Number Theory in Cryptology

Abhijit Das

Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur

October 15, 2011

What is Number Theory?

- Theory of natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$.
- Uses larger algebraic structures $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- **Modular arithmetic:** $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.
- **Finite fields:** $\mathbb{F}_{p^n}$, $p \in \mathbb{P}$, $n \in \mathbb{N}$.
- **Elliptic curves:** Arithmetic algebraic geometry.
- **Algebraic number theory:** Study of number fields and number rings.
- **Analytic number theory:** Use of complex analysis tools.

- All these are extensively used in cryptography and cryptanalysis.

Uses in Cryptology: Examples

- **Modular arithmetic:** RSA, ElGamal, Rabin and many other cryptosystems.
- **Finite fields:** Diffie-Hellman key agreement, ElGamal, DSA.
- **Elliptic curves:** ECDSA.
- **Pairing on elliptic curves:** Identity-based cryptosystems, multi-party key agreement, short signature schemes.
- **Algebraic number theory:** Number-field sieve method.
- **Analytic number theory:** Density estimates (like prime number theorem, Riemann hypothesis).

Modular Arithmetic

- Modulus $n \in \mathbb{N}$, $n \geqslant 2$.
- $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$.
- Arithmetic in $\mathbb{Z}_n$:
  - Addition: $a +_n b = \begin{cases} a+b & \text{if } a+b < n \\ a+b-n & \text{otherwise} \end{cases}$
  - Subtraction: $a -_n b = \begin{cases} a-b & \text{if } a \geqslant b \\ a-b+n & \text{otherwise} \end{cases}$
  - Multiplication: $a \times_n b = (ab) \operatorname{rem} n$.
  - Division:
    - a is invertible modulo n if and only if $\gcd(a, n) = 1$.
    - Extended gcd calculation: $ua + vn = \gcd(a, n)$ for some integers u, v.
    - If $\gcd(a, n) = 1$, u as the inverse of a modulo n.

Modular Exponentiation

To compute $a^e \pmod{n}$

- Binary expansion: $e = (e_{s-1}e_{s-2}\ldots e_1e_0)_2$.
- Initialize $t = 1$.
- For $i = s-1, s-2, \ldots, 1, 0$ do:
  - Set $t = t^2 \pmod{n}$.
  - If $e_i = 1$, set $t = ta \pmod{n}$.
- Return t.

The Multiplicative Group of $\mathbb{Z}_n$

- $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$.
- Euler-phi function: $\phi(n) = |\mathbb{Z}_n^*|$.
- If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then

$$\phi(n) = p_1^{e_1-1}(p_1 - 1)p_2^{e_2-1}(p_2 - 1) \cdots p_k^{e_k-1}(p_k - 1) = n \prod_{\substack{p \in \mathbb{P} \\ p|n}} \left(1 - \frac{1}{p}\right).$$

- $\mathbb{Z}_n^*$ is cyclic if and only if $n = 2, 4, p^e, 2p^e$ with $p \in \mathbb{P}$, $p \neq 2$, and $e \in \mathbb{N}$.
- **Special case:** $n = p \in \mathbb{P}$.
  - $\mathbb{Z}_p$ is a field.
  - $\mathbb{Z}_p^* = \{1, 2, \ldots, p - 1\}$.
  - $\phi(p) = p - 1$.
  - $\mathbb{Z}_p^*$ is cyclic.

Finite Fields

- Every finite field is of size p^n for $p \in \mathbb{P}$, $n \in \mathbb{N}$.
- For $q = p^n$, denote $\mathbb{F}_q = \mathbb{F}_{p^n}$ to be the finite field of size q.
- If the extension degree n is 1, $\mathbb{F}_p = \mathbb{Z}_p$.
- If $n > 1$, $\mathbb{F}_{p^n} \neq \mathbb{Z}_{p^n}$.
- **Polynomial-basis representation:**
  - Choose an irreducible polynomial $f(x) \in \mathbb{F}_p[x]$ of degree n.
  - Elements of $\mathbb{F}_{p^n}$ are represented as polynomials:

$$\mathbb{F}_{p^n} = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \mid a_i \in \mathbb{F}_p\}.$$

  - Arithmetic operations in $\mathbb{F}_{p^n}$: polynomial operations modulo $f(x)$.
- **Extensions of extensions:** Let $q = p^n$ and $m \in \mathbb{N}$.

$$\mathbb{F}_{q^m} = \{\alpha_0 + \alpha_1 y + \alpha_2 y^2 + \cdots + \alpha_{m-1} y^{m-1} \mid \alpha_i \in \mathbb{F}_{p^n}\}.$$

Arithmetic in $\mathbb{F}_{q^m}$ is the polynomial arithmetic of $\mathbb{F}_q[y]$ modulo an irreducible polynomial $g(y) \in \mathbb{F}_q[y]$ of degree m.

Some Properties of Finite Fields

- $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ is cyclic.
- There are $\phi(q-1)$ generators of $\mathbb{F}_q^*$.
- **Fermat's little theorem:**
  - $\alpha^{q-1} = 1$ for all $\alpha \in \mathbb{F}_q^*$.
  - $\beta^q = \beta$ for all $\beta \in \mathbb{F}_q$.
- **Multiplicative order:** Let $\alpha \in \mathbb{F}_q^*$. The smallest *positive* integer h satisfying $\alpha^h = 1$ is the order of α, denoted $h = \mathrm{ord}(\alpha)$.
- $\mathrm{ord}(\alpha) | (q-1)$.

Elliptic Curves

Let K be a field.

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

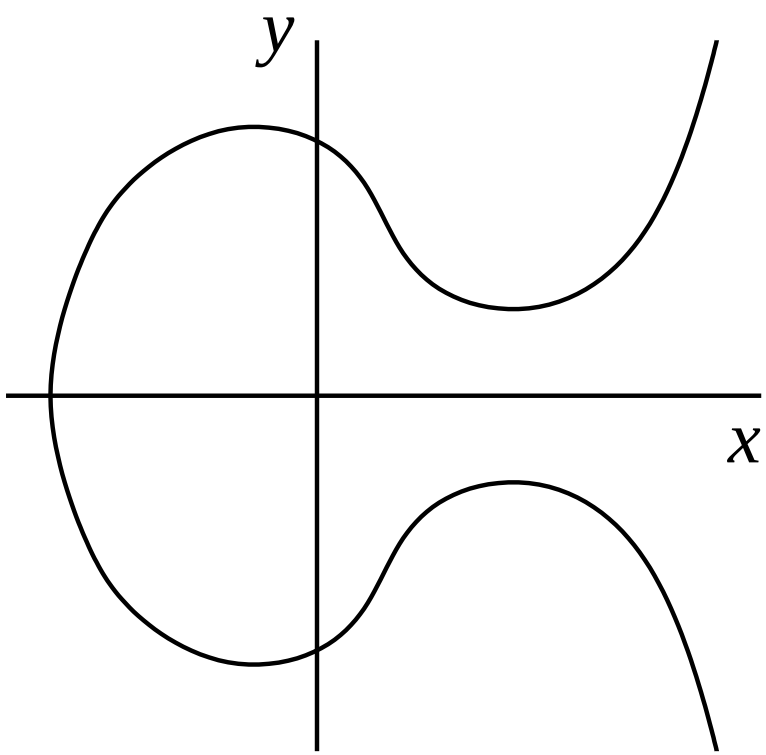
$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in K.$$

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

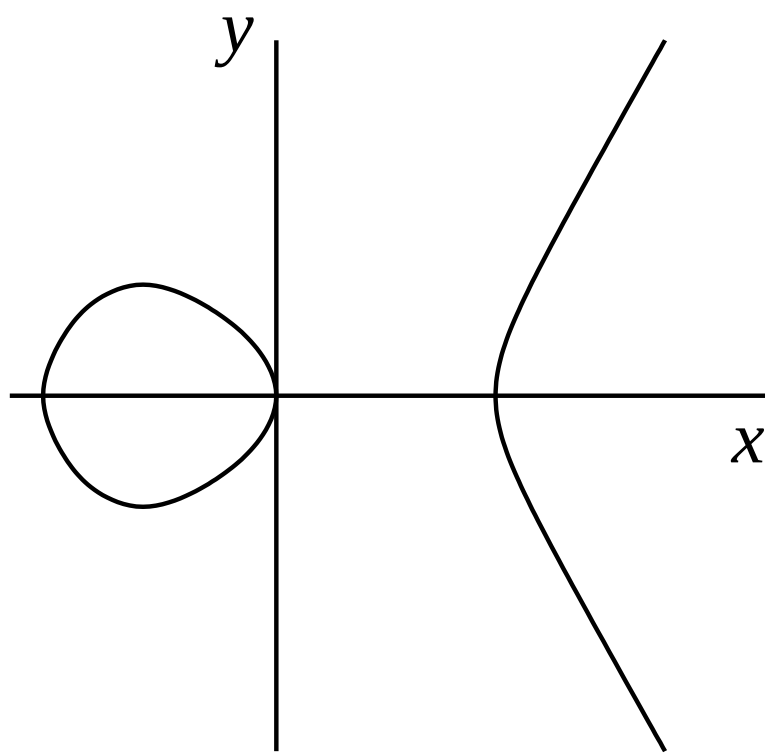
Special forms

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

Real Elliptic Curves: 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.

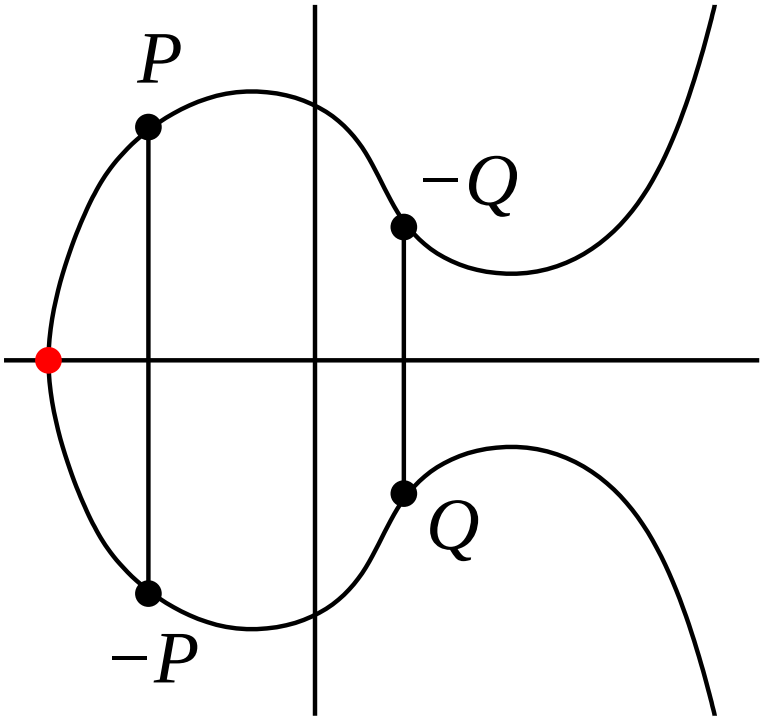
$E(K)$ is the set of all finite K-rational points on E and the point at infinity.

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

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

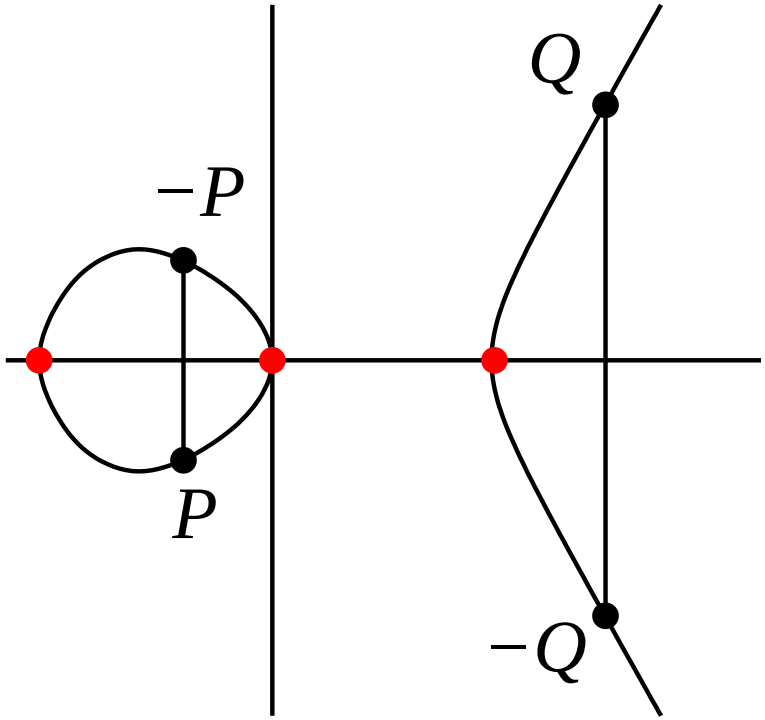
The Opposite of a Point

- Ordinary Points



(a)

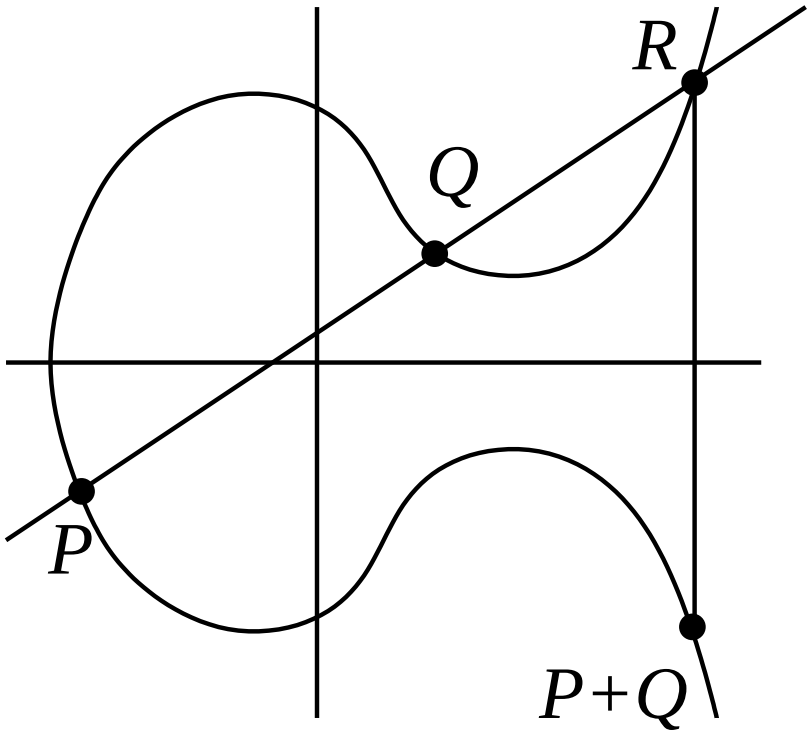
- Special Points



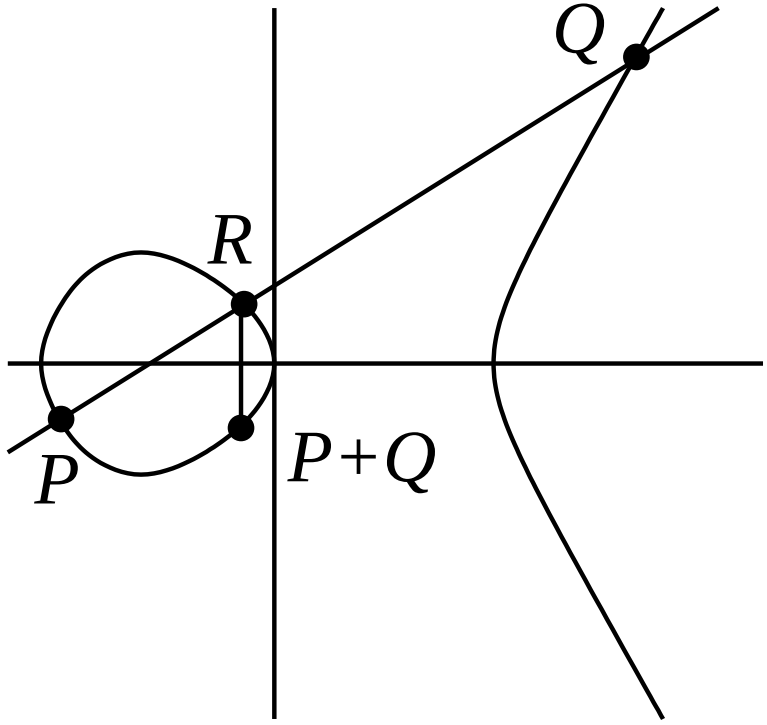
(b)

Addition of Two Points

Chord and tangent rule



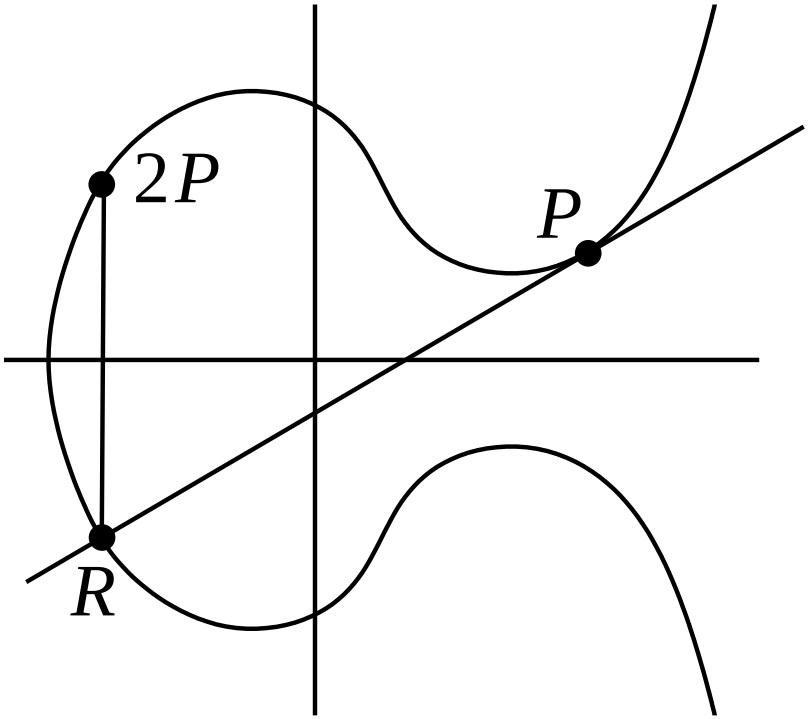
(a)



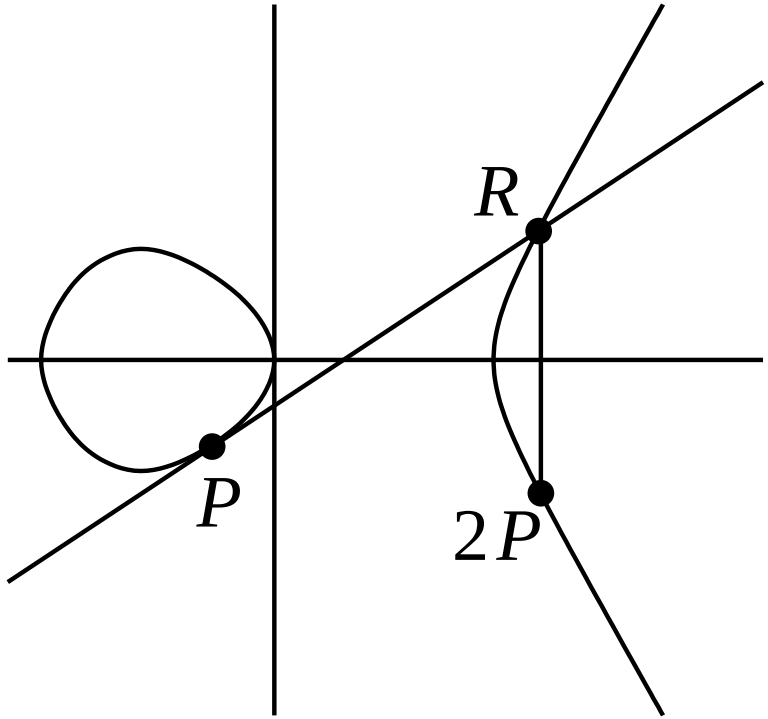
(b)

Doubling of a Point

Chord and tangent rule



(a)



(b)

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 $P = Q$).

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

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

Addition and Doubling in Non-supersingular Curves

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

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

Addition and Doubling in Supersingular Curves

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

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

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 $p|t$, 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.

Formal Sums and Free Abelian Groups

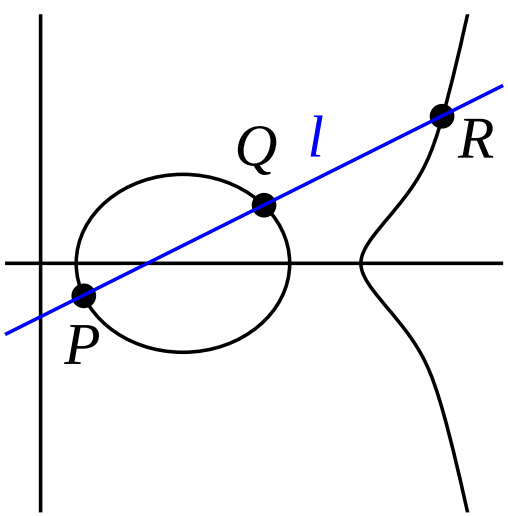
- Let a_i, $i \in I$, be *symbols* indexed by I.
- A **finite formal sum** of a_i, $i \in I$, is an expression of the form $\sum_{i \in I} m_i a_i$ with $m_i \in \mathbb{Z}$ such that $m_i = 0$ except for only finitely many $i \in I$.
- The sum $\sum_{i \in I} m_i a_i$ is formal in the sense that the symbols a_i are not meant to be evaluated. They act as *placeholders*.
- Define $\sum_{i \in I} m_i a_i + \sum_{i \in I} n_i a_i = \sum_{i \in I} (m_i + n_i) a_i$
- Also define $-\sum_{i \in I} m_i a_i = \sum_{i \in I} (-m_i) a_i$
- The set of all finite formal sums is an Abelian group called the **free Abelian group** generated by a_i, $i \in I$.

Divisors on Curves

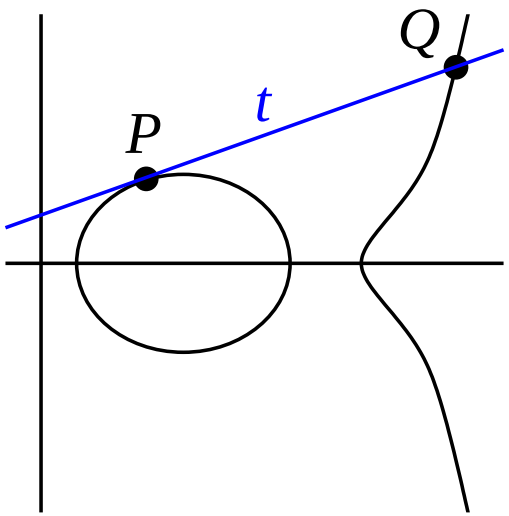
Let C be a projective curve defined over K.
K is assumed to be *algebraically closed*.

- A **divisor** is a formal sum of the K-rational points on C.
- Notation: $D = \sum_P m_P[P]$.
- The **support** of D is the set of points P for which $m_P \neq 0$.
- The **degree** of D is the sum $\sum_P m_P$.
- All divisors on C form a group denoted by $\mathrm{Div}_K(C)$ or $\mathrm{Div}(C)$.
- All divisors on C of degree 0 form a subgroup denoted by $\mathrm{Div}^0_K(C)$ or $\mathrm{Div}^0(C)$.
- **Divisor of a rational function** $R(x,y)$ is $\mathrm{Div}(R) = \sum_P \mathrm{ord}_P(R)[P]$.
- A **principal divisor** is the divisor of a rational function.
- Principal divisors satisfy: $\mathrm{Div}(R) + \mathrm{Div}(S) = \mathrm{Div}(RS)$ and $\mathrm{Div}(R) - \mathrm{Div}(S) = \mathrm{Div}(R/S)$.

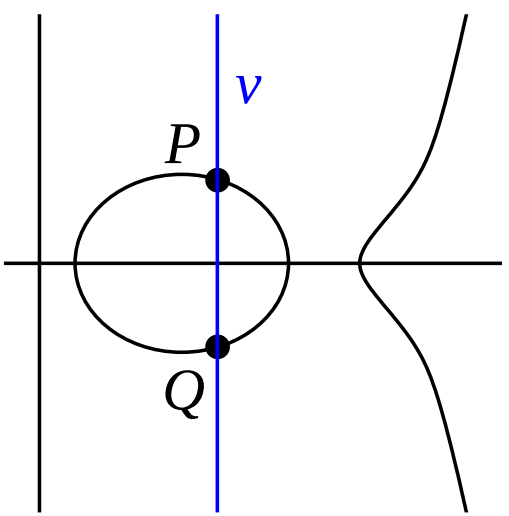
Divisor of a line: Example



(a)



(b)



(c)

- (a) $\mathrm{Div}(l) = [P] + [Q] + [R] - 3[\mathcal{O}]$.
- (b) $\mathrm{Div}(t) = 2[P] + [Q] - 3[\mathcal{O}]$.
- (c) $\mathrm{Div}(v) = [P] + [Q] - 2[\mathcal{O}]$.

Divisors and the Chord-and-Tangent Rule

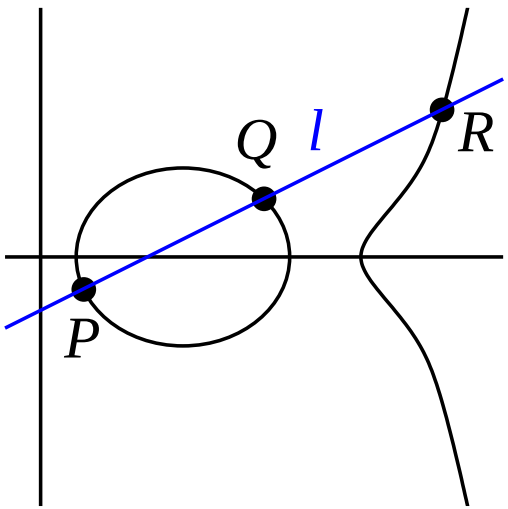
Let C be an elliptic curve over an algebraically closed field K.

- For every $D \in \mathrm{Div}_K^0(C)$, there exist a unique rational point P and a rational function R such that $D = [P] - [\mathcal{O}] + \mathrm{Div}(R)$.
- D is identified with $[P] - [\mathcal{O}]$.
- This bijection leads to the chord-and-tangent rule in the following sense:

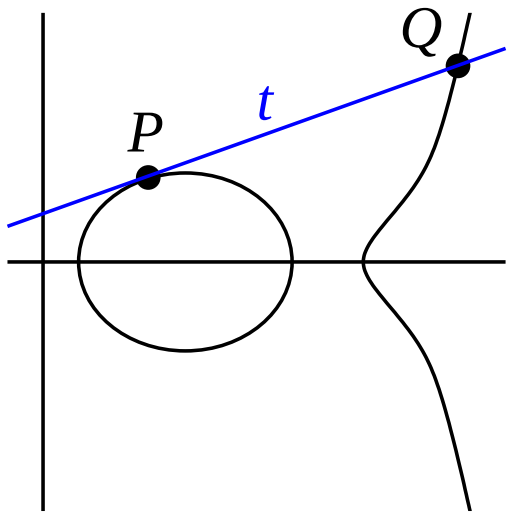
Let $D = \sum_P m_P[P] \in \mathrm{Div}_K(C)$. Then, D is a principal divisor if and only if

- $\sum_P m_P = 0$ (integer sum), and
- $\sum_p m_P P = \mathcal{O}$ (sum under the chord-and-tangent rule).

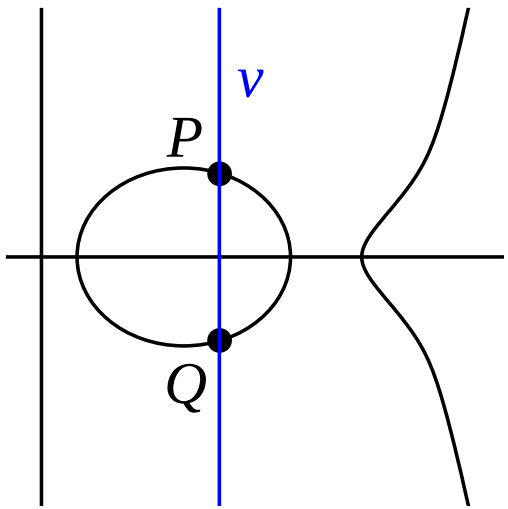
Illustrations of the Chord-and-Tangent Rule



(a)



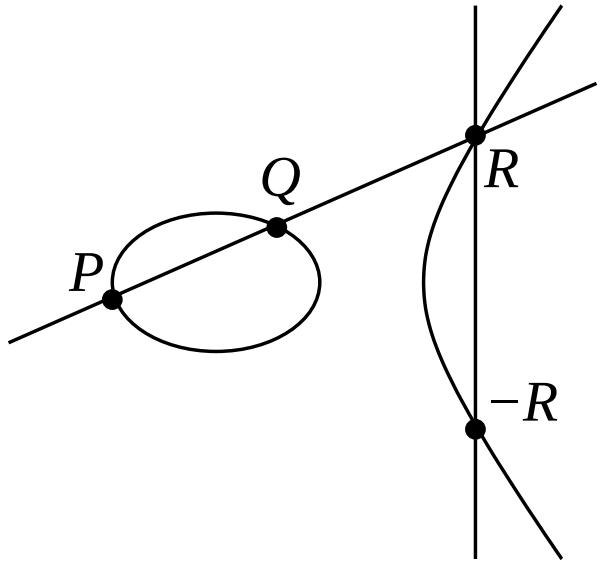
(b)



(c)

- **Identity:** $\mathcal{O}$ is identified with $[\mathcal{O}] - [\mathcal{O}] = 0 = \mathrm{Div}(1)$.
- **Opposite:** By Part (c), $\mathrm{Div}(v) = ([P] - [\mathcal{O}]) + ([Q] - [\mathcal{O}])$ is 0. By the correspondence, $P + Q = \mathcal{O}$, that is, $Q = -P$.
- **Sum:** By Part (a), $\mathrm{Div}(l) = ([P] - [\mathcal{O}]) + ([Q] - [\mathcal{O}]) + ([R] - [\mathcal{O}])$ is 0, that is, $P + Q + R = \mathcal{O}$, that is, $P + Q = -R$.
- **Double:** By Part (b), $\mathrm{Div}(t) = ([P] - [\mathcal{O}]) + ([P] - [\mathcal{O}]) + ([Q] - [\mathcal{O}])$ is 0, that is, $P + P + Q = \mathcal{O}$, that is, $2P = -Q$.

More on Divisors



- $\mathrm{Div}(L_{P,Q}) = [P] + [Q] + [R] - 3[\mathcal{O}]$.
- $\mathrm{Div}(L_{R,-R}) = [R] + [-R] - 2[\mathcal{O}]$.
- $\mathrm{Div}(L_{P,Q}/L_{R,-R}) = [P] + [Q] - [-R] - [\mathcal{O}] = [P] + [Q] - [P+Q] - [\mathcal{O}]$.
- $[P] - [\mathcal{O}]$ is equivalent to $[P+Q] - [Q]$.
- $([P] - [\mathcal{O}]) + ([Q] - [\mathcal{O}])$ is equivalent to $[P+Q] - [\mathcal{O}]$.
- For both these cases of equivalence, the pertinent rational function is $L_{P,Q}/L_{P+Q,-(P+Q)}$ which can be easily computed. We can force this rational function to have leading coefficient 1.

More on Divisors (contd)

- Let $D = \sum_P n_P[P]$ be divisor on E and $f \in \bar{K}(E)$ a rational function such that the supports of D and $\mathrm{Div}(f)$ are disjoint. Define

$$f(D) = \prod_{P \in E} f(P)^{n_P} = \prod_{P \in \mathrm{Supp}(D)} f(P)^{n_P}.$$

- $\mathrm{Div}(f) = \mathrm{Div}(g)$ if and only if $f = cg$ for some non-zero constant $c \in \bar{K}^*$.
- If D has degree 0, then
$f(D) = g(D) \prod_P c^{n_P} = g(D) c^{\sum_P n_P} = g(D) c^0 = g(D)$.

- **Weil reciprocity theorem:** If f and g are two non-zero rational functions on E such that $\mathrm{Div}(f)$ and $\mathrm{Div}(g)$ have disjoint supports, then

$$f(\mathrm{Div}(g)) = g(\mathrm{Div}(f)).$$

Weil Pairing: Definition

Let E be an elliptic curve defined over a finite field $K = \mathbb{F}_q$.
Take a positive integer m coprime to $p = \operatorname{char} K$.
Let μ_m denote the m-th roots of unity in $\bar{K}$.
We have $\mu_m \subseteq \mathbb{F}_{q^k}$, where $k = \operatorname{ord}_m(q)$ is called the **embedding degree**.
Let $E[m]$ be those points in $E = E_{\bar{K}}$, whose orders divide m.

- **Weil pairing** is a function

$$e_m : E[m] \times E[m] \to \mu_m$$

defined as follows.

- Take $P_1, P_2 \in E[m]$.
- Let D_1 be a divisor equivalent to $[P_1] - [\mathcal{O}]$. Since $mP_1 = \mathcal{O}$, there exists a rational function f_1 such that $\operatorname{Div}(f_1) = mD_1 = m[P_1] - m[\mathcal{O}]$.
- Similarly, let D_2 be a divisor equivalent to $[P_2] - [\mathcal{O}]$. There exists a rational function f_2 such that $\operatorname{Div}(f_2) = mD_2 = m[P_2] - m[\mathcal{O}]$.
- D_1 and D_2 are chosen to have disjoint supports.
- Define $e_m(P_1, P_2) = f_1(D_2)/f_2(D_1)$.

Properties of Weil Pairing

Let P, Q, R be arbitrary points in $E[m]$.

- **Bilinearity:**

$$\begin{aligned} e_m(P+Q,R) &= e_m(P,R)e_m(Q,R), \\ e_m(P,Q+R) &= e_m(P,Q)e_m(P,R). \end{aligned}$$

- **Alternating:** $e_m(P,P) = 1$.
- **Skew symmetry:** $e_m(Q,P) = e_m(P,Q)^{-1}$.
- **Non-degeneracy:** If $P \neq \mathcal{O}$, then $e_m(P,Q) \neq 1$ for some $Q \in E[m]$.
- **Compatibility:** If $S \in E[mn]$ and $Q \in E[n]$, then $e_{mn}(S,Q) = e_n(mS,Q)$.
- If m is a prime and $P \neq \mathcal{O}$, then $e_m(P,Q) = 1$ if and only if Q lies in the subgroup generated by P (that is, $Q = aP$ for some integer a).

Computing Weil Pairing: The Functions $f_{n,P}$

- Let $P \in E$.
- For $n \in \mathbb{Z}$, define the rational functions $f_{n,P}$ as having the divisor

$$\mathrm{Div}(f_{n,P}) = n[P] - [nP] - (n-1)[\mathcal{O}].$$

$f_{n,P}$ are unique up to multiplication by elements of $\bar{K}^*$.
We may choose the unique monic polynomial for $f_{n,P}$.

- $f_{n,P}$ satisfy the recurrence relation:

$$\begin{aligned} f_{0,P} &= f_{1,P} = 1, \\ f_{n+1,P} &= \left(\frac{L_{P,nP}}{L_{(n+1)P,-(n+1)P}} \right) f_{n,P} \quad \text{for } n \geqslant 1, \\ f_{-n,P} &= \frac{1}{f_{n,P}} \quad \text{for } n \geqslant 1. \end{aligned}$$

- If $P \in E[m]$, then $\mathrm{Div}(f_{m,P}) = m[P] - [mP] - (m-1)[\mathcal{O}] = m[P] - m[\mathcal{O}]$.
- Computing $f_{m,P}$ using the above recursive formula is too inefficient.

Computing Weil Pairing: More about $f_{n,P}$

- The rational functions $f_{n,P}$ also satisfy

$$f_{n+n',P} = f_{n,P}\, f_{n',P} \times \left(\frac{L_{nP,n'P}}{L_{(n+n')P,-(n+n')P}} \right).$$

- In particular, for $n = n'$, we have

$$f_{2n,P} = f_{n,P}^2 \times \left(\frac{L_{nP,nP}}{L_{2nP,-2nP}} \right).$$

Here, $L_{nP,nP}$ is the line tangent to E at the point nP.

- This and the recursive expression of $f_{n+1,P}$ in terms of $f_{n,P}$ yield a repeated double-and-add algorithm.
- The function $f_{n,P}$ is usually kept in the factored form.
- It is often not necessary to compute $f_{n,P}$ explicitly. The value of $f_{n,P}$ at some point Q is only needed.

Miller's Algorithm for Computing $f_{n,P}$

- **Input:** A point $P \in E$ and a positive integer n.
- **Output:** The rational function $f_{n,P}$.
- **Steps**
  - Let $n = (n_s n_{s-1} \ldots n_1 n_0)_2$ be the binary representation of n with $n_s = 1$.
  - Initialize $f = 1$ and $U = P$.
  - For $i = s-1, s-2, \ldots, 1, 0$, do the following:
    - /* Doubling */
    - Update $f = f^2 \times \left(\frac{L_{U,U}}{L_{2U,-2U}} \right)$ and $U = 2U$.
    - /* Conditional adding */
    - If $(n_i = 1)$, update $f = f \times \left(\frac{L_{U,P}}{L_{U+P,-(U+P)}} \right)$ and $U = U + P$.
  - Return f.
- **Note:** One may supply a point $Q \in E$ and wish to compute the value $f_{n,P}(Q)$ (instead of the function $f_{n,P}$). In that case, the functions $L_{U,U}/L_{2U,-2U}$ and $L_{U,P}/L_{U+P,-(U+P)}$ should be evaluated at Q before multiplication with f.

Weil Pairing and the Functions $f_{n,P}$

Let $P_1, P_2 \in E[m]$, and we want to compute $e_m(P_1, P_2)$.

- Choose a point T not equal to $\pm P_1, -P_2, P_2 - P_1, \mathcal{O}$.
- We have $e_m(P_1, P_2) = \dfrac{f_{m,P_2}(T)\ f_{m,P_1}(P_2 - T)}{f_{m,P_1}(-T)\ f_{m,P_2}(P_1 + T)}$.
- If $P_1 \neq P_2$, then we also have $e_m(P_1, P_2) = (-1)^m\ \dfrac{f_{m,P_1}(P_2)}{f_{m,P_2}(P_1)}$.
- Miller's algorithm for computing $f_{n,P}(Q)$ can be used.
- All these invocations of Miller's algorithm have $n = m$.
- So a single double-and-add loop suffices.
- For efficiency, one may avoid the division operations in Miller's loop by separately maintaining polynomial expressions for the numerator and the denominator of f. After the loop terminates, a single division is made.

Some Intractable Number-theoretic Problems of Cryptographic Significance

- **Integer factorization problem (IFP):** Given a composite integer n with unknown prime divisors, factor n.
- **Square root problem (SQRTP):** Given a composite integer n with unknown factorization, and a modular square $a \in \mathbb{Z}_n$, compute $x \in \mathbb{Z}_n$ such that $x^2 \equiv a \pmod{n}$.
- **Discrete logarithm problem (DLP):** Let G be a finite cyclic group generated by g. Given $a \in G$, find x such that $g = a^x$ in G.
- **Diffie-Hellman problem (DHP):** Let G be a finite cyclic group generated by g. Given $g^x, g^y \in G$ (but not x or y), compute g^{xy} in G.
- DLP and DHP apply to many number-theoretic groups like $\mathbb{F}_q^*$ and $E(\mathbb{F}_q)$.
- **Bilinear Diffie-Hellman problem (BDHP):** Let $e : G \times G \to G'$ be a pairing map. Given $P, aP, bP, cP \in G$ only, compute $e(P, P)^{abc} \in G'$.

Cryptanalysis: Factoring Integers

Exponential algorithms

- Trial division
- Pollard rho method
- Pollard $p-1$ method
- Williams $p+1$ method

Sub-exponential algorithms

- CFRAC method
- Dixon's method
- Quadratic sieve method
- Cubic sieve method
- Elliptic curve method
- Number-field sieve method

$$L(n,\omega,c) = \exp\left[(c+\mathrm{o}(1))(\ln n)^{\omega}(\ln\ln n)^{1-\omega}\right]$$

The Number-field Sieve Method

- Based on Fermat's method of squares: Compute a, b with $a^2 \equiv b^2 \pmod{n}$ and $a \neq \pm b \pmod{n}$. In this case, $\gcd(a-b, n)$ is a non-trivial factor of n.
- Choose an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ and a positive integer H such that $f(H)$ is a small multiple of n. Let $d = \deg f(x)$.
- Define the number field

$$K = \mathbb{Q}[x]/\langle f(x)\rangle = \{g(x) \in \mathbb{Q}[x] \mid \deg g(x) \leqslant d-1\}.$$

Arithmetic in K is the polynomial arithmetic of $\mathbb{Q}[x]$ modulo $f(x)$.

- Let O_K be the ring of integers in K. Assume that O_K supports element-wise unique factorization.
- Consider the map $\Phi : \mathrm{O}_K \to \mathbb{Z}_n$ taking $x \mapsto H$.
- **Relation:** Let $\Phi(\alpha_1)\Phi(\alpha_2)\cdots\Phi(\alpha_k) \equiv \prod_{i=1}^{t} p_i^{e_i} \pmod{n}$.
- Combine many relations to obtain $a^2 \equiv b^2 \pmod{n}$.

Questions?

"*In mathematics you don't understand things. You just get used to them.*"

– John von Neumann

Some Recommended Textbooks

- Das, *Computational Number Theory*, CRC, 2012 (?).
- Das and Veni Madhavan, *Public-key Cryptography: Theory and Practice*, Pearson, 2009.
- Zuckerman, Montgomery, Niven and Niven, *An Introduction to the Theory of Numbers*, Wiley, 1991.
- Bressoud, *Factorization and Primality Testing*, Springer UTM, 1989.
- Cohen, *A Course in Computational Algebraic Number Theory*, Springer GTM, 1993.
- Crandall and Pomerance, *Prime Numbers: A Computational Perspective*, Springer, 2001.
- Enge, *Elliptic Curves and Their Applications to Cryptography*, Kluwer, 1999.
- Blake, Seroussi and Smart, *Advances in Elliptic Curve Cryptography*, Cambridge, 2005.
- Charlap and Robbins, *An Elementary Introduction to Elliptic Curves*, CRD Report, 1988.
- Martin, *Introduction to Identity-Based Encryption*, Artech House, 2008.
- Mollin, *Fundamental Number Theory with Applications*, CRC, 1998.
- Mollin, *Algebraic Number Theory*, CRC, 1999.