Elementary Number Theory - Overview

Markus Schwagenscheidt
ETH Zürich

Spring semester 2023

Primes and Divisibility

- **Euclid:** There are infinitely many primes.
- **Fundamental Theorem of Arithmetic.** Every natural number $n > 1$ has a prime factorization

$$n = p_1 \cdots p_r,$$

  which is unique up to order.
- **Division with remainder:** $a = qb + r$ with $0 \leq r < |b|$.
- **Bézout's Lemma:** There exist $a, b \in \mathbb{Z}$ with $\gcd(a, b) = ax + by$.
- **Euclidean Algorithm:** Computes $\gcd(a, b)$, as well as $x, y \in \mathbb{Z}$ with $\gcd(a, b) = ax + by$.
- **Bertrand's Postulate:** There's always a prime between n and $2n$.
- **Prime Number Theorem:** $\pi(x) \sim \frac{x}{\log(x)}$ for large x.

Number-theoretic functions

- **Important examples:** $e(n), \mathbf{1}(n), \sigma_k(n), \sigma(n), \tau(n), \varphi(n), \mu(n)$.
- **Basic properties of multiplicative functions:** $f(1) = 1$, $f \cdot g$ is multiplicative.
- **Summatory function** $F(n) = \sum_{d|n} f(d)$
- **Examples:** $\sum_{d|n} \varphi(d) = n$ and $\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{otherwise.} \end{cases}$
- **Theorem.** f multiplicative $\Leftrightarrow$ F multiplicative.
- **Dirichlet convolution** $(f * g)(n) = \sum_{d|n} f(d)g(n/d)$.
- **Proposition.** f with $f(1) \neq 0$ has an inverse w.r.t. convolution.
- **Moebius inversion formula:** $F = f * \mathbf{1} \Leftrightarrow f = F * \mu$.
- **Important application:** Proof that φ is multiplicative.
- **Explicit formula:** $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$.

Perfect and amicable numbers

- **Definition.** n is perfect if it is equal to the sum of its proper divisors, i.e. $\sigma(n) = 2n$.
- **Theorem** (Euclid, Euler): An *even* n is perfect iff it is of the form

$$n = 2^{m-1}(2^m - 1) \quad \text{and} \quad 2^m - 1 \text{ is prime}$$

  for some $m \in \mathbb{N}$.
- First few are $6, 28, 496, 8128$.
- **Lemma.** If $2^m - 1$ is prime, then m must be prime.
- **Definition.** $M_p = 2^p - 1$ the p-th *Mersenne number*.
- **Definition.** m, n are amicable if m is the sum of the proper divisors of n, and vice versa. Smallest pair is $(220, 284)$.
- **Thabit's Rule:** If

$$T_k = 3 \cdot 2^k - 1, \quad T_{k-1} = 3 \cdot 2^{k-1} - 1, \quad R_k = 9 \cdot 2^{2k-1} - 1$$

  are all prime, then $m = 2^k T_k T_{k-1}$ and $n = 2^k R_k$ are amicable.

Modular arithmetic

- **Proposition.** a has an inverse modulo m iff $\gcd(a, m) = 1$.
- **Chinese Remainder Theorem.** If $m_1, \dots, m_k$ are pairwise coprime, then the system

$$x \equiv a_1 \pmod{m_1}, \quad \dots, \quad x \equiv a_k \pmod{m_k}$$

  has a unique solution modulo $m = \prod m_i$.
- **Euler-Fermat.** If $\gcd(a, m) = 1$ then

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

- **Fermat's Little Theorem.** If $\gcd(a, p) = 1$ then

$$a^{p-1} \equiv 1 \pmod{p}.$$

- **Applications:**
  1. Computing inverse modulo m.
  2. Computing powers modulo m.

Lagrange, Wilson, and Wolstenholme

- **Lagrange** A polynomial $f \in \mathbb{Z}[x]$ whose coefficients are not all divisible by p has at most $\deg(f)$ roots modulo p.
- **Wilson** $n > 1$ is prime iff $(n-1)! \equiv -1 \pmod{n}$.
- **Wolstenholme** For $p > 3$ the numerator of

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

  is divisible by p^2.
- **Proof idea:** Consider the polynomials

$$g(x) = x^{p-1} - 1, \qquad h(x) = (x-1)(x-2)\cdots(x-(p-1))$$

  and use Fermat's Little Theorem and Lagrange to deduce $g(x) - h(x) \equiv 0 \pmod{p}$. Then look at the constant and linear coefficient in $g(x) - h(x)$.

Quadratic residues

- **Definition.** $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue mod } p, \\ 0, & \text{if } p \mid a. \end{cases}$
- **Theorem.** Half of the elements in $(\mathbb{Z}/p\mathbb{Z})^*$ are quadratic residues.
- **Euler's criterion.** $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ if $\gcd(a, p) = 1$.
- **Theorem.** Legendre symbol is completely multiplicative.
- **First supplement.** $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$
- **Second supplement.** $\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$
- **Quadratic reciprocity.** $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.
- **Algorithm.** Computation of the Jacobi symbol using quadratic reciprocity, but without factoring.

Primality testing

- **Fermat test**: Choose a and check if $a^{n-1} \equiv 1 \pmod{n}$.
- **Carmichael number:** n composite such that $a^{n-1} \equiv 1 \pmod{n}$ whenever $\gcd(a, n) = 1$. **Example:** 561
- **Korselt's criterion:** n is Carmichael iff n square-free and $(p-1) \mid (n-1)$ for every prime $p \mid n$.
- **Solovay-Strassen test**: Choose a and check $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$.
- **Theorem.** There are no analogs of Carmichael numbers that can fool the Solovay-Strassen test.

The RSA cryptosystem

- **Key generation:**
  1. Choose two large primes p, q.
  2. Compute RSA modulus $N = pq$.
  3. Compute $\varphi(N) = (p-1)(q-1)$.
  4. Choose public key e with $1 < e < \varphi(N)$ and $\gcd(e, \varphi(N)) = 1$.
  5. Compute private key d with $1 < d < \varphi(N)$ and $ed \equiv 1 \pmod{\varphi(N)}$.
- **Encode** a message m as a natural number.
- **Encryption:** $c = m^e \pmod{N}$.
- **Decryption:** $m = c^d \pmod{N}$.
- **Proof that this works:** Euler-Fermat, at least if $\gcd(m, N) = 1$.
- **Important:** Long message $m > N$ has to be split into blocks $< N$.

Sums of squares

- **Fermat:** An odd prime p is a sum of two squares iff $p \equiv 1 \pmod{4}$.
- **Legendre:** A number n is a sum of three squares iff it is not of the form $4^a(8b+7)$.
- **Lagrange:** Every natural number is a sum of four squares.
- **Proof ingredients:**
  1. Euler's four square identity, so we can reduce to primes p.
  2. Show that $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ for some m.
  3. Method of infinite descent: If $m > 1$, construct a new solution such that $y_1^2 + y_2^2 + y_3^2 + y_4^2 = rp$ with $r < m$.
  4. Continue until $m = 1$.

Binary quadratic forms

- $Q(x, y) = ax^2 + bxy + cy^2$, discriminant $D = b^2 - 4ac$.
- **Lemma.** Q positive definite iff $D < 0$ and $a > 0$.
- $\mathrm{SL}_2(\mathbb{Z})$ acts on quadratic forms by $Q \circ M = M^t QM$.
- Equivalent forms have the same discriminant and represent the same numbers.
- **Theorem.** For fixed D, there are finitely many $\mathrm{SL}_2(\mathbb{Z})$-classes of quadratic forms of discriminant D.
- **Proof** using weakly reduced forms,

  $$|b| \leq |a| \leq |c|$$

  and reduction algorithm.
- **Definition**. For $D < 0$, the class number $h(D)$ is the number of $\mathrm{SL}_2(\mathbb{Z})$-classes of primitive positive definite quadratic forms of discriminant D.
- **Algorithm** to compute the class number: list all reduced forms of discriminant D.
- **Gauss composition** turns the set of eqivalence classes into a finite abelian group (GAUSS COMPOTISITION WILL NOT BE ASKED IN THE EXAM).

Pell's equation

- **Pell's equation** $x^2 - dy^2 = 1$ with $d > 0$ non-square.
- **Trivial solutions** $(x, y) = (\pm 1, 0)$.
- **Fundamental solution** $(x_1, y_1) \in \mathbb{N}^2$ with minimal $x > 1$.
- **Lagrange:** Every solution with $x > 1$ is of the form (x_n, y_n) where

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n.$$

- Solutions (x, y) yield rational approximation $\frac{x}{y}$ to $\sqrt{d}$ with

$$\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{2y^2}.$$

Continued fractions

- **Continued fraction** $[a_0, \ldots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots}}$.
- **Algorithm** to compute the expansion of a rational number.
- **Quadratic irrational** w satisfies $aw^2 + bw + c = 0$ with $a, b, c \in \mathbb{Z}$.
- **Theorem.** w quadratic irrational iff w has a periodic CFE.
- **Algorithm** to compute expansion of quadratic irrational, e.g. $\frac{1+\sqrt{5}}{2}$.
- **Theorem.** $\sqrt{d}$ has CFE of the form

$$\sqrt{d} = [a_0, \overline{a_1, \ldots, a_{n-1}, 2a_0}], \quad a_0 = \lfloor \sqrt{d} \rfloor.$$

- **Main Theorem.** Let n be minimal in $\sqrt{d}$ above.
  1. If n is even, put $\frac{x}{y} = [a_0, \ldots, a_{n-1}]$.
  2. If n is odd, put $\frac{x}{y} = [a_0, \ldots, a_{2n-1}]$.

  Then (x, y) is the fundamental solution to $x^2 - dy^2 = 1$.

Pythagorean Triples

- **Pythagorean triple:** $(a, b, c) \in \mathbb{N}^3$ with $a^2 + b^2 = c^2$.
- **Theorem.** Every primitive Pythagorean triple with odd a is of the form

  $$(m^2 - n^2, 2mn, m^2 + n^2)$$

  for unique coprime $m > n$ of different parity.

Congruent numbers

- **Congruent number** n: area of a right-angled triangle with rational side lengths.
- **Example:** $n = 6$ is congruent, the triangle has sides $(3, 4, 5)$.
- **Lemma.** n is congruent iff $d^2 n$ is congruent for every $d \in \mathbb{Q} \setminus \{0\}$.
- **Fermat:** $1, 2, 3$ are not congruent numbers.
- **Corollary:** $x^4 + y^4 = z^4$ has no non-trivial integer solutions.
- **Tunnell:** Let n be square-free, and put

$$
\begin{aligned}
A(n) &= \#\{(x, y, z) \in \mathbb{Z}^3 \,:\, 2x^2 + y^2 + 8z^2 = n\}, \\
B(n) &= \#\{(x, y, z) \in \mathbb{Z}^3 \,:\, 2x^2 + y^2 + 32z^2 = n\}, \\
C(n) &= \#\{(x, y, z) \in \mathbb{Z}^3 \,:\, 8x^2 + 2y^2 + 16z^2 = n\}, \\
D(n) &= \#\{(x, y, z) \in \mathbb{Z}^3 \,:\, 8x^2 + 2y^2 + 64z^2 = n\}.
\end{aligned}
$$

  Then:

  1. If n is an *odd* congruent number, then $A(n) = 2B(n)$.
  2. If n is an *even* congruent number, then $C(n) = 2D(n)$.

- **Example** 10 is not a congruent number.

Partitions - WILL NOT BE ASKED IN THE EXAM

- $p(n)$ counts the number of partitions of n.
- **Example:** $p(4) = 5$ since
  $4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1.$
- **Generating function:**

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{n=1}^{\infty} \frac{1}{1 - x^n}.$$

- **Euler's Pentagonal Number Theorem:**

$$\prod_{n=1}^{\infty}(1 - x^n) = \sum_{k=-\infty}^{\infty} (-1)^k x^{k(3k-1)/2}.$$

- **Recursions:**
  - $p(n) = \sum_{k=1}^{n} p(n, k)$ and $p(n, k) = p(n - 1, k - 1) + p(n - k, k)$.
  - $p(n) = \frac{1}{n} \sum_{k=1}^{n} p(n - k)\sigma(k)$ where $\sigma(k) = \sum_{d|k} d$.
  - $p(n) = \sum_{k=1}^{\infty}(-1)^{k+1} \left[p\left(n - \frac{k(3k-1)}{2}\right) + p\left(n - \frac{k(3k+1)}{2}\right)\right]$.