NUMBER THEORY

AMIN WITNO

www.witno.com

Number Theory

Outlines and Problem Sets

Amin Witno <www.witno.com>

Preface

These notes are mere outlines for the course Math 313 given at Philadelphia University in the Fall 2005 semester with 33 students (and a half) for whom these have been prepared.

Chapter 1 **Divisibility**

The Integers, Greatest Common Divisors, The Euclidean Algorithm, Linear Equation Theorem. Project 1: Extended Euclidean Algorithm

Chapter 2 **Prime Numbers**

The Infinitude of Primes, The Fundamental Theorem of Arithmetic, Prime Number Conjectures, Primes in Arithmetic Progressions, The Prime Number Theorem. Project 2: Fermat Factorization

Chapter 3 **Congruences**

Modular Arithmetic, Linear Congruence Theorem, Modular Inverses, Chinese Remainder Theorem, Wilson's Theorem. Project 3: Divisibility Tests

Chapter 4 **Modular Exponentiation**

Successive Squaring Algorithm, Fermat's Little Theorem, Euler Phi-Function, Euler's Theorem, Modular Root Extraction. Project 4: The RSA Cryptosystem

Chapter 5 **Primitive Roots**

Orders, Primitive Roots Modulo Primes, Primitive Root Theorem, Discrete Logarithms. Project 5: Secret Key Exchange

Chapter 6 **Quadratic Residues**

Legendre Symbol, The Law of Quadratic Reciprocity, Jacobi Symbol, Modular Square Roots. Project 6: Electronic Coin Tossing

Appendix **Primes < 4,000; Hints and Answers**

References

1. David M. Burton, Elementary Number Theory, 6th edition 2007, McGraw Hill
2. Joseph H. Silverman, A Friendly Introduction to Number Theory, 3rd edition 2006, Prentice Hall
3. Kenneth H. Rosen, Elementary Number Theory and Its Applications, 5th edition 2005, Addison Wesley
4. Niven, Zuckerman, and Montgomery, An Introduction to the Theory of Numbers, 5th edition 1991, Wiley

Copyrights

Last Edited: 26–2–2006

Chapter 1
Divisibility

The natural numbers 1, 2, 3, ... together with their negatives and zero are called the integers. Number Theory is the study of integers. Every number represented throughout these notes will be understood an integer unless otherwise stated.

Definition: The number d **divides** m or m is **divisible** by d if the rational number m/d is an integer. The number d is then called a **divisor** of m, while m a **multiple** of d, and this relation can be written $d \mid m$, or $d \nmid m$ if it is not true. For example $3 \mid 18$, $5 \nmid 12$, and 2 divides all even numbers.

1.1 Proposition: Properties of Divisibility

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

Definition: The **greatest common divisor** of two integers m and n 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 $6 \mid 24$.

Example: Find $\gcd(36, 48)$.

Definition: For every real number x, the notation $[x]$ denotes the greatest integer $\leq x$. For example $[3.14] = 3$ and $[2] = 2$. Now with $d > 0$ define the **modulo operation** by $m \bmod d = m - [m/d]\, d$. For example $73 \bmod 4 = 1$. This quantity is also called the **remainder** upon dividing m by d and it lies in the range $0 \leq m \bmod d \leq d - 1$.

Example: Compute $1234 \bmod 5$, $24 \bmod 3$, $7 \bmod 11$.

1.2 The Euclidean Algorithm: $\gcd(m, n) = \gcd(n, m \bmod n)$

Example: Use Euclidean Algorithm to compute $\gcd(12345, 67890)$.

1.3 Theorem: $\gcd(m, n) = am + bn$ for some integers a and b.

Example: Find a and b such that $\gcd(12345, 67890) = 12345\, a + 67890\, b$.

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

1.5 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

$$(x = x_0 - k\, n/d\,,\ y = y_0 + k\, m/d)$$

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

Example: What are the solutions of these equations?

1. $17x + 18y = 1$
2. $12x + 18y = 1$
3. $12x + 18y = 6$
4. $12x + 18y = 30$

1.6 Corollary: gcd(m, n) = 1 if and only if $mx + ny = 1$ has a solution.

1.7 Lemma: Let S be the set of all integral linear combinations of m and n. Then
1. S is equal to the set of all multiples of gcd(m, n).
2. gcd(m, n) is the smallest positive element of S.
3. gcd(m, n) = 1 if and only if S is the set of all integers.

1.8 Proposition: Properties of Greatest Common Divisors
1. If $d \mid m$ and $d \mid n$ then $d \mid$ gcd(m , n).
2. If $k > 0$ then gcd(km, kn) = k gcd(m, n).
3. If gcd(m, n) = d then gcd(m/d, n/d) = 1.
4. If gcd(a, m) = 1 and gcd(a, n) = 1 then gcd(a, mn) = 1.
5. If $m \mid a$ and $n \mid a$ and gcd(m, n) = 1 then $mn \mid a$.

Problems:
1. Does 3 divide 250313?
2. The time is now 11 o'clock in the morning. What will it be 100 hours later?
3. Find all solutions of gcd(n, 12) = 1 in the range $1 \le n \le 12$.
4. Compute gcd(12345, 54321).
5. Find a solution of $34x + 55y = 1$.
6. Find all the solutions of $25x + 65y = 270$.
7. I made two calls today using my MobileCom account, one call to another MobileCom line for 6 piasters per minute and another call to a FastLink number for 16 piasters per minute. The total charge was 90 piasters. For how long did I talk in each call?
8. Investigate true or false.
    a) If $m \mid n$ then $m \le n$.
    b) If $m \mid n$ and $n \mid m$ then $m = n$.
    c) If $c \mid m$ and $d \mid n$ then $cd \mid mn$.
    d) If $d \mid mn$ then either $d \mid m$ or $d \mid n$.
    e) If $dn \mid mn$ then $d \mid m$.
9. Investigate true or false.
    a) gcd(m, n) > 0
    b) gcd(m, n) = gcd($m - n$, n)
    c) gcd(n, $n + 1$) = 1
    d) gcd(n, $n + 2$) = 2
10. Prove that if $d \mid$ gcd(m, n) then gcd(m/d, n/d) = gcd(m, n)/d.
11. Prove that $n^2 + n$ is even.
12. Prove that $n^2 + 2$ is not divisible by 4.
13. Prove that $n^2 - 1$ is a multiple of 8 if n is odd.
14. Prove that $6 \mid n^3 - n$.
15. Prove that $24 \mid n^3 - n$ if n is odd.
16. Prove that $30 \mid n^5 - n$.

Chapter 2
Prime Numbers

Definition: An integer $p > 1$ with no positive divisors except 1 and itself is called a **prime** number. 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 3 | 21. Throughout these notes we shall designate p to denote a prime number.

2.1 Proposition: Properties of Primes
1. Every integer greater than 1 has a prime divisor.
2. p is a prime if and only if it has no prime divisor $\leq \sqrt{p}$.
3. $\gcd(p, n) = p$ if $p \mid n$, otherwise $\gcd(p, n) = 1$.
4. If $p \mid mn$ then either $p \mid m$ or $p \mid n$.

2.2 Theorem: There are infinitely many prime numbers.

2.3 The Fundamental Theorem of Arithmetic: Every integer greater than 1 is a product of prime numbers in a unique way up to reordering.

2.4 Corollary: Suppose $m = \prod p_i^{m_i}$, $n = \prod p_i^{n_i}$ where the primes in each product are distinct and $m_i, n_i \geq 0$. Then $\gcd(m, n) = \prod p_i^{e_i}$ where $e_i = \min\{m_i, n_i\}$.

Example: Find $\gcd(2^4 \cdot 5^2 \cdot 7 \cdot 11^3, 2^7 \cdot 3^2 \cdot 5 \cdot 11^3)$.

2.5 Conjectures: Unsolved problems concerning prime numbers.
1. There are infinitely many primes in the sequence $\{n^2 + 1\}$.
2. *Twin Primes*: There are infinitely many primes in the sequence $\{p + 2\}$.
3. *Mersenne Primes*: There are infinitely many primes in the sequence $\{2^p - 1\}$.
4. *Fermat Primes*: Only finitely many primes are in the sequence $\{2^{2^n} + 1\}$.
5. *Goldbach's Conjecture*: Every even number ≥ 4 is a sum of two primes.

2.6 Dirichlet's Theorem on Primes in Arithmetic Progressions: There are infinitely many primes in the sequence $\{an + b\}$ if and only if $\gcd(a, b) = 1$.
Proof for $a = 4$ and $b = 3$.

2.7 The Prime Number Theorem: Let $\pi(x)$ denote the number of primes $\leq x$. Then

$$\lim_{x \to \infty} \frac{\pi(x)}{x / \log x} = 1 .$$

Even more accurately, $\pi(x)$ can be estimated by $x / (\log x - 1)$ for large values of x.
No Proof.

Problems
1. Factor the number 250313 into primes.
2. Find all the divisors of $300 = 2^2 \cdot 3 \cdot 5^2$.
3. How many positive integers divide the number $n = 2^4 \cdot 3^2 \cdot 5 \cdot 7^3$?
4. Find all pairs of twin primes less than 100.

5. Find all primes in the form $n^2 + 1$ less than 100.
6. Write the number 2006 as a sum of two primes in five different ways.
7. Find five Mersenne primes.
8. Find five Fermat primes.
9. Estimate the number of primes which are less than one million.
10. Estimate how many prime numbers among the ten-digit integers.
11. Investigate true or false.
    a) $n^2 + n + 41$ is prime for all $n > 0$.
    b) $n^2 - 81n + 1681$ is prime for all $n > 0$.
    c) If $p \mid n^2$ then $p \mid n$.
    d) If p divides abc then p divides a or b or c.
12. The **least common multiple** of two integers is the smallest positive integer which is divisible by both. For example lcm(4, 6) = 12.
    a) Use prime factorization to find a formula for lcm(m, n).
    b) Find a relation between gcd(m, n) and lcm(m, n).
    c) Illustrate your formula using $m = 600$ and $n = 630$.
13. Prove that if $d^2 \mid m^2$ then $d \mid m$.
14. Prove that $\gcd(m^2, n^2) = \gcd(m, n)^2$.
15. Find all prime triplets: p, $p + 2$, $p + 4$, all of which are primes.
16. Prove that there are infinitely many primes in the sequence $\{6n + 5\}$.

Chapter 3
Congruences

Definition: Two integers a and b are **congruent** modulo $n > 0$ if $n \mid a - b$, in which case we write $a \equiv b \pmod{n}$. Equivalently $a \equiv b \pmod{n}$ can be defined as $a \bmod n = b \bmod n$ and in particular $a \equiv a \bmod n \pmod{n}$. For example $13 \equiv 1 \equiv 4 \pmod 3$ and all even numbers $n \equiv 0 \pmod 2$. Note that congruence is an equivalence relation.

3.1 Proposition: Properties of Congruences
1. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a + c \equiv b + d \pmod{n}$.
2. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$.
3. If $a \equiv b \pmod{n}$ then $f(a) \equiv f(b) \pmod{n}$ for any integral polynomial $f(x)$.
4. If $ma \equiv mb \pmod{n}$ and $\gcd(m, n) = 1$ then $a \equiv b \pmod{n}$.
5. If $ma \equiv mb \pmod{mn}$ then $a \equiv b \pmod{n}$.

Definition: Congruence modulo n is an equivalence relation over the integers with n **congruence classes** which are the classes of integers with remainders $0, 1, 2, \ldots, n - 1 \bmod n$. A set of n numbers form a **complete residue system** modulo n if each comes from a different congruence class modulo n. For example a complete residue system modulo 7 can be $\{0, 1, 2, 3, 4, 5, 6\}$, $\{1, 2, 3, 4, 5, 6, 7\}$, or $\{1, 2, 3, 11, 75, -1, 0\}$ etc.

Example: Find a complete residue system modulo 7 with only even numbers.

3.2 Linear Congruence Theorem: The congruence $mx \equiv c \pmod{n}$ has a solution if and only if $d = \gcd(m, n) \mid c$ in which case it has exactly d solutions modulo n:

$$x \equiv x_0 + k\, n/d \pmod{n}$$

for $k = 0, 1, 2, \ldots, d-1$ and for any particular solution x_0.

Example: Count how many solutions each congruence has, then find them.
1. $30x \equiv 5 \pmod{40}$
2. $27x \equiv 1 \pmod{209}$
3. $2x \equiv 3 \pmod{1023}$
4. $32x \equiv 7 \pmod{49}$

Definition: a and b are **inverses** of each other modulo n if $ab \equiv 1 \pmod{n}$.

3.3 Modular Inverse Theorem: The number a has an inverse modulo n if and only if $\gcd(a, n) = 1$, in which case its inverse $b = a^{-1}$ is unique modulo n.

Example: Find a^{-1} modulo n if it exists.
1. $a = 2,\ n = 7$
2. $a = -5,\ n = 8$
3. $a = 35,\ n = 42$
4. $a = 27,\ n = 209$

3.4 Chinese Remainder Theorem: If $\gcd(m, n) = 1$ then the two congruences $x \equiv c \pmod{m}$ and $x \equiv d \pmod{n}$ have a unique common solution modulo mn.

Example: Find the common solution of $x \equiv 5 \pmod 8$ and $x \equiv 7 \pmod{11}$.

Definition: m and n are **relatively prime** if $\gcd(m, n) = 1$. Three integers, or more, are **pairwise relatively prime** if they are relatively prime one to another.

3.5 Chinese Remainder Theorem: Suppose $n_1, n_2, ..., n_k$ are pairwise relatively prime. Then the system of congruences $x \equiv c_i \pmod{n_i}$ where $i = 1, 2, ..., k$ has a unique solution modulo $N = n_1 n_2 ... n_k$. Explicitly the solution is given by

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

where each inverse is taken modulo n_i.

Example: Find x satisfying $x \equiv 5 \pmod 8$, $x \equiv 7 \pmod{11}$, and $x \equiv 12 \pmod{15}$.

3.6 Lemma: If $a^2 \equiv 1 \pmod p$ then $a \equiv \pm 1 \pmod p$.

3.7 Wilson's Theorem: If p is prime then $(p - 1)! \equiv -1 \pmod p$.

Example: Find $k!$ mod 13 for $k = 11, 12, 13, 14$.

Problems

1. Find a complete residue system modulo 9 with only odd numbers.
2. Find a complete residue system modulo 5 with only prime numbers.
3. Find all the solutions of $12x \equiv 18 \pmod{54}$.
4. Find the inverse of 7 modulo 12.
5. Which integers $1 \le a \le 12$ have an inverse modulo 12?
6. Find the smallest integer $x > 1$ satisfying the three congruences $x \equiv 1 \pmod 7$, $x \equiv 1 \pmod{11}$, and $x \equiv 1 \pmod{13}$.
7. Find all solutions to the following system of four congruences: $x \equiv 2 \pmod 5$, $x \equiv 1 \pmod 8$, $x \equiv 7 \pmod 9$, and $x \equiv -3 \pmod{11}$.
8. I have less than 3 dinars left in my MobileCom prepaid account. If I use it all for sending local SMSs for 3 piasters each then 1 piaster will be left. If I use it all for sending international SMSs for 7 piasters each then 3 piasters will be left. If I use it all for sending MMSs for 13 piasters each then 2 piasters will be left. How much credits exactly do I have?
9. Investigate true or false.
    a) If $a \equiv b \pmod n$ then $ma \equiv mb \pmod{mn}$.
    b) If $a \equiv b \pmod n$ and $d \mid n$ then $a \equiv b \pmod d$.
    c) If $a \equiv b \pmod n$ then $\gcd(a, n) = \gcd(b, n)$.
10. Prove that $37 \mid 35! - 1$.
11. Prove that $37 \mid 34! - 18$.
12. Prove that if a is odd then $a^2 \equiv 1 \pmod 8$.
13. Prove that if $p \equiv 1 \pmod 3$ then $p \equiv 1 \pmod 6$.
14. Prove that if $a^2 \equiv b^2 \pmod p$ then $a \equiv b \pmod p$ or $a \equiv -b \pmod p$.
15. Prove that if $a \equiv b \pmod m$ and $a \equiv b \pmod n$ then $a \equiv b \pmod{\text{lcm}(m, n)}$.
16. Prove that the converse of Wilson's Theorem is also true.

Chapter 4
Modular Exponentiation

4.1 Successive Squaring Algorithm: To efficiently compute $a^k \bmod n$ for large integer k, first compute $a^2, a^4, a^8, \ldots \bmod n$ up to the highest power of 2 in the binary equivalent of k.

Example: Compute $3^{99} \bmod 20$.

4.2 Lemma: 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.

4.3 Fermat's Little Theorem: If $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$.

Example: Compute the following modular exponentiation.

1. $8^{40} \bmod 41$
2. $8^{2345} \bmod 41$
3. $5^{495} \bmod 239$

Definition: The **Euler phi-function** $\varphi(n)$ is the number of positive integers up to n which are relatively prime to n. For example $\varphi(10) = 4$ and $\varphi(11) = 10$.

Definition: A **reduced residue system** modulo n is a subset of a complete residue system modulo n consisting of the $\varphi(n)$ numbers relatively prime to n. For example $\{1, 3, 5, 7\}$ is a reduced residue system modulo 8.

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

Example: Illustrate the above lemma with $a = 4$ and $n = 9$.

4.5 Euler's Theorem: If $\gcd(a, n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Example: Compute $7^{26} \bmod 10$.

Remark: As a computational corollary, when $\gcd(a, n) = 1$ then $a^k \bmod n$ can be reduced to $(a \bmod n)^{k \bmod \varphi(n)} \bmod n$. Unfortunately the theorem is not true when $\gcd(a, n) \neq 1$, nevertheless we still have the periodicity of $a, a^2, a^3, \ldots \bmod n$.

Example: Compute the following modular exponentiation.

1. $2^{26} \bmod 10$
2. $50^{345} \bmod 12$
3. $11^{123} \bmod 32$
4. $77^{3456} \bmod 900$

4.6 Theorem: If gcd(m, n) = 1 then $\varphi(mn) = \varphi(m)\,\varphi(n)$.

4.7 Proposition: Evaluation of Euler Phi-Function

1. $\varphi(p) = p - 1$
2. $\varphi(p^k) = p^k - p^{k-1}$
3. If $n = \prod p_i^{n_i}$ then $\varphi(n) = \prod p_i^{n_i-1}(p_i-1) = n\prod\left(1 - \frac{1}{p_i}\right)$.

Example: Find $\varphi(61)$, $\varphi(62)$, $\varphi(63)$, $\varphi(64)$.

4.8 Modular Root Extraction: If gcd(a, n) = 1 and gcd(j, $\varphi(n)$) = 1 then the congruence $x^j \equiv a \pmod{n}$ has a unique root $x \equiv a^k \pmod{n}$ where $k \equiv j^{-1} \pmod{\varphi(n)}$.

Example: Solve for x .

1. $x^7 \equiv 2 \pmod{11}$
2. $x^{13} \equiv 5 \pmod{32}$
3. $x^{239} \equiv 23 \pmod{2005}$

Problems

1. Find a reduced residue system modulo 24.
2. Find a reduced residue system modulo 15 with only odd numbers.
3. Find $\varphi(250313)$.
4. Find all positive integers n such that $\varphi(n) = 4$.
5. Compute $5^{1434} \bmod 307$.
6. Compute $25^{1434} \bmod 309$.
7. What is the last digit if we compute the number 1234^{5678}?
8. Find the last two digits of the number 123^{45678}.
9. Solve the congruence $x^{39} \equiv 5 \pmod{121}$.
10. Investigate true or false.
    a) $2^{6600} \equiv 1 \pmod{6601}$ hence the number 6601 must be a prime.
    b) $2^{1762} \equiv 742 \pmod{1763}$ hence 1763 cannot be a prime number.
    c) If $a \equiv b \pmod{n}$ then $a^k \equiv b^k \pmod{n}$.
    d) If $j \equiv k \pmod{n}$ then $a^j \equiv a^k \pmod{n}$.
11. Prove that Fermat's Little Theorem is equivalent to the following statement: $a^p \equiv a \pmod{p}$ for any integer a.
12. Prove that if $a^k \equiv 1 \pmod{n}$ for some $k > 0$ then gcd(a, n) = 1.
13. Another property of $\varphi(n)$ is that $\Sigma\,\varphi(d) = n$ where the sum is taken over all the positive divisors d of n. Verify this property for $n = 24$ and $n = 30$.
14. Prove that $\varphi(2n) = 2\varphi(n)$ if n is even and $\varphi(2n) = \varphi(n)$ if n is odd.
15. Prove that if $d \mid n$ then $\varphi(d) \mid \varphi(n)$.
16. Prove that $\varphi(n)$ is even for all $n > 2$.

Chapter 5
Primitive Roots

Definition: Suppose a and n are relatively prime. The **order** of a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$. We denote this quantity by $|a|_n$ or simply $|a|$ when there is no ambiguity. Note that $|a|_n \le \varphi(n)$ due to Euler's Theorem.

Example: Find $|3|_7$, $|3|_{10}$, $|7|_{24}$.

5.1 Proposition: Properties of Orders
1. If $a \equiv b \pmod{n}$ then $|a|_n = |b|_n$.
2. $a^k \equiv 1 \pmod{n}$ if and only if $|a|_n \mid k$. In particular $|a|_n \mid \varphi(n)$.
3. $a^j \equiv a^k \pmod{n}$ if and only if $j \equiv k \pmod{|a|_n}$.
4. $|a^k| = |a|$ if and only if $\gcd(k,|a|) = 1$.
5. If $\gcd(|a|,|b|) = 1$ then $|ab| = |a|\,|b|$.

Definition: If $|a|_n = \varphi(n)$ then a is called a **primitive root** modulo n. For example 3 is a primitive root modulo 7 because $|3|_7 = 6 = \varphi(7)$.

Example: Find all the primitive roots modulo 8 if any.

5.2 Proposition: Properties of Primitive Roots
1. If a is a primitive root modulo n then $\{a, a^2, a^3, ..., a^{\varphi(n)}\}$ is a reduced residue system modulo n.
2. If any exists, there are exactly $\varphi(\varphi(n))$ primitive roots modulo n.

5.3 Lemma: The number of solutions of $f(x) \equiv 0 \pmod{p}$ is at most the degree of f.

5.4 Corollary: If $d \mid p-1$ then $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

5.5 Theorem: Every prime p has exactly $\varphi(p-1)$ primitive roots.

5.6 Primitive Root Theorem: Primitive roots exist only modulo 1, 2, 4, p^k, or $2p^k$ where p is any odd prime and $k > 0$.
No Proof.

Example: Is there a primitive root modulo 4? 5? 25? 50? 100? How many?

5.7 Artin's Conjecture: The number 2 is a primitive root for infinitely many primes.

5.8 Discrete Logarithm Problem: The congruence $a^x \equiv b \pmod{p}$ with $p \nmid ab$ can be solved by rewriting the congruence in exponentiations whose base is a primitive root modulo p. This can be done according to Proposition 5.2.1. The following table gives an illustration for exponentiation base 2 as a primitive root modulo 13.

k	1	2	3	4	5	6	7	8	9	10	11	12
$2^k \bmod 13$	2	4	8	3	6	12	11	9	5	10	7	1

Example: Find the solutions using the above table.

1. $4^x \equiv 10 \pmod{13}$
2. $5^x \equiv 9 \pmod{13}$
3. $10\,(7^x) \equiv 3 \pmod{13}$
4. $5\,(8^x) \equiv 11 \pmod{13}$

Example: Find the solutions using the same technique as above.

1. $8x \equiv 5 \pmod{13}$
2. $3x \equiv 1 \pmod{13}$
3. $x^7 \equiv 12 \pmod{13}$
4. $2x^4 \equiv 5 \pmod{13}$

Problems

1. Find the order of 4 modulo 25.
2. Is 5 a primitive root modulo 29?
3. Find all the primitive roots of 9.
4. Suppose $|a| = 6$. Find $|a^k|$ for $k = 2, 3, 4, 5, 6$.
5. One of the primitive roots modulo 11 is 2. Find the rest.
6. Is there a primitive root modulo 250313?
7. How many primitive roots are there modulo 1250?
8. Find three primes modulo which 2 is not a primitive root.
9. Solve the congruence $10\,(6^x) \equiv 12 \pmod{13}$.
10. Investigate true or false.
    a) $|-a| = |a|$.
    b) If $|a|_n = |b|_n$ then $a \equiv b \pmod{n}$.
    c) If $a^j \equiv a^k \pmod{n}$ then $j \equiv k \pmod{n}$.
    d) $a^k \equiv 1 \pmod{n}$ is not possible if $\gcd(a, n) \neq 1$.
11. Prove that if $|a|_n = n - 1$ then n must be a prime.
12. Prove that modular inverses have equal orders.
13. Suppose that p is an odd prime. Prove that if a is a primitive root modulo p then $a^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$.
14. Prove that 4 is not a primitive root modulo any prime.
15. Prove that if a and b are primitive roots modulo an odd prime p then ab is not a primitive root modulo p.
16. Prove that if a is a primitive root modulo an odd prime p then $-a$ is also a primitive root modulo p if and only if $p \equiv 1 \pmod{4}$.

Chapter 6
Quadratic Residues

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 quadratic non-residue because $x^2 \equiv 7 \pmod 5$ has no solution.

Definition: Let p be an odd prime. The **Legendre symbol** $\left(\frac{a}{p}\right)$ is defined to be +1 if a is a quadratic residue modulo p, or –1 if a is a quadratic non-residue modulo p, and 0 if $p \mid a$.

6.1 Proposition: Properties of the Legendre Symbol

1. $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b \pmod p$
2. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$ **(Euler's Criterion)**
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

6.2 Corollary: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Example: Is –28 a quadratic residue modulo 5?

6.3 Gauss' Lemma: If $A = \{a, 2a, 3a, ..., \tfrac{1}{2}(p-1)a\}$ with $p \nmid a$ then $\left(\frac{a}{p}\right) = (-1)^n$ where n is the number of integers in A whose remainders mod p are larger than $p/2$.

Example: Illustrate Gauss' Lemma with $a = 5$ and $p = 11$.

6.4 Corollary: Let a be odd and $p \nmid a$.

1. $\left(\frac{a}{p}\right) = (-1)^m$ where $m = \sum_{j=1}^{\frac{1}{2}(p-1)} \left[\frac{ja}{p}\right]$ **(Eisenstein's Lemma)**
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Example: Illustrate Eisenstein's Lemma with $a = 5$ and $p = 11$.

6.5 The Law of Quadratic Reciprocity: If p and q are distinct odd primes then

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

i.e. $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if p or $q \equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ if $p \equiv q \equiv 3 \pmod 4$.

Example: Is 816 a quadratic residue modulo 239?

Definition: Let $P = p_1 p_2 \ldots p_k$ be the product of odd prime numbers, not necessarily distinct. Define the **Jacobi symbol** $\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$ and also $\left(\frac{a}{1}\right) = 1$.

Note that if gcd(a, P) = 1 then $\left(\frac{a}{P}\right) = \pm 1$ or else $\left(\frac{a}{P}\right) = 0$.

6.6 Proposition: Properties of the Jacobi Symbol

1. $\left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$ if $a \equiv b \pmod P$
2. $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$
3. $\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right)\left(\frac{a}{Q}\right)$

6.7 Generalized Law of Quadratic Reciprocity: For odd numbers P, $Q > 0$:

1. $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$
2. $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$
3. $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{(\frac{P-1}{2})(\frac{Q-1}{2})}$

Example: Evaluate $\left(\frac{-42}{61}\right)$.

6.8 Modular Square Root: If a is a quadratic residue modulo $p \equiv 3 \pmod 4$ then the congruence $x^2 \equiv a \pmod p$ has exactly two solutions given by $x \equiv \pm a^{\frac{1}{4}(p+1)} \pmod p$.

Example: Find all solutions.

1. $x^2 \equiv 2 \pmod{23}$
2. $x^2 - 2x + 3 \equiv 0 \pmod{11}$
3. $x^2 \equiv 10 \pmod{21}$
4. $x^2 \equiv 31 \pmod{55}$

Problems

1. Find all the quadratic residues and non-residues modulo 11.
2. Evaluate the Legendre symbol $\left(\frac{7}{11}\right)$ using (a) Euler's Criterion (b) Gauss'

Lemma (c) Eisenstein's Lemma (d) Quadratic Reciprocity Law.

3. Does the congruence $x^2 \equiv 186 \pmod{557}$ have a solution?
4. Does the congruence $x^2 - 6x \equiv (2 \bmod 79)$ have a solution?
5. Does the congruence $x^2 - 5x + 2 \equiv 0 \pmod{29}$ have a solution?
6. Evaluate the Jacobi symbol $\left(\frac{218}{385}\right)$.
7. Characterize the prime numbers modulo which 5 is a quadratic residue.
8. Find all solutions of the congruence $x^2 \equiv 8 \pmod{31}$.
9. Find all solutions of the congruence $2x^2 + x + 2 \equiv 0 \pmod{31}$.
10. Find all solutions of the congruence $x^2 \equiv 29 \pmod{35}$.
11. Investigate true or false.

    a) $\left(\frac{713}{1009}\right) = +1$ hence $x^2 \equiv 713 \pmod{1009}$ has a solution.

    b) $\left(\frac{2}{15}\right) = +1$ so the congruence $x^2 \equiv 2 \pmod{15}$ has a solution.

    c) $\left(\frac{7}{15}\right) = -1$ so the congruence $x^2 \equiv 7 \pmod{15}$ has no solution.

12. Suppose that a is relatively prime to an odd prime p. Prove that the congruence $x^2 \equiv a \pmod{p}$ has either exactly two solutions or none.
13. Prove that –1 is a square modulo an odd prime p if and only if $p \equiv 1 \pmod{4}$.
14. Prove that 2 is a square modulo an odd prime p if and only if $p \equiv \pm 1 \pmod{8}$.
15. Prove that –2 is a square modulo an odd prime p if and only if either $p \equiv 1 \pmod{8}$ or $p \equiv 3 \pmod{8}$.
16. Prove that –3 is a square modulo an odd prime p if and only if $p \equiv 1 \pmod{6}$.

Appendix 1

Primes < 4,000

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
877	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	1051	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
1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053
2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
2221	2237	2239	2243	2251	2267	2269	2273	2281	2287
2293	2297	2309	2311	2333	2339	2341	2347	2351	2357
2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531
2539	2543	2549	2551	2557	2579	2591	2593	2609	2617
2621	2633	2647	2657	2659	2663	2671	2677	2683	2687
2689	2693	2699	2707	2711	2713	2719	2729	2731	2741
2749	2753	2767	2777	2789	2791	2797	2801	2803	2819
2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
2909	2917	2927	2939	2953	2957	2963	2969	2971	2999
3001	3011	3019	3023	3037	3041	3049	3061	3067	3079
3083	3089	3109	3119	3121	3137	3163	3167	3169	3181
3187	3191	3203	3209	3217	3221	3229	3251	3253	3257
3259	3271	3299	3301	3307	3313	3319	3323	3329	3331
3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491	3499	3511
3517	3527	3529	3533	3539	3541	3547	3557	3559	3571
3581	3583	3593	3607	3613	3617	3623	3631	3637	3643
3659	3671	3673	3677	3691	3697	3701	3709	3719	3727
3733	3739	3761	3767	3769	3779	3793	3797	3803	3821
3823	3833	3847	3851	3853	3863	3877	3881	3889	3907
3911	3917	3919	3923	3929	3931	3943	3947	3967	3989

Appendix 2
Hints and Answers

	Chapter 1	Chapter 2	Chapter 3	Chapter 4	Chapter 5	Chapter 6
1	No	7 x 35759	1, 3, 5, 7, 9, 11, 13, 15, 17	1, 5, 7, 11, 13, 17, 19, 23	10	1, 3, 4, 5, 9 & 2, 6, 7, 8, 10
2	111 mod 24	18 total	2, 3, 5, 11, 19	1, 7, 11, 13, 17, 19, 23, 29	No	–1
3	1, 5, 7, 11	120	x ≡ 6 (mod 9)	214548	2 & 5	No
4	3	8 pairs total	7	5, 8, 10, 12	3, 2, 3, 6, 1	Yes
5	(–21, 13)	2, 5, 17, 37	1, 5, 7, 11	70	2^3, 2^7, 2^9	No
6	(3 – 13k, 3 + 5k)	3 + 2003, etc.	1002	34	No	–1
7	7 minutes & 3 minutes	3, 7, 31, 127, 8191	1537 (mod 3960)	6	200	p ≡ ±1 (mod 5)
8	F F T F T	3, 5, 17, 257, 65537	2.62 dinars	69	7, 17, 31	15 & 16
9	T T T F	≈ 7.8 x 10^4	T T T	75	x ≡ 4 (mod 12)	22 & 24
10	Use 1.7.2	≈ 4.0 x 10^8	Use 3.7	F T T F	F F F T	8, 13, 22, 27
11	Start: either n is even or odd	F F T T	Use 3.7 & find inverse	Use 3.1.4	Use 4.7 & 5.1.2	T F T
12	Start: either n is even or odd	lcm(m,n) x gcd(m,n) = mn	Start: a ≡ 1, 3, 5, or 7 (mod 8)	Use 3.3	Show that (a^–1)^k = (a^k)^–1	Use Problem 3.14
13	Start: n = 2k + 1	Use 2.3	Start: p = 3k + 1	Check	Use 3.6 & 4.3	Use 6.2
14	3 | one of these: (n–1) n (n+1)	Use 2.4	Like 3.6	Use 4.6 & 4.7	4 = 2^2 & use Problem 13	Use 6.4.2
15	Use Problems 13 & 14	3, 5, 7	See Problem 2.12	Use 4.7.3	Use Problem 13	Use Problems 13 & 14
16	Start: (n–2) (n–1) n (n+1) (n+2)	Like 2.6 with 6 P2P3 ... Pm + 5	Show that (n–1)! ≡ 0 (mod n)	Use Problem 15	Use Problem 13	Use 6.2 & 6.5