

# Number Theory

## MATH3431 UNSW

Jeremy Le

2024T1

Definitions: Purple, Theorems: Blue, Properties/Lemmas: Green

## Contents

<b>1</b>	<b>The Ring of Integers</b>	<b>2</b>
1.1	The Set of All Integers . . . . .	2
1.2	Ring . . . . .	2
1.3	Divisibility in Commutative Rings . . . . .	3
1.4	Ideals . . . . .	4
<b>2</b>	<b>Diophantine Equations and Congruences</b>	<b>5</b>
2.1	Congruences . . . . .	5
2.2	Arithmetic Functions . . . . .	5
<b>3</b>	<b>Introduction to Groups</b>	<b>6</b>
3.1	Fields . . . . .	6
3.2	Units of a Ring . . . . .	6
3.3	Groups . . . . .	7
3.4	Group Isomorphism . . . . .	7
3.5	Wilson's Theorem . . . . .	8
<b>4</b>	<b>The Structure of <math>\mathbb{U}_m</math> and <math>\mathbb{Z}_m</math></b>	<b>8</b>
4.1	Subgroups and Cyclic Groups . . . . .	8
4.2	Direct Product of Groups . . . . .	9
4.3	Decomposition of $\mathbb{U}_m$ . . . . .	10
4.4	Primitive Roots . . . . .	11
<b>5</b>	<b>Quadratic Reciprocity</b>	<b>12</b>
5.1	Quadratic Congruences . . . . .	12
5.2	Quadratic Residues . . . . .	12
5.3	Euler's Criterion . . . . .	12
5.4	Legendre's Symbol . . . . .	12
5.5	Gauss' Lemma . . . . .	13
5.6	Quadratic Reciprocity . . . . .	14
<b>6</b>	<b>Gaussian Integers</b>	<b>14</b>

# 1 The Ring of Integers

## 1.1 The Set of All Integers

**Divisor** Let  $a$  and  $b$  be integers. We say that  $a$  is a divisor of  $b$  if there exists an integer  $k$  such that  $b = ka$ . If  $a$  is a divisor not equal to  $b$  we call it a proper divisor.

**Divisibility Properties** Let  $a, b, c \in \mathbb{Z}$ . Then

- a) If  $a \mid b$  and  $b \mid c$  then  $a \mid c$ .
- b)  $a \mid a$ .
- c) If  $a \mid b$  and  $b \mid a$  then  $b = \pm a$ .
- d) If  $a \mid b$  and  $a \mid c$  then  $a \mid (xb + yc)$  for any  $x, y \in \mathbb{Z}$ .

**Euclid's Theorem** There are infinitely many primes in  $\mathbb{Z}$ .

## 1.2 Ring

**Ring** A ring consist of a non-empty set  $R$  together with two operations defined on elements of  $R$ , addition (+) and multiplication (denoted by juxtaposition, or sometimes by  $\star$  or  $\times$ ) where all the following properties hold:

1. Closure under addition: if  $a, b \in R$  then  $a + b \in R$ .
2. Commutativity of addition: for all  $a, b \in R$ ,  $a + b = b + a$ .
3. Associativity of addition: for all  $a, b, c \in R$ ,  $(a + b) + c = a + (b + c)$ .
4. Zero element: There is an element  $0$  of  $R$  such that if  $a \in R$  then  $a + 0 = a$ .
5. Negatives.  $\forall a \in R$  there is  $-a \in R$  such that  $a + (-a) = 0$ .
6. Closure under multiplication: if  $a, b \in R$  then  $ab \in R$ .
7. Associativity of multiplication:  $\forall a, b, c \in R$ ,  $(ab)c = a(bc)$ .
8. Distributive laws: for all  $a, b, c \in R$ ,  $a(b + c) = ab + ac$  and  $(a + b)c = ac + bc$ .

**Subtraction** For any  $a, b$  in a ring  $R$ , we define  $a - b = a + (-b)$

**Ring Properties** Let  $R$  be a ring and  $a, b, c \in R$ . Then the following hold:

1. if  $a + b = a + c$  then  $b = c$ ;
2.  $0$  is unique and  $0a = a0 = 0$ ;
3. for each  $a$ ,  $-a$  is unique;

4.  $a - b = 0$  if and only if  $a = b$ ;
5.  $-(ab) = (-a)b = a(-b)$ ;
6.  $ab - ac = a(b - c)$  and  $ac - bc = (a - b)c$ .

**Commutative Ring** A commutative ring is a ring  $R$  in which multiplication is commutative, that is,  $ab = ba$  for all  $a, b \in R$ .

**Identity Element** An identity element in the ring  $R$  is an element, usually denoted by 1, with the property that  $1a = a1 = a$  for all  $a \in R$ . Sometimes we are more explicit and call 1 the multiplicative identity.

**Divisors of Zero** In a ring  $R$ , if  $a$  and  $b$  are non-zero elements such that  $ab = 0$ , then  $a$  and  $b$  are called divisors of zero.

**Integral Domain** An integral domain is a commutative ring with identity in which there are no divisors of zero. Explicitly, an integral domain is a non-empty set  $R$  together with operations of addition and multiplication, such that the ring axioms (1) - (8) hold as well as the following:

9. Commutativity of multiplication. If  $a, b \in R$  then  $ab = ba$ .
10. Identity element. There exists an element 1 of  $R$  such that if  $a \in R$  then  $1a = a$ .
11. No divisors of zero. For all  $a, b \in R$ , if  $ab = 0$  then either  $a = 0$  or  $b = 0$ .

**Cancellation Law for Integral Domains** Let  $R$  be an integral domain and  $a, b, c \in R$  and suppose  $a \neq 0$ . If  $ab = ac$  then  $b = c$ .

### 1.3 Divisibility in Commutative Rings

**Divisors in Rings** Let  $\alpha, \beta$  be elements in a commutative ring  $R$ . We say that  $\alpha$  is a divisor of  $\beta$ , denoted by  $\alpha \mid \beta$ , if there exists an element  $\kappa$  of  $R$  such that  $\beta = \kappa\alpha$ .

**Unit of Rings** Let  $R$  be a commutative ring with identity. An element of  $R$  having a multiplicative inverse is called a unit of  $R$ .

#### Associates, Irreducibles and Primes

- Elements  $a$  and  $b$  of an integral domain  $R$  are called associates if  $a = ub$ , for some unit  $u$  of  $R$ .
- An element  $\rho$  of the integral domain  $R$  is said to be irreducible if it has the property

$$\forall \alpha, \beta \in R, \text{ if } \rho = \alpha\beta \text{ then } \alpha \text{ or } \beta \text{ is a unit.}$$

- A non-zero, non-unit element  $\rho$  of the integral domain  $R$  is said to be prime if it has the property

$$\forall \alpha, \beta \in R, \text{ if } \rho \mid \alpha\beta \text{ then } \rho \mid \alpha \text{ or } \rho \mid \beta.$$

**Primes are Irreducible** In an integral domain every prime is irreducible.

**Greatest Common Divisor** Let  $a, b$  be integers, not both zero. Then a positive integer  $g$  is the greatest common divisor of  $a$  and  $b$  if and only if  $g$  is a common divisor and every common divisor is a factor of  $g$ .

**GCD in Rings** Let  $a, b$  be elements in a commutative ring  $R$ . An element  $g \in R$  is a greatest common divisor of  $a$  and  $b$  in  $R$  if  $g \mid a, g \mid b$  and every common divisor of  $a$  and  $b$  is a factor of  $g$ .

## 1.4 Ideals

**Ideal** Let  $R$  be a commutative ring with identity. A subset  $I$  of  $R$  is called an ideal of  $R$  if it has the following three properties:

- 0 is in  $I$ .
- If  $a, b$  are in  $I$  then  $a + b$  is in  $I$ .
- If  $a \in I$  and  $x \in R$  then  $ax \in I$ .

**Smallest Ideal** Let  $R$  be a commutative ring with identity, and  $\{a_1, \dots, a_n\} \subset R$ . Then the set

$$\{r_1 a_1 + \dots + r_n a_n : r_1, \dots, r_n \in R\}$$

is the smallest ideal of  $R$  containing  $\{a_1, \dots, a_n\}$ .

**Principal Ideal** An ideal  $I$  of a ring  $R$  is said to be principal if there exists  $a \in R$  such that  $I = \langle a \rangle = \{ax : x \in R\}$ .

**Every Ideal is Principal** Every ideal in  $\mathbb{Z}$  is principal. In particular, if  $a, b$  are not both zero then  $\langle a, b \rangle = \langle \gcd(a, b) \rangle$ .

**Principal Ideal Domain** A principal ideal domain is an integral domain in which every ideal is principal.

**Integral and Principal Ideal Domains** Let  $R$  be an integral domain.

- If  $R$  has a division algorithm then  $R$  is a principal ideal domain.
- If  $R$  is a principal ideal domain, then every non-zero element of  $R$  which is not a unit has

a unique (up to associates and order) factorisation into irreducibles.

**Big-Oh and Little-Oh Notations** For two functions  $f(x)$ ,  $f : \mathbb{R} \rightarrow \mathbb{C}$ , and  $g(x)$ ,  $g : \mathbb{R} \rightarrow \mathbb{R}^+$ , we say that

- $f(x) = O(g(x))$  iff  $\limsup_{x \rightarrow \infty} |f(x)|/g(x) < \infty$  or, alternatively iff there is a constant  $c > 0$  such that  $|f(x)| \leq cg(x)$  for all sufficiently large  $x$ .
- $f(x) = o(g(x))$  iff  $\lim_{x \rightarrow \infty} |f(x)|/g(x) = 0$  or, alternatively, iff for any  $\epsilon > 0$  we have  $|f(x)| \leq \epsilon g(x)$  for all sufficiently large  $x$ .

**Prime Number Theorem (PNT)** For  $x \rightarrow \infty$ , we have

$$\pi(x) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right) = (1 + o(1))\frac{x}{\log x}.$$

## 2 Diophantine Equations and Congruences

### 2.1 Congruences

**Cancelling in Congruences** Let  $a, b, c$  and  $m$  be integers, with  $c \neq 0$ .

- The congruences  $cax \equiv cb \pmod{cm}$  and  $ax \equiv b \pmod{m}$  have the same solutions.
- If  $\gcd(c, m) = 1$  then the congruences  $cax \equiv cb \pmod{m}$  and  $ax \equiv b \pmod{m}$  have the same solutions.

**Multiplicative Inverse** Let  $a \in \mathbb{Z}_m$  and  $m \in \mathbb{Z}^+$ . If  $ax \equiv 1 \pmod{m}$ , we call  $x$  the multiplicative inverse of  $a$  modulo  $m$ , or the multiplicative inverse of  $a$  in  $\mathbb{Z}_m$ .

### 2.2 Arithmetic Functions

**Notation of Factors** For any positive integer  $n$  we define  $d(n)$  to be the number of (positive) factors of  $n$ , and  $\sigma(n)$  to be the sum of all (positive) factors of  $n$ .

**Formula for  $d(n)$**  If  $n \in \mathbb{Z}^+$  has canonical factorisation into prime powers  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$  then

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_s + 1) = \prod_{k=1}^s (\alpha_k + 1)$$

**Formula for  $\sigma(n)$**  If  $n \in \mathbb{Z}^+$  has canonical factorisation into prime powers

$$\begin{aligned} n &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} \text{ then} \\ \sigma(n) &= (1 + p_1 + p_1^2 + \dots + p_1^{\alpha_1}) \dots (1 + p_s + p_s^2 + \dots + p_s^{\alpha_s}) \\ &= \prod_{k=1}^s \frac{p_k^{\alpha_k+1} - 1}{p_k - 1} \end{aligned}$$

**Multiplicative Functions** Suppose that  $f$  is a function with domain  $\mathbb{Z}^+$ . We call  $f$  multiplicative if

$$f(mn) = f(m)f(n),$$

whenever  $\gcd(m, n) = 1$ .

**$d, \sigma$  Multiplicative** Both  $d$  and  $\sigma$  are multiplicative.

**Perfect Numbers** A number  $n$  is called perfect if  $\sigma(n) = 2n$ .

**Euclid-Euler** Let  $n$  be even. Then  $n$  is perfect if and only if there is an integer  $k > 1$  such that  $n = 2^{k-1}(2^k - 1)$  and  $2^k - 1$  is prime.

## 3 Introduction to Groups

### 3.1 Fields

**Field** A field  $K$  is a commutative ring with identity in which every non-zero element has a multiplicative inverse.

**No Divisors of Zero in Fields** A field contains no divisors of zero.

**All fields are Integral Domains** A field is an integral domain.

**Inverse and GCD** An element  $n \in \mathbb{Z}_m^*$  has an inverse if and only if  $\gcd(m, n) = 1$ .

**Rings and Fields** The ring  $\mathbb{Z}_m$  is a field if and only if  $m$  is prime.

### 3.2 Units of a Ring

**Notation for Set of Units** In  $\mathbb{Z}_m$ , we denote the set of units by  $\mathbb{U}_m$ .

**Units in Commutative Rings with Identity** Let  $R$  be a commutative ring with identity.

- a) 1 is a unit of  $R$
- b) If  $a$  and  $b$  are units in  $R$ , then so is their product  $ab$ .
- c) If  $a$  is a unit in  $R$  then so is  $a^{-1}$

**Units are Closed in Commutative Rings with Identity** In any commutative ring with identity, the set of all units is closed under multiplication and inverse.

### 3.3 Groups

**Groups** A group is a non-empty set  $G$  on which an operation  $\star$  is defined, such that the following properties hold:

- 1. Closure: if  $a, b \in G$  then  $a \star b \in G$ .
- 2. Associativity: if  $a, b, c \in G$  then  $(a \star b) \star c = a \star (b \star c)$ .
- 3. Identity element: there is an element  $e$  of  $G$  such that for all  $a \in G$  we have  $a \star e = e \star a = a$
- 4. Inverses: for each  $a$  in  $G$  there is an element  $b$  of  $G$  such that  $a \star b = b \star a = e$ . This element is usually denoted  $a^{-1}$ .

**Abelian Groups** If the operation is commutative, i.e.  $a \star b = b \star a$ , for all  $a, b \in G$ , the group is called commutative, or Abelian.

**Properties of Groups** In any group  $G$  the following properties hold.

- a There is only one identity element in  $G$ .
- b Each  $x$  in  $G$  has only one inverse.
- c If  $x, y \in G$  then  $(xy)^{-1} = y^{-1}x^{-1}$ .
- d If  $x, y, z \in G$  and  $xy = xz$  then  $y = z$ .

### 3.4 Group Isomorphism

**Group Isomorphism** Let  $G$  and  $H$  be groups with operations  $\star$  and  $\bullet$  respectively. An isomorphism for  $G$  to  $H$  is a bijective function  $\psi : G \rightarrow H$  with the property that

$$\psi(a \star b) = \psi(a) \bullet \psi(b) \quad \text{for all elements } a, b \in G.$$

The groups  $G$  and  $H$  are said to be isomorphic if there exists such a function. We write  $G \cong H$  to indicate that  $G$  and  $H$  are isomorphic.

**Identities and Inverses in Isomorphic Groups** Suppose that  $G$  and  $H$  are groups with identities  $e_G$  and  $e_H$ , respectively. Let  $\psi : G \rightarrow H$  be a group isomorphism. Then

1.  $\psi(e_G) = e_H$ ,
2.  $\psi(a^{-1}) = (\psi(a))^{-1}$  for all  $a \in G$ ,
3.  $\psi(a^n) = \psi(a)^n$  for all  $n \in \mathbb{Z}$ ,
4. If  $\psi : G \rightarrow H, \theta : H \rightarrow K$  homomorphic then  $\theta \circ \psi : G \rightarrow K$  is also homomorphic,
5. If  $\psi : G \rightarrow H$  is a isomorphic then  $\psi^{-1} : H \rightarrow G$  is also isomorphic.

### 3.5 Wilson's Theorem

**Wilson's Theorem** Let  $p \geq 2$ . Then  $p$  is prime if and only if  $(p-1)! \equiv -1 \pmod{p}$ .

## 4 The Structure of $\mathbb{U}_m$ and $\mathbb{Z}_m$

### 4.1 Subgroups and Cyclic Groups

**Subgroup** Let  $G$  be a group, and let  $H$  be a subset of  $G$  which is itself a group under the same operations as  $G$ . Then we say that  $H$  is a subgroup of  $G$ .

**The Subgroup Lemma** Let  $G$  be a group and  $H$  a non-empty subset of  $G$ . Then  $H$  is a subgroup of  $G$  if and only if it is closed under the group operation and inverse.

**Cyclic Groups** A group  $G$  is said to be cyclic if there exists an element  $g \in G$  such that  $G = \langle g \rangle$ , i.e.  $G$  is generated by a single element.

**Order of a Group and Element** The order of a finite group  $G$  is the number of elements in  $G$ ,  $|G|$ .

The order of an element  $g$  in a group  $G$  is the smallest positive integer  $n$  (if any) such that  $g^n = e$ . We write  $o(g)$  for the order of the element  $g$ .

**Distinct Powers of Elements** If  $g \in G$  has order  $n$ , then the elements  $e, g, g^2, \dots, g^{n-1}$  are all distinct.

**Isomorphic Cyclic Groups** Two finite cyclic groups are isomorphic if and only if they have the same order.

**Prime Order is Isomorphic is Cycle Group** Any group of prime order  $p$  is isomorphic to the cyclic group  $C_p$ .



**Groups of Prime Order are Abelian** Any group of prime order is abelian.

**All Subsets Closed under Operation are Subgroups** Let  $G$  be a group with operation  $\star$ . If  $H$  is a non-empty finite subset of  $G$  that is closed under  $\star$ , then  $H$  is a subgroup of  $G$ .

**Lagrange's Theorem** If  $G$  is a finite group and  $H$  is a subgroup of  $G$ , then  $|H|$  is a factor of  $|G|$ .

**Left Coset** Let  $G$  be a group and  $H$  a subgroup of  $G$ . For any  $g \in G$  we define the left coset of  $H$  by  $g$  to be

$$gH = \{gh \mid h \in H\}.$$

If we used additive notation we would write a coset of  $H$  as  $g + H$ .

**Order of Elements in a Group is a Divisor of the Group** Suppose  $G$  is a group of finite order and  $g \in G$ . Then  $g^{|G|} = e$ .

**Fermat's Little Theorem** If  $p$  is a prime and  $a$  is not a multiple of  $p$ , then  $a^{p-1} \equiv 1 \pmod{p}$ .

**Corollary of Fermat's Little Theorem** If  $p$  is prime and  $a$  is any integer, then  $a^p \equiv a \pmod{p}$ .

**Euler's Theorem** Let  $n$  be a positive integer, and let  $a$  be an integer relatively prime to  $n$ . Then  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

## 4.2 Direct Product of Groups

**Cartesian Product** Let  $A$  and  $B$  be two sets. The Cartesian production of the two sets is defined by

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

**Cartesian Proudct of Any Sets is a Group** Let  $H$  and  $K$  groups with operation  $\star$  and  $\times$ , respectively. The set  $H \times K$  with the operation  $\bullet$  defined by

$$(h_1, k_1) \bullet (h_2, k_2) = (h_1 \star h_2, k_1 \times k_2)$$

is a group.

**Cartesian Product of Groups** The group in the above Lemma is called the direct product of  $H$  and  $K$  and it is denoted by  $H \otimes K$ .

**Condition of Isomorphism for Cartesian Products** Let  $G$  be a finite abelian group. If  $H$  and  $K$  are subgroups of  $G$  such that  $|H||K| = |G|$  and  $H \cap K = \{e\}$ , then the mapping

$$\psi : H \otimes K \rightarrow G, \quad \text{where} \quad \psi((h, k)) = h, k$$

is an isomorphism.

**Direct Sum** The direct sum of two additive abelian subgroups  $H$  and  $K$  is

$$H \oplus K = \{(h, k) \mid h \in H \text{ and } k \in K\},$$

with operation defined by

$$(h_1, k_1) + (h_2, k_2) = (h_1 + h_2, k_1 + k_2).$$

**Decomposition of  $\mathbb{Z}_n$**  Suppose positive integer  $n$  factorises as  $n = st$ .

If  $s$  and  $t$  are relatively prime, then  $\mathbb{Z}_n \cong \mathbb{Z}_s \oplus \mathbb{Z}_t$ .

Conversely, if  $s$  and  $t$  are not relatively prime, then  $\mathbb{Z}_n \not\cong \mathbb{Z}_s \oplus \mathbb{Z}_t$ .

**Direct Sum Cyclic if Pairwise Relatively Prime** Let  $s_1, s_2, \dots, s_k$  be positive integers. Then the direct sum  $\mathbb{Z}_{s_1} \oplus \mathbb{Z}_{s_2} \oplus \dots \oplus \mathbb{Z}_{s_k}$  is cyclic if and only if  $s_1, s_2, \dots, s_k$  are pairwise relatively prime.

**The Chinese Remainder Theorem** Suppose that the integers  $m_1, m_2, \dots, m_t$  are pairwise coprime, and let  $b_1, b_2, \dots, b_t$  be any integers. Then the simultaneous congruences

$$x \equiv b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}, \quad \dots, \quad x \equiv b_t \pmod{m_t}$$

have a unique solution modulo  $m_1 m_2 \dots m_t$ .

### 4.3 Decomposition of $\mathbb{U}_m$

**Decomposition of  $\mathbb{U}_m$**  If  $n = st$  is a positive integer,  $\mathbb{U}_n \cong \mathbb{U}_s \otimes \mathbb{U}_t$  if and only if  $s$  and  $t$  are coprime.

**Euler Function Multiplicative** The Euler's function  $\varphi$  is multiplicative.

**Formula for  $\varphi(n)$**  Let  $n$  be a positive integer with canonical factorisation  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ . Then

$$\varphi(n) = \prod_{k=1}^s (p_k^{\alpha_k} - p_k^{\alpha_k-1}) = \prod_{k=1}^s (p_k - 1) p_k^{\alpha_k-1} = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

**Quotient Depends on Prime Factors** The quotient  $\varphi(n)/n$  depends on the prime factors of  $n$ , but not on their multiplicity.

**GCD involving Phi** Suppose that  $\gcd(s, t) = g$ . Then

$$\varphi(g)\varphi(st) = g\varphi(s)\varphi(t).$$

**Cyclic Sets of Units** Let  $p$  be a prime,  $p \neq 2$ . Then  $\mathbb{U}_{p^\alpha}$  is cyclic,

$$\mathbb{U}_{p^\alpha} \cong C_{(p-1)p^{\alpha-1}}.$$

For powers of 2 we have  $\mathbb{U}_2 \cong C_1, \mathbb{U}_4 \cong C_2$  and

$$\mathbb{U}_{2^a} \cong C_2 \otimes C_{2^{a-2}} \quad \text{for } a \geq 3.$$

**Condition for Cyclic Units** Let  $n \geq 2$ . Then  $\mathbb{U}_n$  is cyclic if and only if  $n = 2, n = 4, n = p^\alpha$  or  $n = 2p^\alpha$ , where  $p$  is an odd prime and  $\alpha$  is a positive integer.

**Generator Implies Order and Relatively Primes** Suppose that  $G$  is a cyclic group of order  $n$  and that  $g$  is a generator of  $G$ . Then

- a) for any integer  $\alpha$ , the order of  $g^\alpha$  is  $n/\gcd(\alpha, n)$ ;
- b)  $g^\alpha$  generates  $G$  if and only if  $\alpha$  is relatively prime to  $n$ .

## 4.4 Primitive Roots

**Primitive Root Modulo** A generator of  $\mathbb{U}_m$  is called a primitive root of modulo  $m$ .

**Existence of Primitive Root** A primitive root modulo  $m$  will exist if and only if  $m = 2, m = 4, m = p^\alpha$  or  $m = 2p^\alpha$ , where  $p$  is an odd prime.

**Powers are Primitive Roots if Co-prime to Order** Let  $g$  be a primitive root modulo  $m$ . Then  $g^\alpha$  is a primitive root modulo  $m$  iff  $\alpha$  is relatively prime to  $\varphi(m)$ , that is iff  $a \in U_{\varphi(m)}$ .

**Number of Primitive Roots** If there are any primitive roots modulo  $m$  then there are  $\varphi(\varphi(m))$  of them.

**Discrete Logarithm** The exponent  $\alpha$  above is called the discrete logarithm of  $a$  modulo  $m$  to the base  $g$ , or the index of  $a$  modulo  $m$ , relative to  $g$ . We write

$$\alpha = \log_g a \quad \text{or} \quad \alpha = \text{ind}_g a.$$

**Addition and Multiplication of Discrete Logarithm** Let  $g$  be a primitive root in  $\mathbb{U}_m$ .

a) If  $a, b \in \mathbb{U}_m$  then  $\text{ind}_g(ab) = \text{ind}_g a + \text{ind}_g b \pmod{\varphi(m)}$ .

b) If  $a \in \mathbb{U}_m$  and  $k \in \mathbb{Z}$  then  $\text{ind}_g(a^k) = k \text{ind}_g a \pmod{\varphi(m)}$ .

## 5 Quadratic Reciprocity

### 5.1 Quadratic Congruences

**Number of Solutions** If  $p$  is an odd prime and  $\gcd(a, p) = 1$  (so  $a \not\equiv 0 \pmod{p}$ ), then  $x^2 \equiv a \pmod{p}$  has exactly 2 solutions or it has no solutions.

### 5.2 Quadratic Residues

**Quadratic Residue** An integer  $a \neq 0$  is a quadratic residue if  $x^2 \equiv a \pmod{p}$  has a solution; otherwise,  $a$  is a quadratic non-residue.

**Half are Quadratic Residues** If  $p$  is an odd prime, then exactly half of the integers  $1, 2, \dots, p-1$  are quadratic residues modulo  $p$ ; furthermore, these are the even powers of any primitive root modulo  $p$ .

### 5.3 Euler's Criterion

**Euler's Criterion** If  $p$  is an odd prime that does not divide  $a$ , then

$$x^2 \equiv a \pmod{p} \text{ has a solution} \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p};$$

equivalently

$$x^2 \equiv a \pmod{p} \text{ has no solution} \iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

### 5.4 Legendre's Symbol

**Legendre Symbol** The Legendre symbol  $\left(\frac{a}{p}\right)$  is given by

$$\frac{a}{p} = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p; \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p; \\ 0 & \text{if } a \text{ is neither (i.e., if } a \equiv 0 \pmod{p}). \end{cases}$$

**Equivalent Statements** Let  $p$  be an odd prime and let  $a$  be an integer with  $\gcd(a, p) = 1$ . Then the following statements are equivalent:

- $x^2 \equiv a \pmod{p}$  has a solution;
- $x^2 \equiv a \pmod{p}$  has precisely two solutions;
- $a$  is a quadratic residue modulo  $p$ ;
- $a$  is an even power of some primitive root modulo  $p$ ;
- $a$  is not an odd power of any primitive root modulo  $p$ ;
- $a^{\frac{p-1}{2}} \not\equiv -1 \pmod{p}$ ;
- $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ;
- $\left(\frac{a}{p}\right) \neq -1$ ;
- $\left(\frac{a}{p}\right) = 1$ .

**Properties of Legendre Symbol** Let  $p$  be an odd prime and let  $a$  and  $b$  be any integers. Then

- if  $a \equiv b \pmod{p}$ , then  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ ;
- $\left(\frac{a^2}{p}\right) = 1$  unless  $a \equiv 0 \pmod{p}$ ;
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$  - multiplicatively;
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ .

**Arithmetic Series - Legendre Symbol** If  $p$  is an odd prime, then  $\left(\frac{1}{p}\right) + \left(\frac{2}{p}\right) + \cdots + \left(\frac{p-1}{p}\right) = 0$ .

**Solutions to Quadratic Congruence**  $x^2 \equiv -1 \pmod{p}$  has a solutions iff  $p \equiv 1 \pmod{4}$  or  $p = 2$ ; if  $p \equiv 1 \pmod{4}$ , then  $\pm \left(\frac{p-1}{2}\right)!$  are the solutions.

## 5.5 Gauss' Lemma

**Gauss' Lemma** For  $S = \{a, 2a, \dots, \frac{p-1}{2}a \pmod{p}$ ,

$$\left(\frac{a}{p}\right) = (-1)^k \text{ where } k = \left| \left\{ s \in S : s > \frac{p-1}{2} \right\} \right|.$$

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

**Corollary Formula for  $\left(\frac{2}{p}\right)$**  For odd primes  $p$ ,

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8}; \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

## 5.6 Quadratic Reciprocity

**Equivlance between Legendre's** For  $a \in \mathbb{N}$  and primes  $p, q$  with  $p \equiv \pm q \pmod{4a}$ , we have

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

**The Law of Quadratic Reciprocity** If  $p$  and  $q$  are odd primes, then

$$\begin{aligned} \left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right), & \text{if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4} \\ \left(\frac{p}{q}\right) &= -\left(\frac{q}{p}\right), & \text{if } p \equiv 3 \pmod{4} \text{ or } q \equiv 3 \pmod{4} \end{aligned}$$

**$\left(\frac{a}{p}\right)$  for Small Integers** If  $p$  is an odd prime, then

- $\left(\frac{0}{p}\right) = 0$ ;  $\left(\frac{1}{p}\right) = 1$ ;
- $\left(\frac{-1}{p}\right) = 1$  if and only if  $p \equiv 1 \pmod{4}$ ;
- $\left(\frac{2}{p}\right) = 1$  if and only if  $p \equiv \pm 1 \pmod{8}$ ;
- $\left(\frac{3}{p}\right) = 1$  if and only if  $p \equiv \pm 1 \pmod{12}$ .

## 6 Gaussian Integers

**Gaussian Integers** The Gaussian Integers are the complex numbers

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\},$$

where  $i$  is the square root of -1.

**Gaussian Integers is an Integral Domain**  $\mathbb{Z}[i]$  is an integral domain.

**Norm** The norm  $\alpha = a + ib \in \mathbb{C}$  is  $N(\alpha) = \alpha\bar{\alpha} = (a + ib)(a - ib) = a^2 + b^2$ .

**Properties of the Norm** Let  $\alpha, \beta \in \mathbb{Z}[i]$  and  $c \in \mathbb{Z}$  be given. Then

- $N(\alpha) \geq 0$  and  $N(\alpha) \in \mathbb{Z}$ ;
- $\sqrt{N(\alpha + \beta)} \leq \sqrt{N(\alpha)} + \sqrt{N(\beta)}$ ;
- $N(\alpha\beta) = N(\alpha) + N(\beta)$
- $N(\alpha) \leq N(\alpha\beta)$  for  $\beta \neq 0$
- $N(c\alpha) = c^2 N(\alpha)$ ,  $N(c) = c^2$ , and  $N(N(\alpha)) = (N(\alpha))^2$ ;
- $N(\alpha) = 1$  if and only if  $\alpha \in \{\pm 1, \pm i\}$ ;
- $N(\alpha) = 0$  if and only if  $\alpha = 0$ .

**Properties of the Identity Norm** The following are equivalent for  $a \in \mathbb{Z}[i]$ :

- $\alpha$  is a unit;
- $N(\alpha) = 1$ ;
- $\alpha \in \{\pm 1, \pm i\}$ .

**Division Algorithm for Gaussian Integers** For all Gaussian integers  $\alpha, \beta \neq 0$ , there exist,  $q, r \in \mathbb{Z}[i]$  for which

$$\alpha = q\beta + r \text{ and } 0 \leq N(r) < N(\beta).$$

**GCD for Gaussian Integers** A greatest common divisor of Gaussian integers  $\alpha$  and  $\beta$  is an element  $\gamma \in \mathbb{Z}[i]$  that is

- a factor of both  $\alpha$  and  $\beta$ ;
- a multiple of every such common factor.

Let  $\gcd(\alpha, \beta)$  be the set of all greatest common divisors  $\alpha$  and  $\beta$ .

**Euclidean Algorithm for Gaussian Integers** For  $\alpha, \beta \neq 0$ , write  $r_0 = \beta$  and use the division algorithm to find  $q_1, r_1 \in \mathbb{Z}[i]$  for which

$$\alpha = q_1\beta + r_1 \quad \text{and} \quad 0 \leq N(r_1) < N(\beta).$$

If  $r_1 \neq 0$ , then we write similarly,

$$\beta = q_2r_1 + r_2 \quad \text{and} \quad 0 \leq N(r_2) < N(r_1).$$

Continuing like this while  $r_k \neq 0$ , we find  $q_{k+1}, r_{k+1} \in \mathbb{Z}[i]$  so that

$$r_{k-1} = q_{k+1}r_k + r_{k+1} \quad \text{and} \quad 0 \leq N(r_{k+1}) < N(r_k).$$

Then  $r_{n+1} = 0$  for some  $n \geq 0$ , and  $\gcd(\alpha, \beta) = \{\pm r_n, \pm r_n i\}$ .

**Ideals in Gaussian Integers** Every ideal in the Gaussian integers is principal.

**Generators for Gaussian Integers** For any element  $\alpha, \beta \in \mathbb{Z}[i]$ , suppose that  $\gamma \in \gcd(\alpha, \beta)$ . Then  $|\alpha, \beta|$  and so  $\gamma = m\alpha + n\beta$  for some  $m, n \in \mathbb{Z}[i]$ .

**Gaussian Primes** The primes of  $\mathbb{Z}[i]$  are called Gaussian primes.

**Every Prime is Irreducible in Integral Domains** Every prime elements of an integral domain is irreducible.

**Primes are Irreducible** A Gaussian integer is a prime if and only if it is irreducible.

**Factorising Gaussian Integers** Each Gaussian integers factors uniquely into Gaussian primes up to order and multiplication by units.

**Integer and Gaussian Primes** An integer prime  $p \in \mathbb{N}$  is a Gaussian prime iff  $p \equiv 3 \pmod{4}$ .

**Conditions for Gaussian Primes** A Gaussian interger  $a \in \mathbb{Z}[i]$  is prime if and only if

- either  $N(\alpha)$  is a prime integer;
- or  $\alpha = \epsilon p$  for a unit  $\epsilon \in \mathbb{Z}[i]$  and a prime  $p \in \mathbb{N}$  with  $p \equiv 3 \pmod{4}$ .

**Sum of Two Squares** If  $m$  and  $n$  are both sum of two squares, then so is  $mn$ .

**Sum of Integer Squares is not Gaussian Prime** For an odd prime  $p$ , the following statements are equivalent:

- $p$  is the sum of two integer squares;
- $p$  is not a Gaussian prime;
- $p \equiv 1 \pmod{4}$ .

**Solutions if  $p$  is a Sum of Two Squares** For each odd prime  $p$ ,  $x^2 \equiv -1 \pmod{p}$  has a solution if and only if  $p$  is the sum of two squares.

**Expressed as Sum of Two Integer Squares** A positive number  $n$  is the sum of two squares if and only if  $p \equiv 3 \pmod{4}$  for all odd primes  $p$  that divide  $n$  an odd number of times.



**Sum of Three Squares** A positive integer  $n$  is the sum of three integer squares if and only if  $n \neq 4^k(8m+7)$  for all non-negative integers of  $n$  and  $k$ .

**Sum of Four Squares** Every positive integer is the sum of four integer squares.

**Waring Problem** Is it true for any integer  $k \geq 1$  there is a number  $g(k)$  such that every positive integer is the sum of  $g(k)$  integer  $k$ -th powers?

**David Hilbert** For any integer  $k \geq 1$  the number  $g(k)$  exists.