Number Theory Summary

Mathematical Notes

October 27, 2025

Contents

1 Divisibility and Primes **3**
- 1.1 Basic Definitions . . . 3
- 1.2 Division Algorithm . . . 3
- 1.3 Greatest Common Divisor . . . 3
- 1.4 Extended Euclidean Algorithm . . . 3
- 1.5 Least Common Multiple . . . 3

2 Fundamental Theorem of Arithmetic **4**
- 2.1 Prime Factorization . . . 4
- 2.2 Prime Counting Function . . . 4
- 2.3 Sieve of Eratosthenes . . . 4

3 Congruences **4**
- 3.1 Basic Properties . . . 4
- 3.2 Linear Congruences . . . 5
- 3.3 Chinese Remainder Theorem . . . 5

4 Fermat's Little Theorem and Euler's Theorem **5**
- 4.1 Fermat's Little Theorem . . . 5
- 4.2 Euler's Totient Function . . . 5
- 4.3 Euler's Theorem . . . 5

5 Quadratic Residues **6**
- 5.1 Definition and Basic Properties . . . 6
- 5.2 Quadratic Reciprocity . . . 6

6 Diophantine Equations **6**
- 6.1 Linear Diophantine Equations . . . 6
- 6.2 Pythagorean Triples . . . 6
- 6.3 Fermat's Last Theorem . . . 6

7 Continued Fractions **7**
- 7.1 Definition . . . 7
- 7.2 Convergents . . . 7

8 Arithmetic Functions **7**
8.1 Multiplicative Functions . . . 7
8.2 Important Arithmetic Functions . . . 7
8.3 Möbius Inversion Formula . . . 7

9 Primitive Roots **8**
9.1 Definition . . . 8
9.2 Discrete Logarithm . . . 8

10 Applications **8**
10.1 Cryptography . . . 8
10.2 Error Detection and Correction . . . 8
10.3 Computer Science . . . 8

11 Analytic Number Theory **8**
11.1 Riemann Zeta Function . . . 8
11.2 Riemann Hypothesis . . . 9

12 Algebraic Number Theory **9**
12.1 Algebraic Integers . . . 9
12.2 Quadratic Fields . . . 9
12.3 Ideal Theory . . . 9

13 Important Algorithms **9**
13.1 Fast Exponentiation . . . 9
13.2 Miller-Rabin Primality Test . . . 9
13.3 Pollard's Rho Algorithm . . . 9

14 Key Theorems **9**
14.1 Wilson's Theorem . . . 9
14.2 Lucas's Theorem . . . 10
14.3 Thue's Theorem . . . 10

15 Open Problems **10**
15.1 Goldbach's Conjecture . . . 10
15.2 Twin Prime Conjecture . . . 10
15.3 Perfect Numbers . . . 10

16 Important Constants **10**

1 Divisibility and Primes

1.1 Basic Definitions

Definition 1.1. For integers a and b with $b \neq 0$, we say b **divides** a (written $b \mid a$) if there exists an integer c such that $a = bc$.

Definition 1.2. A **prime number** is a positive integer $p > 1$ whose only positive divisors are 1 and p.

Definition 1.3. A **composite number** is a positive integer $n > 1$ that is not prime.

1.2 Division Algorithm

Theorem 1.1 (Division Algorithm)**.** For any integers a and b with $b > 0$, there exist unique integers q and r such that:

$$a = bq + r \quad \text{where} \quad 0 \leq r < b$$

1.3 Greatest Common Divisor

Definition 1.4. The **greatest common divisor** of integers a and b (not both zero) is the largest positive integer d such that $d \mid a$ and $d \mid b$. We write $\gcd(a, b) = d$.

Theorem 1.2 (Euclidean Algorithm)**.** To find $\gcd(a, b)$ where $a > b > 0$:

1. Apply the division algorithm: $a = bq_1 + r_1$ where $0 \leq r_1 < b$
2. If $r_1 = 0$, then $\gcd(a, b) = b$
3. Otherwise, apply the division algorithm to b and r_1: $b = r_1 q_2 + r_2$
4. Continue until $r_n = 0$. Then $\gcd(a, b) = r_{n-1}$

1.4 Extended Euclidean Algorithm

Theorem 1.3 (Bézout's Identity)**.** For any integers a and b (not both zero), there exist integers x and y such that:

$$\gcd(a, b) = ax + by$$

1.5 Least Common Multiple

Definition 1.5. The **least common multiple** of positive integers a and b is the smallest positive integer m such that $a \mid m$ and $b \mid m$. We write $\text{lcm}(a, b) = m$.

Theorem 1.4. For positive integers a and b:

$$\gcd(a, b) \cdot \text{lcm}(a, b) = ab$$

2 Fundamental Theorem of Arithmetic

2.1 Prime Factorization

Theorem 2.1 (Fundamental Theorem of Arithmetic)**.** Every positive integer $n > 1$ can be written uniquely as a product of primes:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

where $p_1 < p_2 < \cdots < p_k$ are primes and $a_1, a_2, \ldots, a_k$ are positive integers.

2.2 Prime Counting Function

Definition 2.1. The **prime counting function** $\pi(x)$ counts the number of primes less than or equal to x.

Theorem 2.2 (Prime Number Theorem)**.**

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

2.3 Sieve of Eratosthenes

Definition 2.2. The **Sieve of Eratosthenes** is an algorithm to find all primes up to a given limit n:

1. List all integers from 2 to n
2. Start with the first number $p = 2$
3. Cross out all multiples of p greater than p
4. Find the next uncrossed number and repeat
5. Continue until $p^2 > n$

3 Congruences

3.1 Basic Properties

Definition 3.1. For integers a, b, and positive integer m, we say a is **congruent** to b modulo m (written $a \equiv b \pmod{m}$) if $m \mid (a - b)$.

Theorem 3.1 (Properties of Congruences)**.** For integers a, b, c, d and positive integer m:

1. $a \equiv a \pmod{m}$ (reflexive)
2. If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$ (symmetric)
3. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$ (transitive)
4. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$
5. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$

3.2 Linear Congruences

Theorem 3.2. The linear congruence $ax \equiv b \pmod{m}$ has a solution if and only if $\gcd(a, m) \mid b$. If $\gcd(a, m) = d$ and $d \mid b$, then there are exactly d solutions modulo m.

3.3 Chinese Remainder Theorem

Theorem 3.3 (Chinese Remainder Theorem)**.** Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime positive integers, and let $a_1, a_2, \ldots, a_k$ be integers. Then the system of congruences:

$$x \equiv a_1 \pmod{m_1} \tag{1}$$
$$x \equiv a_2 \pmod{m_2} \tag{2}$$
$$\vdots \tag{3}$$
$$x \equiv a_k \pmod{m_k} \tag{4}$$

has a unique solution modulo $m_1 m_2 \cdots m_k$.

4 Fermat's Little Theorem and Euler's Theorem

4.1 Fermat's Little Theorem

Theorem 4.1 (Fermat's Little Theorem)**.** If p is prime and $\gcd(a, p) = 1$, then:

$$a^{p-1} \equiv 1 \pmod{p}$$

4.2 Euler's Totient Function

Definition 4.1. Euler's **totient function** $\phi(n)$ counts the number of positive integers less than or equal to n that are relatively prime to n.

Theorem 4.2. For a prime p and positive integer k:

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

Theorem 4.3. For relatively prime positive integers m and n:

$$\phi(mn) = \phi(m)\phi(n)$$

Theorem 4.4. For $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$:

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

4.3 Euler's Theorem

Theorem 4.5 (Euler's Theorem)**.** If $\gcd(a, n) = 1$, then:

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

5 Quadratic Residues

5.1 Definition and Basic Properties

Definition 5.1. An integer a is a **quadratic residue** modulo m if there exists an integer x such that $x^2 \equiv a \pmod{m}$.

Definition 5.2. The **Legendre symbol** $\left(\frac{a}{p}\right)$ for odd prime p and integer a is defined as:

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

5.2 Quadratic Reciprocity

Theorem 5.1 (Law of Quadratic Reciprocity)**.** For distinct odd primes p and q:

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

Theorem 5.2 (Supplemental Laws)**.** For odd prime p:

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

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

6 Diophantine Equations

6.1 Linear Diophantine Equations

Definition 6.1. A **linear Diophantine equation** in two variables is an equation of the form $ax + by = c$ where a, b, and c are integers.

Theorem 6.1. The equation $ax + by = c$ has integer solutions if and only if $\gcd(a, b) \mid c$.

6.2 Pythagorean Triples

Definition 6.2. A **Pythagorean triple** is a set of three positive integers (a, b, c) such that $a^2+b^2 = c^2$.

Theorem 6.2. All primitive Pythagorean triples (a, b, c) with a odd are given by:

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2$$

where $m > n > 0$ are relatively prime integers of opposite parity.

6.3 Fermat's Last Theorem

Theorem 6.3 (Fermat's Last Theorem)**.** For $n > 2$, the equation $x^n + y^n = z^n$ has no positive integer solutions.

7 Continued Fractions

7.1 Definition

Definition 7.1. A **continued fraction** is an expression of the form:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

where a_0 is an integer and $a_1, a_2, a_3, \ldots$ are positive integers.

7.2 Convergents

Definition 7.2. The n-th **convergent** of a continued fraction is the rational number obtained by truncating the continued fraction after n terms.

Theorem 7.1. The convergents of a continued fraction provide the best rational approximations to the value of the continued fraction.

8 Arithmetic Functions

8.1 Multiplicative Functions

Definition 8.1. An arithmetic function f is **multiplicative** if $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$.

Definition 8.2. An arithmetic function f is **completely multiplicative** if $f(mn) = f(m)f(n)$ for all positive integers m and n.

8.2 Important Arithmetic Functions

- **Divisor function**: $\tau(n) = \sum_{d|n} 1$ (number of divisors)
- **Sum of divisors**: $\sigma(n) = \sum_{d|n} d$
- **Möbius function**: $\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^k & \text{if } n \text{ is square-free with } k \text{ prime factors} \\ 0 & \text{if } n \text{ has a squared prime factor} \end{cases}$
- **Euler's totient function**: $\phi(n)$

8.3 Möbius Inversion Formula

Theorem 8.1 (Möbius Inversion Formula)**.** If f and g are arithmetic functions such that:

$$g(n) = \sum_{d|n} f(d)$$

then:

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$$

9 Primitive Roots

9.1 Definition

Definition 9.1. A **primitive root** modulo n is an integer g such that the powers of g generate all integers relatively prime to n modulo n.

Theorem 9.1. A positive integer n has a primitive root if and only if $n = 2$, $n = 4$, $n = p^k$, or $n = 2p^k$ where p is an odd prime and k is a positive integer.

9.2 Discrete Logarithm

Definition 9.2. If g is a primitive root modulo n and $\gcd(a, n) = 1$, then the **discrete logarithm** of a to the base g modulo n is the smallest positive integer k such that $g^k \equiv a \pmod{n}$.

10 Applications

10.1 Cryptography

- **RSA encryption**: Based on the difficulty of factoring large integers
- **Diffie-Hellman key exchange**: Uses discrete logarithms
- **Elliptic curve cryptography**: Uses elliptic curves over finite fields

10.2 Error Detection and Correction

- **Check digits**: Using modular arithmetic for error detection
- **ISBN codes**: Weighted checksums modulo 11
- **Credit card numbers**: Luhn algorithm

10.3 Computer Science

- **Hashing**: Using modular arithmetic for hash functions
- **Random number generation**: Linear congruential generators
- **Fast exponentiation**: Modular exponentiation algorithms

11 Analytic Number Theory

11.1 Riemann Zeta Function

Definition 11.1. The **Riemann zeta function** is defined as:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

for $\text{Re}(s) > 1$.

Theorem 11.1 (Euler Product)**.** For $\text{Re}(s) > 1$:

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

11.2 Riemann Hypothesis

Conjecture 11.1 (Riemann Hypothesis)**.** All non-trivial zeros of the Riemann zeta function have real part equal to $\frac{1}{2}$.

12 Algebraic Number Theory

12.1 Algebraic Integers

Definition 12.1. An **algebraic integer** is a complex number that is a root of a monic polynomial with integer coefficients.

12.2 Quadratic Fields

Definition 12.2. A **quadratic field** is $\mathbb{Q}(\sqrt{d})$ where d is a square-free integer.

12.3 Ideal Theory

Definition 12.3. An **ideal** in a ring R is a subset I such that:

1. $0 \in I$
2. If $a, b \in I$, then $a + b \in I$
3. If $a \in I$ and $r \in R$, then $ra \in I$

13 Important Algorithms

13.1 Fast Exponentiation

Theorem 13.1 (Binary Exponentiation)**.** To compute $a^n \bmod m$:

1. Write n in binary: $n = \sum_{i=0}^{k} b_i 2^i$
2. Compute $a^{2^i} \bmod m$ for $i = 0, 1, \ldots, k$
3. Multiply the appropriate powers: $a^n \equiv \prod_{i=0}^{k} a^{b_i 2^i} \pmod{m}$

13.2 Miller-Rabin Primality Test

Theorem 13.2. The Miller-Rabin test is a probabilistic algorithm to test if a number is prime.

13.3 Pollard's Rho Algorithm

Theorem 13.3. Pollard's rho algorithm is used to find non-trivial factors of composite numbers.

14 Key Theorems

14.1 Wilson's Theorem

Theorem 14.1 (Wilson's Theorem)**.** A positive integer $p > 1$ is prime if and only if:

$$(p-1)! \equiv -1 \pmod{p}$$

14.2 Lucas's Theorem

Theorem 14.2 (Lucas's Theorem)**.** For prime p and integers m and n:

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}$$

where m_i and n_i are the digits of m and n in base p.

14.3 Thue's Theorem

Theorem 14.3 (Thue's Theorem)**.** For any integer $a > 1$ and any positive integer n, there exist integers x and y such that $0 < |x|, |y| \leq \sqrt{n}$ and $ax \equiv y \pmod{n}$.

15 Open Problems

15.1 Goldbach's Conjecture

Conjecture 15.1 (Goldbach's Conjecture)**.** Every even integer greater than 2 can be expressed as the sum of two primes.

15.2 Twin Prime Conjecture

Conjecture 15.2 (Twin Prime Conjecture)**.** There are infinitely many pairs of primes that differ by 2.

15.3 Perfect Numbers

Conjecture 15.3. All even perfect numbers are of the form $2^{p-1}(2^p - 1)$ where $2^p - 1$ is prime (Mersenne prime).

16 Important Constants

- **Euler's constant**: $\gamma \approx 0.5772$
- **Golden ratio**: $\phi = \frac{1+\sqrt{5}}{2} \approx 1.6180$
- **Natural logarithm base**: $e \approx 2.7183$
- **Pi**: $\pi \approx 3.1416$
- **Square root of 2**: $\sqrt{2} \approx 1.4142$