_i} \right) \left( \frac{N}{n_i} \right)^{-1} \equiv c_i \pmod{n_i} \) for each \( i \), hence the given formula does satisfy the system, as long as each modular inverse actually exists. In view of the Modular Inverse Theorem we need only verify that \( \gcd(n_i, N/n_i) = 1 \). But \( N/n_i \) is just the product of integers relatively prime to \( n_i \), hence itself is relatively prime to \( n_i \) by repeated use of Theorem 1.8(3).

To see that this solution is unique, Theorem 3.10 already proved the case \( k = 2 \). Since \( \gcd(n_1 n_2 \cdots n_{i-1}, n_i) = 1 \) by, again, Theorem 1.8(3), then the proof can be completed by way of induction.

**Example.** Let us solve the system of three congruences \( x \equiv 2 \pmod{3} \), \( x \equiv 1 \pmod{4} \), and \( x \equiv 3 \pmod{5} \). A quick check verifies that 3, 4, 5, are pairwise
relatively prime, so we may use the formula in Theorem 3.11. The following results can be obtained via Extended Euclidean Algorithm, or by inspection.

\[
\begin{align*}
(4 \cdot 5)^{-1} & \equiv 2 \pmod{3} \\
(3 \cdot 5)^{-1} & \equiv 3 \pmod{4} \\
(3 \cdot 4)^{-1} & \equiv 3 \pmod{5}
\end{align*}
\]

The general solution is given by

\[
x \equiv (2)(20)(2) + (1)(15)(3) + (3)(12)(3) = 233 \pmod{3 \cdot 4 \cdot 5 = 60},
\]

that is the residue class \([53]_{60}\).

**Exercise 3.17.** Follow the above example to solve the system of congruences.

a) \(x \equiv 1 \pmod{2}, \ x \equiv 2 \pmod{3}, \ x \equiv 3 \pmod{5}\)

b) \(x \equiv 3 \pmod{4}, \ x \equiv 2 \pmod{5}, \ x \equiv 5 \pmod{7}\)

c) \(x \equiv 1 \pmod{9}, \ x \equiv 2 \pmod{10}, \ x \equiv 3 \pmod{11}\)

d) \(x \equiv 1 \pmod{2}, \ x \equiv 2 \pmod{3}, \ x \equiv 1 \pmod{5}, \ x \equiv 2 \pmod{7}\)

e) \(x \equiv 2 \pmod{5}, \ x \equiv 1 \pmod{8}, \ x \equiv 7 \pmod{9}, \ x \equiv -3 \pmod{11}\)

### 3.4 Divisibility Tests

In the absence of a calculator, there are relatively quick tests we can perform to find small factors of a given number \(n\). Normally it suffices to seek only prime factors of \(n\), but for the sake of a nice illustration, our first divisibility test is for determining whether or not \(n\) is a multiple of 9.

A number \(n\) is divisible by 9 if and only if the sum of its decimal digits is divisible by 9. For example a multiple of 9 is the number 1504296 = 9 \cdot 167144 where its digit sum is 1 + 5 + 0 + 4 + 2 + 9 + 6 = 27, again a multiple of 9.

To see why this is true, let

\[
n = a_n(10^n) + a_{n-1}(10^{n-1}) + \cdots + a_2(10^2) + a_1(10) + a_0
\]

with \(0 \leq a_i \leq 9\) for each term. The equation simply comes from the decimal representation of \(n\) with digits, from right to left, \(a_0, a_1, a_2, \ldots, a_n\). Since \(10 \equiv 1 \pmod{9}\), Proposition 3.2(3) turns the equation to the congruence \(n \equiv \sum a_i \pmod{9}\).

Let us take one more example: Is 989796959493929 divisible by 9? Take its digit sum, and since 9 is really 0 modulo 9, ignore them: \(8 + 7 + 6 + 5 + 4 + 3 + 2 = 35\). Unsure whether or not 35 is divisible by 9, say, we apply the same test to it, \(3 + 5 = 8\). We know 9 \(\not|\) 8, so the answer is no.

Similarly \(n\) is divisible by 7, 11, or 13 if and only if the alternating sum of its consecutive 3-digit blocks of \(n\) is divisible by 7, 11, or 13, respectively.

To illustrate this let \(n = 007656103\), where the two leading zeros have been
added to make the number of digits a multiple of 3. We have \(007 - 656 + 103 = -546 = -2 \cdot 3 \cdot 7 \cdot 13\). It follows that \(n\) is divisible by 7 and 13 but not by 11.

**Exercise 3.18.** Prove this claim using the fact that \(1000 \equiv -1 \pmod{7, 11, 13}\) and prove also that \(n\) is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.

**Exercise 3.19.** Given an integer \(n\), remove the unit digit (the right-most digit), say \(u\), and denote what remains by \(t\). Then \(n\) is divisible by 17 if and only if \(t - 5u\) is. For example with \(n = 209865\) we have \(u = 5\) and \(t = 20986\), hence \(t - 5u = 20986 - 25 = 20961\). Let this number be the new \(n\) and repeat the test: \(2096 - 5 = 2091\), and again: \(209 - 5 = 204\), and again: \(20 - 20 = 0\). Now \(17 \mid 0\) hence \(17 \mid n\). Verify this fact using several more examples and try to prove it.

**Exercise 3.20.** Similar to the last exercise, \(19 \mid n\) if and only if \(19 \mid (t + 2u)\).

**Assignment.** Explore further on your own and make a summary of Divisibility Tests to determine when a number \(n\) is divisible by \(d = 2, 3, \ldots, 19\) and illustrate each test using your full-valued PUN (not just 6 digits) as \(n\). In the end try to factor \(n\) into primes.
Continuing with modular arithmetic, we focus in this chapter more on the operation of exponentiation or powering. This particular arithmetic plays an important role in much of today’s practice of cryptographical procedures. On the theoretical side we begin with an elegant theorem of Fermat and its generalization by Euler.

4.1 Fermat’s Theorem and Euler’s Function

Recall that a complete residue system modulo $n$ means a set of representatives of the residue classes modulo $n$, exactly one representative for each class. The following lemma will lead to our first theorem in modular exponentiation.

**Lemma 4.1.** If $\gcd(a, n) = 1$ then \( \{r_1, r_2, \ldots, r_n\} \) is a complete residue system modulo $n$ if and only if \( \{ar_1, ar_2, \ldots, ar_n\} \) is also a complete residue system modulo $n$.

**Proof.** By Proposition 3.3, \( ar_j \equiv ar_k (\text{mod} n) \) implies \( r_j \equiv r_k (\text{mod} n) \) if $\gcd(a, n) = 1$, in which case \( \{ar_1, ar_2, \ldots, ar_n\} \) represents distinct congruence classes modulo $n$ if and only if \( \{r_1, r_2, \ldots, r_n\} \) also represents distinct congruence classes modulo $n$.

**Example.** We illustrate this lemma with $a = 4$ and $n = 9$. An example of a complete residue system modulo 9 is \( \{0, 1, 2, 3, 4, 5, 6, 7, 8\} \). Multiplying each number by 4, which is relatively prime to 9, results in another complete residue system \( \{0, 4, 8, 12, 16, 20, 24, 28, 32\} \). We double check this finding by taking residues mod 9 without changing the order in which these elements are written: \( \{0, 4, 8, 3, 7, 2, 6, 1, 5\} \).
Theorem 4.2 (Fermat’s Little Theorem\(^1\)). If \(p\) is a prime not dividing \(a\) then \(a^{p-1} \equiv 1 \pmod{p}\).

Proof. By Lemma 4.1 the numbers 0, \(a\), 2, \(a\), \(a\), ..., \((p-1)\) form a complete residue system modulo \(p\), hence their residues mod \(p\) are 0, 1, 2, ..., \(p-1\), not necessarily in this order. Leaving out 0, we obtain the following congruence upon multiplying those numbers.

\[
a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}
\]

Wilson’s Theorem then gives \(-a^{p-1} \equiv -1 \pmod{p}\) and the desired result. \(\nabla\)

For example, with \(p = 101\) and \(a = 2\), Fermat’s Little Theorem states that \(2^{100} \equiv 1 \pmod{101}\). Note, however, that sometimes a composite may also satisfy a similar congruence, for instance \(29^{34} \equiv 1 \pmod{35}\). Hence Fermat’s Little Theorem, unlike Wilson’s Theorem, cannot be used as a primality criterion. (Nevertheless it is used as the basis of a great deal of primality testing algorithms developing today.)

Exercise 4.1. Investigate true or false.

a) Assume \(2^{6000} \equiv 1 \pmod{6601}\). Conclusion: 6601 is a prime.
b) Assume \(2^{1762} \not\equiv 1 \pmod{1763}\). Conclusion: 1763 is a composite.
c) If \(a \equiv b \pmod{n}\) then \(a^k \equiv b^k \pmod{n}\).
d) If \(j \equiv k \pmod{n}\) then \(a^j \equiv a^k \pmod{n}\).

Exercise 4.2. Show that Fermat’s Little Theorem is equivalent to the following statement: If \(p\) is a prime then \(a^p \equiv a \pmod{p}\) for any integer \(a\).

Definition. The Euler phi-function \(\phi(n)\) is the number of positive integers up to \(n\) which are relatively prime to \(n\). For example in the range 1 to 12, the integers relatively prime to 12 are 1, 5, 7, and 11, therefore \(\phi(12) = 4\). Similarly \(\phi(11) = 10\).

Exercise 4.3. Evaluate \(\phi(n)\) for the following values of \(n\).

a) \(n = 13\)
b) \(n = 14\)
c) \(n = 15\)
d) \(n = 16\)

\(^1\)Little, in comparison to his bigger, then unproven, Last Theorem, which states that the diophantine equation \(x^n + y^n = z^n\) has no nontrivial solution for \(n \geq 3\).
4.1. FERMAT’S THEOREM AND EULER’S FUNCTION

We are now on our way to establishing Euler’s Theorem, which generalizes Fermat’s Little Theorem in the way that the modulus may now be a composite. The structures of both proofs are so similar that in many number theory texts, Euler’s Theorem is presented first before stating Fermat’s Little Theorem as a direct corollary.

Definition. A reduced residue system modulo \( n \) is a subset of a complete residue system modulo \( n \) consisting of the \( \phi(n) \) numbers relatively prime to \( n \). For example \( \{1, 2, 4, 5, 7, 8\} \) is a reduced residue system modulo 9.

Exercise 4.4. Find a reduced residue system modulo \( n \).

a) \( n = 12 \)
b) \( n = 13, \) odd numbers only
c) \( n = 14, \) prime numbers only
d) \( n = 15, \) prime numbers only
e) \( n = 24 \)

Lemma 4.3. If \( \gcd(a, n) = 1 \) then \( \{r_1, r_2, \ldots, r_{\phi(n)}\} \) is a reduced residue system modulo \( n \) if and only if \( \{ar_1, ar_2, \ldots, ar_{\phi(n)}\} \) is also a reduced residue system modulo \( n \).

Proof. As in the proof of Lemma 4.1, either both sets represent distinct congruence classes or neither does. To finish the proof we need to show that \( \gcd(ar_i, n) = 1 \) if and only if \( \gcd(r_i, n) = 1 \), but this follows from Theorem 1.8(3) since \( \gcd(a, n) = 1 \). \( \triangle \)

Example. Let us take \( \{1, 2, 4, 5, 7, 8\} \) as a reduced residue system modulo 9. Multiplying each number by 4, which is relatively prime to 9, gives us another reduced residue system \( \{4, 8, 16, 20, 28, 32\} \). This can be verified by taking residues mod 9, without changing the order in which these elements are listed: \( \{4, 8, 7, 2, 1, 5\} \).

Theorem 4.4 (Euler’s Theorem). If \( \gcd(a, n) = 1 \) then \( a^{\phi(n)} \equiv 1 \pmod{n} \).

Proof. If \( \gcd(a, n) = 1 \) then by Lemma 4.3 we may choose a pair of reduced residue systems modulo \( n \) which looks like \( \{r_1, r_2, \ldots, r_{\phi(n)}\} \) and another \( \{ar_1, ar_2, \ldots, ar_{\phi(n)}\} \). If we multiply all the elements in each set then

\[
 a^{\phi(n)} \cdot r_1 \cdot r_2 \cdots r_{\phi(n)} \equiv r_1 \cdot r_2 \cdots r_{\phi(n)} \pmod{n}
\]

Now since each element \( r_i \) in the set is relatively prime to \( n \), Proposition 3.3 completes the proof by cancelling the common terms off both sides. \( \triangle \)

Exercise 4.5. Prove that if \( a^k \equiv 1 \pmod{n} \) for some \( k > 0 \) then \( \gcd(a, n) = 1 \).
For practical purposes Euler’s Theorem is not of much use until we learn a more feasible way to evaluate $\phi(n)$. We devote the rest of the section solely with this goal in mind.

**Theorem 4.5.** If $\gcd(m, n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$.

**Proof.** Let $M$, $N$, and $MN$ be reduced residue systems modulo $m$, $n$, and $mn$, respectively. Also denote by $M \times N$ the set consisting of the elements $(c, d)$ with $c$ from $M$ and $d$ from $N$. To complete the proof we shall provide a one-to-one correspondence between $M \times N$ and $MN$, thereby showing that $\phi(m)\phi(n) = \phi(mn)$.

Pick an element $a$ in $MN$. We have $\gcd(a, mn) = 1$, thus $\gcd(a, m) = 1$ and $\gcd(a, n) = 1$. Since $M$ and $N$ are reduced residue systems, there exists a unique pair $(c, d)$ in $M \times N$ such that $a \equiv c \pmod{m}$ and $a \equiv d \pmod{n}$. Conversely given a pair of congruences $x \equiv c \pmod{m}$ and $x \equiv d \pmod{n}$ with $(c, d)$ in $M \times N$, by Chinese Remainder Theorem (Theorem 3.10) and Theorem 1.8(3), $x = a$ is the unique element in $MN$ which solves the system. This establishes the one-to-one correspondence between the two sets. △

**Proposition 4.6.** The following results show how to evaluate $\phi(n)$.

1) If $p$ is a prime then $\phi(p) = p - 1$.
2) For a prime power we have $\phi(p^k) = p^k - p^{k-1}$.
3) If $n$ has been factored into powers of distinct primes, $n = \prod p_i^{k_i}$ then $\phi(n) = \prod (p_i^{k_i} - p_i^{k_i-1})$.

**Proof.** The first claim is trivial. Next, $\phi(p^k)$ is the number of integers from 1 to $p^k$ which are relatively prime to $p^k$. Since $p$ is the only prime divisor of $p^k$, this number is $p^k$ minus the number of multiples of $p$, which are $p, 2p, 3p, \ldots, (p^{k-1})p$. Thus $\phi(p^k) = p^k - p^{k-1}$. From this the last claim follows by Theorem 4.5. △

**Exercise 4.6.** Evaluate $\phi(n)$ for the following values of $n$.

a) $n = 240$

b) $n = 625$

c) $n = 1024$

d) $n = 4800$

e) $n = 250313$

**Exercise 4.7.** Find all positive integers $n$ satisfying $\phi(n) = 4$.

**Exercise 4.8.** Prove the following properties about $\phi(n)$.
4.2. COMPUTING POWERS AND ROOTS

a) If \( n \) is odd then \( \phi(2n) = \phi(n) \).
b) If \( n \) is even then \( \phi(2n) = 2\phi(n) \).
c) If \( d \mid n \) then \( \phi(d) \mid \phi(n) \).
d) The value of \( \phi(n) \) is even for any \( n > 2 \).

**Exercise 4.9.** Another property of \( \phi(n) \) is that \( \sum \phi(d) = n \) where the sum is taken over all the positive integers \( d \) which divide \( n \). Verify this property for \( n = 24 \) and \( n = 30 \).

4.2 Computing Powers and Roots

In many computational applications, such as in cryptography, it is often necessary to perform exponentiation in the form \( a^k \% n \) with a very large value of \( k \). One obvious way to compute \( a^k \) is multiplying \( a \) by itself \( k \) times, where the partial product in each step can be reduced to its residue mod \( n \) in order to keep the size small. Doing so will have no effect on the final answer, as claimed in the following exercise.

**Exercise 4.10.** Show that \( a^{2 \% n} = (a \% n)^2 \% n \). In general prove that \( ab \% n = (a \% n)(b \% n) \% n \).

Let us combine this property with Euler’s Theorem. When \( \gcd(a, n) = 1 \), the computation of \( a^k \% n \) can be reduced by first replacing \( a \) by \( a \% n \) and \( k \) by \( k \% \phi(n) \). The following is an illustration.

**Example.** Let us compute \( 1234^{5678} \% 11 \). Since \( 1234 \% 11 = 2 \) we may as well compute \( 2^{5678} \% 11 \). Next we check that \( \gcd(2, 11) = 1 \) hence Euler’s Theorem applies (so does Fermat’s Little Theorem, 11 being a prime). Evaluate \( \phi(11) = 10 \) and we have \( 2^{10} \equiv 1 \) (mod 11). It follows that

\[
2^{5678} = 2^{10(567)+8} = (2^{10})^{567} \cdot 2^8 \equiv 1^{567} \cdot 2^8 = 2^8 \pmod{11}
\]

In other words, since \( 5678 \% \phi(11) = 8 \), then \( 2^{5678} \% 11 \) is reduced to \( 2^8 \% 11 \). The final result: \( 1234^{5678} \% 11 = 256 \% 11 = 3 \).

**Exercise 4.11.** Compute these residues with the help of Euler’s Theorem.

a) \( 83^{3418} \% 24 \)
b) \( 49^{324} \% 41 \)
c) \( 3337^{3331} \% 64 \)
d) \( 2234^{2600} \% 97 \)
e) \( 3294^{3845} \% 143 \)

**Exercise 4.12.** What is the unit digit of the number \( 123^{45678} \)?
Euler’s Theorem is not true, however, when \( \gcd(a, n) \neq 1 \). And worse, since the only known method for evaluating \( \phi(n) \) is through factoring, Euler’s Theorem is not at all meant for practical computations. This will not matter anyhow later on when we have learned the right powering algorithm. In the meantime we still want to amuse ourselves by exploring the possibilities when \( \gcd(a, n) > 1 \).

**Theorem 4.7** (A Generalization of Euler’s Theorem). Let \( a \) and \( n \) be arbitrary positive integers. Set \( n_0 = n \) and \( d_0 = \gcd(a, n) \). Then for \( i \geq 1 \) we define \( n_i \) and \( d_i \) recursively by \( n_i = n_{i-1}/d_{i-1} \) and \( d_i = \gcd(a, n_i) \). If \( k \) is the smallest integer for which \( d_k = 1 \) then

\[
a^{\phi(n_k)} a^k \equiv a^k \pmod{n}
\]

with which Euler’s Theorem coincides in the case \( k = 0 \).

**Proof.** We claim that the following congruences are all equivalent, so that we are done since the very last one is true by Euler’s Theorem.

- \( a^{\phi(n_k)} a^k \equiv a^k \pmod{n} \)
- \( a^{\phi(n_k)} a^k / d_0 \equiv a^k / d_0 \pmod{n_1} \)
- \( a^{\phi(n_k)} a^{k-1} \equiv a^{k-1} \pmod{n_1} \)
- \( a^{\phi(n_k)} a^{k-1} / d_1 \equiv a^{k-1} / d_1 \pmod{n_2} \)
- \( a^{\phi(n_k)} a^{k-2} \equiv a^{k-2} \pmod{n_2} \)
  
  ... 
- \( a^{\phi(n_k)} a / d_{k-1} \equiv a / d_{k-1} \pmod{n_k} \)
- \( a^{\phi(n_k)} \equiv 1 \pmod{n_k} \)

To justify the equivalence, note that the pattern down the list repeats every other row. To get the next even row we divide through the congruence including the modulus \( n_i \) by \( d_i \) to obtain the next modulus \( n_{i+1} \). For the next odd row we divide the congruence, without the modulus, by \( a/d_i \). This is allowed by Proposition 3.3 as \( d_i = \gcd(a, n_i) \) implies \( \gcd(a/d_i, n_{i+1}) = 1 \) by Corollary 1.7.

**Example.** Let us illustrate Theorem 4.7 with \( a = 2^3 \cdot 3^2 \cdot 5 \) and \( n = 2^7 \cdot 3 \cdot 5^2 \cdot 7 \),

\[
\begin{align*}
n_0 &= n = 2^7 \cdot 3 \cdot 5^2 \cdot 7 & d_0 &= \gcd(a, n_0) = 2^3 \cdot 3 \cdot 5 \\
n_1 &= n_0/d_0 = 2^4 \cdot 5 \cdot 7 & d_1 &= \gcd(a, n_1) = 2^3 \cdot 5 \\
n_2 &= n_1/d_1 = 2 \cdot 7 & d_2 &= \gcd(a, n_2) = 2 \\
n_3 &= n_2/d_2 = 7 & d_3 &= \gcd(a, n_3) = 1
\end{align*}
\]
4.2. COMPUTING POWERS AND ROOTS

We have $k = 3$ with $\phi(n_3) = \phi(7) = 6$, hence $a^6 a^3 \equiv a^3 \pmod{n}$. Note that this implies $a^{6j} a^3 \equiv a^3 \pmod{n}$ for any integer $j > 1$. To see why, observe $a^{6j} a^3 = a^{6(j-1)}(a^6 a^3) \equiv a^{6(j-1)}a^3 \equiv \cdots \equiv a^6 a^3 \equiv a^3 \pmod{n}$.

Then, for instance, we wish to compute $a^{8888} \pmod{n}$. Noting that $8888 = 6(1481) + 2$ we do a little trick,

$$a^{8888} = a^{6(1480)+8} = a^{6(1480)} a^3 a^5 \equiv a^3 a^5 = a^8 \pmod{n}$$

Thus the reduction we are allowed is $a^{8888} \pmod{n} = a^8 \pmod{n}$.

Exercise 4.13. Compute these residues following the above example.

a) $2^{456} \pmod{10}$
b) $10^{456} \pmod{36}$
c) $42^{654} \pmod{88}$
d) $126^{9999} \pmod{432}$
e) $385^{3422} \pmod{900}$

Corollary 4.8. If $n$ has no repeated prime factors then $a^{\phi(n)} a \equiv a \pmod{n}$.

Proof. The condition implies $k \leq 1$ in Theorem 4.7. Either $k = 0$, which is trivially Euler’s Theorem, or $k = 1$ and $a^{\phi(n)} a \equiv a \pmod{n}$. Exercise 4.8(c) shows us why $\phi(n_1) | \phi(n)$, say $\phi(n) = \phi(n_1)j$ for some $j \geq 1$. But then

$$a^{\phi(n_1)j} a = a^{\phi(n_1)(j-1)}(a^{\phi(n_1)} a) \equiv a^{\phi(n_1)(j-1)} a \equiv \cdots \equiv a^{\phi(n_1)} a \equiv a \pmod{n}$$

and the result follows. \[ \Box \]

The right algorithm we hinted earlier, for computing $a^k \pmod{n}$, is called the Successive Squaring Algorithm. The idea is to repeatedly square the number $a$, thus the name, and cleverly write $a^k$ as a product of some of these squares. The algorithm, given below, reduces computation time significantly\(^2\) and completely outperform Euler’s Theorem in practice.

Step 1) Express $k$ as the sum of powers of 2, say $k = \sum 2^{e_i}$.

Step 2) Compute $a^{2^{e_i}} n$, $a^{4^{e_i}} n$, $a^{8^{e_i}} n$, ... up to the highest exponent appearing in the first step.

Step 3) Compute $a^{k} \pmod{n}$ by substituting $a^k = \prod a^{2^{e_i}}$.

---

\(^2\)It uses only $O(\log n)$ instead of $n$ multiplications.
Example (Successive Squaring Algorithm). Compute $23^{106} \mod 97$. We have $106 = 64 + 32 + 8 + 2 = 2^6 + 2^5 + 2^3 + 2^1$ so that $23^{106} = (23^6)(23^{32})(23^8)(23^2)$. The successive squaring part goes

$$(23)^2 \mod 97 = 44$$

$$23^4 \mod 97 = (44)^2 \mod 97 = 93$$

$$23^8 \mod 97 = (93)^2 \mod 97 = 16$$

$$23^{16} \mod 97 = (16)^2 \mod 97 = 62$$

$$23^{32} \mod 97 = (62)^2 \mod 97 = 61$$

$$23^{64} \mod 97 = (61)^2 \mod 97 = 35$$

Hence $23^{106} \mod 97 = (35)(61)(16)(44) \mod 97 = 25$.

Exercise 4.14. Use successive squaring to compute these residues.

a) $3^{57} \mod 20$

b) $25^{99} \mod 79$

c) $47^{250} \mod 200$

d) $5^{1434} \mod 307$.

e) $25^{1434} \mod 309$.

Exercise 4.15. Find the two right-most digits of the number $123^{45678}$.

If instead of computing $a^k \mod n$ we are given one and asked to retrieve $a$, then what we are facing is a more difficult problem of modular root extraction. Under some relatively prime conditions the problem is not difficult to solve, at least theoretically. The following result is in fact a key principle employed in the RSA cryptosystem, the topic of the next section. More about root extractions will later be encountered in Section 5.3.

Theorem 4.9. If both gcd$(a, n)$ and gcd$(e, \phi(n))$ equal 1 then the congruence $x^e \equiv a \mod n$ has a unique root modulo $n$ given by $x \equiv a^d \mod n$ where $d \equiv e^{-1} \mod \phi(n)$.

Proof. Modular Inverse Theorem (Corollary 3.6) guarantees the existence, and uniqueness, of $d$ modulo $\phi(n)$, say $de = 1 + \phi(n)h$ for some integer $h$. Now raise to the power $d$ both sides of the congruence $x^e \equiv a \mod n$:

$$a^d \equiv x^{de} = x^{1+\phi(n)h} = x(x^{\phi(n)})^h \equiv x \mod n$$

by way of Euler’s Theorem, noting that $x$ is relatively prime to $n$ because $a$ is. This shows too that the root $x$ is unique for a fixed choice of $d$. But all inverses of $e$ modulo $\phi(n)$ are of the form $d + \phi(n)j$, for which $a^{d+\phi(n)j} = a^d(a^{\phi(n)})^j \equiv a^d \mod n$ hence they all generate the same $x$. □
Exercise 4.16. Solve for $x$.

a) $x^7 \equiv 12 \pmod{13}$

b) $x^{13} \equiv 5 \pmod{32}$

c) $x^{39} \equiv 5 \pmod{121}$

d) $x^{121} \equiv 30 \pmod{899}$

e) $x^{239} \equiv 23 \pmod{2005}$

4.3 The RSA Cryptosystem

Sensitive messages, when transferred over electronic media such as the internet, may need to be encrypted, meaning changed into a secret code in such a way that only the intended receiver who has the secret key is able to decrypt it. It is common that alphabetical characters are converted to their numerical ASCII equivalents before they are encrypted, hence the coded message will look like integer strings.

The RSA\(^3\) Cryptosystem provides an encryption-decryption algorithm which is widely employed today. In practice the encryption key may be made public and doing so will not risk the security of the system. This feature is a characteristic of the so-called public-key cryptosystem.

How does it work? Let’s say the two communicating parties are represented by Alia and Bob. Alia selects two distinct primes $p$ and $q$ which are very large, like a hundred digits each. She computes $n = pq$ and $\phi(n) = \phi(pq) = (p-1)(q-1)$. Next she determines a number $e$ less than and relatively prime to $\phi(n)$ which will serve as her encryption key, and another number $d < n$ for her decryption key satisfying $de \% \phi(n) = 1$. When all is ready Alia gives to Bob the pair $(n, e)$ and keeps the rest secret. Now whenever Bob wants to send a message (integer) $m < n$ to Alia, he encrypts it to $s = m^e \% n$. Upon receiving $s$, Alia decrypts it back to $m = s^d \% n$.

Why does this work? First of all, there are plenty of primes 100-digits long, in fact there are roughly $\pi(10^{100}) - \pi(10^{99}) \approx 3.9 \times 10^{97}$ of them, and they are not too hard to find using primality testing algorithms available today. Secondly, Theorem 4.9 ensures that the decryption process does return the intended value of $m$. As for determining $e$ and $d$, it is not too hard for Alia with the help of Euclidean Algorithm. Neither it is hard encrypting $s = m^e \% n$ or decrypting $m = s^d \% n$ with the use of Successive Squaring Algorithm. But what if a bad guy intercepts the secret message $s$, together with $e$ and $n$? Well, $d$ is yet to be found in order to read the message, and in turn he also will need the factors $p$ and $q$ in order to compute

\(^3\)Rivest, Shamir, and Adleman patented it in 1983, hence the name.
φ(n). Woe to him, pq has over 200 digits and factoring a large integer this size will take a lifetime on today’s best computer.

Example. By way of an illustration, Alia chooses \( n = 19 \cdot 53 = 1007 \) with \( \phi(n) = 18 \cdot 52 = 936 \). She also selects her encryption key \( e = 5 \), which is relatively prime to 936. After working it out shortly using Extended Euclidean Algorithm, she finds \( d = 749 \) is the right decryption key. She double checks \( 749 \cdot 5 \equiv 1 \pmod{936} \) and proceeds to send \((1007,5)\) to Bob, say, via email.

Later, Bob wishes to send the message I LOVE U to Alia. Using ASCII standard \( 65 = A, 66 = B, \ldots, 90 = Z \), and 32 for blank space, the encrypted message looks like \( 73327679866985 \). To make \( m < n = 1007 \) (Remember that in real practice \( n \) is much bigger), Bob cuts up this string into blocks of 3 digits: \( 073 \ 327 \ 679 \ 866 \ 985 \). He then sends the five values of \( s \) in a sequence, the first of which is \( 735 \equiv 73 \pmod{1007} \).

Upon receiving, Alia decrypts \( 973^{749} \equiv 73 \pmod{1007} \), plus the other four, then reunites the results back into a single string and reverses the ASCII conversion to read the encouraging message from Bob.

Exercise 4.17. In this RSA exercise, Alia picks \( n = 127 \cdot 79 = 10033 \), \( e = 17 \).

a) What is her decryption key \( d \)?
b) Wanting to say HI, what does Bob send to her?
c) Verify that Alia does get this greeting correctly.
d) Another time she receives \( s = 8411 \). What is the intended message?

Theorem 4.9 assumes, in the context of RSA, that \( \gcd(s,n) = 1 \). In practice, however, the encrypted message \( s \) may fail to be relatively prime to \( n \). The probability of such coincidence is extremely small as \( n \) is a very large number with only two prime divisors. Nevertheless we can prove that the decryption algorithm will anyhow return the correct message \( m \). This is the problem for the next exercise.

Exercise 4.18. Suppose that \( \gcd(s,n) \neq 1 \). Show that anyway \( s^d \equiv n \pmod{m} \).

RSA works under a crucial assumption that it is hard to evaluate \( \phi(n) \) without factoring \( n = pq \). The difficulty of evaluating \( \phi(n) \) is at least equivalent to that of factoring \( n \) in the sense that solving one solves the other as well. Here is why: Knowing \( p \) and \( q \) means knowing \( \phi(n) = (p-1)(q-1) \). Conversely knowing \( \phi(n) \) leads to the discovery of \( p \) and \( q \) as the roots of the following quadratic polynomial.

\[
x^2 - (n - \phi(n) + 1)x + n = x^2 - (pq - (p-1)(q-1) + 1)x + pq = (x - p)(x - q)
\]
4.4 PROJECT: RSA CYCLING ATTACK

Example. Suppose \( n = 1007 \) and \( \phi(n) = 936 \) as before. Knowing only these two values, we look for the roots of
\[
x^2 - (1007 - 936 + 1)x + 1007 = x^2 - 72x + 1007.
\]
The quadratic formula gives us
\[
x = \frac{72 \pm \sqrt{72^2 - 4 \cdot 1007}}{2} = 36 \pm \sqrt{289} = 36 \pm 17.
\]
Thus we discover \( 1007 = (36 + 17)(36 - 17) = 53 \cdot 19 \).

Exercise 4.19. Given \( n = pq \) and \( \phi(n) \) find \( p, q \).

a) \( \phi(209) = 180 \)

b) \( \phi(2231) = 2112 \)

c) \( \phi(11371) = 11152 \)

d) \( \phi(147911) = 147000 \)

The RSA Laboratories is currently offering factoring challenges at their site [www.rsa.com/rsalabs/](http://www.rsa.com/rsalabs/) with prizes ranging from US$10,000 to $200,000. Here is one of the challenge numbers for $50,000 called RSA-768, which has 232 decimal digits:

\[
n = 12301866845301177551304949583849627207728535695953
34792197322452151726400507263657518745202199786469
38995647494277406384592519255732630345373154826850
79170261221429134616704292143116022212404792747377
94080665351419597459856092143413
\]

Exercise 4.20. In the context of RSA, suppose \( n = 51983 \). Find \( p, q \), knowing that they are a pair of twin primes.

Exercise 4.21. Two companies are implementing RSA with \( n_1 = 30227 \) and \( n_2 = 35657 \), respectively. Suppose we know that they are sharing a common prime factor. Find a quick way to factor \( n_1, n_2 \).

4.4 RSA Cycling Attack

[Project 4]

Over the years there have been various attempts to break the RSA cryptosystem. So far none of these attacks is a serious blow to the system in general, and in the meantime a vast amount of research has been done to study certain circumstances under which a specific implementation of the RSA becomes vulnerable. For instance we have studied in Section 2.4 that if \( p \) and \( q \) are quite close together, say of equal digit lengths, then it is not difficult to factor \( n \) using Fermat Factorization. Therefore when implementing RSA it is important to select \( p \) and \( q \) of slightly different sizes.

Attacks on the RSA cryptosystem can be a subject of its own. It is not our intention to go over the topic, except to present one particular case called the **cycling attack**. The algorithm, described below, employs
recursive exponentiation to retrieve the message \( m \) without any knowledge of the decryption key \( d \).

Let \( s_0 = s \) and subsequently let \( s_k = s_{k-1}^e \mod n \). It can be shown that eventually this will lead to a term \( s_K = s \). Then \( s_{K-1}^e \equiv s \pmod{n} \) and by the uniqueness of modular root in Theorem 4.9 we conclude \( s_{K-1} = m \). Fortunately, or unfortunately if you are the bad guy, this scheme is generally too slow to be effective and there are simple ways to make the system immune to it.

**Example.** Let \( n = 299 = 13 \cdot 23 \) and \( e = 17 \). Suppose that the encrypted message is \( s = 123 \). Armed with only Successive Squaring Algorithm, we start calculating,

\[
\begin{align*}
123^{17} \mod 299 & = 197 \\
197^{17} \mod 299 & = 6 \\
6^{17} \mod 299 & = 288 \\
288^{17} \mod 299 & = 32 \\
32^{17} \mod 299 & = 210 \\
210^{17} \mod 299 & = 292 \\
292^{17} \mod 299 & = 119 \\
119^{17} \mod 299 & = 71 \\
71^{17} \mod 299 & = 41 \\
41^{17} \mod 299 & = 123 = s
\end{align*}
\]

The last result reveals that \( m = 41 \).

**Assignment.** In the context of RSA, let \( n = 1003669 \) and \( e = 3 \). Using your 6-digit PUN as \( s \), find \( m \) following the above example. Then try to break this code, perhaps using Fermat Factorization, in order to find the decryption key \( d \). Then using \( d \), decrypt \( s \) once more to verify that it agrees with the answer you obtain from the cycling attack algorithm.
Chapter 5

Primitive Roots

Still dealing with modular exponentiation \(a^k \% n\), we narrow down our focus upon the case \(\text{gcd}(a, n) = 1\). Note that the sequence \(a \% n, a^2 \% n, a^3 \% n, \ldots\) must eventually reach 1 and make a loop back to the first term. In fact Euler’s Theorem guarantees that the length of this periodicity should be no more than \(\phi(n)\). We will be interested in the idea of the least such length for a given \(a\) and whether it can sometimes equal \(\phi(n)\).

5.1 Orders and Primitive Roots

Definition. Suppose \(a\) and \(n > 0\) are relatively prime. The order of \(a\) modulo \(n\) is the smallest positive integer \(k\) such that \(a^k \% n = 1\). We denote this quantity by \(|a|_n\) or simply \(|a|\) when there is no ambiguity. For example \(|2|_7 = 3\) because \(k = 3\) is the smallest positive solution of the congruence \(2^k \equiv 1 \pmod{7}\).

Exercise 5.1. Find these orders.
a) \(|3|_7\) 
b) \(|3|_{10}\) 
c) \(|5|_{12}\) 
d) \(|7|_{24}\) 
e) \(|4|_{25}\)

Exercise 5.2. Investigate true or false.
a) \(|-a| = |a|\) 
b) \(|a|_n = |b|_n\) if and only if \(a \equiv b \pmod{n}\). 
c) If \(a^j \equiv a^k \pmod{n}\) then \(j \equiv k \pmod{n}\). 
d) The congruence \(a^k \equiv 1 \pmod{n}\) has no solution if \(\text{gcd}(a, n) \neq 1\).
Exercise 5.3. Prove that if \(|a|_n = n - 1\) then \(n\) must be a prime.

We reiterate that the notation \(|a|_n\) implicitly assumes that \(\gcd(a, n) = 1\), for otherwise it makes no sense. In particular we have \(|a|_n \leq \phi(n)\) by Euler’s Theorem. It is also clear that the definition of order extends to residue classes, meaning that \(|a|_n = |b|_n\) whenever \(a \equiv b \pmod{n}\).

**Proposition 5.1.** The following statements hold.

1) \(a^k \equiv 1 \pmod{n}\) if and only if \(|a|_n | k\). In particular \(|a|_n | \phi(n)\).

2) \(a^j \equiv a^k \pmod{n}\) if and only if \(j \equiv k \pmod{|a|_n}\).

3) \(|a^k| = |a|\) if and only if \(\gcd(k, |a|) = 1\).

4) If \(\gcd(|a|, |b|) = 1\) then \(|ab| = |a||b|\).

**Proof.**

1) Let \(j = \lceil k/|a|_n \rceil\) so that we may write \(k = j|a|_n + k \mod{|a|_n}\). Then

\[
a^k = (a^{|a|_n})^j \cdot a^{k \mod{|a|_n}} \equiv a^{k \mod{|a|_n}} \pmod{n}
\]

and with the fact \(k \mod{|a|_n} < |a|_n\), the congruence \(a^k \equiv 1 \pmod{n}\) holds if and only if \(k \mod{|a|_n} = 0\), or equivalently \(|a|_n | k\).

2) The congruence \(a^j \equiv a^k \pmod{n}\) is equivalent to \(a^{j-k} \equiv 1 \pmod{n}\) and the result follows from (1).

3) Observe that the following congruence

\[
a^{ik} = (a^i)^k = (a^k)^i \equiv 1 \pmod{n}
\]

is true if we let \(j = |a|\), in which case \(|a^k| | |a|\) by (1). It is also true with \(j = |a^k|\) and similarly \(|a| | k|a^k|\). If \(\gcd(k, |a|) = 1\) then by Euclid’s Lemma \(|a| | |a^k|\) and so \(|a^k| = |a|\). Conversely if \(\gcd(k, |a|) = d > 1\), since the congruence holds for \(j = |a|/d\), we have \(|a^k| \leq |a|/d < |a|\).

4) Suppose \(\gcd(|a|, |b|) = 1\). Again we have the following congruence.

\[
a^{|b||ab|} = a^{|b|(|ab|(|b|))^{|ab|}} = (ab)^{|a|b|b|} \equiv 1 \pmod{n}
\]

Hence by (1) \(|a| | |b| |a| |b|\) and in turn, by Euclid’s Lemma \(|a| | |ab|\). Now by symmetry \(|b| | |ab|\) and so \(|a| |b| | |ab|\) by Proposition 1.8(2). It is clear, however, that \(|ab| \leq |a| |b|\) so it follows that \(|ab| = |a| |b|\). \(\nabla\)

**Exercise 5.4.** Suppose \(|a| = 6\). Find \(|a^k|\) for \(k = 2, 3, 4, 5, 6\).
Exercise 5.5. Prove that $|a^k| = |a|/\gcd(k, |a|)$ for any $k > 0$.

Exercise 5.6. Prove that modular inverses have equal orders.

Definition. An integer $g$ is called a primitive root modulo $n$ if $|g|_n = \phi(n)$. For example 3 is a primitive root modulo 7 because $|3|_7 = 6 = \phi(7)$.

Exercise 5.7. Is 5 a primitive root modulo 29?

By the definition of order, the concept of primitive roots also extends to residue classes. Thus $g$ is a primitive root modulo $n$ if and only if every integer in $[g]_n$ is also a primitive root modulo $n$. Consequently we use the word distinct or incongruent primitive roots modulo $n$ to mean those belonging to different residue classes.

In particular to search for a primitive root modulo $n$ it suffices to look at a reduced residue system modulo $n$. For example a reduced residue system modulo 8 is $\{1, 3, 5, 7\}$ where all its elements have orders at most $2 < \phi(8)$. (See Exercise 3.1) Hence there are no primitive roots modulo 8.

Exercise 5.8. Find all the primitive roots modulo $n$, if any.

a) $n = 6$

b) $n = 7$

c) $n = 9$

d) $n = 10$

e) $n = 12$

Proposition 5.2. The following statements hold.

1) $g$ is a primitive root modulo $n$ if and only if $\{g, g^2, g^3, \ldots, g^{\phi(n)}\}$ is a reduced residue system modulo $n$.

2) $g$ is a primitive root modulo $n$ if and only if the congruence $g^x \equiv c \pmod{n}$ has a solution for every integer $c$ relatively prime to $n$.

3) If $k$ is relatively prime to $\phi(n)$ then $g^k$ is a primitive root modulo $n$ if and only if $g$ is too.

4) If any exists, there are exactly $\phi(\phi(n))$ primitive roots modulo $n$.

Proof. Let $G = \{g, g^2, g^3, \ldots, g^{\phi(n)}\}$.

1) If $g$ is a primitive root then clearly each element in $G$ is relatively prime to $n$. We show now that they represent distinct congruence classes, for if $g^j \equiv g^k \pmod{n}$ then by Proposition 5.1(2), $\phi(n) \mid (j - k)$. But this relation is not possible since $|j - k| < \phi(n)$ unless $j = k$. It follows that $G$ is a reduced residue system modulo $n$. Conversely if $g$ is not a primitive root then $g^k \equiv 1 \pmod{n}$ with $k < \phi(n)$ and $G$ is not a reduced residue system for then $g^{k+1} \equiv g \pmod{n}$ where both $g^{k+1}$ and $g$ belong to $G$. 
2) Equivalent to (1), $G$ is a reduced residue system modulo $n$ if and only if it represents all congruence classes of $c$ with $\gcd(c, n) = 1$.

3) This statement is a special case of Proposition 5.1(3).

4) Exactly $\phi(\phi(n))$ elements $g^k$ in $G$ satisfy $\gcd(k, \phi(n)) = 1$ and by (3) these and only these are primitive roots modulo $n$.

Exercise 5.9. One of the primitive roots modulo 11 is 2. Find the rest.

Exercise 5.10. Prove the following claims, $p$ denotes a prime.

a) If $g$ is a primitive root modulo $p > 2$ then $g^{(p-1)/2} \equiv -1 \pmod{p}$.

b) The number 4 is not a primitive root modulo any prime.

c) The product of two primitive roots modulo $p > 2$ is not a primitive root.

d) If $p \equiv 1 \pmod{4}$ then $g$ is a primitive root modulo $p$ if and only if $-g$ is.

5.2 The Existence of Primitive Roots

We have seen that not all moduli have primitive roots. The objective in this section is to show that primitive roots exist for any prime modulus. For the general composite case we will state the theorem without proof as none of the subsequent results will be dependent on it.

**Theorem 5.3.** Let $f(x)$ be an integral polynomial of degree $n$. The congruence $f(x) \equiv 0 \pmod{p}$ has at most $n$ distinct solutions modulo the prime $p$.

**Proof.** For a linear congruence, $ax + b \equiv 0 \pmod{p}$ has a unique solution according to the Linear Congruence Theorem since $\gcd(a, p) = 1$ and so the theorem is true.

By way of induction, assume the claim is true for polynomials of degree up to $n - 1$. Let $f(x)$ be a polynomial with leading term $ax^n$ and with $p \nmid a$. If $f(x)$ has less than $n$ roots then there is nothing to prove, else let $r_1, r_2, \ldots, r_n$ be distinct roots of $f(x)$ modulo $p$ and let

$$g(x) = f(x) - a(x - r_1)(x - r_2) \cdots (x - r_n)$$

Note that the degree of $g(x)$ is less than $n$, and yet it has the same $n$ roots of $f(x)$. By induction hypothesis this is impossible unless $g(x)$ is the zero polynomial (mod $p$), so

$$f(x) \equiv a(x - r_1)(x - r_2) \cdots (x - r_n) \pmod{p}$$

and by Theorem 2.3, $f(x) \equiv 0 \pmod{p}$ if and only if $x \equiv r_i \pmod{p}$ for one of these roots. Thus $f(x)$ has only these $n$ roots modulo $p$. □
5.2. THE EXISTENCE OF PRIMITIVE ROOTS

Corollary 5.4. If $p$ is a prime and $d \mid (p - 1)$ then the congruence $x^d \equiv 1 \pmod{p}$ has exactly $d$ solutions modulo $p$.

Proof. Suppose $dk = p - 1$ so that we have the following polynomial identity:

$$x^{p-1} - 1 = (x^d - 1)((x^d)^{k-1} + (x^d)^{k-2} + \cdots + x^d + 1)$$

By Fermat’s Little Theorem the left-hand side has exactly $p - 1$ roots modulo $p$. Since $p$ is prime, these roots must come from those of the two polynomials on the right, which by Theorem 5.3 have at most $d$ and $d(k - 1) = p - 1 - d$ roots, respectively. The only way this can happen is if their roots are exactly $d$ and $p - 1 - d$.

Theorem 5.5. There are exactly $\phi(p - 1)$ incongruent primitive roots modulo every prime $p$.

Proof. In view of Proposition 5.2(4), it suffices to show that there is at least one primitive root modulo $p$.

Let $p - 1 = \prod q_i^{e_i}$ where the $q_i$’s are distinct primes and $e_i \geq 1$. By Corollary 5.4 there are exactly $q_1^{e_1}$ integer solutions of $x^{q_1^{e_1}} \equiv 1 \pmod{p}$, all of which have orders a power of $q_1$ according to Proposition 5.1(1). Similarly, however, $q_1^{e_1 - 1}$ of these integers satisfy the congruence $x^{q_1^{e_1 - 1}} \equiv 1 \pmod{p}$ hence their orders are no more than $q_1^{e_1 - 1}$. It follows that there exist $q_1^{e_1 - 1} - q_1^{e_1 - 1}$ integers of order $q_1^{e_1}$. By symmetry we have an integer of order $q_i^{e_i}$ for each of the distinct prime factors of $p - 1$. And the product of these integers, by Proposition 5.1(4), is of order $p - 1$, that is a primitive root.

Exercise 5.11. How many are the primitive roots modulo $p$?

a) $p = 5$
b) $p = 7$
c) $p = 11$
d) $p = 89$

Theorem 5.6 (Primitive Root Theorem). Primitive roots exist only modulo $1, 2, 4, p^k,$ or $2p^k$ for any prime $p > 2$ and $k > 0$.

No Proof. The proof is set aside as an independent library assignment.

Exercise 5.12. Is there a primitive root modulo $n$? How many?

a) $n = 25$
b) $n = 50$
c) $n = 100$
d) \( n = 1250 \)
e) \( n = 250313 \)

Knowing exactly when a primitive root exists does not help us in actually finding one. Even for prime moduli, the search for primitive roots has up to now produced only incomplete theorems and endless numerical tables. We do not even know, for instance, for which prime moduli 2 is a primitive root.

**Conjecture 5.7** (Artin’s Conjecture). The number 2 is a primitive root modulo infinitely many primes.

*Exercise 5.13.* Find three primes modulo which 2 is not a primitive root.

### 5.3 Discrete Logarithm Problems

Suppose, instead of computing \( b = a^k \% n \) we are given one and asked to find the exponent \( k \). In ordinary arithmetic we would be computing the logarithm \( k = \log_a b \). In modular arithmetic, however, the *discrete logarithm problem* is very difficult to solve especially when the value of \( n \) is very large. This difficulty, similar to that of factoring in RSA, has in fact become the key idea in other public-key cryptosystems.

For relatively small modulus \( n \), solving a discrete logarithm problem can be done with the help of a primitive root \( g \), if exists, and a table of reduced residue system modulo \( n \) consisting of powers of \( g \), as allowed by Proposition 5.2(1). We illustrate the technique in the next example.

*Example.* Let us solve the congruence \( 4^x \equiv 10 \pmod{13} \). We choose \( g = 2 \) for a primitive root modulo 13 and generate the following table showing a reduced residue system modulo 13.

\[
\begin{array}{cccccccccc}
   k & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\
2^k \% 13 & 2 & 4 & 8 & 3 & 6 & 12 & 11 & 9 & 5 & 10 & 7 & 1 \\
\end{array}
\]

Next we rewrite the congruence using only powers of 2, hence \((2^2)^x \equiv 2^{10} \pmod{13}\). This is equivalent to, by Proposition 5.1(2), the congruence \( 2x \equiv 10 \pmod{12} \). Linear Congruence Theorem takes it from here. We have \( \gcd(2, 12) = 2 \mid 10 \) and a particular solution \( x_0 = 5 \), hence the unique solution given by \([5]_6\).

*Exercise 5.14.* Solve these congruences following the above example.

a) \( 5^x \equiv 9 \pmod{13} \)
b) \( 2 \cdot 7^x \equiv 3 \pmod{13} \)
c) \(6 \cdot 8^x \equiv 7 \pmod{13}\)
d) \(10 \cdot 6^x \equiv 12 \pmod{13}\).

Exercise 5.15. Follow the above example, in a similar way, to solve again the congruences \(8^x \equiv 5 \pmod{13}\) from Exercise 3.6(a) and \(x^7 \equiv 12 \pmod{13}\) from Exercise 4.16(a).

Exercise 5.16. Find a primitive root modulo 17 and use it to solve the congruence \(12^3 \cdot 7^x \equiv 7 \cdot 11^x \pmod{17}\).

This technique of replacing the integer by its exponent, or \textit{index}, with respect to a chosen primitive root is named \textit{index arithmetic}. With this method we are able to tackle some more root extraction problems, as follows.

**Theorem 5.8.** Suppose \(\gcd(a,n) = 1\) and that there exists a primitive root modulo \(n\). Let \(d = \gcd(k, \phi(n))\). Then the congruence \(x^k \equiv a \pmod{n}\) has a solution if and only if \(a^{\phi(n)/d} \equiv 1 \pmod{n}\), in which case there are exactly \(d\) distinct solutions modulo \(n\).

\textit{Proof.} Let \(g\) be a primitive root modulo \(n\) such that \(g^c \equiv a \pmod{n}\) for some \(c \geq 0\). It suffices to seek for solutions for \(x\) in the reduced residue system \(G = \{g, g^2, g^3, \ldots, g^{\phi(n)}\}\). Let \(x = g^y\) so we may rewrite the congruence as \((g^y)^k \equiv g^c \pmod{n}\), which is equivalent to \(ky \equiv c \pmod{\phi(n)}\). By Linear Congruence Theorem a solution for \(y\) exists if and only if \(d \mid c\), in which case it is unique modulo \(\phi(n)/d\), hence \(d\) distinct solutions of the form \(x = g^y\) in \(G\). At the same time the congruence \(a^{\phi(n)/d} \equiv g^{\phi(n)/c} \equiv 1 \pmod{n}\) holds if and only if \(|g|_n = \phi(n) | \phi(n)c/d\) by Proposition 5.1(1), and this is the same condition \(d \mid c\).

\(\Box\)

\textit{Example.} Consider the congruence \(x^2 \equiv 3 \pmod{13}\). We have \(\gcd(2,12) = 2\) and check that \(3^{12/2} = 3^6 \equiv 1 \pmod{13}\) so we know a solution exists. Now use the primitive root 2 from the previous table to obtain \(2^{2y} \equiv 2^4 \pmod{13}\) and hence \(2y \equiv 4 \pmod{12}\). The solution set for \(y\) is \([2]_6\), therefore the two values for \(x\) are \(2^2\) and \(2^8\). These give two residue classes \([4]_{13}\) and \([9]_{13}\).

Exercise 5.17. Solve each congruence, when possible.

\begin{itemize}
  \item[a)] \(x^2 \equiv 10 \pmod{13}\)
  \item[b)] \(x^9 \equiv 1 \pmod{13}\)
  \item[c)] \(x^5 \equiv 3 \pmod{14}\)
  \item[d)] \(x^4 \equiv 5 \pmod{17}\)
  \item[e)] \(x^8 \equiv 16 \pmod{17}\)
\end{itemize}

Exercise 5.18. Without solving it, count how many distinct solutions the congruence \(x^{45} \equiv 53 \pmod{729}\) has, if any at all.
**Corollary 5.9.** Let \( p \) be a prime not dividing \( a \) and let \( d = \gcd(k, p - 1) \). The congruence \( x^k \equiv a \pmod{p} \) has a solution if and only if \( a^{(p-1)/d} \equiv 1 \pmod{p} \), in which case it has exactly \( d \) incongruent solutions modulo \( p \).

**Proof.** Primitive roots exist modulo any prime so Theorem 5.8 applies. \( \Box \)

### 5.4 Secret Key Exchange  

[Project 5]

For cryptological purposes, Alia and Bob need to establish a common secret key. However, the only available means of communication between them is the mobile phone, which they know is being tapped by the enemy. They resort to the Diffie-Hellman Key Exchange protocol as follows.

Alia picks a large prime \( p \), a primitive root \( g \), and a positive integer \( m < p \). She gives to Bob, over the non-secure mobile line, the numbers \( p, g, \) and \( g^m \pmod{p} \) but keeps \( m \) secret. In turn Bob selects a secret number \( n \) and gives to Alia \( g^n \pmod{p} \). They agree that their common secret key is \( g^{mn} \pmod{p} \), which, via Successive Squaring Algorithm, Alia obtains by computing \( (g^n)^m \pmod{p} \) and Bob, independently, \( (g^m)^n \pmod{p} \).

If the enemy gathers this information (but not \( m \) and \( n \) for they are not transmitted across) they will have to solve the congruence \( g^x \equiv b \pmod{p} \) where \( b = g^m \pmod{p} \), or similarly \( b = g^n \pmod{p} \), in order to capture the secret key. But the fact is, there is no efficient algorithm known for solving the discrete logarithm problem, and for large \( p \) it will not be computationally feasible to do it by trial and error.

**Assignment.** To illustrate the above idea, let \( p = 313, \; g = 10, \) and \( m \) be the residue mod \( p \) of your PUN. Compute the number Alia sends to Bob, \( g^m \pmod{p} \). Suppose Bob’s number to Alia is \( g^n \pmod{p} = 248 \). Compute the common secret key \( g^{mn} \pmod{p} \). Try to find \( n \).

**Exercise 5.19.** Will this idea work if \( g \) is not a primitive root modulo \( p \)? Discuss.
Chapter 6

Quadratic Residues

We shall continue the discussion on modular root extraction, but limiting ourselves to the case exponent 2. The existence problem for square roots modulo prime numbers climaxes with the celebrated Law of Quadratic Reciprocity, and that has been, more or less, the objective of this little workbook.

6.1 Quadratic Residues and the Legendre Symbol

Definition. A number $a$ which is relatively prime to $n$ is a quadratic residue modulo $n$ if the congruence $x^2 \equiv a \pmod{n}$ has a solution. If it has no solution then $a$ is called a quadratic non-residue modulo $n$.

For example 19 is a quadratic residue modulo 5 since $19 \equiv 2^2 \pmod{5}$ whereas 7 is a non-residue because $x^2 \equiv 7 \pmod{5}$ has no solution. It is clear that being a quadratic residue, or non-residue, applies to the entire residue class of $a$ modulo $n$. Hence, as usual, we say distinct or incongruent quadratic (non-)residues to mean those belonging to different residue classes.

Moreover the solutions of the congruence $x^2 \equiv a \pmod{n}$, if any, are also given by residue classes. In particular the task of separating the quadratic residues from the non-residues can be done within a chosen reduced residue system. For example modulo 5 we look at $\{1, 2, 3, 4\}$. We have $1^2 \equiv 4^2 \equiv 1 \pmod{5}$ and $2^2 \equiv 3^2 \equiv 4 \pmod{5}$. Thus the quadratic residues modulo 5 are given by $[1]_5$ and $[4]_5$, whereas quadratic non-residues by $[2]_5$ and $[3]_5$.

Exercise 6.1. Find all the quadratic residues and non-residues modulo $n$.

a) $n = 7$
b) $n = 8$
c) $n = 9$
d) $n = 10$
Exercise 6.2. Suppose $g$ is a primitive root modulo $n > 2$.

a) Prove that $g^k$ is a quadratic residue modulo $n$ if and only if $k$ is even.

b) Show that the quadratic residues and non-residues modulo $n$ are equal in number.

c) Give an example where (b) is false when modulo $n$ has no primitive roots.

d) Prove that the product $ab$ is a quadratic residue modulo $n$ if and only if either both $a, b$ are quadratic residues or both non-residues modulo $n$.

Definition. With a prime $p > 2$, the Legendre symbol is defined as follows.

$$\left(\frac{a}{p}\right) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue modulo } p \\
-1 & \text{if } a \text{ is a quadratic non-residue modulo } p \\
0 & \text{if } p \mid a 
\end{cases}$$

For example we have seen that $\left(\frac{19}{7}\right) = 1$ and $\left(\frac{7}{7}\right) = -1$. We have also $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ whenever $a \equiv b \pmod{p}$, hence in particular $\left(\frac{a^{\frac{p-1}{2}}}{p}\right)$.

Exercise 6.3. Investigate true or false.

a) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ implies $a \equiv b \pmod{p}$

b) $\left(\frac{1}{p}\right) = 1$

c) $\left(\frac{-1}{p}\right) = -1$

d) $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)^2$

Now Corollary 5.9 can be fitted for the quadratic case in a nice way with the use of Legendre symbol. Before that, however, we shall henceforth agree that the number $p$ in the symbol $\left(\frac{a}{p}\right)$ is always understood an odd prime, that is a prime larger than 2.

**Theorem 6.1** (Euler’s Criterion). $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$

**Proof.** It is trivial if $p \mid a$, else apply Corollary 5.9 with $k = 2$.

**Corollary 6.2.** The following equalities hold.

1) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$

2) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

**Proof.** The case $p \mid a$ is again trivial, else those numbers are all $\pm 1$. In each of the two equations, by Theorem 6.1, both sides are congruent modulo $p > 2$. The only way this can happen is when both are 1 or both $-1$. □
Exercise 6.4. Prove that $-1$ is a quadratic residue modulo a prime $p > 2$ if and only if $p \equiv 1 \pmod{4}$.

Example. Let us evaluate $(\frac{-75}{17})$. We apply Corollary 6.2 to obtain $(\frac{-75}{17}) = (\frac{-1}{17}) (\frac{5}{17})^2 (\frac{3}{17}) = (\frac{3}{17})$. And $(\frac{3}{17}) \equiv 3^8 \pmod{17}$ according to Euler’s Criterion. Successive Squaring Algorithm helps us, $3^8 \equiv 16 \pmod{17}$ hence $(\frac{-75}{17}) = -1$.

Note that there are different ways to arrive at this same result. For instance since $-75 \equiv 27 \pmod{17}$ then $(\frac{-75}{17}) = (\frac{27}{17}) = (\frac{3}{17})^3 = (\frac{3}{17})$. Or by the fact that $-75 \equiv 10 \pmod{17}$, we have $(\frac{-75}{17}) = (\frac{10}{17}) \equiv 10^8 \equiv -1 \pmod{17}$.

Exercise 6.5. Evaluate the Legendre symbol $(\frac{a}{p})$ in several ways.

a) $a = -28$ and $p = 5$

b) $a = 48$ and $p = 7$

c) $a = -35$ and $p = 11$

d) $a = 54$ and $p = 13$

As a matter of fact there are yet more ways by which we can evaluate the Legendre symbol. These are given by the next two lemmas and the Law of Quadratic Reciprocity, our main result for this section.

Lemma 6.3 (Gauss’ Lemma). If $p \nmid a$ then $(\frac{a}{p}) = (-1)^n$ where $n$ is the number of integers $x$ in $A = \{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$ satisfying $x \not\equiv 0 \pmod{p}$.

Proof. Exactly half of the numbers in $\{1, 2, \ldots, p-1\}$ are larger than $\frac{p}{2}$, and subtracting them by $p$ gives us another reduced residue system modulo $p$, call it $S = \{\pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}\}$. Since $p \nmid a$ then $A$ contains only distinct elements modulo $p$, hence $n$ is the number of negative integers in $S$ which are congruent modulo $p$ to some elements in $A$.

In $S$ we claim that if $k$ is congruent to some element in $A$ then $-k$ is not congruent to any element in $A$. If it were not so then there existed $ia, ja$ in $A$, with $1 \leq i < j \leq \frac{p-1}{2}$, for which $ia \equiv k \equiv -ja \pmod{p}$. But $p \nmid a$ would imply $i \equiv -j \pmod{p}$. This is impossible as both $i$ and $-j$ belong to $S$, a reduced residue system.

It follows that, modulo $p$, the elements of $A$ are reordering of the numbers $1, 2, \ldots, \frac{p-1}{2}$, only that $n$ of them have a negative sign:

$$a \cdot 2a \cdot 3a \cdots \frac{p-1}{2}a \equiv (-1)^n \cdot 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \pmod{p}$$

The common terms are relatively prime to $p$ hence cancellable: $a^{(p-1)/2} \equiv (-1)^n \pmod{p}$. Now apply Euler’s Criterion to obtain the desired result. ▽
CHAPTER 6. QUADRATIC RESIDUES

Example. We illustrate Gauss’ Lemma with \( a = 5 \) and \( p = 11 \). The set \( A = \{5, 10, 15, 20, 25\} \), whose residues mod 11 are \( \{5, 10, 4, 9, 3\} \). Those larger than 11/2 are 9 and 10. Hence \( \left( \frac{5}{11} \right) = (-1)^2 = 1 \).


Corollary 6.4. \( \left( \frac{2}{p} \right) = (-1)^{(p^2-1)/8} \)

Proof. Let us keep the notations as in the proof of Lemma 6.3.

By definition \( ka = \lfloor ka/p \rfloor p + ka \% p \), where the numbers \( ka \% p \) for \( k = 1, 2, \ldots, \frac{p-1}{2} \) are congruent modulo \( p \), perhaps not in this order, to \( 1, 2, \ldots, \frac{p-1}{2} \) but exactly \( n \) of them should have a negative sign. Denote by \( r \)'s those which should have been negatives and the rest by \( s \)'s so that

\[
\sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} \lfloor ka/p \rfloor p + \sum_{i=1}^{n} p - r_i + \sum_{j=1}^{\frac{p-1}{2} - n} s_j \tag{6.1}
\]

On the other hand we also have

\[
\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{i=1}^{n} r_i + \sum_{j=1}^{\frac{p-1}{2} - n} s_j \tag{6.2}
\]

Next subtract Equation (6.2) from Equation (6.1),

\[
(a - 1) \sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{\frac{p-1}{2}} \lfloor ka/p \rfloor p + \sum_{i=1}^{n} p - 2 \sum_{i=1}^{n} r_i \tag{6.3}
\]

Keep in mind that the number \( n \) is such that \((-1)^n = \left( \frac{2}{p} \right) \). Now let \( a = 2 \) and reduce Equation (6.3) mod 2 to obtain

\[
\sum_{k=1}^{(p-1)/2} k \equiv \sum_{k=1}^{(p-1)/2} \lfloor 2k/p \rfloor + n \pmod{2},
\]

since \( p \equiv 1 \pmod{2} \). But each term \( \lfloor 2k/p \rfloor = 0 \) because \( 2k < p \), hence \( n \equiv 1 + 2 + \cdots + \frac{p-1}{2} \equiv \frac{p^2-1}{8} \pmod{2} \). This says that \( n \) and \( \frac{p^2-1}{8} \) are both even or both odd and therefore \( \left( \frac{2}{p} \right) = (-1)^n = (-1)^{(p^2-1)/8} \). △

Lemma 6.5 (Eisenstein’s Lemma). If \( a \) is odd and not divisible by \( p \) then \( \left( \frac{a}{p} \right) = (-1)^m \) where \( m = \sum_{k=1}^{(p-1)/2} \lfloor ka/p \rfloor \).

Proof. Reduce Equation (6.3) mod 2, this time \( a \equiv p \equiv 1 \pmod{2} \), yielding \( 0 \equiv m + n \pmod{2} \). Again this means that \( m \) is of the same parity as the number \( n \) in Gauss’ Lemma, thereby making the two lemmas equivalent. △
Example. We illustrate Eisenstein’s Lemma with \( a = 5 \) and \( p = 11 \). We have \( m = \left\lfloor \frac{5}{11} \right\rfloor + \left\lfloor \frac{10}{11} \right\rfloor + \left\lfloor \frac{15}{11} \right\rfloor + \left\lfloor \frac{20}{11} \right\rfloor + \left\lfloor \frac{25}{11} \right\rfloor = 0 + 0 + 1 + 1 + 2 = 4 \). Hence \( \left( \frac{5}{11} \right) = (-1)^4 = 1 \).


Theorem 6.6 (The Law of Quadratic Reciprocity). If \( p \) and \( q \) are distinct odd primes then

\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{\frac{(p-1)(q-1)}{2}}
\]

Proof. Consider all ordered pairs \((x, y)\) satisfying \( 1 \leq x \leq \frac{p-1}{2} \) and \( 1 \leq q \leq \frac{q-1}{2} \). There are exactly \( \frac{(p-1)(q-1)}{2} \) such elements, which can be grouped into two classes, the first with \( py < qx \) and the second \( py > qx \). Note that \( py = qx \) is not possible as \( p \nmid qx \). For each \( x \) the condition \( py < qx \) is equivalent to \( 1 \leq y \leq \left\lfloor \frac{qx}{p} \right\rfloor \) hence the first class consists of \( m_1 = \sum_{x=1}^{p-1} \left\lfloor \frac{qx}{p} \right\rfloor \) elements and similarly the second \( m_2 \), resulting in the equation

\[
\frac{(p-1)(q-1)}{2} = m_1 + m_2 = \sum_{x=1}^{p-1} \left\lfloor \frac{qx}{p} \right\rfloor + \sum_{y=1}^{q-1} \left\lfloor \frac{py}{q} \right\rfloor
\]

Hence \( (-1)^{\frac{(p-1)(q-1)}{2}} = (-1)^{m_1}(-1)^{m_2} = \left( \frac{q}{p} \right) \left( \frac{q}{p} \right) \) by Lemma 6.5. \( \nabla \)

Exercise 6.8. Show that for any odd primes \( p, q \) we have \( \left( \frac{q}{p} \right) = \left( \frac{p}{q} \right) \) except when \( p \equiv q \equiv 3 \) (mod 4), in which case \( \left( \frac{q}{p} \right) = -\left( \frac{p}{q} \right) \).

Example. Let us evaluate \( \left( \frac{4459}{6247} \right) \). By factoring and repeated application of Theorem 6.6, and reducing \( \left( \frac{a}{p} \right) \) to \( \left( \frac{a \%(p)}{p} \right) \) in each step, we have

\[
\left( \frac{4459}{6247} \right) = \left( \frac{7}{6247} \right) \left( \frac{7}{6247} \right) \left( \frac{7}{6247} \right) \left( \frac{13}{6247} \right)
\]
\[
\left( \frac{7}{6247} \right) = -\left( \frac{6247}{7} \right) = -\left( \frac{3}{7} \right) = \left( \frac{7}{3} \right) = 1
\]
\[
\left( \frac{13}{6247} \right) = \left( \frac{6247}{13} \right) = \left( \frac{7}{13} \right) = \left( \frac{13}{7} \right) = \left( \frac{6}{7} \right) = \left( \frac{-1}{7} \right) = (-1)^3 = -1
\]

Putting these together, we conclude \( \left( \frac{4459}{6247} \right) = -1 \).

Exercise 6.9. Evaluate the Legendre symbol \( \left( \frac{a}{p} \right) \) using Theorem 6.6.
Exercise 6.10. Fix a prime modulus \( p > 2 \). Prove the following statements.

a) \( +2 \) is a quadratic residue if and only if \( p \% 8 = 1 \) or 7.
b) \( -2 \) is a quadratic residue if and only if \( p \% 8 = 1 \) or 3.
c) \( +3 \) is a quadratic residue if and only if \( p \equiv \pm 1 \pmod{12} \).
d) \( -3 \) is a quadratic residue if and only if \( p \% 6 = 1 \).

Exercise 6.11. Modulo which primes is 5 a quadratic residue?

6.2 The Jacobi Symbol

Despite all the variety of tools we have for evaluating the Legendre symbol \( \left( \frac{a}{p} \right) \), we just cannot avoid the need of factoring \( a \). This slows down computation time a great deal especially with large numbers. The Jacobi symbol is a generalization of the Legendre symbol in the way that \( p \) is now allowed to be an odd composite, and that in turn provides a fast way to compute the Legendre symbol, almost in a similar way that Euclidean Algorithm enables us to compute \( \gcd \) without factoring.

**Definition.** Let \( n = p_1 \cdot p_2 \cdot \cdots \cdot p_k \) be the product of odd prime numbers, not necessarily distinct. Define the *Jacobi symbol*

\[
\left( \frac{a}{n} \right) = \left( \frac{a}{p_1} \right) \left( \frac{a}{p_2} \right) \cdots \left( \frac{a}{p_k} \right)
\]

where each term on the right is the Legendre symbol. Moreover let \( \left( \frac{7}{n} \right) = 1 \).

As an example we have \( \left( \frac{14}{1275} \right) = \left( \frac{14}{3} \right) \left( \frac{14}{5} \right) \left( \frac{14}{17} \right) \) because 1275 = 3 \cdot 5^2 \cdot 17. Note that if \( \gcd(a,n) = 1 \) then the value of \( \left( \frac{a}{n} \right) \) is \( \pm 1 \), and 0 otherwise. In addition, if \( k = 1 \) then Jacobi symbol is really Legendre symbol. It is furthermore true that if \( \left( \frac{a}{n} \right) = -1 \) then \( a \) is a quadratic non-residue modulo \( n \), but the converse is sometimes false.

**Exercise 6.12.** Evaluate \( \left( \frac{14}{1275} \right) \). Is 14 a quadratic residue modulo 1275?

Surprisingly enough the Jacobi symbol behaves just like the Legendre symbol, in the sense that it satisfies all the properties of the Legendre symbol given in the previous section, including the law of reciprocity.
6.2. THE JACOBI SYMBOL

Proposition 6.7. Let \( n, m \) denote odd positive numbers.
1) \( \left( \frac{a}{n} \right) = \left( \frac{b}{n} \right) \) if \( a \equiv b \pmod{n} \)
2) \( \left( \frac{ab}{n} \right) = \left( \frac{a}{n} \right) \left( \frac{b}{n} \right) \)
3) \( \left( \frac{a}{mn} \right) = \left( \frac{a}{n} \right) \left( \frac{a}{m} \right) \)

Proof. The congruence \( a \equiv b \pmod{n} \) implies \( a \equiv b \pmod{p_i} \) for each prime \( p_i \) dividing \( n \). Thus
\[
\left( \frac{a}{n} \right) = \left( \frac{a}{p_1} \right) \left( \frac{a}{p_2} \right) \cdots \left( \frac{a}{p_k} \right) = \left( \frac{b}{p_1} \right) \left( \frac{b}{p_2} \right) \cdots \left( \frac{b}{p_k} \right) = \left( \frac{b}{n} \right)
\]
This proves the first claim. In a very similar way the others follow straight from the definition of Jacobi symbol.

\[ \Box \]

Theorem 6.8. Let \( n, m \) denote odd positive numbers.
1) \( \left( \frac{-1}{n} \right) = (-1)^{(n-1)/2} \)
2) \( \left( \frac{2}{n} \right) = (-1)^{(n^2-1)/8} \)
3) \( \left( \frac{m}{n} \right) = \left( \frac{n}{m} \right) (-1)^{\frac{(m-1)(n-1)}{2}} \)

Proof. Let \( n = p_1 p_2 \cdots p_k \) with odd prime factors, not assumed distinct.
1) Define \( f(n) = \left( \frac{-1}{n} \right) (-1)^{(n-1)/2} \) over the set of odd positive integers. It suffices to show that \( f(n) = 1 \) all the time. We do this by claiming that \( f(ab) = f(a) f(b) \) so that \( f(n) = \prod f(p_i) = 1 \) by Corollary 6.2(2). Now the integer \( \frac{ab - 1}{2} \) is of the same parity as \( \frac{a - 1}{2} + \frac{b - 1}{2} \). To verify, we check that their difference is an even number since \( a, b \) are odd:
\[
\frac{ab - 1}{2} - \frac{a - 1}{2} - \frac{b - 1}{2} = \frac{ab - a - b + 1}{2} = \frac{(a - 1)(b - 1)}{2}
\]
Hence \( f(ab) = \left( \frac{ab}{n} \right) (-1)^{\frac{ab - 1}{2}} = \left( \frac{a}{n} \right) \left( \frac{b}{n} \right) (-1)^{\frac{a - 1}{2}} (-1)^{\frac{b - 1}{2}} = f(a) f(b) \).

2) Similarly we define \( f(n) = \left( \frac{2}{n} \right) (-1)^{(n^2-1)/8} \) over the set of odd positive integers. We will prove that \( f(n) = 1 \) for all by showing \( f(ab) = f(a) f(b) \) and so \( f(n) = \prod f(p_i) = 1 \) by Corollary 6.4. By the result of Exercise 1.7(c) we claim that \( \frac{a^2 b^2 - 1}{8} \) is of the same parity as \( \frac{a^2 - 1}{8} + \frac{b^2 - 1}{8} \) by verifying that their difference is an even number:
\[
\frac{a^2 b^2 - 1}{8} - \frac{a^2 - 1}{8} - \frac{b^2 - 1}{8} = \frac{a^2 b^2 - a^2 - b^2 + 1}{8} = \frac{(a^2 - 1)(b^2 - 1)}{8}
\]
Hence \( f(ab) = \left( \frac{ab}{n} \right) (-1)^{\frac{a^2 b^2 - 1}{8}} = \left( \frac{a}{n} \right) \left( \frac{b}{n} \right) (-1)^{\frac{a^2 - 1}{8}} (-1)^{\frac{b^2 - 1}{8}} = f(a) f(b) \).
3) If \( \gcd(m, n) > 1 \) then both sides equal zero. Otherwise once more we let
\[
f(m, n) = \left( \frac{m}{n} \right) \left( \frac{n}{m} \right)^{\frac{(m-1)(n-1)}{2}}
\]
and we will show that \( f(m, n) = 1 \) for every pair of relatively prime odd integers \( m, n > 0 \). Using Equation 6.4 again, we have \( f(m, ab) = f(m, a)f(m, b) \) and \( f(ab, n) = f(a, n)f(b, n) \).

If we write \( m = q_1q_2\cdots q_l \) for its prime factorization, then
\[
f(m, n) = \prod f(m, p_i) = \prod \prod f(q_j, p_i) = 1 \text{ by Theorem 6.6.}
\]

\[\Box\]

**Example.** We illustrate again the evaluation of the Legendre symbol \( \left( \frac{4459}{6247} \right) \), this time with the help of Jacobi symbol.

\[
\left( \frac{4459}{6247} \right) = \left( \frac{6247}{4459} \right) = -\left( \frac{1788}{4459} \right) = -\left( \frac{2}{4459} \right)^2 \left( \frac{447}{4459} \right)
\]

\[
\left( \frac{4459}{447} \right) = \left( \frac{449}{447} \right) = \left( \frac{436}{447} \right) = -\left( \frac{2}{447} \right)^2 \left( \frac{109}{447} \right)
\]

\[
\left( \frac{109}{447} \right) = \left( \frac{109}{109} \right) = \left( \frac{109}{109} \right) = \left( \frac{10}{109} \right)
\]

\[
\left( \frac{10}{109} \right) = \left( \frac{2}{109} \right) \left( \frac{5}{109} \right) = (-1)^{1485} \left( \frac{109}{5} \right) = -\left( \frac{4}{5} \right) = -1
\]

The same conclusion \( \left( \frac{4459}{6247} \right) = -1 \). Note that neither 4459 nor 447 is prime, and that the only factoring needed is for the powers of 2.

**Exercise 6.13.** Evaluate the Jacobi symbol \( \left( \frac{218}{385} \right) \).

**Exercise 6.14.** Redo Exercise 6.9 with the help of Jacobi symbol.

### 6.3 Computing Square Roots

Having developed the tools to answer the existence question, we turn now to the actual problem of finding the modular square root. If \( a \) is a quadratic residue modulo the prime \( p > 2 \) then Corollary 5.9 says that the congruence \( x^2 \equiv a \pmod{p} \) has exactly two solutions modulo \( p \) which, since \( p \) is odd, are given by \( \pm x_0 \pmod{p} \) for any particular solution \( x_0 \). Still this knowledge does not help us to actually find \( x_0 \), except in the following special case.

**Theorem 6.9.** If \( a \) is a quadratic residue modulo a prime \( p \equiv 3 \pmod{4} \) then the congruence \( x^2 \equiv a \pmod{p} \) has exactly two solutions given by \( x \equiv \pm a^{(p+1)/4} \pmod{p} \).

**Proof.** By Euler’s Criterion, \( (a^{(p+1)/4})^2 = a^{(p+1)/2} = a^{(p-1)/2} \equiv a \pmod{p} \). That the two solutions are distinct is clear since \( p \nmid 2a \), thus the theorem follows from Corollary 5.9.

\[\Box\]
Example. Solve the congruence \( x^2 \equiv 14 \pmod{11} \). We first check that \( \left( \frac{14}{11} \right) = \left( \frac{3}{11} \right) = -\left( \frac{3}{11} \right) = -1 \), hence Theorem 6.9 applies with a particular solution \( x_0 = 3^{(11+1)/4} = 3^3 = 27 \). One solution class is given by \([27]_{11} = [5]_{11}\) and the other \([-5]_{11} = [6]_{11}\).

Exercise 6.15. Solve the following congruences.

- \( x^2 \equiv 2 \pmod{23} \)
- \( x^2 \equiv 8 \pmod{83} \)
- \( x^2 - 2x + 3 \equiv 0 \pmod{11} \)
- \( 2x^2 + x + 2 \equiv 0 \pmod{31} \)

For the general composite modulus \( n \), solving \( x^2 \equiv a \pmod{n} \) can get very complex. We demonstrate next a simpler case when \( n \) is the product of two distinct primes, hence Chinese Remainder Theorem comes in play.

Example. Solve the congruence \( x^2 \equiv 54 \pmod{115} \). We note that 115 = 5 \cdot 23. By Chinese Remainder Theorem the congruence is equivalent to the pair \( y^2 \equiv 54 \equiv 4 \pmod{5} \) and \( z^2 \equiv 54 \equiv 8 \pmod{23} \). The first has two solutions \( y \equiv \pm 2 \pmod{5} \) and the second, by Theorem 6.9, \( z \equiv \pm 8 \equiv \pm 13 \pmod{23} \).

Now by Chinese Remainder Theorem again, we conclude that there is a total of four distinct solutions modulo 115:

\[
\begin{align*}
  y &\equiv +2 \pmod{5} \quad \text{and} \quad z \equiv +13 \pmod{23} & \leftrightarrow & & x \equiv +82 \pmod{115} \\
  y &\equiv +2 \pmod{5} \quad \text{and} \quad z \equiv -13 \pmod{23} & \leftrightarrow & & x \equiv -13 \pmod{115} \\
  y &\equiv -2 \pmod{5} \quad \text{and} \quad z \equiv +13 \pmod{23} & \leftrightarrow & & x \equiv +13 \pmod{115} \\
  y &\equiv -2 \pmod{5} \quad \text{and} \quad z \equiv -13 \pmod{23} & \leftrightarrow & & x \equiv -82 \pmod{115} 
\end{align*}
\]

Exercise 6.16. Solve these congruences modulo \( n = pq \).

- \( x^2 \equiv 10 \pmod{21} \)
- \( x^2 \equiv 29 \pmod{35} \)
- \( x^2 \equiv 31 \pmod{55} \)
- \( x^2 \equiv 106 \pmod{119} \)
- \( x^2 \equiv 102 \pmod{341} \)

Theoretically the above techniques generalize to any modulus \( n \), by factoring it into distinct prime powers. Then for each prime power modulus we have seen a solution technique demonstrated following Theorem 5.8 making use of a primitive root. However the powers of 2 have no primitive roots beyond the second, and even so primitive roots in general are not readily available. Instead of pursuing further in this topic we shall close with an observation that solving the general quadratic congruence \( ax^2 + bx + c \equiv 0 \pmod{p} \) is essentially equivalent to extracting a square root. This is given as an exercise.
Exercise 6.17. Let $p$ be an odd prime relatively prime to $a$. Prove that the quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{p}$ has a solution if and only if 

$$\left( \frac{b^2 - 4ac}{p} \right) \geq 0$$

Exercise 6.18. Using Exercise 6.17, determine if there is a solution.

a) $x^2 \equiv -1 \pmod{101}$

b) $x^2 - 5x + 2 \equiv 0 \pmod{29}$

c) $2x^2 - x \equiv 17x + 24 \pmod{43}$

d) $13x^2 - 56x \equiv 44 \pmod{79}$

e) $211x^2 \equiv 73x - 186 \pmod{557}$

6.4 Electronic Coin Tossing [Project 6]

In a game of coin tossing, two players have a fifty-fifty chance of winning by betting on the outcome, either Head or Tail. How can this game be played electronically, over email for instance?

Alia selects two large primes with the condition $p \equiv 3 \pmod{4}$ and $q \equiv 3 \pmod{4}$ and sends the product $n = pq$ to Bob. In turn Bob chooses an integer $h < n$ and sends $a = h^2 \pmod{n}$ to Alia. Using Theorem 6.9 plus Chinese Remainder Theorem, Alia is able to solve $x^2 \equiv a \pmod{n}$ and finds four roots in the forms $x \equiv \pm h, \pm t \pmod{n}$.

Now Alia must guess Bob’s number, either $h$ or $t$. If Alia sends $h$ to Bob, Alia wins. If, however, she bets on $t$ then Bob wins and he shall prove his victory by returning to Alia the factors $p, q$, which supposedly only she knows. How will Bob do it? Knowing both $h$ and $t$ enables him to find one of the factors $p, q$ as $\gcd(h + t, n)$, which he can compute in no time\(^1\) using the Euclidean Algorithm.

Exercise 6.19. In this context, verify that the congruence $x^2 \equiv a \pmod{pq}$ has four roots whose residues mod $pq$ equal $h, pq - h, t, pq - t$. Then prove that $\gcd(h + t, pq) = p$ or $q$.

Assignment. Suppose Alia has selected the two primes $p, q$ and sent to Bob the number $n = 1000061$. Bob borrowed your 6-digit PUN for his number $h$ and sent to Alia $a = h^2 \pmod{n}$. Please help Alia to solve the congruence $x^2 \equiv a \pmod{n}$. Now suppose Alia sends the wrong square root to Bob. Help Bob to find the factors $p, q$ in order to tell Alia that he wins.

\(^1\)Well, in at most $O(\log^2 n)$ time.
Appendix A

To Learn More

This is a very brief collection of well-recommended books to read next on your own. We group them in four categories, altogether listed in a rough order of readability.

**Elementary Number Theory.** These contain all the materials we have presented and much more.


**Computational Number Theory.** Elementary topics with emphases on computational algorithms and implementations.


Analytic Number Theory. The branch of number theory which employs the techniques of calculus.


Algebraic Number Theory. A more advanced subject, presuming a knowledge in abstract algebra.


Appendix B

Answers & Hints

Chapter 1

1. No
2. (a,b) Only for positive numbers (c) True (d) False (e) True
3. 83437
4. (a) 4 (b) 0 (c) 9 (d) 2 (e) 7
5. 111 % 24
6. Show \((n^2 + 2) \% 4 \neq 0\), treating \(n\) even and odd separately.
7. (a,b) Factor it and use Proposition 1.3. (c) Let \(n = 2k + 1\).
   (d) Multiply \((n - 2)(n - 1)n(n + 1)(n + 2)\) and compare.
8. (a) 14 (b) 12 (c) 24 (d) 1 (e) 1
9. 1, 5, 7, 11
10. (a) True (b) True (c) Only for \(m > 0\) (d) True (e) Only if \(m\) is even
11. (a) 24 (b) 1 (c) 25 (d) 15 (e) 3
12. Theorem 1.5 and Proposition 1.1(4).
13. (a) \(a = 1, b = -3\) (b) \(-72, 143\) (c) \(-11\) (d) 11, \(-2\) (e) 3617, \(-822\)
14. Follow the proof of Corollary 1.7.
15. Exercise 1.7 and Theorem 1.8(2).
16. \(x = -231, y = 143\)
17. It follows from Theorem 1.9.
18. (a) \(x = -11 - 55k, y = 7 + 34k\) (b) \(x = -2 - 25k, y = 1 + 12k\)
   (c) none (d) \(x = 5 - 13k, y = -2 + 5k\) (e) \(x = 5 + 2k, y = 5 + 3k\)
19. 7 minutes each

Chapter 2

1. 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47
2. (a) prime (b) composite (c) composite (d) prime (e) composite
APPENDIX B. ANSWERS & HINTS

3. (a) False (b) False (c) True (d) True
4. (a) $3 \cdot 41$ (b) $2^4 \cdot 5^2$ (c) $2^4 \cdot 3^2 \cdot 5$ (d) $3 \cdot 5^2 \cdot 101$ (e) $7 \cdot 35759$
5. (a) 18 (b) 30 (c) 11 (d) 32 (e) 4
6. 1, 2, 4, 8, 11, 22, 44, 88, 121, 242, 484, 968
7. Let $m$ be factored into primes.
8. (a) 80 (b) 2940 (c) $n$ (d) 1 (e) 4400
9. Keep the notations as in Corollary 2.5.
10. (a) Like Corollary 2.5, max instead of min. (b) Follows from (a).
    (c) $\gcd(m, n) \cdot \operatorname{lcm}(m, n) = |mn|$ (d) 30 $\cdot$ 12600 = 600 $\cdot$ 630
11. (a) 78,030 (b) 661,458 (c) 61,967 (d) 403,310,428
12. Similar to the proof in Theorem 2.8, use $6(N-1) + 5$.
13. It is divisible by $2^d - 1$ where $d \mid k$.
14. (a) 2, 5, 17, 37, 101 (b) 3, 5, 17, 257, 65537
    (c) 3, 7, 31, 127, 8191 (d) 2, 3, 5, 11, 23
15. (3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61), (71, 73)
16. 3, 5, 7
17. (a) $2 + 2$ (b) $5 + 23 = 11 + 17$ (c) $227 + 229$ etc. (d) $491 + 509$ etc.
18. (a) $29 \cdot 73$ (b) $97 \cdot 173$ (c) $11 \cdot 67 \cdot 89$ (d) $239 \cdot 293$

Chapter 3

1. See Exercise 1.7(c).
2. Write $p = 3k + 1$ and show that $k$ must be even.
3. (a) True (b) True (c) True (d) True (e) False
4. One way requires Euclid’s Lemma.
5. (a) $\{0, \pm 2, \pm 4, \pm 6, \pm 8\}$ (b) $\{1, 3, 5, 7, 9, 11, 13\}$ (c) $\{0, 4, 8, 12, 16\}$
    (d) $\{2, 3, 5, 11, 19\}$ (e) impossible
6. (a) $[12]_{13}$ (b) $[3]_7$ (c) $[6]_9$ (d) $[31]_{209}$ (e) $[172]_{341}$
7. (a) $[4]_7$ (b) $[3]_8$ (c) $[7]_{12}$ (d) none (e) $[31]_{209}$
8. See Exercise 1.9.
10. Start with 36! then multiply by 36$^{-1}$ and 35$^{-1}$ modulo 37.
11. Show that if $n$ is composite then $(n-1)! \equiv 0 \pmod{n}$.
12. 1000
13. Use Exercise 2.10(b).
14. Prove independently mod $p, q$ then apply Theorem 3.9.
15. (a) $[5]_6$ (b) $[23]_{30}$ (c) $[19]_{28}$ (d) $[29]_{88}$
16. 3 dinars and 43 piasters
17. (a) $[23]_{30}$ (b) $[47]_{140}$ (c) $[-8]_{990}$ (d) $[191]_{210}$ (e) $[1537]_{3960}$
18. Similar to the proof with mod 9.
19. Let $n = 10t + u = 17k$. Conversely let $t - 5u = 17k$.
20. Let $n = 10t + u = 19k$. Conversely let $t + 2u = 19k$. 
Chapter 4

1. (a) False (b) True (c) True (d) False
2. Prove the two cases $p | a$ and $p \nmid a$ separately.
3. (a) 12 (b) 6 (c) 8 (d) 8
4. (a) $\{1, 5, 7, 11\}$ (b) $\{\pm 1, \pm 3, \pm 5, \pm 7, \pm 9, \pm 11\}$ (c) $\{3, 5, 11, 13, 23, 29\}$
   (d) $\{7, 11, 13, 17, 19, 23, 29, 31\}$ (e) $\{1, 5, 7, 11, 13, 17, 19, 23\}$
5. Use Corollary 3.6.
6. (a) 64 (b) 500 (c) 512 (d) 1280 (e) 214548
7. 5, 8, 10, 12
8. (a) Theorem 4.5 (b,c) Proposition 4.6(3) (d) Use (b) and (c).
9. Check!
10. Apply Proposition 3.1.
11. (a) 1 (b) 37 (c) 25 (d) 62 (e) 122
12. 9
13. (a) 6 (b) 28 (c) 16 (d) 0 (e) 625
14. (a) 3 (b) 46 (c) 49 (d) 70 (e) 34
15. 69
16. (a) $[12]_{13}$ (b) $[21]_{32}$ (c) $[75]_{121}$ (d) $[30]_{899}$ (e) $[1132]_{2005}$
17. (a) 4625 (b) 6791 (c) 7273 (d) 0K
18. Use Corollary 4.8 or Theorem 3.9.
19. (a) 11 \cdot 19 (b) 23 \cdot 97 (c) 83 \cdot 137 (d) 211 \cdot 701
20. 227 \cdot 229
21. 167 \cdot 181, 181 \cdot 197

Chapter 5

1. (a) 6 (b) 4 (c) 2 (d) 2 (e) 10
2. (a) False (b) False (c) False (d) True
3. Show that $\phi(n) = n - 1$.
4. 3, 2, 3, 6, 1
5. Try to generalize from Proposition 5.1(3).
6. Show that $(a^{-1})^k \equiv (a^k)^{-1}$.
7. No.
8. (a) 5 (b) 3, 5 (c) 2, 5 (d) 3, 7 (e) none
9. $2^3, 2^7, 2^9$
10. (a) Lemma 3.7 (b,c,d) Follow from (a).
11. (a) 2 (b) 2 (c) 4 (d) 40
12. (a) 8 (b) 8 (c) 0 (d) 200 (e) 0
13. 7, 17, 31
14. (a) no solution (b) $[9]_{12}$ (c) $[2]_4$ (d) $[4]_{12}$
15. $[12]_{13}$
16. $[1]_4$
17. (a) $[±6]_{13}$ (b) $[1,3,9]_{13}$ (c) $[5]_{14}$ (d) no (e) $[3,5,6,7,10,11,12,14]_{17}$
18. 9
19. For discussion only.

Chapter 6

1. (a) $[1,2,4]_7$ and $[3,5,6]_7$ (b) $[1]_8$ and $[3,5,7]_8$ (c) $[1,4,7]_9$ and $[2,5,8]_9$
   (d) $[1,9]_{10}$ and $[3,7]_{10}$
2. (a) Proposition 5.2(1) (c) $n = 8$ (b,d) From (a)
3. (a) False (b) True (c) False (d) True
4. It follows from Corollary 6.2(2).
5. (a) $-1$ (b) $-1$ (c) $1$ (d) $-1$
6. See Exercise 6.5.
7. See Exercise 6.5.
8. In Theorem 6.6 multiply the equation by $\left(\frac{p}{q}\right)$.
9. (a) $1$ (b) $-1$ (c) $-1$ (d) $-1$ (e) $1$
10. (a) Corollary 6.4 (b) By (a) and Exercise 6.4 (c,d) Theorem 6.6
11. $p \equiv \pm 1 \pmod{5}$
12. 1, No
13. $-1$
15. (a) $[±5]_{25}$ (b) no solution (c) $[4,9]_{11}$ (d) $[22,24]_{31}$
16. (a) no solution (b) $[±8,±13]_{35}$ (c) $[±14,±19]_{55}$ (d) $[±15,±36]_{119}$
   (e) $[±28,±127]_{341}$
17. Complete the square!
18. (a) Yes (b) No (c) Yes (d) Yes (e) No
19. Observe the example with $n = 115$. 
Appendix C

Primes < 10,000

2  3  5  7 11 13 17 19 23 29
31 37 41 43 47 53 59 61 67 71
73 79 83 89 97 101 103 107 109 113
127 131 137 139 149 151 157 163 167 173
179 181 191 193 197 199 211 223 227 229
233 239 241 251 257 263 269 271 277 281
283 293 307 311 313 317 331 337 347 349
353 359 367 373 379 383 389 397 401 409
419 421 431 433 439 443 449 457 461 463
467 479 487 491 499 503 509 521 523 541
547 557 563 569 571 577 587 593 599 601
607 613 617 619 631 641 643 647 653 659
661 673 677 683 691 701 709 719 727 733
739 743 751 757 761 769 773 787 797 809
811 821 823 827 829 839 853 857 859 863
869 881 883 887 907 911 919 929 937 941
947 953 967 971 977 983 991 997 1009 1013
1019 1021 1031 1033 1039 1049 1061 1063 1069
1087 1091 1093 1097 1103 1109 1117 1123 1129 1151
1153 1163 1171 1181 1187 1193 1201 1213 1217 1223
1229 1231 1237 1249 1259 1277 1279 1283 1289 1291
1297 1301 1303 1307 1319 1321 1327 1361 1367 1373
1381 1399 1409 1423 1427 1429 1433 1439 1447 1451
1453 1459 1471 1481 1483 1487 1489 1493 1499 1511
1523 1531 1543 1549 1553 1559 1567 1571 1579 1583
1597 1601 1607 1609 1613 1619 1621 1627 1637 1657
1663 1667 1669 1693 1697 1699 1709 1721 1723 1733
1741 1747 1753 1759 1777 1783 1787 1789 1801 1811
1823 1831 1847 1861 1867 1871 1873 1877 1879 1889
65
<table>
<thead>
<tr>
<th>Prime Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>2063</td>
</tr>
<tr>
<td>2131</td>
</tr>
<tr>
<td>2203</td>
</tr>
<tr>
<td>2257</td>
</tr>
<tr>
<td>2317</td>
</tr>
<tr>
<td>2389</td>
</tr>
<tr>
<td>2453</td>
</tr>
<tr>
<td>2549</td>
</tr>
<tr>
<td>2621</td>
</tr>
<tr>
<td>2713</td>
</tr>
<tr>
<td>2847</td>
</tr>
<tr>
<td>2939</td>
</tr>
<tr>
<td>3023</td>
</tr>
<tr>
<td>3121</td>
</tr>
<tr>
<td>3217</td>
</tr>
<tr>
<td>3319</td>
</tr>
<tr>
<td>3413</td>
</tr>
<tr>
<td>3511</td>
</tr>
<tr>
<td>3613</td>
</tr>
<tr>
<td>3697</td>
</tr>
<tr>
<td>3779</td>
</tr>
<tr>
<td>3881</td>
</tr>
<tr>
<td>3967</td>
</tr>
<tr>
<td>4049</td>
</tr>
<tr>
<td>4129</td>
</tr>
<tr>
<td>4229</td>
</tr>
<tr>
<td>4297</td>
</tr>
<tr>
<td>4409</td>
</tr>
<tr>
<td>4507</td>
</tr>
<tr>
<td>4591</td>
</tr>
<tr>
<td>4663</td>
</tr>
<tr>
<td>4783</td>
</tr>
<tr>
<td>4871</td>
</tr>
<tr>
<td>4957</td>
</tr>
<tr>
<td>5017</td>
</tr>
<tr>
<td>5101</td>
</tr>
<tr>
<td>5197</td>
</tr>
<tr>
<td>5309</td>
</tr>
<tr>
<td>5413</td>
</tr>
<tr>
<td>5507</td>
</tr>
<tr>
<td>5599</td>
</tr>
<tr>
<td>5689</td>
</tr>
<tr>
<td>5783</td>
</tr>
<tr>
<td>5851</td>
</tr>
</tbody>
</table>