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: $p_1 \mid q_1 \cdots q_k$ □

- 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 □

- 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 □

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 $a+p$ ☐

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 ☐

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

Proof. induction ☐

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

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 ☐

- 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 ☐

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* $\operatorname{disc}(f) = \operatorname{disc}(f')$

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

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

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,* $\operatorname{disc}(f) = d$*, $a \neq 0$,*

(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, $-a < b \leq a < c$ or $0 \leq b \leq a = c$

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 $|x| \geq |y| > 0$, then $f \geq a - |b| + c$, similarly for $|y| \geq |x|$ □

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, $\mathrm{disc}(f) = d$, 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, $\mathrm{disc}(f) = d$*

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

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 $p \equiv a \pmod{n}$*

Proposition 4.2. *$x \geq 10$, then $\sum_{p \leq x} \frac{1}{p} \geq \log\log x - \frac{1}{2}$*

Proof. $\prod (1 - \frac{1}{p})^{-1} \geq \log x$, $\log\left(1 - \frac{1}{p}\right)^{-1} - \frac{1}{p} \leq \frac{1}{2p(p-1)}$ □

Fact. $\sum \frac{1}{p} = \log\log x + c + O(\frac{1}{\log x})$

Corollary 4.3. *infinitely many primes*

- $\pi(x)$ —— # primes $\leq x$

Proposition 4.4. *$\pi \geq c \log x$ for some $c > 0$*

Proof. $y = m^2 \prod p_i^{\alpha_i}$ □

- Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ —— $\mathrm{Re}(s) > 1$

Lemma 4.5. $\mathrm{Re}(s) > 1$,

(i) *$\sum \frac{1}{n^s}$ converges absolutely*

(ii) *converges uniformly on $\mathrm{Re}(s) \geq 1 + \delta$, hence analytic on $\mathrm{Re}(s) > 1$*

Proposition 4.6 (Euler product for ζ). *$\mathrm{Re}(s) > 1$, then $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$*

Proof. $\prod_{p \leq N} \left(1 + p^{-s} + \cdots + p^{-Ms}\right)$ where $p^M < N$, then uniform bound in M, $M \to \infty$, then $N \to \infty$ □

Lemma 4.7. *$Re(s) > 1$, then $\zeta(s) \neq 0$*

Proof. $|\zeta(s) \times \prod_{p \leq x}(1 - p^{-s})| \geq 1 - \sum_{n=x+1} n^{-\sigma} \geq \frac{1}{2}$ □

– Gamma function $\Gamma(z) = \int_0^\infty e^{-t} t^{z-1} dt$ —— for $\mathrm{Re}(z) > 0$

Fact. $z\Gamma(z) = \Gamma(z-1)$

Fact. $\Gamma(n) = (n-1)!$

– completed ζ function $\Xi(s) = \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s)$

Fact. $\Xi(s) = \Xi(1-s)$

– trivial zeros —— at $s = -2, -4, -6, \ldots$

– Mobius function $\mu(n) = \begin{cases} (-1)^k & \text{if } n = p_1 \cdots p_k \text{ where } p_i \text{ distinct primes} \\ 0 & \text{if } n \text{ not square-free} \end{cases}$

– Mertans function $\sum_{n \leq x} \mu(n)$

– $f \sim g \iff \lim \frac{f}{g} \to 1$

Theorem 4.8 (Prime Number Theorem)**.** $\pi(x) \sim \frac{x}{\log x}$

Theorem 4.9 (Prime Number Theorem)**.** $\pi(x) = \int_2^x \frac{dt}{\log t} + O(xe^{-c\sqrt{\log x}})$

– Von Mangoldt function $\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \\ 0 & \text{otherwise} \end{cases}$

– $\psi(x) = \sum_{1 \leq n \leq x} \Lambda(n)$

Fact. $\psi(x) \sim x$

– Dirichlet series for (a_n) —— $\sum \frac{a_n}{n^s}$

Lemma 4.10. *if* $\mathrm{Re}(s) > 1$*, then* $\frac{\zeta'(s)}{\zeta(s)} = -\sum \frac{\Lambda(n)}{n^s}$

Proof. $\zeta(s) = \prod(1 - p^{-s})^{-1}$, then differentiate $\log(\zeta(s))$ □

Fact. $\psi(x) = x - \sum_\rho \frac{x^\rho}{\rho} - \frac{\zeta'(0)}{\zeta(0)}$ *where* ρ *all zeros of* ζ

– $N(x, \sqrt{x})$ —— # n not divisible by any prime $\leq \sqrt{x}$, $1 \leq n \leq x$

– $A_i = \{n : i \mid n\}$

Proposition 4.11 (Legendre's formula)**.** *$x \geq 10$,*

(i) $\pi(x) = \pi(\sqrt{x}) - 1 + N(x, \sqrt{x})$

(ii) $N(x, \sqrt{x}) = \lfloor x \rfloor - \sum |A_i| + \sum |A_{i_1} \bigcap A_{i_2}| - \cdots + (-1)^{\pi(\sqrt{x})} |\bigcap A_p|$

Proof. trivial, -1 as not counting 1 $\square$

Lemma 4.12. *$n \in \mathbb{N}$, $\frac{2^{2n}}{2n} \leq \binom{2n}{n} < 2^{2n}$*

Proof. $2n\binom{2n}{n} \geq (1+1)^{2n} > \binom{2n}{n}$ $\square$

– primorial function $\prod_{p \leq x} p$

Lemma 4.13. *$x \in \mathbb{R}$, $x \geq 1$, then $\prod_{p \leq x} p \leq 4^x$*

Proof. $\prod_{k+2 \leq p \leq 2k+1} p \mid \binom{2k+1}{k+1}$, $2\binom{2k+1}{k+1} = \binom{2k+1}{k+1} + \binom{2k+1}{k}$ $\square$

Theorem 4.14 (Bertrand's postulate)**.** *$n \in \mathbb{N}$, then $\exists p$, $n < p \leq 2n$*

Proof. $\alpha(p, N) = v_p(N!)$, $\alpha(p) = \alpha(p, 2n) - 2\alpha(p, n)$
bound on power: $\alpha(p) \leq \frac{\log(2n)}{\log p}$, $p^{\alpha(p)} \leq 2n$
bound on larger prime: $p^2 > n$, $\alpha(p) \leq 1$
$\frac{2n}{3} < p \leq n$, $\alpha(p) = 0$

$$\begin{cases} T_1 = \prod_{p \leq \sqrt{2n}} p^{\alpha(p)} \leq (2n)^{\pi(2n)} \\ T_2 = \prod_{\sqrt{2n} < p \leq n} p^{\alpha(p)} \leq \prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p \leq 4^{\frac{2n}{3}} \\ T_3 = \prod_{n < p \leq 2n} p \end{cases}$$

$1 + \pi\left(\sqrt{2n}\right) < \frac{1}{2}\sqrt{2n}$ $\square$

5 Continued Fractions

Proposition 5.1 (Dirichlet)**.** *$\theta \in \mathbb{R}$, $N \in \mathbb{N}$, then $\exists \frac{a}{q}$, $1 \leq q \leq N$ st $|\theta - \frac{a}{q}| \leq \frac{1}{qN}$*

Proof. $0, \ldots, N\theta$, pigeonhole on $[\frac{j}{N}, \frac{j+1}{N}]$ □

- continued fraction $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \ldots}}}$ —— $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}$
- partial quotients $[a_0, a_1, \ldots]$
- finite $[a_0, \ldots, a_n]$
- infinite

Convention. *For* $[a_0, \ldots, a_n]$,

(i) $a_n > 1$

(ii) a_n *something other than natural number*

Lemma 5.2. $1-1$ *correspondence between finite continued fractions and rational numbers*

Proof. ($\Leftarrow$) trivial
($\Rightarrow$) strictly decresing denominators □

- convergents for $[a_0, a_1, \ldots]$ —— $[a_0], [a_0, a_1], \ldots$
- (p_n), (q_n) —— $\begin{cases} p_0 = a_0 \\ p_1 = a_0 a_1 + 1 \\ p_n = a_n p_{n-1} + p_{n-2} \end{cases}$, $\begin{cases} q_0 = 1 \\ q_1 = a_1 \\ q_n = a_n q_{n-1} + q_{n-2} \end{cases}$, $a_i \in \mathbb{R}$, $a_1, \cdots \geq 1$

Lemma 5.3. $\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$

Proof. induction □

Lemma 5.4. $n \geq 1$, $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$

Proof. induction □

Lemma 5.5. *if* $a_0, \ldots, a_n \in \mathbb{Z}$, *then* $(p_n, q_n) = 1$

Proof. use above □

Proposition 5.6. *$\theta \in \mathbb{R} \backslash \mathbb{Q}$, then $\frac{p_n}{q_n} \to \theta$*

Proof. $\theta = [a_0, \ldots, a_n, \alpha_{n+1}] = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}}$, expand $|\theta - \frac{p_n}{q_n}|$, q_n strictly increasing □

Lemma 5.7. $\frac{1}{q_{n+2}} \leq |q_n\theta - p_n| \leq \frac{1}{q_{n+1}}$

Proof. $|q_n\theta - p_n| = \frac{1}{\alpha q_n + q_{n-1}}$ and $\alpha_{n+1} = \lfloor a_{n+1} \rfloor$ □

Fact. $|q_n\theta - p_n| \leq |q_{n-1}\theta - p_{n-1}|$

Setting 1. *$\theta \in \mathbb{R} \backslash \mathbb{Q}$ with convergents $\frac{p_n}{q_n}$*

Theorem 5.8 (”best rational approximation”)**.** *$n \in \mathbb{N}$, $p, q \in \mathbb{Z}$, $0 < q < q_n$, then $|q\theta - p| \geq |q_{n-1} - p_{n-1}|$*

Proof. $\det \begin{pmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{pmatrix} = (-1)^n$, $\begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}$ for some $u, v \in \mathbb{Z}$, size of $q \Rightarrow u, v$ opposite sign, $\theta - \frac{p_{n-1}}{q_{n-1}}$, $\theta - \frac{p_n}{q_n}$ opposite sign □

Corollary 5.9. *$p \in Z$, $q \in \mathbb{N}$, $|\theta - \frac{p}{q}| < \frac{1}{2q^2}$, then $\frac{p}{q}$ convergent for θ*

Proof. $q_n \leq q < q_{n+1}$, bound st $|\frac{p}{q} - \frac{p_n}{q_n}| < \frac{1}{q_n q}$ □

- Diophantine equation $x^2 - Ny^2 = 1$ —— $N \in \mathbb{N}$ not square
- Pell’s equation

Corollary 5.10. *$N \in \mathbb{N}$, not square, $x, y > 0$, $x^2 - Ny^2 = 1$, then $\frac{x}{y}$ convergent for $\sqrt{N}$*

Proof. $(x - y\sqrt{N}) < \frac{1}{2y}$ □

- eventually periodic $[a_0, \ldots, a_{n-1}; \overline{a_n, \ldots, a_{n+m-1}}]$
- purely periodic $[\overline{a_0, \ldots, a_{m-1}}]$
- θ quadratic irrational —— $a\theta^2 + b\theta + c = 0$ for some $a, b, c \in \mathbb{Z}$, $a \neq 0$

Theorem 5.11 (Lagrange). *$\theta \in \mathbb{R}$, θ quadratic irrational $\iff$ continued fraction eventually periodic*

Proof. ($\Leftarrow$) $\phi = [\overline{a_n, \ldots, a_{n+m-1}}]$, then $\phi = [a_n, \ldots, a_{n+m-1}, \phi]$ quadratic irrational, then $\theta = \frac{\phi p_{n-1}+p_{n-2}}{\phi q_{n-1}+q_{n-2}}$ quadratic irrational
($\Rightarrow$) $f(x,y) = ax^2 + bxy + cy^2$, $f(\theta, 1) = 0$, finitely many $f(p_n, q_n)$, so finitely many α_n □

Theorem 5.12. *$\sqrt{N} = [a_0; \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}]$ (symmetric, then $2a_0$)*

Proposition 5.13. *$N \in \mathbb{N}$, not square, then $\exists$ convergent $\frac{p_n}{q_n}$ for $\sqrt{N}$ with $p_n^2 - Nq_n^2 = 1$*

Proof. $\sqrt{N} = [a_0; \overline{a_1, \ldots, a_n, 2a_0}] = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}}$, $\alpha_{n+1} = [\overline{2a_0, a_1, \ldots, a_n}] = a_0 + \sqrt{N}$, then plug in and sol for p_n, q_n, then $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1} = p_n^2 - Nq_n^2$, then
n odd, (p_n, q_n) sol
n even, (p_{2n+1}, q_{2n+1}) sol □

Lemma 5.14. *$(x_1, y_1), (x_2, y_2)$ solutions to $x^2 - Ny^2 = 1$, then $(x_1x_2 + y_1y_2N, x_1y_2 + x_2y_1)$ also solution*

Proof. $(x_1 \pm y_1\sqrt{N})(x_2 \pm y_2\sqrt{N})$ □

– $(x_1, y_1) * (x_2, y_2) = (x_1x_2 + y_1y_2N, x_1y_2 + x_2y_1)$

Fact.

(i) *solution to $x^2 - Ny^2 = 1$ group under $*$*

(ii) *group cyclic*

– fundamental unit —— generator of the group above

6 Primality Testing and Factorisation

– (Fermat) pseudoprime to base b —— n odd composite, $(b, n) = 1$, $b^{n-1} \equiv 1 \pmod{n}$

Lemma 6.1. *n pseudoprime to bases b_1, b_2, then n pseudoprime to base b_1b_2, $b_1b_2^{-1}$*

Proposition 6.2. *n not pseudoprime to some base b, then at least half of bases, n not pseudoprime*

Proof. $B = \{\text{all bases st } n \text{ pseudoprime}\}$, then $f : B \to \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times \setminus B$, $f(b_1) = f(bb_1)$, injection as B group ☐

- Carmichael number —— odd composite $n \in \mathbb{N}$, pseudoprime to every base

Fact. *$\exists$ infinite many Carmichael numbers*

- Euler pseudoprime to base b —— n odd composite, $(b, n) = 1$, $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod n$

Proposition 6.3. *n not Euler pseudoprime to some base b, then at least half of bases, n not Euler pseudoprime*

Proof. similar ☐

Fact. *Euler $\Rightarrow$ Fermat*

Proposition 6.4. *n odd composite, then n Euler pseudoprime to at most half of all bases*

Proof. if $p^2 \mid n$, pick $b = g^{p-1}$ as $p \nmid n - 1$

if n distict product primes, pick $\left(\frac{\lambda}{p}\right) = -1$, $\begin{cases} b \equiv \lambda \pmod p \\ b \equiv 1 \pmod{\frac{n}{p}} \end{cases}$ ☐

- Solovay-Strassen primality test —— random bases, check whether Euler
- probabilistic primality test
- strong pseudoprime to base b —— n odd composite, $(b, n) = 1$, $n - 1 = 2^s t$, $b^t \equiv 1 \pmod n$ or $b^{2^r t} \equiv -1 \pmod n$ for $0 \leq r \leq s - 1$

Proposition 6.5. *strong $\Rightarrow$ Euler*

Theorem 6.6. *n odd composite, n strong pseudoprime at most $\frac{1}{4}$ all possible bases*

- Miller-Rabin primality test —— check for b^t, b^{2t} and so on
- deterministic tests

Setting 2. $N = ab$, *odd composite, not square,* $\begin{cases} r = \frac{a+b}{2} \\ s = \frac{a-b}{2} \end{cases}$

Fact. $N = r^2 - s^2$

Example (Fermat factorisation). ***(i)*** $r = \lfloor \sqrt{N} \rfloor + 1, \lfloor \sqrt{N} \rfloor + 2, \ldots$

(ii) *if* $r^2 - N = s^2$, *then* $N = (r-s)(r+s)$

- least absolute residue of b, $\langle b \rangle$
- factor base B —— set of few small primes, with -1
- B-number —— $\left\langle b^2 \right\rangle$ product of elements from B

Example (Factor base method).

(i) *choose factor base* B

(ii) *choose some* B*-numebers* $b_1, \ldots, b_k$

(iii) *Find* I *st* $\prod_I \left\langle b_i^2 \right\rangle$ *square*

(iv) $b = \prod_I b_i$, $c^2 = \prod_I \left\langle b_i^2 \right\rangle$

(v) *compute* $(N, b+c), (N, b-c)$ *hope not trivial factor*

Fact. *consider vector space over* $\mathcal{F}_2$, $\#$ B*-numbers* $\geq |B| + 1$, *guarantees to have dependence*

Fact. *try* $\lfloor kN \rfloor, \lfloor kN \rfloor + 1$ *for* B*-numbers*

Lemma 6.7. $\frac{p_n}{q_n}$ *convergent for* $\sqrt{N}$, *then*

(i) $\left\langle p_n^2 \right\rangle = p_n^2 - q_n^2 N$

(ii) $|\left\langle p_n^2 \right\rangle| \leq 2\sqrt{N}$

Example (Continued fraction method). *calculate* $\left\langle p_n^2 \right\rangle$ *to find* B*-numbers*

Example (Pollard's $p-1$ method). ***(i)*** k *product of small prime (e.g.* $(1, \ldots, B)$*)*

(ii) (a, N) *(e.g.* $a = 2, 3$ *or random)*

(iii) *compute* $a^k \pmod{N}$

(iv) *compute* $(N, a^k - 1)$ *and hope for proper factor*