AS.110.304: Elem. Number Theory

Theorems and Definitions

James Guo (sguo45)

May 4, 2023

Contents

1 Mathematical Induction

1.1 Princ.: Principle of Mathematical Induction

To show a statement $P(n)$ about $n \in \mathbb{Z}_{>0}$ is true for all $n \in \mathbb{Z}_{>0}$, it's suffices to show that:

1. Base case: $P(1)$ is true;
2. Inductive case: For any $k \in \mathbb{Z}_{>0}$, if $P(k)$ is true, then $P(k+1)$ is true.

1.2 Princ.: Well-Ordering Principle

Any non-empty set of positive integers has the least element.
Rmk.: This is equivalent to the principle of mathematical induction.

2 Euclid's Division Lemma

2.1 Thm.: Euclid's Division Lemma

Let $a, b \in \mathbb{Z}$ and $b > 0$. There exist unique integers q and r such that $0 \leq r < b$ and $a = qb + r$.

3 Divisibility

3.1 Defn.: Divisibility

Let $a, b \in \mathbb{Z}$. We say b divides a, or b is a divisor of a, or a is a multiple of b, if there exists an integer q such that $a = qb$.
If b divides a, we write $b|a$. If b does not divide a, we write $b \nmid a$.
Rmk.: By definition, b can be 0, where 0 only divides 0.

3.2 Thm.: Linear Combinations of Multiples are Multiples

Let $a, b, c \in \mathbb{Z}$. If $a|b$ and $a|c$, then $a|(mb + nc)$ for all integral m and n.

3.3 Defn.: Greatest Common Divisor

The greatest common divisor of two integers a and b, not both zero, is the largest positive integer that divides both a and b, denotes $\gcd(a, b)$.
Rmk.: If a, and b are integers, not both zero, then $\gcd(a, b)$ always exists and is unique.
Rmk.: $\gcd(\pm a, \pm b) = \gcd(\pm a, \mp b)$.

3.4 Mthd.: Euclidean Algorithm

If $a = qb + r$ where $a, b, q, r \in \mathbb{Z}$ and $b \neq 0$, then $\gcd(a, b) = \gcd(b, r)$.
In Euclidean Algorithm, write $a = r_1$ as $a_i = qb + r_{i+1}$ until we finish $r_n = 0$ while r_{n-1} is $\gcd(a, b)$.

3.5 Thm.: Integral Solutions to Linear Equations

Let $a, b, c \in \mathbb{Z}$. Suppose that a and b are not both zero. There exists integers x and y such that $ax + by = c$ if and only if $\gcd(a, b)|c$.

3.6 Defn.: Prime

A positive integer $p \neq 1$ is said to be prime if its only positive divisors are 1 and p.

3.7 Defn.: Co-prime

Two integers are said to be co-prime (or relatively prime) if their only positive common divisor (equivalent to the greatest common divisor when the integers are not both 0) is 1.

3.8 Thm.: Divisibility of Composite Numbers

Let $a, b, c \in \mathbb{Z}$. If $\gcd(a, c) = 1$ and $a|(bc)$, then $a|b$.
Cor.: Let $a, b \in \mathbb{Z}$ and p be prime. If $p|(ab)$ and $p \nmid a$, then $p|b$.
Cor.: Let $a_1, a_2, \cdots, a_n$ be integers. Let p be a prime. If $p|(a_1 a_2 \cdots a_n)$, then there exists some $1 \leq i \leq n$ such that $p|a_i$.

4 Linear Diophantine Equations

4.1 Thm.: Solutions to Linear Diophantine Equations

If $\gcd(a, b) = 1$ and (x_0, y_0) is a solution to $ax + by = c$ is $\{(x, y) | x = x_0 + bt, y = y_0 - at, t \in \mathbb{Z}\}$.

4.2 Mthd.: Solving Linear Diophantine Equations

To solve the equation $ax + by = c$ where $a, b, c \in \mathbb{Z}$ for $a, b \neq 0$.

1. Reduce to the case where $\gcd(a, b) = 1$;
2. Find a solution (x_0, y_0) by Euclidean Algorithm;
3. Find all integral solutions with form $\begin{cases} x = x_0 + bt \\ y = y_0 - at \end{cases}$ where $t \in \mathbb{Z}$.

5 Fundamental Theorem of Arithmetic

5.1 Princ.: Principle of Strong Induction

Let $P(n)$ be a statement about positive integer n. To show that $P(k)$ is true for all $n \in \mathbb{Z}_{>0}$, it suffices to show the following statements:

1. $P(1)$ is true;
2. For any $n \in \mathbb{Z}_{>0}$, if $P(k)$ is true for all positive integers $k < n$, then $P(n)$ is true.

5.2 Thm.: Fundamental Theorem of Arithmetic

For each integer $n > 1$, there exist primes $p_1 < p_2 < \cdots < p_r$ and positive integer n_i, $1 \le i \le k$ such that $n = \prod_{i=1}^{k} p_i^{n_i}$ call a prime factorization, and this factorization is unique.

6 Permutations and Combinations

6.1 Defn.: Permutation

An r-permutation of a set S of n elements is an ordered selection of r elements from S $(0 \le r \le n)$.

6.2 Thm.: Calculation of Permutation

The number of r-permutations of a set of n elements, denotes by ${}_nP_r$, is ${}_nP_r = n(n-1)\cdots(n-r+1) = \dfrac{n!}{(n-r)!}$.

6.3 Defn.: Combination

An r-combination of a set S of n elements in a subset of S having r elements $(0 \le r \le n)$.

6.4 Thm.: Calculation of Combination

The number of r-combinations of a set of n elements, denotes by $\binom{n}{r}$, is $\dbinom{n}{r} = \dfrac{{}_nP_r}{{}_rP_r} = \dfrac{n(n-1)\cdots(n-r+1)}{r!} = \dfrac{n!}{(n-r)!r!}$.
Cor.: The product of any n consecutive positive integers is divisible by $n!$, i.e., $n!|N(N-1)\cdots(N-n+1)$ because $\dfrac{N(N-1)\cdots(N-n+1)}{n!} = \dbinom{N}{n} \in \mathbb{Z}$.

7 Congruence

7.1 Defn.: Congruence

Let $a, b, n \in \mathbb{Z}$. a is congruent to b modulo n, denotes $a \equiv b (\bmod n)$ if $n|(a-b)$.
Remark: n can be zero by our definition.

7.2 Thm.: Properties of Congruence

Let $a, b, c, n \in \mathbb{Z}$:

1. Reflexive: $a \equiv a (\bmod n)$;
2. Symmetric: If $a \equiv b (\bmod n)$, then $b \equiv a (\bmod n)$;
3. Transitive: If $a \equiv b (\bmod n)$ and $b \equiv c (\bmod n)$, then $a \equiv c (\bmod n)$.

Rmk.: In other words, Congruence modulo is an equivalence relation.

7.3 Thm.: Ring Structure of Congruence

Let $a_1, a_2, b_1, b_2, n \in \mathbb{Z}$ such that $a_1 \equiv a_2 (\bmod n)$ and $b_1 \equiv b_2 (\bmod n)$. Then:

1. Addition: $a_1 + b_1 \equiv b_1 + b_2 (\bmod n)$;
2. Subtraction: $a_1 - b_1 \equiv a_2 - b_2 (\bmod n)$;
3. Multiplication: $a_1 b_1 \equiv a_2 b_2 (\bmod n)$.

Rmk.: Division does not necessarily preserve the congruence.

8 Residue Systems

8.1 Defn.: Residue

If $a, b, m \in \mathbb{Z}$ and $a \equiv b (\bmod m)$, b is a residue of a modulo m.
Rmk.:: b may not satisfy $0 \leq b < m - 1$ by definition.

8.2 Defn.: Complete Residue System

A set of integers $\{r_1, r_2, \cdots, r_n\}$ is called a complete residue system modulo m if:

1. $r_i \not\equiv r_j (\bmod m)$ whenever $i \neq j$;
2. For any $n \in \mathbb{Z}$, there exists an r_i such that $n \equiv r_i (\bmod m)$.

8.3 Thm.: A Complete Residue System

The set $\{0, 1, \cdots, m - 1\}$ is a complete residue system modulo m.

8.4 Thm.: Length of Complete Residue System

Any complete residue system of modulo m are consisted of exactly m elements.

8.5 Defn.: Reduced Residue System

A set of integers $\{r_1, r_2, \cdots, r_s\}$ is called a reduced residue system modulo m if:

1. $\gcd(r_i, m) = 1$ for all $1 \leq i \leq s$;
2. $r_i \not\equiv r_j (\bmod m)$ whenever $i \neq j$;
3. For any $n \in \mathbb{Z}$ such that $\gcd(n, m) = 1$, there exists an r_i such that $n \equiv r_i (\bmod m)$.

8.6 Thm.: A Reduced Residue System

Let S be a complete residue system modulo m. Then $\{r \in S | \gcd(r, m) = 1\}$ is a reduced residue system modulo m.

8.7 Defn.: Euler ϕ Function

The Euler ϕ function, denotes $\phi(n)$, is defined to be the cardinality of $\{n \in \mathbb{Z} | 0 \leq n \leq m-1, \gcd(n,m) = 1\}$.

8.8 Thm.: Length of Reduced Residue System

Any reduced residue system modulo m is consisted of exactly $\phi(m)$ elements.

9 Linear Congruence

9.1 Thm. Solutions to Linear Congruence

Let $a, b, c \in \mathbb{Z}$ where a and b are non-zero. Denote $d = \gcd(a, b)$. Then the congruence $ax \equiv c (\mathrm{mod}\, b)$ has a solution if and only if $d | c$.
Rmk.: If $d|c$, then $ax \equiv c (\mathrm{mod}\, b)$ has d mutually incongruent solutions modulo c.
Cor.: For $ax \equiv c (\mathrm{mod}\, b)$, if $\gcd(a,b) = 1$, then all the solutions are congruent modulo b, where the solution of $ax \equiv c (\mathrm{mod}\, b)$ is unique modulo b.

9.2 Mthd: Solving Linear Congruence

To solve the linear congruence $ax \equiv c (\mathrm{mod}\, b)$, where $a, b, c \in \mathbb{Z}$.

1. Find one solution: Use Euclidean Algorithm, find solutions using properties of congruence;
2. Find all incongruent integral solutions: Use Theory of Linear Diophantine Equations and properties of congruence;
3. Find all integral solutions: Find all the solutions.

9.3 Defn.: Inverse

If $\gcd(a, b) = 1$, the unique solution modulo b to $ax \equiv 1 (\mathrm{mod}\, b)$ is the inverse of a modulo b.

10 Theorems of Euler, Fermat, and Wilson (Leibniz)

10.1 Thm.: Euler's Theorem

Let $m \in \mathbb{Z}_{>0}$ and $a \in \mathbb{Z}$. If $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 (\mathrm{mod}\, m)$.

10.2 Thm.: Fermat's Little Theorem

If p is a prime and $a \in \mathbb{Z}$, then $a^p \equiv a (\mathrm{mod}\, p)$.

10.3 Thm.: Wilson's/Leibniz's Theorem

Let $m \in \mathbb{Z}_{>1}$. Then $(m-1)! \equiv -1 (\mathrm{mod}\, m)$ if and only if m is a prime.

11 Chinese Remainder Theorem

11.1 Thm.: Chinese Remainder Theorem

Let m_1, m_2, $\cdots$, m_s be pairwise co-prime, non-zero integers. Denote $M = \prod_{i=1}^{s} m_i$. Let a_1, a_2, $\cdots$, a_s be integers such that $\gcd(a_i, m_i) = 1$ for all $1 \leq i \leq s$. Then the system of congruences $\begin{cases} a_1 x \equiv b_1 (\bmod m_1) \\ a_2 x \equiv b_2 (\bmod m_2) \\ \vdots \\ a_s x \equiv b_s (\bmod m_s) \end{cases}$ has a simultaneous solution that is unique modulo M.

Rmk.: The Chinese Remainder Theorem is the polynomial congruences of degree 1.

11.2 Mthd.: Solving a System of Linear Congruence

Let m_1, m_2, $\cdots$, m_s be pairwise co-prime, non-zero integers. Denote $M = \prod_{i=1}^{s} m_i$. Let a_1, a_2, $\cdots$, a_s be integers such that $\gcd(a_i, m_i) = 1$ for all $1 \leq i \leq s$. Then the system of congruences $\begin{cases} a_1 x \equiv b_1 (\bmod m_1) \\ a_2 x \equiv b_2 (\bmod m_2) \\ \vdots \\ a_s x \equiv b_s (\bmod m_s) \end{cases}$ can be converted to s system of congruences, where the i-th system is: $\begin{cases} a_i x \equiv b_i (\bmod m_i) \\ a_j x \equiv 0 (\bmod m_j) \text{ for all } j \neq i \end{cases}$.

12 Polynomial Congruence

12.1 Thm. Maximum Number of Solutions for Polynomial Congruence

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ be a polynomial with integral coefficients and $a_n \neq 0$. If p is a prime such that $p \nmid a_n$, then the congruence $f(x) \equiv 0 (\bmod p)$ has at most n mutually incongruent solutions modulo p.

Rmk.: $f(x) \equiv 0 (\bmod p)$ does not always have solution when $p \nmid a_n$.

12.2 Defn.: Degree of the 0 Polynomial

The 0 polynomial is declared to have degree $-\infty$.

13 Euler's ϕ Function

13.1 *(8.7)* Defn.: Euler ϕ Function

The Euler ϕ function, denotes $\phi(n)$, is defined to be the cardinality of $\{n \in \mathbb{Z} | 0 \leq n \leq m-1, \gcd(n, m) = 1\}$.

13.2 Prep.: $\phi(p^n)$

If p is a prime and $n \in \mathbb{Z}_{\geq 1}$, then $\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.

13.3 Thm.: Sum over Euler ϕ Function of Divisors

The sum over ϕ function of positive division of n, denotes $\sum_{d|n} \phi(d)$, equals to n, i.e., $\sum_{d|n} \phi(d) = n$.

13.4 Thm.: Multiplicativity of Euler ϕ Function

Let $m, n \in \mathbb{Z}_{\geq 1}$ be co-prime. Then $\phi(mn) = \phi(m)\phi(n)$.
Cor.: Let p be a prime. Euler ϕ function of n can be written as the product of n and the product over all the one minus the inverse of prime factors of n, denotes $\prod_{p|n} \left(1 - \frac{1}{p}\right)$, i.e., $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$.

14 d and σ Function

14.1 Defn.: $d(n)$

For $n \in \mathbb{Z}_{\geq 1}$, $d(n)$ is defined as the number of positive divisors of n.

14.2 Prep.: $d(p^n)$

If p is a prime and $n \in \mathbb{Z}_{\geq 1}$, then $d(p^n) = n + 1$.

14.3 Thm. Multiplicativity of d Function

Let $m, n \in \mathbb{Z}_{\geq 1}$ be co-prime. Then $d(mn) = d(m)d(n)$.
Cor.: For $n = \prod_{i=1}^{k} p_i^{n_i}$ where p_i's are positive distinct primes and $n_i \in \mathbb{Z}_{\geq 1}$, $d(n) = \prod_{i=1}^{k} (n_i + 1)$.

14.4 Defn.: $\sigma(n)$

For $n \in \mathbb{Z}_{\geq 1}$, $\sigma(n)$ is defined as the sum of all positive divisors of n.

14.5 Prep.: $\sigma(p^n)$

If p is a prime and $n \in \mathbb{Z}_{\geq 1}$, then $\sigma(p^n) = \dfrac{p^{n+1} - 1}{p - 1}$.

14.6 Thm.: Multiplicativity of σ Function

Let $m, n \in \mathbb{Z}_{\geq 1}$ be co-prime. Then $\sigma(mn) = \sigma(m)\sigma(n)$.
Cor.: For $n = \prod_{i=1}^{k} p_i^{n_i}$ where p_i's are positive distinct primes and $n_i \in \mathbb{Z}_{\geq 1}$, $\sigma(n) = \prod_{i=1}^{k} \dfrac{p_i^{n_i+1} - 1}{p_i - 1}$.

Rmk.: For $n = \prod_{i=1}^{k} p_i^{n_i}$, m is a positive divisor of n if and only if $m = \prod_{i=1}^{k} p_i^{m_i}$ where $0 \leq m_i \leq n_i$. Therefore, $\sigma(n) = \prod_{i=1}^{k} \left(\sum_{m_i=0}^{n_i} p_i^{m_i} \right)$.

15 Multiplicative Arithmetic Function

15.1 Defn.: Arithmetic Function

An arithmetic function is a map $f \colon \mathbb{Z}_{\geq 1} \to \mathbb{C}$. An arithmetic function is multiplicative if $f(mn) = f(m) \cdot f(n)$ whenever $\gcd(m, n) = 1$.

15.2 *(13.4, 14.3, 14.6)* Prep.: Examples of Multiplicative Arithmetic Functions

$\phi(n)$, $d(n)$, and $\sigma(n)$ are multiplicative arithmetic functions.

15.3 Defn.: Möbius Function

For $n \in \mathbb{Z}_{\geq 1}$, $\mu(n) = \begin{cases} 1, \text{ if } n = 1 \\ 0, \text{ if } p^2 | n \text{ for some prime} p \\ (-1)^r, \text{ if } n = p_1 p_2 \cdots p_r \text{ where } p_i\text{'s are distinctive primes} \end{cases}$ or equivalently defined as $\mu(n) = \begin{cases} 0, \text{ if } p^2 | n \text{ for some prime } p \\ 1, \text{ if } n \text{ is square free and has an even number of prime factors} \\ -1, \text{ if } n \text{ is square free and has an odd number of prime factors} \end{cases}$.

15.4 Thm.: Multiplicativity of Möbius Function

$\mu(n)$ is a multiplicative arithmetic function.

16 Möbius Inversion Formula

16.1 Thm. Sum of Möbius Function of Divisors

For $n \in \mathbb{Z}_{\geq 1}$, $\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } n > 1 \end{cases}$.

16.2 Thm.: Möbius Inversion Formula

Let $f(n)$ and $g(n)$ be arithmetic functions. The following conditions are equivalent:

1. $f(n) = \sum_{d|n} g(d)$ for all n;
2. $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$ for all n.

16.3 Defn.: Möbius Pair

If two arithmetic functions $f(n)$ and $g(n)$ satisfy one of the condition that:

1. $f(n) = \sum_{d|n} g(d)$ for all n;
2. $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$ for all n.

Then, $(f(n), g(n))$ is a Möbius pair. **Rmk.**: If $(f(n), g(n))$ is a Möbius pair, $(g(n), f(n))$ is not necessarily a Möbius pair.
E.g.: $(n, \phi(n))$, $(d(n), 1)$, and $(\sigma(n), n)$ are Möbius pairs.

16.4 Thm.: Equivalence in Multiplicativity

Let $(f(n), g(n))$ be a Möbius pair of arithmetic functions. Then $f(n)$ is multiplicative if and only if $g(n)$ is multiplicative.

17 Primitive Roots

17.1 Defn.: Order

Let $m \in \mathbb{Z}_{>0}$, $a \in \mathbb{Z}$. Suppose $\gcd(a, m) = 1$. The multiplicative order of a modulo m is the smallest positive integer d such that $a^d \equiv 1 (\operatorname{mod} m)$.
Rmk.: The smallest of such a d exists and $d \leq \phi(m)$ by Euler Theorem.

17.2 Thm. Divisibility of Order

If d is the order of a modulo m, and $a^n \equiv 1 (\operatorname{mod} m)$ for some $n \in \mathbb{Z}_{\geq 0}$, then $d|n$.

17.3 Defn.: Primitive Roots

If $\phi(n)$ is the order of a modulo m, then a is a primitive root modulo m.
Rmk.: A primitive root may not exist.

17.4 Thm.: Reduced Residue System from Primitive Root

If a is a primitive root modulo m, then $a, a^2, \cdots, a^{\phi(m)}$ form a reduced residue system modulo m.

17.5 Thm.: Order of the Powers

If d is the order of a modulo m and n is a positive integer such that $\gcd(n, d) = e$, then $\frac{d}{e}$ is the order of a^n modulo m.
Cor.: If a is a primitive root modulo m, then a^n is a primitive root modulo m if and only if $\gcd(n, \phi(m)) = 1$.
Cor.: If there exists a primitive root modulo m, then there are exactly $\phi(\phi(m))$ mutually incongruent primitive roots modulo m.

17.6 Thm.: Primes have Primitive Root

If p is a prime, there exists a primitive root modulo p.

18 Asymptotic Distribution of Primes

18.1 Defn.: $\pi(x)$

For $x \in \mathbb{R}_{>0}$, denote by $\pi(x)$ the number of primes less than or equal to x.

18.2 Thm.: Euclid's Theorem

There are infinitely many primes, i.e., $\lim_{x\to\infty} \pi(x) = \infty$.
Rmk.: For $x \in \mathbb{R}_{>0}$, $\pi(x) \leq [x] \leq x$.

18.3 Thm.: Prime Number Theorem

For $x \in \mathbb{R}_{>0}$, $\lim_{x\to\infty} \dfrac{\pi(x)}{x/\log x} = 1$.

18.4 Tchebychev's Theorem

There exists $c_1, c_2 > 0$ such that $c_1 \dfrac{x}{\log x} < \pi(x) < c_2 \dfrac{x}{\log x}$ for all $x \geq 2$.

18.5 Thm.: Weaker Results of Prime Number Theorem

For any $k \in \mathbb{Z}_{>0}$, $\dfrac{\pi(x)}{x} \leq \dfrac{\phi(k)}{k} + \dfrac{k}{x}$.
If $M \in \mathbb{Z}_{>1}$ and $p_1, p_2, \cdots, p_s$ are all primes in $\{1, 2, \cdots, M\}$, then $\displaystyle\sum_{n=1}^{M} \frac{1}{n} < \frac{1}{\prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right)}$.

Cor.: Suppose $p_1 < p_2 < \cdots$ are all the prime numbers. Then $\displaystyle\sum_{i=1}^{\infty} \frac{1}{p_i} = \infty$.

$\lim_{x\to\infty} \dfrac{\pi(x)}{x} = 0$.

19 Quadratic Residue and Euler's Criterion

19.1 Defn.: Quadratic Residue

Let p be a prime and $a \in \mathbb{Z}$. If $p \nmid a$ and $x^2 \equiv a (\operatorname{mod} p)$ has a solution, then a is a quadratic residue modulo p.

19.2 Thm.: Quadratic Residue and Primitive Root

Let p be an odd prime and $a \in \mathbb{Z}$ such that $p \nmid a$. Let g be a primitive root modulo p. Let $r \in \mathbb{Z}$ be such that $g^r \equiv a (\operatorname{mod} p)$. Then a is a quadratic residue modulo p if and only if r is even.

19.3 Euler's Criterion

Let p be an odd prime, and $a \in \mathbb{Z}$, then a is a quadratic residue modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

20 Legendre Symbol

20.1 Defn.: Legendre Symbol

Let p be an odd prime and $a \in \mathbb{Z}$. The Legendre symbol of a over p, denotes $\left(\frac{a}{p}\right)$, is defined to be

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

20.2 Thm.: Properties of Legendre Symbol

Let p be an odd prime, the follow properties are ture:

1. If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;
3. $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

20.3 Defn.: Jacobi Symbol

If $m = p_1 p_2 \cdots p_r$ where p_i are odd primes (not necessarily distinct), then $\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)\left(\frac{n}{p_2}\right)\cdots\left(\frac{n}{p_r}\right)$.

21 Quadratic Reciprocity Law

21.1 Thm.: Gaussian's Lemma

Let p be an odd prime and $a \in \mathbb{Z}$ such that $p \nmid a$. For $n \in \mathbb{Z}$ define the least residue of n modulo p (denoted by $r(n)$) to be the unique integer $x \in \left(-\frac{p}{2}, \frac{p}{2}\right]$ such that $n \equiv x \pmod{p}$. Let m be the number of integers in $\{a, 2a, \cdots, \frac{p-1}{2}a\}$ whose least modulo p are negative. Then $\left(\frac{a}{p}\right) = (-1)^m$.

Cor.: If p is an odd prime, then $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Cor.: If p is an odd prime, then $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

21.2 Thm.: Quadratic Reciprocity Law

If p and q are distinct odd primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$.

Rmk.: $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ only if $p \equiv q \equiv 3 \pmod 4$, and $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ otherwise.

21.3 Thm.: Existence of Quadratic Residue

Let p be an odd prime and $a \in \mathbb{Z}$ such that $p \nmid a$. Let $n \in \mathbb{Z}_{>0}$, then the Congruence $x^2 \equiv a \pmod{p^n}$ has a solution if and only if $\left(\frac{a}{p}\right) = 1$.

22 Sum of Two Squares

22.1 Fermat's Theorem on Sum of Two Squares

Let p be an odd prime. There exist integers $x, y \in \mathbb{Z}$ such that $p = x^2 + y^2$ if and only if $p \equiv 1 \pmod 4$.