Number Theory

1 Numbers and Sets

- natural numbers
- divides —— $\exists k$ st $b = ka$
- factor
- divisor
- divisible
- prime —— only factor are 1 and n
- composite
- prime counting function $\pi(x)$ —— # primes $\leq x$

Lemma 1.1. *$n > 1$, then n has prime factor*

Theorem 1.2. *$\exists$ infinitely many primes*

- highest common factor / greatest common divisor
- coprime / relatively prime
- Euclid's algorithm

Proposition 1.3. *Euclid's algorithm works*

Theorem 1.4 (Bezout)**.** *$a, b, c \in \mathbb{N}$, then $\exists m, n$ st $am + bn = c \iff (a, b) \mid c$*

Proposition 1.5. *p prime, $p \mid ab$, then $p \mid a$ or $p \mid b$*

Proof. assume $p \nmid a$, then Bezout $\square$

Theorem 1.6 (Fundamental Theorem of Arithmetic). *$n \in \mathbb{N}$, then n can be factorised as product of primes uniquely (up to reordering)*

Proof. Existence: induction
Uniqueness: $p_1 \mid q_1 \cdots q_k$ $\square$

– congruent to b modulo n —— $n \mid a - b$

Lemma 1.7. *$n > 1$, $(a, n) = 1$, then $\exists m$ st $am \equiv 1$ (multiplicative inverse mod n)*

Proof. Bezout $\square$

– unit —— invertible elements

– multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ or $(\mathbb{Z}/n\mathbb{Z})^*$ —— group of unit

– Euler totient function $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$

Fact. $\phi(p) = p - 1$

Theorem 1.8 (Fermat-Euler). *$n > 1$, $(a, n) = 1$, then $a^\phi(n) \equiv 1 \pmod n$*

Proof. Langrange's $\square$

Corollary 1.9 (Fermat's Little Theorem). *$a^{p-1} \equiv 1 \pmod p$*

Theorem 1.10 (Chinese remainder theorem). *$m_1, m_2 > 1$, $(m_1, m_2) = 1$, $a_1, a_2 \in \mathbb{Z}$, then $\exists n$ st $\begin{cases} n \equiv a_1 \pmod{m_1} \\ n \equiv a_2 \pmod{m_2} \end{cases}$, unique up to modulo $m_1 m_2$*

Fact. *extend to more congruences as long as pairwise coprime*

Fact. $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$

Corollary 1.11. *In addition, $(a_1, m_1) = 1, (a_2, m_2) = 1$, then $(n, m_1 m_2) = 1$*

Fact. $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z})^\times$

– multiplicative —— $f(mn) = f(m)f(n)$ whenever m, n coprime

– totally multiplicative —— $f(mn) = f(m)f(n)$ for all m, n

Corollary 1.12. *ϕ Euler function multiplicative*

Proof. $(\mathbb{Z}/m_1m_2\mathbb{Z})^\times = (\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times$ □

Lemma 1.13. *p prime, $k \in \mathbb{N}$, then $\phi(p^k) = p^{k-1}(p-1)$*

Proof. direct counting $p^k - p^{k-1}$ □

$\sum_{d|n} \phi(d)$

Lemma 1.14. *$n \in \mathbb{N}$, then $\sum_{d|n} \phi(d) = n$*

Proof. prove multiplicity, then work on p^k □

Corollary 1.15. *f multiplicative $\Rightarrow \sum_{d|n} f(d)$ multiplicative*

- $d(n) = \tau(n) = \sum_{d|n} 1 = \#$ divisors
- $\sigma(n) = \sum_{d|n} d =$ sum of divisors

Theorem 1.16 (Lagrange Theorem)**.** *p prime, $f(x) = a_nx^n + \cdots + a_1x + a_0$, $a_n \nmid p$, then $f(x) \equiv 0 \pmod p$ at most n solutions*

Proof. induction, $(x - x_0)g(x) \equiv 0 \pmod p$, $\mathbb{Z}/p\mathbb{Z}$ no zero divisor □

Theorem 1.17. *p prime, $(\mathbb{Z}/p\mathbb{Z})$ cyclic*

Proof. $d \mid p-1$, $S_d = \{a : \text{order } d\}$, $x^d - 1 \equiv 0$ at most d solution, then either 0 or $\phi(d)$ solution, but $\sum \phi(d) = p - 1$ □

- primitive root

Lemma 1.18. *p prime, then $\exists$ primitive root g st $g^{p-1} = 1 + bp$ where $(b, p) = 1$*

Proof. primitive root a, then a or $a+p$ $\square$

Lemma 1.19. *$p > 2$ prime, $j \in \mathbb{N}$, then $\exists$ primitive root g mod p st* $g^{p^{j-1}(p-1)} \not\equiv 1 \pmod{p^{j+1}}$

Proof. induction, same g expansion $\square$

Theorem 1.20. *$p > 2$ prime, $j \in \mathbb{N}$, then $(\mathbb{Z}/p^j\mathbb{Z})^\times$ cyclic*

Proof. induction $\square$

Proof. False for $p = 2$, $(\mathbb{Z}/8\mathbb{Z})^\times$ $\square$

2 Quadratic residue

- quadratic residue —— $(a, n) = 1$, $\exists$ solution for $x^2 \equiv a \pmod n$
- quadratic non-residue

Lemma 2.1. *p odd prime, then $\exists$ exactly $\frac{p-1}{2}$ quadratic residues modulo p*

Proof. **Method 1:** pair $a, -a$, then at most $\frac{p-1}{2}$, then no duplicate
Method 2: primitive root $\square$

- Legendre symbol $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ quadratic residue modulo } p \\ -1 & \text{if } a \text{ quadratic non-residue modulo } p \\ 0 & \text{if } (a, p) > 1 \end{cases}$

Theorem 2.2 (Euler's criterion)**.** *p odd prime, then* $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$

Proof. $p \mid a$ trivial, $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$, primitive root g, $a = g^{2i}$ give $\frac{p-1}{2}$ sol, so rest are non-residue $\square$

Corollary 2.3. *p prime, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ (total multiplicative)*

Proof. $p = 2$ trivial, $p > 2$ follows from Euler's criterion $\square$

Corollary 2.4. *p odd prime, then* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Proof. Euler criterion $\Rightarrow \equiv$, but both $\in \{0, \pm 1\}$ $\square$

– $\langle b \rangle$ —— p odd prime, lies in $[-\frac{p}{2}, \frac{p}{2}]$

Proposition 2.5 (Gauss' lemma)**.** *p odd prime, $(a,p) = 1$, then* $\left(\frac{a}{p}\right) = (-1)^{\nu}$ *where* $\nu = \#\left\{k : k \in [1, \frac{p-1}{2}], \langle ka \rangle < 0\right\}$

Proof. $\langle a \rangle, \ldots, \left\langle \frac{p-1}{2} a \right\rangle$ are $\pm 1, \ldots, \pm \left(\frac{p-1}{2}\right)$ in some order $\square$

Corollary 2.6. *p odd prime, then* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Theorem 2.7 (Law of Quadratic Reciprocity)**.** *p, q odd primes, then* $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)$

Proof. write $\langle bq \rangle = bq - cp$, then count (b, c) in $[0, \frac{p}{2}] \times [0, \frac{q}{2}]$ $\square$

– Jacobi symbol $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_k}\right)$ —— $n = p_1 \cdots p_k$

Fact. $\left(\frac{a}{n}\right) = 1 \not\Rightarrow a$ *quadratic residue*

Lemma 2.8.

(i) *n odd, $a, b \in \mathbb{Z}$, then* $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$

(ii) *m, n odd, $a \in \mathbb{Z}$, then* $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$

Lemma 2.9. *n odd, then* $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$ *and* $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

Proof. count $p_i \equiv -1 \pmod 4$ and $p_i \equiv \pm 3 \pmod 8$ $\square$

Theorem 2.10 (LQR for Jacobi symbol)**.** *m, n odd, then* $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right)$

Proof. consider $\prod_i \prod_j (-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}$, count $p_i, q_j \equiv -1 \pmod 4$ $\square$

3 Binary Quadratic Forms

– binary quadratic form $f(x,y) = ax^2 + bxy + cy^2$

Notation. (a,b,c) *or* $\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$

Fact. $f = (x,y)\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$

– unimodular substitution —— $\begin{cases} X = px + qy \\ Y = rx + sy \end{cases}$, $ps - qr = 1$

Fact. *Equivalently,* $\begin{pmatrix} X \\ Y \end{pmatrix} = A\begin{pmatrix} x \\ y \end{pmatrix}$ *where* $A \in SL_2(\mathbb{Z})$

– equivalent —— $(a,b,c) \sim (a',b',c')$ or $f \sim f'$ if related to unimodular substitution

Fact. $T \sim A^\top T A$ *where* $A \in SL_2(\mathbb{Z})$

– discriminant $disc(f) = b^2 - 4ac$

Lemma 3.1. $f \sim f'$, *then* $\mathrm{disc}(f) = \mathrm{disc}(f')$

Proof. $T = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$, then $\mathrm{disc}(f) = -4\det(T)$ and $\mathrm{disc}(f') = -4\det\big(A^\top T A\big)$ □

Lemma 3.2. $\exists$ *BQF* f, $\mathrm{disc}(f) = d \iff d \equiv 0, 1 \pmod 4$

Proof. $(\Rightarrow)$ $d = b^2 - 4ac$
$(\Leftarrow)$ $(1, 0, -\frac{d}{4})$ and $(1, 0, \frac{1-d}{4})$ □

– positive definite $f(x,y) \geq 0$ for all x, y

– negative definite $f(x,y) \leq 0$ for all x, y

– indefinite $f(x,y) > 0$ and $f(x',y') < 0$ for some x, y, x', y'

Lemma 3.3. f *BQF,* $\mathrm{disc}(f) = d$, $a \neq 0$,

(i) $d < 0$, $a > 0$, *then* f *positive definite*

(ii) $d < 0$, $a < 0$, *then* f *negative definite*

(iii) $d > 0$, *then* f *indefinite*

Proof. $4af(x,y) = (2ax+by)^2 - dy^2$
$d < 0$, trivial, equality iff $x = y = 0$
$d > 0$, $4af(x,y) = 4a^2(x - \theta_+ y)(x - \theta_- y)$, $\theta_\pm = -\left(\frac{b \pm \sqrt{d}}{2a}\right)$ □

- $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $S : (a,b,c) \mapsto (c, -b, a)$
- $T_\pm = \begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}$, $T_\pm : (a,b,c) \mapsto (a, b \pm 2a, a \pm b + c)$
- reduced —— positive definite BQF, $-a < b \le a < c$ or $0 \le b \le a = c$

Lemma 3.4. *every positive define BQF $\sim$ reduced form*

Proof. apply $S, T_\pm$ □

Lemma 3.5. *f reduced positive definite BQF, coprime x, y or $x = y = 0$, then $0, a, c, a - |b| + c$ smallest integers represented by f*

Proof. $x, y \in \{0, \pm 1\}$, if $|x| \ge |y| > 0$, then $f \ge a - |b| + c$, similarly for $|y| \ge |x|$ □

Theorem 3.6. *(Uniqueness) every positive define BQF $\sim$ unique reduced form*

Proof. smallest represented int $\Rightarrow a = a'$, then 2nd smallest $\Rightarrow c = c'$, by disc, $b = \pm b'$, $(a,b,c), (a,-b,c)$ both reduced $\Rightarrow \begin{cases} f(\pm 1, 0) \\ f(0, \pm 1) \end{cases}$ match $\begin{cases} f'(\pm 1, 0) \\ f'(0, \pm 1) \end{cases}$, then $\begin{pmatrix} p & q \\ r & s \end{pmatrix} = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so $b = 0$ □

Proposition 3.7. *$d < 0$ fixed, then finite reduced form with $\mathrm{disc}(f) = d$*

Proof. $b^2 < ac$ bound a, hence $|b|$, then c uniquely determined through disc □

- class number of d, $h(d)$ —— # reduced form with $\mathrm{disc}(f) = d$

Lemma 3.8. $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$*, then x', y' coprime $\iff$ x, y coprime*

Proof. $(x, y) \mid (x', y')$ $\square$

- f represents n —— f BQF, $\exists x, y, f(x, y) = n$
- f properly represents n —— f BQF, $\exists x, y, f(x, y) = n$, $(x, y) = 1$

Fact. *equivalent form properly represent the same numbers*

Lemma 3.9. *$n \in \mathbb{N}$, n properly represented by $f \iff f \sim f'$ which first coefficient n*

Proof. $\Leftarrow$ trivial
$\Rightarrow$ Bezout $\square$

Theorem 3.10. *$n \in \mathbb{N}$,*

(i) *n properly represented by f, $\operatorname{disc}(f) = d$, then $\exists$ solution to $\omega^2 \equiv d \pmod{4n}$*

(ii) *if $\exists$ solution to $\omega^2 \equiv d \pmod{4n}$, then $\exists$ f st n properly represented by f, $\operatorname{disc}(f) = d$*

Proof. f' first coefficient n, $\operatorname{disc}(f') = b^2 - 4nc = d$ $\square$

Fact. *$h(d) = 1$, then n properly represented by $f \iff \exists$ solution to $\omega^2 \equiv d \pmod{4n}$*

Proposition 3.11 (Hensel's Lemma)**.** *f polynomial, p odd prime, $f(x_1) \equiv 0 \pmod p$, $f'(x_1) \not\equiv 0 \pmod p$, then $\exists x_r$ st $f(x_r) \not\equiv 0 \pmod{p^r}$ for each $r \geq 1$*

Proof. $x_r = x_{r-1} + \lambda p^{r-1}$ $\square$

Theorem 3.12. *$n = x^2 + y^2$ where $(x, y) = 1 \iff 4 \nmid n$ and all odd prime factors $p_i \equiv 1 \pmod 4$*

Proof. n properly represented $\iff \exists$ sol to $\omega^2 \equiv -4 \pmod{4n}$, then CRT, Hensel $\square$

Corollary 3.13. *$n = x^2 + y^2 \iff$ each $p_i \equiv 3 \pmod 4$ occurs to even power*

Theorem 3.14 (Langrange)**.** *every $n \in \mathbb{N}$ sum of four squares*

4 Distribution of Primes

Theorem 4.1 (Dirichlet's theorem)**.** *$n > 1$, $(n, a) = 1$, then $\exists$ infinite many primes $p \equiv a \pmod n$*