MATH 402 Notes

Contents

1 Arithmetic in $\mathbb{Z}$ Revisited

1.1 Division Theorem

Given non-zero integers a and b where $b > 0$, there exists unique integers q and r such that $a = bq + r$ where $0 \leq r < b$

1.2 Divisibility

Given $a, b \in \mathbb{Z}$, $b \mid a$ means there exists $c \in \mathbb{Z}$ such that $a = bc$

1.3 Greatest Common Divisors

Given non-zero integers a and b, $\gcd(a, b) = (a, b)$ is the largest common divisor of a and b

- Finding $\gcd(a, b)$ by brute force

  Let $\mathcal{D}_a = \{\text{divisors of } a\}$ and $\mathcal{D}_b = \{\text{divisors of } b\}$. Then $\mathcal{D}_a \cap \mathcal{D}_b = \{\text{common divisors of } a \text{ and } b\}$. Hence, $\gcd(a, b) = \max(\mathcal{D}_a \cap \mathcal{D}_b)$

- Finding $\gcd(a, b)$ by the Euclidean algorithm

  Lemma 1.3.1. *If $b \mid a$, then $\gcd(a, b) = |b|$*

  Lemma 1.3.2. *If $x = yz + w$, then $\gcd(x, y) = \gcd(y, w)$*

  Given non-zero integers a and b, the recursive Euclidean Algorithm computes $\gcd(a, b)$

  *A full definition of the Euclidean Algorithm can be found in **MATH 300 Notes**, page 12*

1.4 Euclid's Lemma

Assume a, b, c are non-zero integers. If $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$

1.5 Diophantine Equations

Any equation of the form $ax + by = c$ where $a, b, c \in \mathbb{Z}$ is called a linear Diophantine equation

- Has no solutions if $\gcd(a, b)$ does not divide c
- Has infinitely many solutions if $\gcd(a, b)$ divides c
- Given a solution where $x = x_0$, $y = y_0$, and $d = \gcd(a, b)$

  $x = x_0 + \frac{b}{d}k$

  $y = y_0 - \frac{a}{d}k$

1.6 Fundamental Theorem of Arithmetics

Given a positive integer $n > 1$ with two prime factorizations

$n = p_1 p_2 ... p_r$

$n = q_1 q_2 ... q_s$

Then $r = s$ and $\{p_1, p_2, ..., p_r\} = \{q_1, q_2, ..., q_s\}$. This means that the prime factorization of n is unique

2 Congruence in $\mathbb{Z}$ and Modular Arithmetic

2.1 Congruence

Given two integers a and b and a modulus $m \geq 1$, a is congruent to $b \bmod m$ if and only if $m \mid a - b$. This is denoted as $a \equiv b \bmod m$

- Congruence is reflexive, symmetric and transitive

2.2 Congruence Class of $a \bmod n$

The congruence class of $a \bmod n$, denoted $[a]_n$, is the set of all integers that are congruent to $a \bmod n$

- $[a]_n = \{x \mid x \equiv a \bmod n\}$
- There are n congruence classes in $\mathbb{Z}_n$, $[0]_n$ $[1]_n$ ... $[n-1]_n$
- Congruence classes are either equal or disjoint
- a is typically the least residue $\bmod n$

2.3 Additive Operations With Congruence Classes

- Behaves the same as integer addition
- $[a]_n + [b]_n = [a+b]_n$

2.4 Multiplicative Operations With Congruence Classes

- Behaves the same as integer multiplication
- $[a]_n \cdot [b]_n = [a \cdot b]_n$

2.5 Units in $\mathbb{Z}_n$

a is a unit in $\mathbb{Z}_n$ if the equation $ax \equiv 1 \bmod n$ has a solution

- Has the associated linear Diophantine equation $ax + ny = 1$
- a is a unit in $\mathbb{Z}_n$ if and only if $\gcd(a, n) = 1$

2.6 Zero Divisor in $\mathbb{Z}_n$

a is a zero divisor in $\mathbb{Z}_n$ if $a \neq 0$ and the equation $ax \equiv 0 \bmod n$ has a non-zero solution for some $x \in \mathbb{Z}_n$

- $\mathbb{Z}_n$ is a disjoint union of $\{0\} \cup \{\text{units}\} \cup \{\text{zero divisors}\}$
- If a is not 0 or a unit, then a is a zero divisor

2.7 Multiplicative Inverse in $\mathbb{Z}_n$

a is invertible in $\mathbb{Z}_n$ if and only if $ax \equiv 1 \bmod n$ has integer solutions

- a is invertible if and only if $\gcd(a, n) = 1$
- x is the inverse of a, denoted a^{-1}
- Given p is prime, $a^{-1} \equiv a^{p-2} \bmod p$

3 Rings

3.1 Rings

A ring is a nonempty set R that can undergo two operations, usually written as addition and multiplication

- Additive operations satisfy the following axioms
  1. Closed under addition: if $a \in R$ and $b \in R$, then $a + b \in R$
  2. Associative: $a + (b + c) = (a + b) + c$
  3. Commutative: $a + b = b + c$
  4. Additive identity: there exists an element $0_R \in R$ such that $a + 0_R = a$ for all a
  5. Additive inverse: for each a, there exists an element $x \in R$ such that $a + x = 0_R$
- Multiplicative operations satisfy the following axioms
  6. Closed under multiplication: if $a \in R$ and $b \in R$, then $ab \in R$
  7. Associative: $a(bc) = (ab)c$
  8. Distributive: $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$

Multiplicative operations are not necessarily commutative, i.e. $ab \neq ba$

Multiplicative operations do not necessarily have a multiplicative identity, i.e. $a1_R = 1_R a = a$ for all a

3.2 Commutative Rings

A commutative ring is a ring R in which multiplication is commutative, i.e. $ab = ba$

3.3 Rings With Identity

A ring with identity is a ring R that contains one multiplicative identity, i.e. $a1_R = 1_R a = a$ for all a

3.4 Fields

A field is a commutative ring with identity where all non-zero elements are units

- i.e. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}_p$
- All fields are integral domains

3.5 Integral Domains

An integral domain is a commutative ring with identity where there are no zero divisors

- Every finite integral domain is a field

3.6 Units in Rings

a is a unit in ring R if the equation $ax = xa = 1_R$ has a solution $x \in R$

3.7 Zero Divisor in Rings

a is a zero divisor in ring R if $a \neq 0$ and the equations $ax = 0_R$ or $xa = 0_R$ has a non-zero solution for some $x \in R$

3.8 Multiplicative Inverse in Rings

a is invertible in ring R if and only if $ax = xa = 1_R$ has solutions $x \in R$

- x is the inverse of a, denoted a^{-1}
- In a non-commutative ring, an inverse x of a that satisfies $ax = xa = 1_R$ is called a two-sided multiplicative inverse

3.9 Subrings

A subring is a nonempty subset S of a ring R that can undergo operations inherited from R

- i.e. $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$
- A subring must satisfy all the axioms of a ring
- Existence of a multiplicative identity is not an inherited property
  - The subring of a ring with identity does not have to contain an identity

3.10 Subring Theorem

Given S is a subset of R, S is a subring of R if and only if it satisfies the following axioms

- Closed under subtraction: if $a \in S$ and $b \in S$, then $a - b \in S$
- Closed under multiplication: if $a \in S$ and $b \in S$, then $ab \in S$

3.11 Subring Set Theory

Given that S and T are subrings of R

- $S \cap T$ is a subring of R
- $S \cup T$ is not a subring of R

3.12 Finite Set $\mathbb{F}_p[\theta]$

$\mathbb{F}_p[\theta]$ are the finite sets containing numbers of the form $a + b\theta$ where $a, b \in \mathbb{F}_p$

- $\mathbb{F}_p$ represents the finite set $\{0, 1, ..., p - 1\}$ where p is prime
- The $\mathbb{F}_p[\theta]$ rings are a family of commutative rings with identity
- $\mathbb{F}_p[\theta]$ rings may or may not be fields

3.13 Complex Set $\mathbb{C}$

$\mathbb{C}$ is the set of complex integers $a + bi$ where $a, b \in \mathbb{R}$

- The $\mathbb{C}$ ring is a field and an integral domain
- $a + bi$ has the multiplicative inverse $\dfrac{a}{a^2 + b^2} - \dfrac{bi}{a^2 + b^2}$ where $a^2 + b^2 \neq 0$
- $x = a + bi$ has a complex conjugate of $\bar{x} = a - bi$

3.14 Gaussian Integers $\mathbb{Z}[i]$

$\mathbb{Z}[i]$ is the set of Gaussian integers $a + bi$ where $a, b \in \mathbb{Z}$

- The $\mathbb{Z}[i]$ ring is an integral domain but not a field
- $\mathbb{Z}[i]$ is a disjoint union of $\{0\} \cup \{\pm 1, \pm i\} \cup \{\text{everything else}\}$
- $\mathbb{Z}[i]$ is a subring of $\mathbb{C}$

3.15 Matrices $M_2(\mathbb{F})$

$M_2(\mathbb{F})$ is the set of 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $a, b, c, d \in \mathbb{F}$

- $\mathbb{F}$ can be $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ or $\mathbb{F}_p$
- The $M_2(\mathbb{F})$ ring is often non-commutative
- $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has the two-sided multiplicative inverse $\frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ where $ad - bc \neq 0$

3.16 Units in $M_2(\mathbb{F})$

A is a unit in ring $M_2(\mathbb{F})$ if its determinant $ad - bc \neq 0$ and its inverse is in $M_2(\mathbb{F})$

- The set of units $GL_2(\mathbb{F}) = \{A \in M_2(\mathbb{F}) \mid \det(A) \neq 0\}$ is the 2×2 general linear group over $\mathbb{F}$
- Multiplicative operations in $GL_2(\mathbb{F})$ satisfy the following axioms
  - Closed under multiplication: if $A \in GL_2(\mathbb{F})$ and $B \in GL_2(\mathbb{F})$, then $AB \in GL_2(\mathbb{F})$
    * If you multiply two invertible matrices, then the product is also invertible
    * AB has the two-sided multiplicative inverse $B^{-1}A^{-1}$
  - Associative: $A(BC) = (AB)C$
  - Multiplicative identity: $AI = IA = A$ for all A
    * $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
  - Multiplicative inverse: for each A, there exists an element $B \in GL_2(\mathbb{F})$ such that $AB = BA = I$
- $GL_2(\mathbb{F})$ is a subset of the ring $M_2(\mathbb{F})$ but it is not a subring

3.17 Continuous Real-Valued Functions $C[0, 1]$

$C[0, 1]$ is the set of continuous real-valued functions on $[0, 1]$

- The $C[0, 1]$ ring is a commutative ring with identity
- $C[0, 1]$ satisfies all the ring axioms
- Additive operations also satisfy the following axioms
  - Addition: $(f + g)(x) = f(x) + g(x)$
  - Closed under addition: if $f(x) \in C[0, 1]$ and $g(x) \in C[0, 1]$, then $f(x) + g(x) \in C[0, 1]$
  - Additive identity: $f(x) + o(x) = f(x)$, where $o(x) = 0$
- Multiplicative operations also satisfy the following axioms
  - Multiplication: $(f \cdot g)(x) = f(x) \cdot g(x)$
  - Closed under multiplication: if $f(x) \in C[0, 1]$ and $g(x) \in C[0, 1]$, then $f(x) \cdot g(x) \in C[0, 1]$
  - Multiplicative identity: $f(x) \cdot i(x) = f(x)$, where $i(x) = 1$

3.18 Ring Homomorphisms

Rings R and S are homomorphic if there exists a well-defined function $\lambda : R \to S$ such that

- $\lambda(a +_R b) = \lambda(a) +_S \lambda(b)$
- $\lambda(a \cdot_R b) = \lambda(a) \cdot_S \lambda(b)$

where $+_R$, $\cdot_R$ are operations defined in R and $+_S$, $\cdot_S$ are operations defined in S

- As a consequence of the two conditions:
  - Unit preserving: $\lambda(\text{unit}_R) = \text{unit}_S$
  - Multiplicative identity preserving: $\lambda(1_R) = 1_S$
  - Additive inverse preserving: $\lambda(-a) = -\lambda(a)$

3.19 Ring Isomorphisms

Rings R and S are isomorphic, denoted $R \cong S$, if there exists a well-defined bijective function $\phi : R \to S$ such that

- $\phi(a +_R b) = \phi(a) +_S \phi(b)$
- $\phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$

where $+_R$, $\cdot_R$ are operations defined in R and $+_S$, $\cdot_S$ are operations defined in S

- The addition and multiplication tables of R and S match when translated via ϕ
- Isomorphic rings have the same size/cardinality
- Isomorphic rings have the same number of units

4 Arithmetic in $\mathbb{F}[x]$

4.1 Polynomials

$R[x]$ is the set of polynomials over ring R of the form $f(x) = a_0 + a_1x + ... + a_nx^n$ where $a_i \in R$ and $n \geq 0$

- a_n is called the leading coefficient
- x is called the indeterminate
- If the largest coefficient $a_n = 1$, then f is called a monic polynomial
- If n is the largest number for which $a_n \neq 0$, then we say f has degree n, that is $\deg(f) = n$
  - The degree of the zero polynomial $f(x) = 0$ is not defined

4.2 Polynomial Rings

Given $p(x) = a_0 + a_1x + ... + a_nx^n$ and $q(x) = b_0 + b_1x + ... + b_mx^m$ in ring $R[x]$ where $m \leq n$

- Addition in $R[x]$
  - $p(x) + q(x) = c_0 + c_1x + ... + c_nx^n$ where $c_i = a_i + b_i$
  - Additive identity is $O(x) = 0$
  - Standard algebraic addition of polynomials
  - Additive inverse is obtained by replacing all coefficients with their additive inverse in R
- Multiplication in $R[x]$
  - $p(x) \cdot q(x) = d_0 + d_1x + ...d_{n+m}x^{n+m}$ where $d_i = \sum_{k=0}^{i} a_kb_{i-k} = a_0b_i + a_1b_{i-1} + ... + a_ib_0$
  - Multiplicative identity is $I(x) = 1$
  - Standard algebraic multiplication of polynomials

$R[x]$ is a commutative ring with multiplicative identity $f(x) = 1$

- R is a subring of $R[x]$
- If R is an integral domain, then $R[x]$ is an integral domain
- If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is an integral domain
- If $\mathbb{F}$ is a field, then the units in $\mathbb{F}[x]$ are precisely the non-zero constant functions
- If $\mathbb{F}$ is a field, then $\mathbb{F}[x] = \{0\} \cup \underbrace{\{0 \text{ degree}\}}_{\text{all units in } \mathbb{F}[x]} \cup \{1 \text{ degree}\} \cup ...$

4.3 Finite Polynomial Rings

Given $\mathbb{F}_p[x]$ where $\mathbb{F}_p = \{0, 1, ..., p-1\}$ and p is prime

- There are $(p-1)p^n$ possible polynomials of degree n
- $\mathbb{F}_p[x]$ is an infinite ring but has finite number of polynomials of degree n

4.4 Division Theorem in Polynomials

Given non-zero polynomials $f(x)$ and $g(x)$ in $\mathbb{F}[x]$ where $\mathbb{F}$ is a field, there exists unique polynomials $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$ where either $r(x) = 0$ or $0 \leq \deg(r) < \deg(g)$

- Use long division to calculate $q(x)$ and $r(x)$

4.5 Divisibility in Polynomials

Given $f(x), g(x) \in \mathbb{F}[x]$, $g(x) \mid f(x)$ means there exists $h(x) \in \mathbb{F}[x]$ such that $f(x) = g(x)h(x)$

4.6 Greatest Common Divisors in Polynomials

Given non-zero polynomials $f(x)$ and $g(x)$, $\gcd(f(x), g(x)) = (f(x), g(x))$ is the monic polynomial of the largest degree that divides both $f(x)$ and $g(x)$

- Finding $\gcd(f(x), g(x))$ by the Euclidean algorithm

  Lemma 4.6.1. *If $g(x) \mid f(x)$, then $\gcd(f(x), g(x)) = g^*(x)$ where $g^*(x)$ is the monicization of $g(x)$*

  Lemma 4.6.2. *If $a(x) = b(x)c(x) + d(x)$, then $\gcd(a(x), b(x)) = \gcd(b(x), d(x))$*

  Given non-zero polynomials $f(x)$ and $g(x)$, the recursive Euclidean Algorithm computes $\gcd(f(x), g(x))$

  The Euclidean Algorithm for polynomials is similar to that for integers

4.7 Bézout's Theorem for Polynomials

If $f(x)$ and $g(x)$ are non-zero polynomials:

> Then there exists polynomials $s(x)$ and $t(x)$ such that $\gcd(f(x), g(x)) = s(x)f(x) + t(x)g(x)$

Bézout's Theorem for polynomials is similar to that for integers

4.8 Polynomial Roots

$\alpha \in \mathbb{F}$ is a root of $f(x) \in \mathbb{F}[x]$ if and only if $f(\alpha) = a_0 + a_1\alpha + ... + a_n\alpha^n = 0$

- α is a root of $f(x)$ if and only if $(x - \alpha) \mid f(x)$
- If $\deg(f) = n$ then $f(x)$ has at most n distinct roots

4.9 Associates

$f(x)$ is an associate of $g(x)$ in $\mathbb{F}[x]$ if and only if $f(x) = c \cdot g(x)$ for some unit $c \in \mathbb{F}$

- $\{\text{associates of } g(x)\} = \{c \cdot g(x) \mid c \text{ is unit}\}$

4.10 Non-Trivial Factorization

$p(x) \in \mathbb{F}[x]$ can be non-trivially factorized if there exists $f(x), g(x) \in \mathbb{F}[x]$ where

> $0 < \deg(f) < \deg(p)$
>
> $0 < \deg(g) < \deg(p)$

such that $p(x) = f(x)g(x)$

4.11 Reducible Polynomials

A non-zero non-unit polynomial $p(x)$ is reducible in field $\mathbb{F}[x]$ if and only if it can be non-trivially factorized

- $p(x)$ is reducible if and only if it can be non-trivially factored such that $p(x) = f(x)g(x)$, where $f(x)$ and $g(x)$ are polynomials of lesser degrees
- If a polynomial is not reducible, it is irreducible

4.12 Irreducible Polynomials

A non-zero non-unit polynomial $p(x)$ is irreducible in field $\mathbb{F}[x]$ if and only if its only divisors are its associates and the non-zero constant polynomial/units

- $p(x)$ is irreducible if and only if it cannot be non-trivially factored such that $p(x) = f(x)g(x)$, where $f(x)$ and $g(x)$ are polynomials of lesser degrees
- If a polynomial is not irreducible, it is reducible
- All polynomials of degree 1 are irreducible by definition

4.13 Theorems on Irreducible Polynomials

Given that $p(x) \in \mathbb{F}[x]$

- Every non-zero non-unit polynomial in $\mathbb{F}[x]$ is a product of irreducible polynomials
- There are infinitely many irreducible polynomials in $\mathbb{F}[x]$
- The factorization of a polynomial into irreducibles is unique
- If $p(x)$ is irreducible and $p(x) \mid b(x)c(x)$, then $p(x) \mid b(x)$ and $p(x) \mid c(x)$
- If $p(x)$ is irreducible and $p(x) = b(x)c(x)$, then either $b(x)$ or $c(x)$ is a non-zero constant polynomial/unit
- Polynomials of degree 1 are always irreducible
- If $\deg(p) = 2$ or 3, then p is irreducible if and only if p has no roots in $\mathbb{F}$
- If p is irreducible and $\deg(p) > 1$ then p has no roots in $\mathbb{F}$
- If p has no roots in $\mathbb{F}$, this does not imply p is irreducible

4.14 Rational Root Test

If $\frac{r}{s} \in \mathbb{Q}$ is a root of $f(x) = a_0 + a_1x + ... + a_nx^n$ where $f(x) \in \mathbb{Z}[x]$, then $r \mid a_0$ and $s \mid a_n$

- Rational root test narrows down the set of possible rational roots
- Check these possible roots manually to determine if they are actual roots

4.15 Gauss' Lemma

$p(x) \in \mathbb{Z}[x]$ is reducible in $\mathbb{Q}[x]$ if and only if it is reducible in $\mathbb{Z}[x]$

- Contrapositive: $p(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$

4.16 Polynomial Reduction $\bmod n$

$\bar{f}(x) = [f(x)]_n$ is the polynomial obtained by reducing all coefficients of $f(x)$ in $\mathbb{Z}[x]$ by $\bmod n$

- If $\bar{f}(x)$ is irreducible in $\mathbb{F}_p[x]$ for any prime p that does not divide the leading coefficient of $f(x)$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$

4.17 Checking Irreducibility

The following algorithm checks if $f(x) \in \mathbb{F}_p[x]$ of degree n is irreducible

1. Plug in $0, 1, ..., p-1$ into $f(x)$ to see if we have a root
2. Consider all polynomials of degree 2 and eliminate those that are reducible
3. Check if the irreducible polynomials of degree 2 divide $f(x)$ via long division
4. Repeat step 2 to step 3 with polynomials of degree $3, 4, ..., \frac{n-1}{2}$

4.18 Eisenstein's Criterion

Suppose $f(x) = a_0 + a_1x + ... + a_nx^n$ where $f(x) \in \mathbb{Z}[x]$, if there exists a prime p such that

- p divides each of $a_0, a_1, ..., a_{n-1}$
- p does not divide a_n
- p^2 does not divide a_0

then $f(x)$ is irreducible in $\mathbb{Q}[x]$

4.19 Fundamental Theorem of Algebra

Every non-constant polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}$

- The irreducible polynomials in $\mathbb{C}[x]$ are precisely the degree 1 polynomials

4.20 Polynomials in $\mathbb{R}[x]$

- All degree 1 polynomials in $\mathbb{R}[x]$ are irreducible
- Only degree 2 polynomials which have complex roots in $\mathbb{R}[x]$ are irreducible
  - Polynomial $ax^2 + bx + c$ in $\mathbb{R}[x]$ has negative discriminant $b^2 - 4ac$
- Complex roots in $\mathbb{R}[x]$ occur in conjugate pairs (i.e. $a \pm bi$ are roots)
  - Product of conjugate pairs is a real polynomial of degree 2

4.21 Roots of Unity

A complex number $z \in \mathbb{C}$ is called an n^{th} root of unity if z is a root of the polynomial $f(x) = x^n - 1$ such that $z^n = 1$

- The primitive n^{th} root of unity is given by the complex number $\omega = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$
  - A root of unity is said to be primitive if it is not the power of another root of unity
- The n^{th} roots of unity are given by $\omega^k = e^{\frac{2k\pi i}{n}} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ for $k = 0, 1, ..., n-1$
- The n^{th} roots of unity represent the vertices of an n sided polygon inscribed in the unit circle
- The n^{th} roots of unity have the identity $1 + \omega + \omega^2 + ... + \omega^{n-1} = 0$
- The complete factorization of $f(x)$ into irreducibles is given by $\prod_{k=0}^{n-1}(x - \omega^k)$
- Roots of unity also exist in $\mathbb{Q}[x]$, $\mathbb{R}[x]$ and $\mathbb{F}_p[x]$

5 Congruence in $\mathbb{F}[x]$ and Congruence-Class Arithmetic

5.1 Polynomial Congruence

Given two polynomials $f(x)$ and $g(x)$ and a modulus $p(x)$, $f(x)$ is congruent to $g(x)$ if and only if $p(x) \mid f(x) - g(x)$. This is denoted as $f(x) \equiv g(x) \bmod p(x)$

- $f(x)$ and $g(x)$ are congruent if they have the same remainder after long division by $p(x)$
- Polynomial congruence is reflexive, symmetric and transitive

5.2 Polynomial Congruence Class of $f(x) \bmod p(x)$

The polynomials congruence class of $f(x) \bmod p(x)$, denoted $[f(x)]_{p(x)}$, is the set of all polynomials that are congruent to $f(x) \bmod p(x)$

- $[f(x)]_{p(x)} = \{g(x) \mid g(x) \equiv f(x) \bmod p(x)\}$
- Polynomial congruence classes are either equal or disjoint
- $f(x)$ is typically the least residue $\bmod p(x)$

5.3 Polynomial Congruence Ring $\mathbb{F}[x]_{p(x)}$

$\mathbb{F}[x]_{p(x)}$ is the set of disjoint classes $[r(x)]_{p(x)}$ where $r(x)$ is are least residues $\bmod p(x)$ such that $r(x) = 0$ or $0 \leq \deg(r) < \deg(p)$

- $\mathbb{F}[x]_{p(x)} = \{r(x) \mid r(x) = 0 \text{ or } 0 \leq \deg(r) < \deg(p)\}$
  $= \{a_0 + a_1 x + ...a_n x^n \mid a_0, a_1, ..., a_n \in \mathbb{F} \text{ and } n = \deg(p) - 1\}$
- $[f(x)]_{p(x)} + [g(x)]_{p(x)} = [f(x) + g(x)]_{p(x)}$
- $[f(x)]_{p(x)} \cdot [g(x)]_{p(x)} = [f(x) \cdot g(x)]_{p(x)}$
- Additive identity is $O(x) = [0]_{p(x)}$
- Multiplicative identity is $I(x) = [1]_{p(x)}$

5.4 Fields in $\mathbb{F}[x]_{p(x)}$

$\mathbb{F}[x]_{p(x)}$ is a field if and only if $p(x)$ is irreducible in $\mathbb{F}[x]$ where $\mathbb{F}$ is a field

- For all $f(x) \in \mathbb{F}[x]$, $\gcd(f(x), p(x)) = 1$

5.5 Finite Fields in $\mathbb{F}_p[x]_{p(x)}$

Given an irreducible polynomial in $\mathbb{F}_p[x]_{p(x)}$ of degree n, we can construct a finite field in $\mathbb{F}_p[x]_{p(x)}$ of order p^n

6 Ideals and Quotient Rings

6.1 Ideals

A subring I of ring R is an ideal in R if $ra \in I$ and $ar \in I$ for all $r \in R$ and $a \in I$

- If-condition can be simplified as $RI \subseteq I$ and $IR \subseteq I$
- A proper ideal I in R satisfies $I \subset R$
- All ideals are subrings
- Not all subrings are ideals

A subset I of a ring R is an ideal in R if and only if has the following properties

1. I is non-empty
2. If $a, b \in I$, then $a - b \in I$
3. If $r \in R$ and $a \in I$, then $ra \in I$ and $ar \in I$

6.2 Maximal Ideals

Let R be a commutative ring with identity. Then ideal M in R is maximal if $M \subset R$ and the only ideals containing M are M and R

- There does not exist an ideal J such that $M \subset J \subset R$
- i.e. M is as large as possible while being a proper subset of R

6.3 Finitely Generated Ideals

Let R be a commutative ring with identity and $c_1, c_2, ..., c_n \in R$. Then $I = \{r_1c_1 + r_2c_2 + ... + r_nc_n \mid r_1, r_2, ..., r_n \in R\}$ is a finitely generated ideal in R

6.4 Principal Ideals Generated by c

Let R be a commutative ring with identity and $c \in R$. Then $I = \{rc \mid r \in R\}$ is the principal ideal generated by c, denoted (c)

- If $(m) \subseteq (n)$, then $n \mid m$
- Principal ideals are a special case of finitely generated ideals where $n = 1$

6.5 Principal Ideal Domains

A principal ideal domain (PID) is an integral domain in which every ideal is principal

- An integral domain is a commutative ring with identity with no zero divisors
- If $\mathbb{F}$ is a field, then $\mathbb{F}$ is a principal ideal domain
- i.e. $\mathbb{Z}$, $\mathbb{F}[x]$, $\mathbb{Z}[i]$

6.6 Ideals in $\mathbb{Z}$

Every subring in $\mathbb{Z}$ is an ideal in $\mathbb{Z}$, and every ideal in $\mathbb{Z}$ is a principal ideal generated by some c

- For every subring I in $\mathbb{Z}$, there exists $c \in \mathbb{Z}$ such that $I = (c)$
- c is the smallest positive element in I
- The maximal ideals in $\mathbb{Z}$ are (p) for prime integers p
- The maximal ideal in $\mathbb{Z}/(p)$ is (p) when p is prime
- $\mathbb{Z}/(p)$ is a field if and only if p is prime

6.7 Ideals in $\mathbb{Z}[i]$

Every ideal in $\mathbb{Z}[i]$ is a principal ideal generated by some $a + bi$

- There are $N(a + bi)$ distinct ideals in $\mathbb{Z}[i]/(a + bi)$
- The maximal ideals in $\mathbb{Z}[i]$ are $(a + bi)$ for Gaussian primes $a + bi$
- The maximal ideal in $\mathbb{Z}[i]$ is $(a + bi)$ when $a + bi$ is a Gaussian prime
- $\mathbb{Z}[i]/(a + bi)$ is a field if and only if $a + bi$ is a Gaussian prime

6.8 Ideal Lattice

Ideal lattices describe the containment relations between different ideals

$$\begin{tikzcd}[arrows=-] & (1) \arrow[dl] \arrow[dr] & \\ (2) \arrow[dr] & & (3) \arrow[dl] \\ & (6) \arrow[d] & \\ & (12) & \end{tikzcd}$$

The ideal lattice tells us that

- (1) contains (2) and (3)
- (2) and (3) contain (6)
- (6) contains (12)

6.9 Ideal Congruence

Given ideal I in ring R and two elements a and b in R, a is congruent to b modulo I if and only if $a - b \in I$ or $a + I = b + I$. This is denoted as $a \equiv b \bmod I$

- Ideal congruence is reflexive, symmetric and transitive

6.10 Ideal Congruence Class of $a \bmod I$

Given ideal I in ring R and element a in R, the ideal congruence class of $a \bmod I$, denoted $[a]_I$, is the set of all elements in R that are congruent to $a \bmod I$

- $[a]_I = \{b \mid b \equiv a \bmod I\} = \underbrace{a + I}_{\text{left coset of } I \text{ represented by } a}$
- Ideal congruence classes / left cosets are either equal or disjoint

6.11 Lagrange's Theorem for Finite Rings

If R is a finite ring and I is an ideal in R, then $|I| \mid |R|$

- The cardinality of the ideal is a divisor of the cardinality of the ring

6.12 Quotient Ring R/I

R/I, also denoted as R_I, is the set of disjoint left cosets $[a]_I = a + I$ where a are elements in R

- $R/I = \{a + I \mid a \in R\}$
- $(a + I) + (b + I) = (a + b) + I$
- $(a + I) \cdot (b + I) = (a \cdot b) + I$
- Additive identity is $0 + I = I = [0]$
- Multiplicative identity is $1 + I = [1]$

6.13 Kernels

The kernel of a ring homomorphism $f : R \to S$ is $\mathrm{Ker}(f) = \{r \in R \mid f(r) = 0_S\}$

- $\mathrm{Ker}(f)$ contains every element in the domain R that has 0 value in the co-domain S
- $\mathrm{Ker}(f)$ is an ideal in R
  - Given $a, b \in \mathrm{Ker}(f)$, $a - b \in \mathrm{Ker}(f)$ since $f(a - b) = f(a) - f(b) = 0_S - 0_S = 0_S$
  - Given $r \in R$ and $a \in \mathrm{Ker}(f)$, $ra \in \mathrm{Ker}(f)$ since $f(ra) = f(r) \cdot f(a) = f(r) \cdot 0_S = 0_S$
- $\mathrm{Ker}(f) = \{0_R\}$ if and only if
  - f is injective
  - R is isomorphic to $f(R)$

6.14 Natural Homomorphisms

A natural homomorphism from R to R/I is a map $\pi : R \to R/I$ given by $\pi(r) = r + I$

- π is a surjective homomorphism with kernel I
- Natural homomorphisms are a special case of surjective homomorphisms

6.15 First Isomorphism Theorem

Let $f : R \to S$ be a surjective homomorphism of rings with $K = \operatorname{Ker}(f)$. Then there exists an isomorphic function $\bar{f}$ between R/K and S

$$\begin{tikzcd} R \arrow[r, "f"] \arrow[d, "\pi"'] & S \\ R/K \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

- $f(r) = \bar{f}(\pi(r)) = \bar{f}(r + K)$

6.16 Product Decomposition Theorem

Let a, b be positive integers and $\gcd(a, b) = 1$. Then $\mathbb{F}/(ab)$ is isomorphic to $\mathbb{F}/(a) \times \mathbb{F}/(b)$

6.17 Product Decomposition Theorem for Polynomials

Let $f(x), g(x)$ be polynomials in $\mathbb{F}[x]$ and $\gcd(f(x), g(x)) = 1$. Then $\mathbb{F}[x]/(f(x)g(x))$ is isomorphic to $\mathbb{F}[x]/(f(x)) \times \mathbb{F}[x]/(g(x))$

6.18 Additional Theorems

- M is a maximal ideal if and only if $\mathbb{F}/M$ is a field
- $\mathbb{F}[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible in $\mathbb{F}[x]$
- $(n) \cap (m) = (\operatorname{lcm}(n, m))$
- $(n) + (m) = (\gcd(n, m))$
- $(n)(m) = (nm)$

6.19 Prime Ideals

An ideal P in ring R is called prime if $bc \in P$ implies $b \in P$ or $c \in P$

- P is a prime ideal in ring R if and only if R/P is an integral domain
- Prime ideals in $\mathbb{Z}$ are (p) where p is prime

6.20 Maximal and Prime Ideals

- If M is a maximal ideal, then M is a prime ideal
- Let $\mathbb{F}$ be a field and I a non-zero ideal in $\mathbb{F}[x]$. The following are equivalent
  - I is a maximal ideal
  - I is a prime ideal
  - $I = (f(x))$ for some irreducible polynomial $f(x) \in \mathbb{F}[x]$

  Similar theorem holds true for integers

7 Arithmetic in $\mathbb{Z}[i]$

7.1 Division Theorem in Gaussian Integers

Given non-zero Gaussian integers $a_1 + a_2i$ and $b_1 + b_2i$, there exists $q_1 + q_2i$ and $r_1 + r_2i$ such that $a_1 + a_2i = (b_1 + b_2i)(q_1 + q_2i) + (r_1 + r_2i)$ where $N(r_1 + r_2i) \leq N(b_1 + b_2i)$

- The quotient and remainder is not unique

7.2 Divisibility in Gaussian Integers

Given $a_1 + a_2i, b_1 + b_2i \in \mathbb{Z}[i]$, $b_1 + b_2i \mid a_1 + a_2i$ means there exists $c_1 + c_2i \in \mathbb{Z}[i]$ such that $a_1 + a_2i = (b_1 + b_2i)(c_1 + c_2i)$

7.3 Greatest Common Divisors in Gaussian Integers

Given non-zero Gaussian integers $a_1 + a_2i$ and $b_1 + b_2i$, $\gcd(a_1 + a_2i, b_1 + b_2i) = (a_1 + a_2i, b_1 + b_2i)$ is a common divisor of $a_1 + a_2i$ and $b_1 + b_2i$ with largest norm

- $a_1 + a_2i$ and $b_1 + b_2i$ are relatively prime if $(a_1 + a_2i, b_1 + b_2i)$ is a unit in $\mathbb{Z}[i]$
  - i.e. $(a_1 + a_2i, b_1 + b_2i) = \pm 1 \text{ or } \pm i$
- The greatest common divisor is not unique
- $\gcd(a_1 + a_2i, b_1 + b_2i)$ can be found by the Euclidean algorithm

7.4 Bézout's Theorem for Gaussian Integers

If $a_1 + a_2i$ and $b_1 + b_2i$ are non-zero Gaussian integers

Then there exists Gaussian integers $s_1 + s_2i$ and $t_1 + t_2i$ such that

$$\gcd(a_1 + a_2i, b_1 + b_2i) = (s_1 + s_2i)(a_1 + a_2i) + (t_1 + t_2i)(b_1 + b_2i)$$

Bézout's Theorem for Gaussian integers is similar to that for integers

7.5 Non-Trivial Factorization

$a_1 + a_2i \in \mathbb{Z}[i]$ can be non-trivially factorized if there exists $b_1 + b_2i \in \mathbb{Z}[i]$ where

$$0 < N(b_1 + b_2i) < N(a_1 + a_2i)$$

such that $(b_1 + b_2i) \mid a_1 + a_2i$

7.6 Unique Factorization Theorem

If there are two factorizations of a Gaussian integer, then each component of the factorizations will equal each other, or differ by a factor of $-1, i$ or $-i$

7.7 Gaussian Primes

If a Gaussian integer $a_1 + a_2 i$ with $N(a_1 + a_2 i) > 1$ has only trivial factors, then it is a Gaussian prime

- The trivial factors are $\pm 1, \pm i, \pm(a_1 + a_2 i), \pm(a_1 + a_2 i)i$

If $a_1 + a_2 i$ is a Gaussian integer and $N(a_1 + a_2 i)$ is a prime integer, then $a_1 + a_2 i$ is a Gaussian prime

- Note that the reverse implication does not hold

If $\pi \in \mathbb{Z}[i]$ is a Gaussian prime, then there exists a prime integer p such that $\pi \mid p$ in $\mathbb{Z}[i]$

- Gaussian primes are the factors of the prime integers in $\mathbb{Z}[i]$

Every Gaussian prime π has one of three forms:

- $\pi = \pm p \text{ or } \pm ip$ for some prime integer p where $p \equiv 3 \bmod 4$
- π is part of an octet of factors $\pm a + \pm b \text{ or } \pm b + \pm a$ such that $p = a^2 + b^2$ and $p \equiv 1 \bmod 4$
- π is one of $\pm 1, \pm i$

8 Appendix

8.1 Rings

Ring	Properties			
$\mathbb{R}$	infinite	commutative	has identity	field
$\mathbb{Q}$	infinite	commutative	has identity	field
$\mathbb{E}$	infinite	commutative	no identity	not field
$\mathbb{Z}$	infinite	commutative	has identity	not field
$\mathbb{Z}_n$	finite	commutative	has identity	not field
$\mathbb{Z}_p$	finite	commutative	has identity	field
$\mathbb{C}$	infinite	commutative	has identity	field
$\mathbb{Q}(\sqrt{2})$	infinite	commutative	has identity	field
$\mathbb{Z}_3[i]$	finite	commutative	has identity	field
$M_2(\mathbb{Z})$	infinite	not commutative	has identity	not field
$M_2(\mathbb{E})$	infinite	not commutative	no identity	not field
$M_2(\mathbb{Z}_n)$	finite	not commutative	has identity	not field
$M_2(\mathbb{Z}_p)$	finite	not commutative	has identity	not field
$\left\{\begin{pmatrix} 0 & r \\ 0 & 0 \end{pmatrix} \mid r \in \mathbb{Z}_n\right\}$	finite	commutative	no identity	not field

8.2 Norm Functions

- $N(a) = a^2$
- $N(a + b\sqrt{-1}) = a^2 + b^2$
- $N(a + b\sqrt{-m}) = a^2 + b^2 m$
- $N(a + b\sqrt{m}) = a^2 - b^2 m \longleftarrow$ verification needed

$\mathbb{E}$ denotes the ring containing all integers divisible by 2, i.e. $-2, 0, 4$

8.3 Quick Proofs

- Every field $\mathbb{F}$ is an integral domain

  Given $a, b \in \mathbb{F}$,

  $ab = 0 \to a^{-1}ab = a^{-1}0 \to b = 0$
  $ab = 0 \to abb^{-1} = 0b^{-1} \to a = 0$

  Therefore, there are no zero divisors in $\mathbb{F}$

- Prove that S is a subring of R

  Given $a, b \in S$

  $a \in R$ and $b \in R$ such that $S \subset R$
  $a - b \in S$ such that S is closed under subtraction
  $ab \in S$ such that S is closed under multiplication

  Therefore, S is a subring of R

- a is a unit / invertible in $\mathbb{Z}_n$ if $\gcd(a, n) = 1$

  Given $\gcd(a, n) = 1$

  By Bézout's Theorem there exists $x, y \in \mathbb{Z}_n$ such that $ax + ny = 1$
  Then $ny = 1 - ax$ and $n \mid 1 - ax$ such that $ax \equiv 1 \mod n$

  Therefore, there exists $x \in \mathbb{Z}_n$ such that $ax = 1$ and a is a unit / invertible

- Check if $\mathbb{F}[x]$ contains units

  Given $A \in \mathbb{F}[x]$

  $N(AB) = N(A)N(B)$
  $N(1) = 1$
  If A is a unit, then there exists $B \in \mathbb{F}[x]$ such that $AB = 1$
  This is equivalent to $N(A)N(B) = N(1) = 1$

  Therefore if A is a unit, then there exists $B \in \mathbb{F}[x]$ such that $N(A)N(B) = 1$