Public-key Cryptography
Theory and Practice

Abhijit Das

Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur

Chapter 2: Mathematical Concepts

Part 1: Number Theory

Divisibility

- **Common sets**

$$
\begin{aligned}
\mathbb{N} &= \{1, 2, 3, \ldots\} \quad \text{(Natural numbers)} \\
\mathbb{N}_0 &= \{0, 1, 2, 3, \ldots\} \quad \text{(Non-negative integers)} \\
\mathbb{Z} &= \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} \quad \text{(Integers)} \\
\mathbb{P} &= \{2, 3, 5, 7, 11, 13, \ldots\} \quad \text{(Primes)}
\end{aligned}
$$

- **Divisibility:** $a \mid b$ if $b = ac$ for some $c \in \mathbb{Z}$.
- **Corollary:** If $a \mid b$, then $|a| \leqslant |b|$.
- **Theorem:** There are infinitely many primes.
- **Euclidean division:** Let $a, b \in \mathbb{Z}$ with $b > 0$. There exist unique $q, r \in \mathbb{Z}$ with $a = qb + r$ and $0 \leqslant r < b$.
- Notations: $q = a \operatorname{quot} b$, $r = a \operatorname{rem} b$.

Greatest Common Divisor (GCD)

- Let $a, b \in \mathbb{Z}$, not both zero. Then $d \in \mathbb{N}$ is called the gcd of a and b, if:
  (1) $d \mid a$ and $d \mid b$.
  (2) If $d' \mid a$ and $d' \mid b$, then $d' \mid d$.
  We denote $d = \gcd(a, b)$.
- **Euclidean gcd:** $\gcd(a, b) = \gcd(b, a \operatorname{rem} b)$ (for $b > 0$).
- **Extended gcd:** Let $a, b \in \mathbb{Z}$, not both zero. There exist $u, v \in \mathbb{Z}$ such that
$$\gcd(a, b) = ua + vb.$$

GCD: Example

$$\begin{aligned} 899 &= 2 \times 319 + 261, \\ 319 &= 1 \times 261 + 58, \\ 261 &= 4 \times 58 + 29, \\ 58 &= 2 \times 29. \end{aligned}$$

Therefore, $\gcd(899, 319) = \gcd(319, 261) = \gcd(261, 58) = \gcd(58, 29) = \gcd(29, 0) = 29$

Extended gcd computation

$$\begin{aligned} 29 &= 261 - 4 \times 58 \\ &= 261 - 4 \times (319 - 1 \times 261) = (-4) \times 319 + 5 \times 261 \\ &= (-4) \times 319 + 5 \times (899 - 2 \times 319) \\ &= 5 \times 899 + (-14) \times 319. \end{aligned}$$

Congruence

- Let $n \in \mathbb{N}$. Two integers a, b are called **congruent** modulo n, denoted $a \equiv b \pmod{n}$, if $n \mid (a - b)$ or equivalently if $a \operatorname{rem} n = b \operatorname{rem} n$.
- **Properties of congruence**
  - Congruence is an equivalence relation on $\mathbb{Z}$.
  - If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.
  - If $a \equiv b \pmod{n}$ and $d \mid n$, then $a \equiv b \pmod{d}$.
  - **Cancellation**
    $ab \equiv ac \pmod{n}$ if and only if $b \equiv c \pmod{n / \gcd(a, n)}$.

Congruence (contd.)

- $\mathbb{Z}_n =$ The set of equivalence classes of the relation "congruence modulo n".
- **Complete residue system:** A collection of n integers, with exactly one from each equivalence class.
- Most common representation: $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.
- Arithmetic of $\mathbb{Z}_n$: Integer arithmetic modulo n.
- **Modular inverse:** $a \in \mathbb{Z}_n$ is called **invertible** modulo n if $ua \equiv 1 \pmod{n}$ for some $u \in \mathbb{Z}_n$.
- **Theorem:** $a \in \mathbb{Z}_n$ is invertible modulo n if and only if $\gcd(a, n) = 1$. In this case, extended gcd gives $ua + vn = 1$. Then, $u \equiv a^{-1} \pmod{n}$.

Euler Totient Function

- Let $n \in \mathbb{N}$. Define

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}.$$

  Thus, $\mathbb{Z}_n^*$ is the set of all elements of $\mathbb{Z}_n$ that are invertible modulo n.
- Call $\phi(n) = |\mathbb{Z}_n^*|$.
- **Example:** If p is a prime, then $\phi(p) = p - 1$.
- **Example:** $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. We have $\gcd(0, 6) = 6$, $\gcd(1, 6) = 1$, $\gcd(2, 6) = 2$, $\gcd(3, 6) = 3$, $\gcd(4, 6) = 2$, and $\gcd(5, 6) = 1$. So $\mathbb{Z}_6^* = \{1, 5\}$, that is, $\phi(6) = 2$.

Euler Totient Function (contd.)

- **Theorem:** Let $n = p_1^{e_1} \cdots p_r^{e_r}$ with distinct primes $p_i \in \mathbb{P}$ and with $e_i \in \mathbb{N}$. Then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

- **Fermat's little theorem:** Let $p \in \mathbb{P}$ and $a \in \mathbb{Z}$ with $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.
- **Euler's theorem:** Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Linear Congruences

- Let $d = \gcd(a, n)$. The congruence $ax \equiv b \pmod{n}$ is solvable if and only if $d \mid b$. In that case, there are exactly d solutions modulo n.
- **Chinese remainder theorem (CRT)**
  For pairwise coprime moduli $n_1, n_2, \ldots, n_r$ with product $N = n_1 n_2 \cdots n_r$, the congruences

  $$x \equiv a_1 \pmod{n_1},\ x \equiv a_2 \pmod{n_2},\ \ldots,\ x \equiv a_r \pmod{n_r},$$

  have a simultaneous solution unique modulo N.

  Let $N_i = N/n_i$ and $v_i \equiv N_i^{-1} \pmod{n_i}$. The simultaneous solution is given by

  $$x \equiv a_i v_i N_i \pmod{N}.$$

CRT: Example

- Solve the following congruences simultaneously:

$$x \equiv 1 \pmod{5}, \quad x \equiv 5 \pmod{6}, \quad x \equiv 3 \pmod{7}.$$

- $n_1 = 5$, $n_2 = 6$ and $n_3 = 7$, so $N = n_1 n_2 n_3 = 210$.
  $a_1 = 1$, $a_2 = 5$ and $a_3 = 3$.
- $N_1 = n_2 n_3 = 42$, $N_2 = n_1 n_3 = 35$, and $N_3 = n_1 n_2 = 30$.
- $v_1 \equiv N_1^{-1} \equiv 42^{-1} \equiv 2^{-1} \equiv 3 \pmod{5}$.
  $v_2 \equiv N_2^{-1} \equiv 35^{-1} \equiv 5^{-1} \equiv 5 \pmod{6}$.
  $v_3 \equiv N_3^{-1} \equiv 30^{-1} \equiv 2^{-1} \equiv 4 \pmod{7}$.
- The simultaneous solution is

$$\begin{aligned} x &\equiv a_1 v_1 N_1 + a_2 v_2 N_2 + a_3 v_3 N_3 \\ &\equiv 126 + 875 + 360 \equiv 1361 \equiv 101 \pmod{210}. \end{aligned}$$

Polynomial Congruences

- Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree $d \geqslant 2$.
  To solve: $f(x) \equiv 0 \pmod{n}$.
  Let $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ be the prime factorization of n.
- Solve $f(x) \equiv 0 \pmod{p_i^{e_i}}$ for all i.
  Combine the solutions by CRT.
- How to solve $f(x) \equiv 0 \pmod{p^e}$ for $p \in \mathbb{P}$, $e \in \mathbb{N}$?
- Solve $f(x) \equiv 0 \pmod{p}$.
- **Hensel lifting**
  Let $x \equiv \xi \pmod{p^r}$ be a solution of $f(x) \equiv 0 \pmod{p^r}$.
  All solutions of $f(x) \equiv 0 \pmod{p^{r+1}}$ are given by
  $$x \equiv \xi + kp^r \pmod{p^{r+1}},$$
  where
  $$f'(\xi)k \equiv -\frac{f(\xi)}{p^r} \pmod{p}.$$

Multiplicative Order

- Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}_n^*$. Define $\operatorname{ord}_n a$ to be the smallest of the *positive* integers h for which $a^h \equiv 1 \pmod{n}$.
- **Example:** $n = 17$, $a = 2$. $a^1 \equiv 2 \pmod{n}$, $a^2 \equiv 4 \pmod{n}$, $a^3 \equiv 8 \pmod{n}$, $a^4 \equiv 16 \pmod{n}$, $a^5 \equiv 15 \pmod{n}$, $a^6 \equiv 13 \pmod{n}$, $a^7 \equiv 9 \pmod{n}$, and $a^8 \equiv 1 \pmod{n}$. So $\operatorname{ord}_{17} 2 = 8$.
- **Theorem:** $a^k \equiv 1 \pmod{n}$ if and only if $\operatorname{ord}_n a \mid k$.
- **Theorem:** Let $h = \operatorname{ord}_n a$. Then, $\operatorname{ord}_n a^k = h / \gcd(h, k)$.
- **Theorem:** $\operatorname{ord}_n a \mid \phi(n)$.

Primitive Root

- If $\operatorname{ord}_n a = \phi(n)$, then a is called a primitive root modulo n.
- **Theorem (Gauss):** An integer $n > 1$ has a primitive root if and only if $n = 2, 4, p^e, 2p^e$, where p is an odd prime and $e \in \mathbb{N}$.
- **Example:** 3 is a primitive root modulo the prime $n = 17$:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$3^k \pmod{17}$	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Primitive Root (contd.)

- **Example:** $n = 2 \times 3^2 = 18$ has a primitive root 5 with order $\phi(18) = 6$:

k	0	1	2	3	4	5	6
$5^k \pmod{18}$	1	5	7	17	13	11	1

- **Example:** $n = 20 = 2^2 \times 5$ does not have a primitive root. We have $\phi(20) = 8$, and the orders of the elements of $\mathbb{Z}_{20}^*$ are $\operatorname{ord}_{20} 1 = 1$, $\operatorname{ord}_{20} 3 = \operatorname{ord}_{20} 7 = \operatorname{ord}_{20} 13 = \operatorname{ord}_{20} 17 = 4$, and $\operatorname{ord}_{20} 9 = \operatorname{ord}_{20} 19 = 2$.

Quadratic Residues

- Quadratic congruence: $ux^2 + vx + w \equiv 0 \pmod{n}$.
- By CRT and Hensel lifting, it suffices to take $n = p \in \mathbb{P}$.
- Assume that $p \neq 2$, that is, p is odd.
- Reduce the congruence to $x^2 \equiv a \pmod{p}$.
- Let $a \in \mathbb{Z}_p^*$ (that is, $a \not\equiv 0 \pmod{p}$).
- a is called a **quadratic residue** modulo p
  if $x^2 \equiv a \pmod{p}$ is solvable.
  a is called a **quadratic non-residue** modulo p
  if $x^2 \equiv a \pmod{p}$ is not solvable.
- There are $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic non-residues modulo p.
- **Example:** Take $p = 11$. The quadratic residues are $1, 3, 4, 5, 9$ and the non-residues are $2, 6, 7, 8, 10$.

Legendre Symbol

- Let p be an odd prime. Define

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

- **Properties**
  - $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
  - $\left(\frac{1}{p}\right) = 1$, $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.
  - **Euler's criterion:** $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.
  - **Law of quadratic reciprocity:** For two odd primes p, q, we have $\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right)$.

Jacobi Symbol

Let $n = p_1 p_2 \cdots p_t$ be an odd positive integer.
Here, p_i are prime (not necessarily all distinct).

Define $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_t}\right)$.

- The Jacobi symbol is an extension of the Legendre symbol.
- The Jacobi symbol loses direct relationship with quadratic residues. For example, $\left(\frac{2}{9}\right) = \left(\frac{2}{3}\right)^2 = (-1)^2 = 1$, but the congruence $x^2 \equiv 2 \pmod{9}$ has no solutions.
- The Jacobi symbol satisfies the law of quadratic reciprocity: $\left(\frac{a}{b}\right) = (-1)^{(a-1)(b-1)/4}\left(\frac{b}{a}\right)$ for two odd integers a, b.
- The Jacobi symbol leads to an efficient algorithm for the computation of the Legendre symbol.

Topics From Analytic Number Theory

- **The prime number theorem (PNT)**

  Let x be a positive real number, and $\pi(x)$ the number of primes $\leqslant x$. Then, $\pi(x) \to x/\ln x$ as $x \to \infty$.

- **Density of smooth integers**

  Let x, y be positive real numbers with $x > y$, $u = \ln x/\ln y$, and $\psi(x, y)$ the fraction of positive integers $\leqslant x$ with all prime factors $\leqslant y$. For $u \to \infty$ and $y \geqslant \ln^2 x$, we have $\psi(x, y) \to u^{-u+o(u)} = e^{-[(1+o(1))u \ln u]}$.

Part 2: Algebra

Groups

A **group** $(G, \diamond)$ is a set G with a binary operation $\diamond$, having the following properties.

- $\diamond$ is associative:
  $a \diamond (b \diamond c) = (a \diamond b) \diamond c$ for all $a, b, c \in G$.
- Existence of an identity element:
  There exists $e \in G$ such that $a \diamond e = e \diamond a = a$ for all $a \in G$.
- Existence of inverse:
  For all $a \in G$, there exists $b \in G$ with $a \diamond b = b \diamond a = e$.

A group $G = (G, \diamond)$ is called **Abelian** or **commutative**, if $\diamond$ is commutative, that is, $a \diamond b = b \diamond a$ for all $a, b \in G$.

Examples

- $\mathbb{Z}$ under integer addition
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ under addition
- $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ under multiplication
- $\mathbb{Z}_n$ under addition modulo n
- $\mathbb{Z}_n^*$ under multiplication modulo n
- The set of all $m \times n$ real matrices under matrix addition
- The set of all $n \times n$ invertible real matrices under matrix multiplication. This group is called the **general linear group** GL_n and is not Abelian.
- The set of all bijective function $f : S \to S$ (for any set S) under composition of functions. This group is not Abelian, in general.

Subgroups

Let $(G, \diamond)$ be a group and $H \subseteq G$.

- H is called a **subgroup** of G if $(H, \diamond)$ is a group.
- **Theorem:** H is a subgroup of G if and only if H is closed under the group operation and the inverse.
- **Theorem:** If G is finite, then H is a subgroup of G if and only if H is closed under the group operation.
- **Lagrange's Theorem:** If G is a finite group and H a subgroup of G, then $|H|$ divides $|G|$.
- **Examples**
  - $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{R}, +)$.
  - $(\mathbb{Q}^*, \times)$ is a subgroup of $(\mathbb{C}^*, \times)$.
  - The set of all $n \times n$ real matrices of determinant 1 is a subgroup of GL_n.

Homomorphisms of Groups

Let $(G, \diamond)$ and $(G', \diamond')$ be groups and $f : G \to G'$ a function.

- f is a called a **homomorphism** if $f(a \diamond b) = f(a) \diamond' f(b)$ for all $a, b \in G$.
- A bijective homomorphism f is called an **isomorphism**, denoted $G \cong G'$. In this case, $f^{-1} : G' \to G$ is again a homomorphism.
- An isomorphism $G \to G$ is called an **automorphism**.
- **Examples**
  - The map $z \mapsto \bar{z}$ (complex conjugation) is an automorphism of both $(\mathbb{C}, +)$ and $(\mathbb{C}^*, \times)$.
  - The map $\mathbb{Z} \to \mathbb{Z}_n$ taking $a \mapsto a \operatorname{rem} n$ is a homomorphism.
  - Let $\gcd(a, n) = 1$. The map $\mathbb{Z}_n^* \to \mathbb{Z}_n^*$ taking $x \mapsto ax \operatorname{rem} n$ is an automorphism of $\mathbb{Z}_n^*$.

Cyclic Groups

Let $G = (G, \cdot)$ be a multiplicative group.

- If there exists $g \in G$ such that every $a \in G$ can be written as $a = g^r$ for some $r \in \mathbb{Z}$, then G is called a **cyclic group**, and g is called a **generator** of G.
- If G is a finite cyclic group of size n, then every element of G can be written as g^r for a unique $r \in \{0, 1, 2, \ldots, r-1\}$.
- **Theorem:** Every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$. Every finite cyclic group is isomorphic to $(\mathbb{Z}_n, +)$ for some n.
- **Theorem:** Every subgroup of a cyclic group is again cyclic.
- **Theorem:** Let G be a finite cyclic group, and H a subgroup of size m. An element $a \in G$ belongs to H if and only if $a^m = e$.

Cyclic Groups (contd.)

Let $(G, \cdot)$ be a finite cyclic group of size n. Let $a \in G$.

- The **subgroup generated by** a is the set $\{a^r \mid r = 0, 1, 2, \ldots, m-1\}$, where m is the smallest positive integer with the property that $a^m = e$.
- m is called the **order** of a, denoted $\mathrm{ord}(a)$.
- By Lagrange's theorem, $m \mid n$.
- a is a generator of G if $m = n$.
- G contains exactly $\phi(n)$ generators.

Examples

- $\mathbb{Z}_n^*$ (under modular multiplication) is cyclic if and only if n is 2, 4, p^e or $2p^e$ for an odd prime p and for $e \in \mathbb{N}$.
- In particular, $\mathbb{Z}_p^*$ is cyclic for every $p \in \mathbb{P}$.
- The number of generators of $\mathbb{Z}_p^*$ is $\phi(p-1)$.

Rings

A **ring** $(R, +, \cdot)$ (commutative with identity) is a set R with two binary operations $+$ and $\cdot$, having the properties:

- $(R, +)$ is an Abelian group.
- $\cdot$ is associative:
  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$.
- $\cdot$ is commutative:
  $a \cdot b = b \cdot a$ for all $a, b \in R$.
- Existence of multiplicative identity:
  There exists an element $1 \in R$ such that $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.
- $\cdot$ is distributive over $+$:
  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ for all $a, b, c \in R$.

Integral Domains and Fields

Let $(R, +, \cdot)$ be a ring.

- If $0 = 1$ in R, then $R = \{0\}$ (the **zero ring**).
- Let $a \in R$. If there exists a non-zero $b \in R$ with $ab = 0$, then a is called a **zero divisor**.
- R is called an **integral domain** if R is not the zero ring and R contains no non-zero zero divisors.
- An element $a \in R$ is called a **unit**, if there exists $b \in R$ with $ab = ba = 1$. The set of all units of R is a multiplicative group denoted R^*.
- R Is called a **field**, if R is not the zero ring, and every non-zero element of R is a unit ($R^* = R \setminus \{0\}$).
- **Theorem:** Every field is an integral domain.
- **Theorem:** Every finite integral domain is a field.

Rings: Examples

- $\mathbb{Z}$ is an integral domain, but not a field.
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.
- $\mathbb{Z}_n$ is a ring.
- $\mathbb{Z}_n$ is an integral domain (equivalently a field) if and only if n is prime.
- Let R be a ring. The set $R[x]$ of all polynomials in one variable x and with coefficients from R is a ring. Likewise, the set $R[x_1, x_2, \ldots, x_n]$ of all n-variable polynomials with coefficients from R is a ring.
- If R is an integral domain, then so also are $R[x]$ and $R[x_1, x_2, \ldots, x_n]$.
- $R[x]$ is not a field (even if R is a field).

Characteristics of Rings

Let $R = (R, +, \cdot)$ be a ring.

- The **characteristic** of R, denoted $\operatorname{char} R$, is the smallest positive integer m such that $1 + 1 + \cdots + 1$ (m times) $= 0$.
- If no such integer exists, we say $\operatorname{char} R = 0$.
- **Examples**
  - The characteristic of $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$ or $\mathbb{C}$ is 0.
  - The characteristic of $\mathbb{Z}_n$ is n.
  - Let a field F have positive characteristic p. Then, p is prime.

Homomorphisms of Rings

Let R and S be rings, and $f : R \to S$ a function.

- f is called a **homomorphism** if the following conditions are satisfied:

  $f(a+b) = f(a) + f(b)$ for every $a, b \in R$,
  $f(ab) = f(a)f(b)$ for every $a, b \in R$, and
  $f(1_R) = 1_S$.

- A bijective homomorphism $f : R \to S$ is called an **isomorphism**. In that case, $f^{-1} : S \to R$ is again a homomorphism.
- An **automorphism** of R is an isomorphism $f : R \to R$.
- **Examples**
  - Complex conjugation ($z \mapsto \bar{z}$) is an automorphism of $\mathbb{C}$.
  - The map $\mathbb{Z} \to \mathbb{Z}_n$ taking $a \mapsto a \operatorname{rem} n$ is a homomorphism.
  - A homomorphism $\mathbb{Z}_m \to \mathbb{Z}_n$ exists if and only if $n \mid m$.

Polynomials

Let K be a field, and $K[x]$ the polynomial ring over K.

- **Euclidean division:** Let $f(x), g(x) \in K[x]$ with $g(x) \neq 0$. There exist polynomials $q(x), r(x) \in K[x]$ such that
  $f(x) = q(x)g(x) + r(x)$, and
  $r(x) = 0$ or $\deg r(x) < \deg g(x)$.
- We denote $q(x) = f(x) \operatorname{quot} g(x)$ and $r(x) = f(x) \operatorname{rem} g(x)$.
- For $f(x), g(x) \in K[x]$, not both zero, the monic polynomial $d(x)$ of the largest degree with $d(x) \mid f(x)$ and $d(x) \mid g(x)$ is called the **gcd** of $f(x)$ and $g(x)$.
- **Euclidean gcd:** $\gcd(f(x), g(x)) = \gcd(g(x), f(x) \operatorname{rem} g(x))$.
- **Extended gcd:** There exist $u(x), v(x) \in K[x]$ such that $\gcd(f(x), g(x)) = u(x)f(x) + v(x)g(x)$. We can choose $u(x), v(x)$ to satisfy $\deg u(x) < \deg g(x)$ and $\deg v(x) < \deg f(x)$.

Algebraic Elements

Let $K \subseteq L$ be an extension of fields.

- An element $\alpha \in L$ is called **algebraic** over K if $f(\alpha) = 0$ for some non-constant $f(x) \in K[x]$.
- A non-algebraic element is called **transcendental**.
- L is called an **algebraic extension** of K if every element of L is algebraic over K.
- **Examples**
  - The element $\alpha = \sqrt[5]{3 + \sqrt{-2}} \in \mathbb{C}$ is algebraic over $\mathbb{Q}$, since $(\alpha^5 - 3)^2 + 2 = 0$.
  - e and π are transcendental over $\mathbb{Q}$.
  - $\mathbb{C}$ is an algebraic extension of $\mathbb{R}$.
  - $\mathbb{C}$ is not an algebraic extension of $\mathbb{Q}$.

Minimal Polynomials

Let $K \subseteq L$ be a field extension, and $\alpha \in L$ algebraic over K.

- The non-constant polynomial $f(x) \in K[x]$ with the smallest degree, such that $f(\alpha) = 0$, is called the **minimal polynomial** of α over K, denoted $\mathrm{minpoly}_{\alpha,K}(x)$.
- $\mathrm{minpoly}_{\alpha,K}(x)$ is an irreducible polynomial of $K[x]$.
- Let $f(x) \in K[x]$. Then, $f(\alpha) = 0$ if and only if $\mathrm{minpoly}_{\alpha,K}(x) \mid f(x)$.
- The roots of $\mathrm{minpoly}_{\alpha,K}(x)$ are called **conjugates** of α (over K).

Field Extensions

Let K be a field, and $f(x) \in K[x]$ be irreducible.

- Let α be a root of $f(x)$.
- Define the set

$$\begin{aligned} K(\alpha) &= \{g(\alpha) \mid g(x) \in K[x]\} \\ &= \{g(\alpha) \mid g(x) \in K[x],\ \deg g(x) < \deg f(x)\}. \end{aligned}$$

- $K(\alpha)$ is a field.
- $K(\alpha)$ is the smallest field that contains K and α.
- **Examples**
  - $\mathbb{C} = \mathbb{R}(\mathrm{i})$ with $\mathrm{minpoly}_{\mathrm{i},\mathbb{R}}(x) = x^2 + 1 \in \mathbb{R}[x]$.
  - $\mathbb{Q}(\mathrm{i}) = \{a + \mathrm{i}b \mid a, b \in \mathbb{Q}\}$ is a proper subfield of $\mathbb{C}$, obtained by adjoining a root of $x^2 + 1$ to $\mathbb{Q}$.
  - $\mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Q}\}$ is an extension of $\mathbb{Q}$, obtained by adjoining a root of $x^3 - 2 \in \mathbb{Q}[x]$.

Finite Fields

- A **finite field** K is a field with $|K|$ finite.
- Simplest examples: $\mathbb{Z}_p$ for $p \in \mathbb{P}$.
- There are other finite fields.
- Let K be a finite field with $|K| = q$.
- K contains a subfield $\mathbb{Z}_p$ for some $p \in \mathbb{P}$.
- $q = p^n$ for some $n \in \mathbb{N}$.
- Any two finite fields of the same size are isomorphic.
- $\mathbb{F}_q =$ The finite field of size q.
- **Prime fields:** $\mathbb{F}_p = \mathbb{Z}_p$ for $p \in \mathbb{P}$.
- **Extension fields:** $\mathbb{F}_{p^n} \neq \mathbb{Z}_{p^n}$ (as rings) for $p \in \mathbb{P}$ and $n \geqslant 2$.

Properties of Finite Fields

- **Fermat's little theorem:**
  $\alpha^{q-1} = 1$ for every $\alpha \in \mathbb{F}_q^*$.
  $\beta^q = \beta$ for every $\beta \in \mathbb{F}_q$.
- The multiplicative group $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ is cyclic.
- There are $\phi(q-1)$ generators of $\mathbb{F}_q^*$.
- Let $\mathbb{F}_q \subseteq \mathbb{F}_{q^m}$ be an extension of finite fields, and d a positive integral divisor of m. Then, there exists a unique intermediate field $\mathbb{F}_{q^d}$ ($\mathbb{F}_q \subseteq \mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^m}$).
- The polynomial $X^{q^r} - X$ is the product of all monic irreducible polynomials of $\mathbb{F}_q[x]$ of degrees dividing r.

Representation of Extension Fields

To represent the finite field $\mathbb{F}_{p^n}$, $n \geqslant 2$.

- For every $p \in \mathbb{P}$ and $n \in \mathbb{N}$, there exists (at least) one irreducible polynomial in $\mathbb{F}_p[x]$ of degree n.
- Let $f(x) \in \mathbb{F}_p[x]$ be irreducible of degree n.
- Let θ be a root of $f(x)$. Since $f(x)$ is irreducible, $\theta \notin \mathbb{F}_p$.
- One can represent $\mathbb{F}_{p^n} = \mathbb{F}_p(\theta) = \{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \mid a_i \in \mathbb{F}_p\}$.
- This is called the **polynomial basis representation** of $\mathbb{F}_{p^n}$, because the elements of $\mathbb{F}_{p^n}$ are $\mathbb{F}_p$-linear combinations of the basis elements $1, \theta, \theta^2, \ldots, \theta^{n-1}$.
- The irreducible polynomial $f(x)$ Is called the **defining polynomial** for this representation.

Arithmetic in Extension Fields

Let $\mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$ with $f(\theta) = 0$.
Let $\alpha = a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1}$ and
$\beta = b_0 + b_1\theta + b_2\theta^2 + \cdots + b_{n-1}\theta^{n-1}$ be two elements of $\mathbb{F}_q$.

- **Addition:** $\alpha + \beta = (a_0 + b_0) + (a_1 + b_1)\theta + (a_2 + b_2)\theta^2 + \cdots + (a_{n-1} + b_{n-1})\theta^{n-1}$, where each $a_i + b_i$ is the addition of $\mathbb{F}_p$ (arithmetic modulo p).
- **Subtraction:** Similar to addition.
- **Multiplication:** Multiply $\alpha(x)$ and $\beta(x)$ as polynomials over $\mathbb{F}_p$. Compute remainder $\rho(x)$ of Euclidean division of this product by $f(x)$. The coefficient arithmetic is that of $\mathbb{F}_p$. Take $\rho = \rho(\alpha) = \alpha\beta$.
- **Inverse:** If $\alpha \neq 0$, then $\gcd(\alpha(x), f(x)) = 1 = u(x)\alpha(x) + v(x)f(x)$ (extended gcd). So $u(\theta)\alpha(\theta) = 1$, that is, $\alpha^{-1} = u(\theta)$.

Arithmetic in $\mathbb{F}_8$

Define $\mathbb{F}_8 = \mathbb{F}_2(\theta)$, where $\theta^3 + \theta + 1 = 0$.

$\mathbb{F}_8 = \{0, 1, \theta, \theta + 1, \theta^2, \theta^2 + 1, \theta^2 + \theta, \theta^2 + \theta + 1\}$.

Take $\alpha = \theta + 1$ and $\beta = \theta^2 + \theta$.

- $\alpha + \beta = \theta^2 + 1$.
- In a field of characteristic 2, we have $-1 = 1$, that is, subtraction is the same as addition.
- $\alpha\beta = (\theta + 1)(\theta^2 + \theta) = \theta^3 + \theta = (\theta^3 + \theta + 1) + 1 = 1$.
- $(\theta + 1)(\theta^2 + \theta) + (\theta^3 + \theta + 1) = 1$, that is, $\alpha^{-1} = \theta^2 + \theta = \beta$.

Arithmetic in $\mathbb{F}_9$

Define $\mathbb{F}_9 = \mathbb{F}_3(\psi)$, where $\psi^2 + 1 = 0$.

$\mathbb{F}_9 = \{0, 1, 2, \psi, \psi + 1, \psi + 2, 2\psi, 2\psi + 1, 2\psi + 2\}$.

Take $\alpha = \psi + 1$ and $\beta = 2\psi + 1$.

- $\alpha + \beta = 3\psi + 2 = 2$.
- $\alpha - \beta = -\psi = 2\psi$.
- $\alpha\beta = (\psi + 1)(2\psi + 1) = 2\psi^2 + 1 = 2(\psi^2 + 1) + 2 = 2$.
- $(\psi + 1)(\psi + 2) + 2(\psi^2 + 1) = 1$, so $\alpha^{-1} = \psi + 2$.

Normal basis representation

Let $\mathbb{F}_q = \mathbb{F}_{p^n} = \mathbb{F}_p(\theta)$ with $f(\theta) = 0$.

- $f(x) = (x - \theta)(x - \theta^p)(x - \theta^{p^2}) \cdots (x - \theta^{p^{n-1}})$.
- The conjugates of θ are $\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}}$. They are all in $\mathbb{F}_q$.
- Suppose that $\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}}$ are linearly independent over $\mathbb{F}_p$, Then, θ is called a **normal element** and $f(x)$ is called a **normal polynomial**.
- The elements $\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}}$ constitute a **normal basis** of $\mathbb{F}_q$ over $\mathbb{F}_p$.
- Every element in $\mathbb{F}_q$ can be represented uniquely as $a_0\theta + a_1\theta^p + a_2\theta^2 + \cdots + a_{n-1}\theta^{p^{n-1}}$ with each $a_i \in \mathbb{F}_p$.
- Normal basis representation often speeds up exponentiation in $\mathbb{F}_q$.

Part 3: Elliptic Curves

The Weierstrass Equation

Let K be a field.

An **elliptic curve** E over K is defined by the equation:

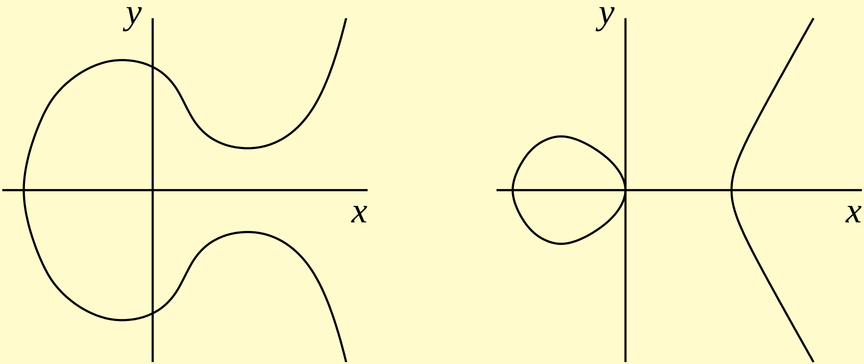
$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in K.$$

The curve should be **smooth** (no singularities).

Special forms

- $\operatorname{char} K \neq 2, 3$: $y^2 = x^3 + ax + b,\ a, b \in K$.
- $\operatorname{char} K \neq 2$: $y^2 = x^3 + b_2x^2 + b_4x + b_6,\ b_i \in K$.
- $\operatorname{char} K = 2$:
  Non-supersingular curve: $y^2 + xy = x^3 + ax^2 + b,\ a, b \in K$.
  Supersingular curve: $y^2 + ay = x^3 + bx + c,\ a, b, c \in K$.

Elliptic Curves Over $\mathbb{R}$: Example



(a) $y^2 = x^3 - x + 1$ (b) $y^2 = x^3 - x$

The Elliptic Curve Group

Any $(x, y) \in K^2$ satisfying the equation of an elliptic curve E is called a K**-rational point** on E.

Point at infinity:

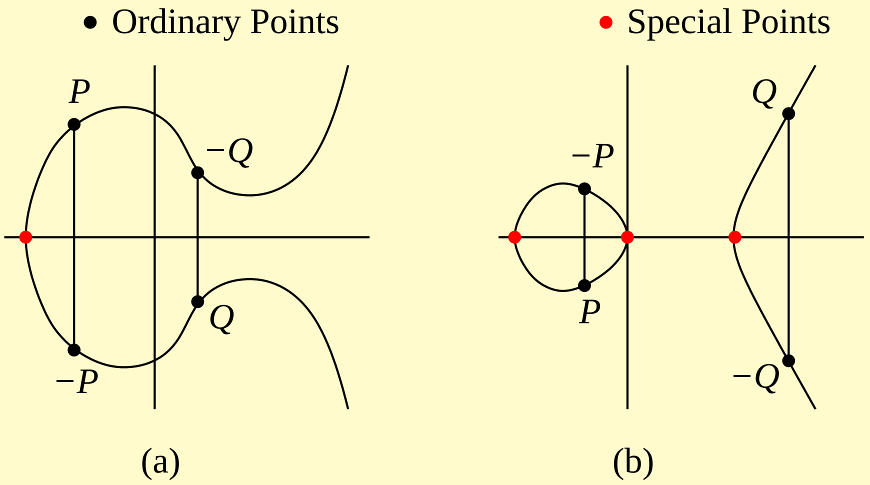
- There is a single point at infinity on E, denoted by $\mathcal{O}$.
- This point cannot be visualized in the two-dimensional (x, y) plane.
- The point exists in the projective plane.

$E(K)$ is the set of all finite K-rational points on E and the point at infinity.

An additive group structure can be defined on $E(K)$.

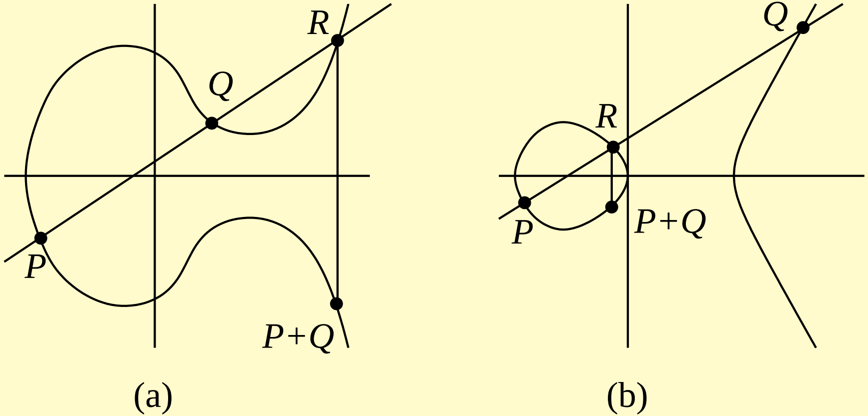
$\mathcal{O}$ acts as the identity of the group.

The Opposite of a Point



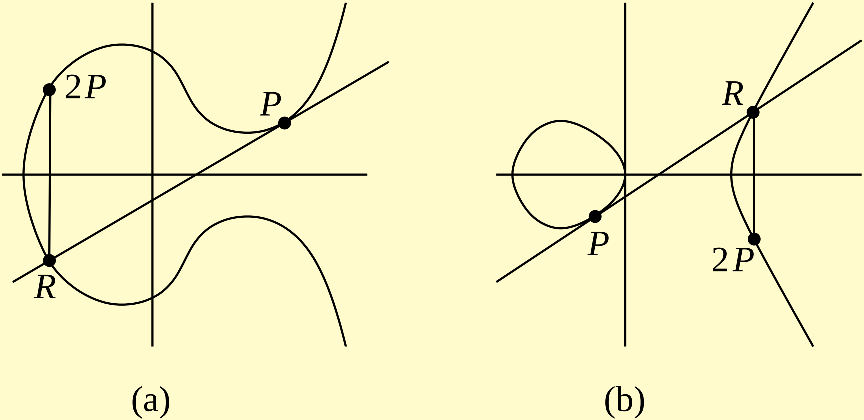
Addition of Two Points

Chord and tangent rule



Doubling of a Point

Chord and tangent rule



Addition and Doubling Formulas

Let $P = (h_1, k_1)$ and $Q = (h_2, k_2)$ be finite points.
Assume that $P + Q \neq \mathcal{O}$ and $2P \neq \mathcal{O}$.
Let $P + Q = (h_3, k_3)$ (Note that $P + Q = 2P$ if $P = Q$).

$E : y^2 = x^3 + ax + b$

$$
\begin{aligned}
-P &= (h_1, -k_1) \\
h_3 &= \lambda^2 - h_1 - h_2 \\
k_3 &= \lambda(h_1 - h_3) - k_1, \text{ where} \\
\lambda &= \begin{cases} \dfrac{k_2 - k_1}{h_2 - h_1}, & \text{if } P \neq Q, \\[2ex] \dfrac{3h_1^2 + a}{2k_1}, & \text{if } P = Q. \end{cases}
\end{aligned}
$$

Addition and Doubling in Non-supersingular Curves

$E : y^2 + xy = x^3 + ax^2 + b$ (with $\operatorname{char} K = 2$).

$$
\begin{aligned}
-P &= (h_1, k_1 + h_1),\\
h_3 &= \begin{cases} \left(\dfrac{k_1+k_2}{h_1+h_2}\right)^2 + \dfrac{k_1+k_2}{h_1+h_2} + h_1 + h_2 + a, & \text{if } P \neq Q,\\[2ex] h_1^2 + \dfrac{b}{h_1^2}, & \text{if } P = Q,\end{cases}\\
k_3 &= \begin{cases} \left(\dfrac{k_1+k_2}{h_1+h_2}\right)(h_1 + h_3) + h_3 + k_1, & \text{if } P \neq Q,\\[2ex] h_1^2 + \left(h_1 + \dfrac{k_1}{h_1} + 1\right) h_3, & \text{if } P = Q.\end{cases}
\end{aligned}
$$

Addition and Doubling in Supersingular Curves

$$E : y^2 + ay = x^3 + bx + c \text{ (with } \operatorname{char} K = 2\text{).}$$

$$\begin{aligned}
-P &= (h_1, k_1 + a), \\
h_3 &= \begin{cases} \left(\dfrac{k_1 + k_2}{h_1 + h_2}\right)^2 + h_1 + h_2, & \text{if } P \neq Q, \\[2ex] \dfrac{h_1^4 + b^2}{a^2}, & \text{if } P = Q, \end{cases} \\
k_3 &= \begin{cases} \left(\dfrac{k_1 + k_2}{h_1 + h_2}\right)(h_1 + h_3) + k_1 + a, & \text{if } P \neq Q, \\[2ex] \left(\dfrac{h_1^2 + b}{a}\right)(h_1 + h_3) + k_1 + a, & \text{if } P = Q. \end{cases}
\end{aligned}$$

Elliptic Curves Over Finite Fields

Example 1

Take $K = \mathbb{F}_7$ and $E_1 : y^2 = x^3 + x + 3$.

There are six points in $E_1(\mathbb{F}_7)$: $P_0 = \mathcal{O}$, $P_1 = (4,1)$, $P_2 = (4,6)$, $P_3 = (5,0)$, $P_4 = (6,1)$ and $P_5 = (6,6)$.

Multiples of these points

P	$2P$	$3P$	$4P$	$5P$	$6P$	ord P
$P_0 = \mathcal{O}$						1
$P_1 = (4,1)$	$(6,6)$	$(5,0)$	$(6,1)$	$(4,6)$	$\mathcal{O}$	6
$P_2 = (4,6)$	$(6,1)$	$(5,0)$	$(6,6)$	$(4,1)$	$\mathcal{O}$	6
$P_3 = (5,0)$	$\mathcal{O}$					2
$P_4 = (6,1)$	$(6,6)$	$\mathcal{O}$				3
$P_5 = (6,6)$	$(6,1)$	$\mathcal{O}$				3

Elliptic Curves Over Finite Fields

Example 2

Represent $\mathbb{F}_8 = \mathbb{F}_2(\xi)$, where $\xi^3 + \xi + 1 = 0$.

Consider the non-supersingular curve
$E_2 : y^2 + xy = x^3 + x^2 + \xi$ over $\mathbb{F}_8$.

There are ten points in $E_2(\mathbb{F}_8)$:

$$
\begin{array}{lcllcl}
P_0 & = & \mathcal{O}, & P_5 & = & (\xi, \xi^2 + \xi), \\
P_1 & = & (0, \xi^2 + \xi), & P_6 & = & (\xi + 1, \xi^2 + 1), \\
P_2 & = & (1, \xi^2), & P_7 & = & (\xi + 1, \xi^2 + \xi), \\
P_3 & = & (1, \xi^2 + 1), & P_8 & = & (\xi^2 + \xi, 1), \\
P_4 & = & (\xi, \xi^2), & P_9 & = & (\xi^2 + \xi, \xi^2 + \xi + 1).
\end{array}
$$

Elliptic Curves Over Finite Fields

Example 2 (contd.)

P	$2P$	$3P$	$4P$	$5P$	$6P$	$7P$	$8P$	$9P$	$10P$	$\operatorname{ord} P$
P_0										1
P_1	$\mathcal{O}$									2
P_2	P_7	P_6	P_3	$\mathcal{O}$						5
P_3	P_6	P_7	P_2	$\mathcal{O}$						5
P_4	P_3	P_9	P_6	P_1	P_7	P_8	P_2	P_5	$\mathcal{O}$	10
P_5	P_2	P_8	P_7	P_1	P_6	P_9	P_3	P_4	$\mathcal{O}$	10
P_6	P_2	P_3	P_7	$\mathcal{O}$						5
P_7	P_3	P_2	P_6	$\mathcal{O}$						5
P_8	P_6	P_4	P_2	P_1	P_3	P_5	P_7	P_9	$\mathcal{O}$	10
P_9	P_7	P_5	P_3	P_1	P_2	P_4	P_6	P_8	$\mathcal{O}$	10

Size of the Elliptic Curve Group

Let E be an elliptic curve defined over $\mathbb{F}_q = \mathbb{F}_{p^n}$.

- **Hasse's Theorem:**
  $|E(\mathbb{F}_q)| = q + 1 - t$, where $-2\sqrt{q} \leqslant t \leqslant 2\sqrt{q}$.
- t is called the **trace of Frobenius** at q.
- If $t = 1$, then E is called **anomalous**.
- If $p \mid t$, then E is called **supersingular**.
- If $p \nmid t$, then E is called **non-supersingular**.
- Let $\alpha, \beta \in \mathbb{C}$ satisfy $1 - tx + qx^2 = (1 - \alpha x)(1 - \beta x)$. Then, $|E(\mathbb{F}_{q^m})| = q^m + 1 - (\alpha^m + \beta^m)$.

Note: $E(\mathbb{F}_q)$ is not necessarily cyclic.

Hyperelliptic Curves

A **hyperelliptic curve** of **genus** $g \in \mathbb{N}$ over a field K is defined by the equation:

$$y^2 + u(x)y = v(x),$$

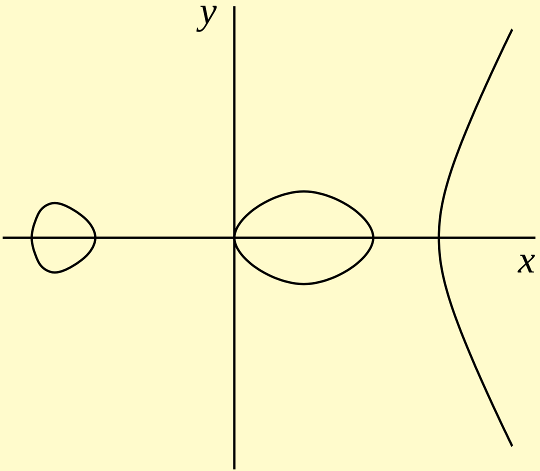
where $u(x), v(x) \in K[x]$, $v(x)$ is monic, $\deg u(x) \leqslant g$, and $\deg v(x) = 2g + 1$.

- Elliptic curves are hyperelliptic curves of of genus 1.
- The curve must be smooth (no points of singularity).
- If $\mathrm{char}\, K \neq 2$, then the equation can be simplified to

$$y^2 = v(x)$$

with $v(x) \in K[x]$ monic of degree $2g + 1$.

Hyperelliptic Curves: Example



A hyperelliptic curve over $\mathbb{R}$: $y^2 = x(x^2 - 1)(x^2 - 2)$

The Hyperelliptic Curve Group

- A group can be defined on the rational points of a hyperelliptic curve.
- The theory of divisors should be used in order to understand the construction of this group.
- For the special case of elliptic curves, this divisor class group can be stated geometrically by the chord-and-tangent rule.
- For hyperelliptic curves of genus $\geqslant 2$, the chord-and-tangent rule holds no longer.
- The hyperelliptic curve group is also used in cryptography.