Number Theory II

1 Euclid and Division

- Division algorithm, Euclid's algorithm, prime numbers, FTA, infinitely many primes

2 Congruences

- Quotient ring, Euler totient function, Euler-Fermat Theorem, Chinese Remainder Theorem
- Multiplicative function f, $\sum_{d|n} f(d)$ multiplicative (Mobius inversion)
- Polynomial ring, division algorithm, factor theorem, number of roots of polynomial equations
- $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. (p.12)
- $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic for odd prime (has prim root) (p.14), $(\mathbb{Z}/2^n\mathbb{Z})^* \cong \{\pm 1\} \times$ cyclic

3 Quadratic Residues

- QR, QNR, precisely half, Legendre symbol, Jacobi symbol
- Euler's Criterion: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$, multiplicative
- Law of QR: $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$
- Gauss' Lemma: $\left(\frac{a}{p}\right) = (-1)^{\nu}$, defined by ... (p.20)
- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$
- $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

4 Binary Quadratic Forms

- BQFs represent, properly represent, equivalent (related by unimodular substitution), discriminant, positive def, negative def, indefinite criteria
- Transformation rule as matrix (which direction)
- Reduced BQF: either $-a < b \leq a \leq c$ or $0 \leq b \leq a = c$
- Bound on a, b in reduced form: $|b| \leq a \leq \sqrt{\frac{|d|}{3}}$ and $b \equiv d \bmod 2$
- Class number $h(d)$ = number of reduced BQF with disc d.
- $d \equiv 0$ or $1 \pmod 4$ is a fundamental discriminant if d is not of the form $d = k^2 d'$ with $k > 1$ and $d' \equiv 0$ or $1 \pmod 4$
- BQF f properly represents $n \iff f$ is equivalent to a form with first coeff n.
- $n > 0$ is properly represented by some form f of disc $diff$ the congruence $x^2 \equiv d \pmod{4n}$ is solvable
- If $\left(\frac{a}{p}\right) = 1$, then $x^2 \equiv a \pmod{p^n}$ is solvable for all $n \geq 1$.

5 Distribution of Primes

- Prime Distribution
- Mobius inversion
- Legendre's Formula $\pi(x) - \pi(\sqrt{x}) + 1 = N_r(x)$, where $N_r(x) = \#\{1 \leq n \leq x \mid n \text{ coprime to } p_1, p_2, \ldots, p_r\}$
- Bertrand's Postulate: there exists prime p with $n \leq p \leq 2n$.

6 Continued Fractions

- Algorithm, partial quotients, convergents, eventually periodic, purely periodic p_n, q_n and relations $p_n = a_n p_{n-1} + p_{n-2}$, ...
- $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$

- $|\theta - p_n/q_n| < \frac{1}{2q_nq_{n-1}}$
- $p_n/q_n \to \theta$
- If θ irrational, $0 < q < q_{n+1}$, then $|q\theta - p| \geq |q_n\theta - p_n|$
- At least one of two successive convergents satisfy $|\theta - p/q| < 1/2q^2$, conversely if p, q satisfy this then it must be one of the convergents
- Quadratic irrational iff eventually periodic
- Pell's equation $x^2 - Ny^2 = 1$ (and generalised version) guarantee for non-trivial solution

7 Primality Test and Factoring

- Fermat Pseudoprime to the base b: $b^N - 1 \equiv 1 \pmod{N}$; Carmichael Number
- Euler pseudoprime: $b^{\frac{N-1}{2}} \equiv \left(\frac{b}{N}\right) \pmod{N}$; no absolute Euler pseudoprime: (proof, p.65) Solovay-Strassen Primality Test
- Strong Test: $N - 1 = 2^s t$, N passes Strong test to base b if $b^t =\equiv 1 \pmod{N}$ or $b^{2r}t \equiv -1 \pmod{N}$ for some $0 \leq r < s$
- Fermat Factorisation: want $N = r^2 - s^2$, try $r = \lfloor N \rfloor + 1, \lfloor N \rfloor + 2, \ldots,$ check if $r^2 - N$ is a square, or replace N by kN
- Factor base method, continued fraction: choose factor base, find convergents p_n that square to B-numbers
- Pollard's $p-1$ algorithm: if N has factor p with $p-1$ product of small primes.

  Choose k a product of small primes, compute $\gcd(a^k - 1, N)$.