Algebraic Curves
An Elementary Introduction

Abhijit Das

Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
August 22, 2011
Part I

Affine and Projective Curves

- Rational Points on Curves
- Polynomial and Rational Functions on Curves
- Divisors and Jacobians on Curves
Affine Curves

- $K$ is a field.
- $\overline{K}$ is the algebraic closure of $K$.
- It is often necessary to assume that $K$ is algebraically closed.
- **Affine plane**: $K^2 = \{(h, k) \mid h, k \in K\}$.
- For $(h, k) \in K^2$, the field elements $h, k$ are called **affine coordinates**.
- **Affine curve**: Defined by a polynomial equation:
  \[ C : f(X, Y) = 0. \]
- It is customary to consider only irreducible polynomials $f(X, Y)$. If $f(X, Y)$ admits non-trivial factors, the curve $C$ is the set-theoretic union of two (or more) curves of smaller degrees.
- **Rational points on $C$**: All points $(h, k) \in K^2$ such that $f(h, k) = 0$.
- Rational points on $C$ are called **finite points**.
Affine Curves: Examples

- **Straight lines**: $aX + bY + c = 0$.
- **Circles**: $(X - a)^2 + (Y - b)^2 - r^2 = 0$.
- **Conic sections**: $aX^2 + bXY + cY^2 + dX + eY + f = 0$.
- **Elliptic curves**: Defined by the Weierstrass equation:
  $Y^2 + (a_1X + a_3)Y = X^3 + a_2X^2 + a_4X + a_6$.
  If char $K \neq 2, 3$, this can be simplified as $Y^2 = X^3 + aX + b$.

- **Hyperelliptic curves of genus $g$**: $Y^2 + u(X)Y = v(X)$ with deg $u \leq g$, deg $v = 2g + 1$, and $v$ monic.
  If char $K \neq 2$, this can be simplified as $Y^2 = w(X)$ with deg $w = 2g + 1$ and $w$ monic.

- Parabolas are hyperelliptic curves of genus 0.
- Elliptic curves are hyperelliptic curves of genus 1.
Projective Plane

Define a relation $\sim$ on $K^3 \setminus \{(0, 0, 0)\}$ as $(h, k, l) \sim (h', k', l')$ if $h' = \lambda h$, $k' = \lambda k$ and $l' = \lambda l$ for some non-zero $\lambda \in K$.

$\sim$ is an equivalence relation on $K^3 \setminus \{(0, 0, 0)\}$.

The equivalence class of $(h, k, l)$ is denoted by $[h, k, l]$.

$[h, k, l]$ can be identified with the line in $K^3$ passing through the origin and the point $(h, k, l)$.

The set of all these equivalence classes is the **projective plane** over $K$.

The projective plane is denoted as $\mathbb{P}^2(K)$.

$h, k, l$ in $[h, k, l]$ are called **projective coordinates**.

Projective coordinates are unique up to multiplication by non-zero elements of $K$.

The three projective coordinates cannot be simultaneously 0.
Relation Between the Affine and the Projective Planes

\( \mathbb{P}^2(K) \) is the affine plane \( K^2 \) plus the points at infinity.

Take \( P = [h, k, l] \in \mathbb{P}^2(K) \).

**Case 1:** \( l \neq 0 \).

\( P = [h/l, k/l, 1] \) is identified with the point \( (h/l, k/l) \in K^2 \).

The line in \( K^3 \) corresponding to \( P \) meets \( Z = 1 \) at \( (h/l, k/l, 1) \).

\( P \) is called a **finite point**.

**Case 2:** \( l = 0 \).

The line in \( K^3 \) corresponding to \( P \) does not meet \( Z = 1 \).

\( P \) does not correspond to a point in \( K^2 \).

\( P \) is a **point at infinity**.

For every slope of lines in the \( X, Y \)-plane, there exists exactly one point at infinity.

A line passes through all the points at infinity. It is the **line at infinity**.

Two distinct lines (parallel or not) in \( \mathbb{P}^2(K) \) always meet at a unique point (consistent with Bézout’s theorem).

Through any two distinct points in \( \mathbb{P}^2(K) \) passes a unique line.
Passage from Affine to Projective Curves

A (multivariate) polynomial is called **homogeneous** if every non-zero term in the polynomial has the same degree.

Example: \(X^3 + 2XYZ - 3Z^3\) is homogeneous of degree 3. \(X^3 + 2XY - 3Z\) is not homogeneous. The zero polynomial is homogeneous of any degree.

Let \(C : f(X, Y) = 0\) be an affine curve of degree \(d\).

\[f^{(h)}(X, Y, Z) = Z^d f(X/Z, Y/Z)\] is the **homogenization** of \(f\).

\(C^{(h)} : f^{(h)}(X, Y, Z) = 0\) is the **projective curve** corresponding to \(C\).

For any non-zero \(\lambda \in K\), we have \(f^{(h)}(\lambda h, \lambda k, \lambda l) = \lambda^d f^{(h)}(h, k, l)\). So \(f^{(h)}(\lambda h, \lambda k, \lambda l) = 0\) if and only if \(f^{(h)}(h, k, l) = 0\).

The rational points of \(C^{(h)}\) are all \([h, k, l]\) with \(f^{(h)}(h, k, l) = 0\).

**Finite points on** \(C^{(h)}\): Put \(Z = 1\) to get \(f^{(h)}(X, Y, 1) = f(X, Y)\). These are the points on \(C\).

**Points at infinity on** \(C^{(h)}\): Put \(Z = 0\) and solve for \(f^{(h)}(X, Y, 0) = 0\). These points do not belong to \(C\).
Examples of Projective Curves

**Straight Line:** \(aX + bY + cZ = 0\).

- Finite points: Solutions of \(aX + bY + c = 0\).
- Points at infinity: Solve for \(aX + bY = 0\).
  
  If \(b \neq 0\), we have \(Y = -(a/b)X\). So \([1, -(a/b), 0]\) is the only point at infinity.
  
  If \(b = 0\), we have \(aX = 0\), that is, \(X = 0\). So \([0, 1, 0]\) is the only point at infinity.

**Circle:** \((X - aZ)^2 + (Y - bZ)^2 = r^2Z^2\).

- Finite points: Solutions of \((X - a)^2 + (Y - b)^2 = r^2\).
- Points at infinity: Solve for \(X^2 + Y^2 = 0\).
  
  For \(K = \mathbb{R}\), the only solution is \(X = Y = 0\), so there is no point at infinity.
  
  For \(K = \mathbb{C}\), the solutions are \(Y = \pm iX\), so there are two points at infinity: \([1, i, 0]\) and \([1, -i, 0]\).
Examples of Projective Curves (contd.)

Parabola: $Y^2 = XZ$.

- Finite points: Solutions of $Y^2 = X$.
- Points at infinity: Solve for $Y^2 = 0$.
  $Y = 0$, so $[1, 0, 0]$ is the only point at infinity.

Hyperbola: $X^2 - Y^2 = Z^2$.

- Finite points: Solutions of $X^2 - Y^2 = 1$.
- Points at infinity: Solve for $X^2 - Y^2 = 0$.
  $Y = \pm X$, so there are two points at infinity: $[1, 1, 0]$ and $[1, -1, 0]$. 
Examples of Projective Curves (contd.)

Elliptic curve: \[ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \]

Finite points: Solutions of \[ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6. \]

Points at infinity: Solve for \[ X^3 = 0. \]

\( X = 0 \), that is, \([0, 1, 0]\) is the only point at infinity.
A hyperelliptic curve of genus 2: $Y^2 = X(X^2 - 1)(X^2 - 2)$

**Hyperelliptic curve:** $Y^2Z^{2g-1} + Z^g u(X/Z)YZ^g = Z^{2g+1}v(X/Z)$.

Finite points: Solutions of $Y^2 + u(X)Y = v(X)$.

Points at infinity: The only $Z$-free term is $X^{2g+1}$ (in $Z^{2g+1}v(X/Z)$). So $[0, 1, 0]$ is the only point at infinity.
Bézout’s Theorem

A curve of degree $m$ and a curve of degree $n$ intersect at exactly $mn$ points.

The intersection points must be counted with proper multiplicity.

It is necessary to work in algebraically closed fields.

Still, the theorem is not true. For example, two parallel lines or two concentric circles never intersect.

Passage to the projective plane makes Bézout’s theorem true.

(a) and (b): Two simple intersections at the points at infinity
(c): Two tangents at the points at infinity
(d): No intersections at the points at infinity
Smooth Curves

Let $C : f(X, Y, Z) = 0$ be a projective curve, and $P = [h, k, l]$ a rational point on $C$.

- $P$ is called a **smooth point** on $C$ if the tangent to $C$ at $P$ is uniquely defined.

**Case 1:** $P$ is a finite point.

Now, $l \neq 0$. Consider the affine equation $f(X, Y) = 0$.

Both $\frac{\partial f}{\partial X}$ and $\frac{\partial f}{\partial Y}$ do not vanish simultaneously at $(h/l, k/l)$.

**Case 2:** $P$ is a point at infinity.

Now, $l = 0$, so at least one of $h, k$ must be non-zero.

If $h \neq 0$, view $C$ as the homogenization of $f_X(Y, Z) = f(1, Y, Z)$. $(k/h, l/h)$ is a finite point on $f_X$. Apply Case 1.

If $k \neq 0$, view $C$ as the homogenization of $f_Y(X, Z) = f(X, 1, Z)$. $(h/k, l/k)$ is a finite point on $f_Y$. Apply Case 1.

$C$ is a **smooth curve** if it is smooth at every rational point on it.
Types of Singularity

(a) A cusp or a spinode: \( Y^2 = X^3 \).

(b) A loop or a double-point or a crunode: \( Y^2 = X^3 + X^2 \).

(c) An isolated point or an acnode: \( Y^2 = X^3 - X^2 \)

For a real curve \( f(X, Y) = 0 \), the type of singularity is determined by the matrix Hessian\( (f) = \begin{pmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial y} \\ \frac{\partial^2 f}{\partial y \partial x} & \frac{\partial^2 f}{\partial y^2} \end{pmatrix} \).
Examples of Smooth Curves

(a) \( Y^2 = X^3 - X \)  
(b) \( Y^2 = X^3 - X + 1 \)  
(c) \( Y^2 = X^3 + X \)

An elliptic or hyperelliptic curve is needed to be smooth by definition.

A curve of the form \( Y^2 = v(X) \) is smooth if and only if \( v(X) \) does not contain repeated roots.

The point at infinity on an elliptic or hyperelliptic curve is never a point of singularity.
Polynomial and Rational Functions on Curves

Let \( C : f(X, Y) = 0 \) be a curve defined by an \textit{irreducible polynomial} \( f(X, Y) \in K[X, Y] \).

Let \( G(X, Y), H(X, Y) \in K[X, Y] \) with \( f \mid (G - H) \). Then, \( G(P) = H(P) \) for every rational point \( P \) on \( C \) (since \( f(P) = 0 \)). Thus, \( G \) and \( H \) represent the same function on \( C \).

Define \( G(X, Y) \equiv H(X, Y) \pmod{f(X, Y)} \) if and only if \( f \mid (G - H) \).

Congruence modulo \( f \) is an equivalence relation on \( K[X, Y] \).

Call the equivalence classes of \( X \) and \( Y \) by \( x \) and \( y \).

The equivalence class of \( G(X, Y) \) is \( G(x, y) \).

\( K[C] = K[X, Y]/\langle f(X, Y) \rangle = K[x, y] \) is an integral domain.

The field of fractions of \( K[C] \) is \( K(C) = \{ G(x, y)/H(x, y) \mid H(x, y) \neq 0 \} = K(x, y) \).
Polynomial and Rational Functions on Elliptic and Hyperelliptic Curves

Consider the elliptic curve \( Y^2 + u(X)Y = v(X) \), where \( u(X) = a_1X + a_3 \) and \( v(X) = X^3 + a_2X^2 + a_4X + a_6 \).

\[ y^2 = -u(x)y + v(x). \]

Every polynomial function on \( C \) can be represented uniquely as \( a(x) + yb(x) \) with \( a(x), b(x) \in K[x] \).

For \( G(x, y) = a(x) + yb(x) \in K[C] \), define:

- **Conjugate of** \( G \): \( \hat{G}(x, y) = a(x) - b(x)(u(x) + y) \).
- **Norm of** \( G \): \( N(G) = G\hat{G} \).

\[ N(G) = a(x)^2 - a(x)b(x)u(x) - v(x)b(x)^2 \in K[x]. \]

Every rational function on \( C \) can be represented as \( s(x) + yt(x) \) with \( s(x), t(x) \in K(x) \).

\( K(C) \) is the quadratic extension of \( K(X) \) obtained by adjoining a root of the irreducible polynomial \( Y^2 + u(X)Y - v(X) \in K(X)[Y] \). The current notion of conjugacy coincides with the standard notion for field extensions.

These results hold equally well for hyperelliptic curves too.
Poles and Zeros of Rational Functions

Let $C : f(X, Y) = 0$ be a plane (irreducible) curve, and $P = (h, k)$ a finite point on $C$.

Let $G(x, y) \in K[C]$. The value of $G$ at $P$ is $G(P) = G(h, k) \in K$.

A rational function $R(x, y) \in K(C)$ is defined at $P$ if there is a representation $R(x, y) = G(x, y)/H(x, y)$ for some polynomials $G, H$ with $H(P) = H(h, k) \neq 0$. In that case, the value of $R$ at $P$ is defined as $R(P) = G(P)/H(P) = G(h, k)/H(h, k) \in K$.

If $R(x, y)$ is not defined at $P$, we take $R(P) = \infty$.

Let $R(x, y) \in K(C)$ and $P$ a finite point on $C$.

- $P$ is a zero of $R$ is $R(P) = 0$.
- $P$ is a pole of $R$ is $R(P) = \infty$.

The set of rational functions on $C$ defined at $P$ is a local ring with the unique maximal ideal comprising functions that evaluate to 0 at $P$.

The notion of value of a rational function can be extended to the points at infinity on $C$. 

Value of a Rational Function at $\mathcal{O}$: Example

Let $C$ be an elliptic curve with $\mathcal{O}$ the point at infinity.

Neglecting lower-degree terms gives $Y^2 \approx X^3$.

$X$ is given a weight 2, and $Y$ a weight 3.

Let $G(x, y) = a(x) + yb(x) \in K[C]$. Define the degree of $G$ as

$$\deg G = \max(2 \deg_x(a), 3 + 2 \deg_x(b)).$$

The leading coefficient of $G$ is that of $a$ or $b$ depending upon whether $2 \deg_x(a) > 3 + 2 \deg_x(b)$ or not.

Let $R(x, y) = G(x, y)/H(x, y) \in K(C)$. Define $R(\mathcal{O})$ as:

- $0$ if $\deg G < \deg H$.
- $\infty$ if $\deg G > \deg H$.
- The ratio of the leading coefficients of $G$ and $H$, if $\deg G = \deg H$.

For hyperelliptic curves, analogous results hold. Now, $X$ and $Y$ are given weights 2 and $2g + 1$ respectively.
Multiplicities of Poles and Zeros

Let $C$ be a curve, and $P$ a rational point on $C$.

There exists a rational function $U_P(x, y)$ (depending on $P$) such that:

1. $U_P(P) = 0$, and
2. every rational function $R(x, y) \in K(C)$ can be expressed as $R = U_P^dS$ with $S$ having neither a pole nor a zero at $P$.

$U_P$ is called a uniformizer.

The integer $d$ is independent of the choice of $U_P$.

Define the order of $R$ at $P$ as $\text{ord}_P(R) = d$.

$P$ is a zero of $R$ if and only if $\text{ord}_P(R) > 0$. Multiplicity is $\text{ord}_P(R)$.

$P$ is a pole of $R$ if and only if $\text{ord}_P(R) < 0$. Multiplicity is $-\text{ord}_P(R)$.

$P$ is neither a pole nor a zero of $R$ if and only if $\text{ord}_P(R) = 0$.

Any (non-zero) rational function has only finitely many poles and zeros.

For a projective curve over an algebraically closed field, the sum of the orders of the poles and zeros of a (non-zero) rational function is 0.
Poles and Zeros for Elliptic Curves

Let \( C : Y^2 + u(X)Y = v(X) \) be an elliptic curve with \( \mathcal{O} \) the point at infinity, and \( P = (h, k) \) a finite point on \( C \).

The **opposite** of \( P \) is defined as \( \tilde{P} = (h, -k - u(h)) \). \( P \) and \( \tilde{P} \) are the only points on \( C \) with \( X \)-coordinate equal to \( h \).

The opposite of \( \mathcal{O} \) is \( \mathcal{O} \) itself.

\( P \) is called an **ordinary point** if \( \tilde{P} \neq P \).

\( P \) is called a **special point** if \( \tilde{P} = P \).

Any line passing through \( P \) but not a tangent to \( C \) at \( P \) can be taken as a **uniformizer** \( U_P \) at \( P \).

For example, we may take \( U_P = \begin{cases} x - h & \text{if } P \text{ is an ordinary point,} \\ y - k & \text{if } P \text{ is a special point.} \end{cases} \)

A **uniformizer** at \( \mathcal{O} \) is \( x/y \).

For hyperelliptic curves, identical results hold. A uniformizer at \( \mathcal{O} \) is \( x^g/y \).
Multiplicities of Poles and Zeros for Elliptic Curves

Let \( G(x, y) = a(x) + yb(x) \in K[C] \).

Let \( e \) be the largest exponent for which \((x - h)^e\) divides both \(a(x)\) and \(b(x)\).

Write \( G(x, y) = (x - h)^e G_1(x, y) \).

Take \( l = 0 \) if \( G_1(h, k) \neq 0 \).

If \( G_1(h, k) = 0 \), take \( l \) to be the largest exponent for which \((x - h)^l \mid N(G_1)\).

\[
\text{ord}_P(G) = \begin{cases} 
  e + l & \text{if } P \text{ is an ordinary point,} \\
  2e + l & \text{if } P \text{ is a special point.}
\end{cases}
\]

\[
\text{ord}_O(G) = -\max(2 \deg_x a, 3 + 2 \deg_x b).
\]

For a rational function \( R(x, y) = G(x, y)/H(x, y) \in K(C) \), we have \( \text{ord}_P(R) = \text{ord}_P(G) - \text{ord}_P(H) \).

For hyperelliptic curves, identical results hold.

The order of \( G \) at \( O \) is \( \text{ord}_O(G) = -\max(2 \deg_x a, 2g + 1 + 2 \deg_x b) \).
Poles and Zeros on Elliptic Curves: Examples

Consider the elliptic curve $C : Y^2 = X^3 - X$.

Rational functions involving only $x$ are simpler. $R_1 = \frac{(x-1)(x+1)}{x^3(x-2)}$ has simple zeros at $x = \pm 1$, a simple pole at $x = 2$, and a pole of multiplicity three at $x = 0$. The points on $C$ with these $x$-coordinates are $P_1 = (0, 0)$, $P_2 = (1, 0)$, $P_3 = (-1, 0)$, $P_4 = (2, \sqrt{6})$ and $P_5 = (2, -\sqrt{6})$. $P_1, P_2, P_3$ are special points, so $\text{ord}_{P_1}(R_1) = -6$, $\text{ord}_{P_2}(R_1) = \text{ord}_{P_3}(R_1) = 2$. $P_4$ and $P_5$ are ordinary points, so $\text{ord}_{P_4}(R_1) = \text{ord}_{P_5}(R_1) = -1$. Finally, note that $R_1 \to \frac{1}{x^2}$ as $x \to \infty$. But $x$ has a weight of 2, so $R_1$ has a zero of order 4 at $\mathcal{O}$. The sum of these orders is $-6 + 2 + 2 - 1 - 1 + 4 = 0$.

Now, consider the rational function $R_2 = \frac{x}{y}$ involving $y$. At the point $P_1 = (0, 0)$, $R_2$ appears to be undefined. But $y^2 = x^3 - x$, so $R_2 = \frac{y}{x^2-1}$ too, and $R_2(P_1) = 0$, that is, $R_2$ has a zero at $P_1$. Using the explicit formula on $y$, show that $e = 0$ and $l = 1$. So $\text{ord}_{P_1}(R_2) = 1$. On the other hand, the denominator $x^2 - 1$ has neither a pole nor a zero at $P_1$. So $\text{ord}_{P_1}(R_2) = 1$.

$\text{ord}_{P_1}(x) = 2$ (since $e = 1$, $l = 0$, and $P_1$ is a special point), so the representation $R_2 = \frac{x}{y}$ also gives $\text{ord}_{P_1}(R_2) = 2 - 1 = 1$. 
Poles and Zeros of a Line: Example

(a) \( \text{ord}_P(l) = \text{ord}_Q(l) = \text{ord}_R(l) = 1 \) and \( \text{ord}_O(l) = -3 \).

(b) \( \text{ord}_P(t) = 2, \text{ord}_Q(t) = 1 \) and \( \text{ord}_O(t) = -3 \).

(c) \( \text{ord}_P(v) = \text{ord}_Q(v) = 1 \) and \( \text{ord}_O(v) = -2 \).
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 \( a_i, \; i \in I \).
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 $\text{Div}_K(C)$ or $\text{Div}(C)$.

All divisors on $C$ of degree 0 form a subgroup denoted by $\text{Div}_K^0(C)$ or $\text{Div}^0(C)$.

**Divisor of a rational function** $R(x, y)$ is $\text{Div}(R) = \sum_P \text{ord}_P(R)[P]$.

A **principal divisor** is the divisor of a rational function.

Principal divisors satisfy: $\text{Div}(R) + \text{Div}(S) = \text{Div}(RS)$ and $\text{Div}(R) - \text{Div}(S) = \text{Div}(R/S)$. 

**Divisors on Curves**
(a) $\text{Div}(l) = [P] + [Q] + [R] - 3[O]$.  

(b) $\text{Div}(t) = 2[P] + [Q] - 3[O]$.  

(c) $\text{Div}(v) = [P] + [Q] - 2[O]$.  

(a) Divisor of a line: Example
Picard Groups and Jacobians

- Suppose that $K$ is algebraically closed.
- Every principal divisor belongs to $\text{Div}_K^0(C)$.
- The set of all principal divisors is a subgroup of $\text{Div}_K^0(C)$, denoted by $\text{Prin}_K(C)$ or $\text{Prin}(C)$.
- Two divisors in $\text{Div}_K(C)$ are called equivalent if they differ by the divisor of a rational function.
- The quotient group $\text{Div}_K(C)/\text{Prin}_K(C)$ is called the divisor class group or the Picard group, denoted $\text{Pic}_K(C)$ or $\text{Pic}(C)$.
- The quotient group $\text{Div}_K^0(C)/\text{Prin}_K(C)$ is called the Jacobian of $C$, denoted $\text{Pic}_K^0(C)$ or $\text{Pic}^0(C)$ or $\mathbb{J}_K(C)$ or $\mathbb{J}(C)$.
- If $K$ is not algebraically closed, $\mathbb{J}_K(C)$ is a particular subgroup of $\mathbb{J}_{\bar{K}}(C)$.

Elliptic- and hyperelliptic-curve cryptography deals with the Jacobian of elliptic and hyperelliptic curves.

For elliptic curves, the Jacobian can be expressed by a more explicit chord-and-tangent rule.
**Divisors and the Chord-and-Tangent Rule**

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

- For every $D \in \text{Div}_K^0(C)$, there exist a unique rational point $P$ and a rational function $R$ such that $D = [P] - [\mathcal{O}] + \text{Div}(R)$.
- $D$ is equivalent to $[P] - [\mathcal{O}]$ in $\mathbb{J}_K(C)$.
- Identify $P$ with the equivalence class of $[P] - [\mathcal{O}]$ in $\mathbb{J}_K(C)$.
- This identification yields a bijection between the set of rational points on $C$ and its Jacobian $\mathbb{J}_K(C)$.
- This bijection also leads to the chord-and-tangent rule in the following sense:

Let $D = \sum_P m_P[P] \in \text{Div}_K(C)$. 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

Identity: \( \mathcal{O} \) is identified with \([\mathcal{O}] - [\mathcal{O}] = 0 = \text{Div}(1)\).

Opposite: By Part (c), \( \text{Div}(v) = ([P] - [\mathcal{O}]) + ([Q] - [\mathcal{O}]) \) is 0 in \( \mathbb{J}(C) \). By the correspondence, \( P + Q = \mathcal{O} \), that is, \( Q = -P \).

Sum: By Part (a), \( \text{Div}(l) = ([P] - [\mathcal{O}]) + ([Q] - [\mathcal{O}]) + ([R] - [\mathcal{O}]) \) is 0 in \( \mathbb{J}(C) \), that is, \( P + Q + R = \mathcal{O} \), that is, \( P + Q = -R \).

Double: By Part (b), \( \text{Div}(t) = ([P] - [\mathcal{O}]) + ([P] - [\mathcal{O}]) + ([Q] - [\mathcal{O}]) \) is 0 in \( \mathbb{J}(C) \), that is, \( P + P + Q = \mathcal{O} \), that is, \( 2P = -Q \).
References for Part I


Part II

Elliptic Curves

- Rational Maps and Endomorphisms on Elliptic Curves
- Multiplication-by-$m$ Maps and Division Polynomials
- Weil and Tate Pairing
Notations and Assumptions

- $K$ is a field.
- $\bar{K}$ is the algebraic closure of $K$.
- Quite often, we will have $K = \mathbb{F}_q$ with $p = \text{char } K$.
- $E : Y^2 + (a_1X + a_3)Y = X^3 + a_2X^2 + a_4X + a_6$ is an elliptic curve defined over $K$ (that is, $a_i \in K$).
- If $L$ is any field with $K \subseteq L \subseteq \bar{K}$, then $E$ is defined over $L$ as well.
- $E_L$ denotes the set of $L$-rational points on $E$.
- $E_L$ always contains the point $O$ at infinity.
- If $L = \mathbb{F}_{q^k}$, we write $E_{q^k}$ as a shorthand for $E_L$.
- $E$ (without any subscript) means $E_{\bar{K}}$.
- A rational function $R$ on $E$ is an element of $\bar{K}(E)$.
- $R$ is defined over $L$ if $R$ has a representation $R = G(x, y)/H(x, y)$ with $G, H \in L[x, y]$. 
Elliptic Curves Over Finite Fields

Let $K$ be not algebraically closed (like $K = \mathbb{F}_q$).

The group $E_{\overline{K}}$ is isomorphic to $J_{\overline{K}}(E)$.

The one-to-one correspondence of $J_{\overline{K}}(E)$ with $E_{\overline{K}}$ allows us to use the chord-and-tangent rule.

If $P$ and $Q$ are $K$-rational, then the chord-and-tangent rule guarantees that $P + Q$ is $K$-rational too.

All $K$-rational points in $E_{\overline{K}}$ together with $O$ constitute a subgroup of $E_{\overline{K}}$.

Denote this subgroup by $E_K$.

$E_K$ can be identified with a subgroup $J_K(E)$ of $J_{\overline{K}}(E)$.

Since $K$ is not algebraically closed, $J_K(E)$ cannot be defined like $J_{\overline{K}}(E)$.

Thanks to the chord-and-tangent rule, we do not need to worry too much about $J_K(E)$ (at least so long as computational issues are of only concern).
Discriminants and $j$-invariants

Define the following quantities for $E$:

\[
\begin{align*}
d_2 &= a_1^2 + 4a_2 \\
d_4 &= 2a_4 + a_1a_3 \\
d_6 &= a_3^2 + 4a_6 \\
d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= d_2^2 - 24d_4 \\
\Delta(E) &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \\
j(E) &= c_4^3/\Delta(E), \text{ if } \Delta(E) \neq 0.
\end{align*}
\]

$\Delta(E)$ is called the **discriminant** of $E$.

$j(E)$ is called the **$j$-invariant** of $E$.

$E$ is smooth (that is, an elliptic curve) if and only if $\Delta(E) \neq 0$.

$j(E)$ is defined for every elliptic curve.

For two elliptic curves $E, E'$, we have $j(E) = j(E')$ if and only if $E$ and $E'$ are isomorphic.
Addition Formula for the General Weierstrass Equation

Let \( P = (h_1, k_1) \) and \( Q = (h_2, k_2) \) be points on \( E \). Assume that \( P, Q, P + Q \) are not \( O \). Let \( R = (h_3, k_3) = P + Q \).

\[
h_3 = \lambda^2 + a_1 \lambda - a_2 - h_1 - h_2, \quad \text{and}
\]

\[
k_3 = -(\lambda + a_1)h_3 - \mu - a_3, \quad \text{where}
\]

\[
\lambda = \begin{cases} 
\frac{k_2 - k_1}{h_2 - h_1} & \text{if } P \neq Q, \\
\frac{3h_1^2 + 2a_2h_1 + a_4 - a_1k_1}{2k_1 + a_1h_1 + a_3} & \text{if } P = Q, \text{ and}
\end{cases}
\]

\[
\mu = k_1 - \lambda h_1 .
\]

The opposite of \( (h, k) \) is \( (h, -k - a_1h - a_3) \).
Choosing a Random Point on an Elliptic Curve

Let $E : Y^2 + (a_1 X + a_3)Y = X^3 + a_2 X^2 + a_4 X + a_6$ be defined over $K$. To obtain a random point $P = (h, k) \in E_K$.

- Choose the $X$-coordinate $h$ randomly from $K$.
- The corresponding $Y$-coordinates are roots of
  \[ Y^2 + (a_1 h + a_3)Y - (h^3 + a_2 h^2 + a_4 h + a_6). \]
- This polynomial is either irreducible over $K$ or has two roots in $K$.
- If $K$ is algebraically closed, then this polynomial has roots in $K$.
- If $K$ is a finite field, then, with probability about $1/2$, this polynomial has roots in $K$.
- Use a root-finding algorithm to compute a root $k$.
- Output $(h, k)$. 
Rational Maps on Elliptic Curves

- A **rational map** on $E$ is a function $E \to E$.

- A rational map $\alpha$ is specified by two rational functions $\alpha_1, \alpha_2 \in \bar{K}(E)$ such that, for any point $P \in E$, $\alpha(P) = \alpha(h, k) = (\alpha_1(h, k), \alpha_2(h, k))$ is again a point on $E$.

- Since $\alpha(P)$ is a point on $E$, $\alpha_1, \alpha_2$ satisfy the equation for $E$ and constitute the elliptic curve $E_{\bar{K}(E)}$.

- Denote the point at infinity on this curve by $O'$. Define $O'(P) = O$ for all $P \in E$.

- For a non-zero $\alpha \in E_{\bar{K}(E)}$ and a point $P \in E$, either both $\alpha_1(P), \alpha_2(P)$ are defined at $P$, or both are undefined at $P$. In the first case, we take $\alpha(P) = (\alpha_1(P), \alpha_2(P))$, and in the second case, $\alpha(P) = O$.

- The addition of $E_{\bar{K}(E)}$ is compatible with the addition of $E$, that is, $(\alpha + \beta)(P) = \alpha(P) + \beta(P)$ for all $\alpha, \beta \in E_{\bar{K}(E)}$ and $P \in E$.

- A rational map is either constant or surjective.
The **zero map** $\mathcal{O}': E \rightarrow E$, $P \mapsto \mathcal{O}$.

The **identity map** $\text{id} : E \rightarrow E$, $P \mapsto P$.

The **translation map** $\tau_Q : E \rightarrow E$, $P \mapsto P + Q$, for a fixed $Q \in E$.

The **multiplication-by-$m$ map** $[m] : E \rightarrow E$, $P \mapsto mP$, where $m \in \mathbb{Z}$.

The **Frobenius map** $\varphi$:

$E$ is defined over $K = \overline{\mathbb{F}}_q$.

For $a \in \bar{K}$, $a^q = a$ if and only if $a \in \mathbb{F}_q$.

For $P = (h, k) \in E$, the point $(h^q, k^q) \in E$.

Define $\varphi(h, k) = (h^q, k^q)$. 
Endomorphisms

A rational map on $E$, which is also a group homomorphism of $E$, is called an endomorphism or an isogeny.

The set of all endomorphisms of $E$ is denoted by $\text{End}(E)$.

Define addition in $\text{End}(E)$ as $(\alpha + \beta)(P) = \alpha(P) + \beta(P)$.

Define multiplication in $\text{End}(E)$ as $(\alpha \circ \beta)(P) = \alpha(\beta(P))$.

$\text{End}(E)$ is a ring under these operations. The additive identity is $O'$. The multiplicative identity is $\text{id}$.

All multiplication-by-$m$ maps $[m]$ are endomorphisms. We have $[m] \neq [n]$ for $m \neq n$.

The translation map $\tau_Q$ is not an endomorphism unless $Q = O$.

The Frobenius map $\varphi$ is an endomorphism with $\varphi \neq [m]$ for any $m$.

If $\text{End}(E)$ contains a map other than the maps $[m]$, $E$ is called a curve with complex multiplication.
The Multiplication-by-$m$ Maps

Identify $[m]$ as a pair $(g_m, h_m)$ of rational functions.

$g_1 = x$, $h_1 = y$.

$g_2 = -2x + \lambda^2 + a_1 \lambda - a_2$ and

$h_2 = -\lambda(g_2 - x) - a_1 g_2 - a_3 - y$,

where $\lambda = \frac{3x^2 + 2a_2 x + a_4 - a_1 y}{2y + a_1x + a_3}$.

For $m \geq 3$, we have the recursive definition:

$g_m = -g_{m-1} - x + \lambda^2 + a_1 \lambda - a_2$ and

$h_m = -\lambda(g_m - x) - a_1 g_m - a_3 - y$,

where $\lambda = \frac{h_{m-1} - y}{g_{m-1} - x}$. 
The Group of $m$-torsion Points

For $m \in \mathbb{N}$, define $E[m] = \{P \in E \mid mP = \mathcal{O}\}$.

Recall that $p = \text{char } K$.

If $p = 0$ or gcd$(p, m) = 1$, then $E[m] \cong \mathbb{Z}_m \times \mathbb{Z}_m$, and so $|E[m]| = m^2$.

Suppose that $p > 0$. Let $m = p^\nu m'$ with gcd$(m', p) = 1$. Then,

$E[m] \cong \begin{cases} 
\mathbb{Z}_{m'} \times \mathbb{Z}_{m'} & \text{if } E[p] = \{\mathcal{O}\}, \\
\mathbb{Z}_{m'} \times \mathbb{Z}_m & \text{otherwise.}
\end{cases}$

If gcd$(m, n) = 1$, we have $E[mn] \cong E[m] \times E[n]$.

For a subset $S \subseteq E$, define the divisor $[S] = \sum_{P \in S}[P]$.

If $p \neq 2, 3$ and $m, n, m + n, m - n$ are all coprime to $p$, we have

$\text{Div}(g_m - g_n) = [E[m + n]] + [E[m - n]] - 2[E[m]] - 2[E[n]]$.

If $p \in \{2, 3\}$, gcd$(m, p) = 1$, and $n = p^\nu n'$ with $\nu \geq 1$ and gcd$(n', p) = 1$, we have

$\text{Div}(g_m - g_n) = [E[m + n]] + [E[m - n]] - 2[E[m]] - 2\alpha^\nu[E[n]]$. 
Division Polynomials

The rational functions \( g_m, h_m \) have poles precisely at the points in \( E[m] \). But they have some zeros also.

We investigate polynomials having zeros precisely at the points of \( E[m] \).

Assume that either \( p = 0 \) or \( \gcd(p, m) = 1 \).

\( E[m] \) contains exactly \( m^2 \) points with \( \sum_{P \in E[m]} P = \mathcal{O} \).

Consider the degree-zero divisor \( [E[m]] - m^2[\mathcal{O}] = \sum_{P \in E[m]} [P] - m^2[\mathcal{O}] \).

There exists a rational function \( \psi_m \) with \( \text{Div}(\psi_m) = [E[m]] - m^2[\mathcal{O}] \).

Since the only pole of \( \psi_m \) is at \( \mathcal{O} \), \( \psi_m \) is a polynomial function.

\( \psi_m \) is unique up to multiplication of elements of \( \bar{K}^* \).

If we arrange the leading coefficient of \( \psi_m \) to be \( m \), then \( \psi_m \) becomes unique and is called the \textbf{\( m \)-th division polynomial}.
Division Polynomials: Explicit Formulas

\[\psi_0 = 0\]
\[\psi_1 = 1\]
\[\psi_2 = 2y + a_1 x + a_3\]
\[\psi_3 = 3x^4 + d_2 x^3 + 3d_4 x^2 + 3d_6 x + d_8\]
\[\psi_4 = [2x^6 + d_2 x^5 + 5d_4 x^4 + 10d_6 x^3 + 10d_8 x^2 + (d_2 d_8 - d_4 d_6) x + d_4 d_8 - d_6^2] \psi_2\]
\[\psi_{2m} = \frac{(\psi_{m+2} \psi_{m-1}^2 - \psi_{m-2} \psi_{m+1}^2) \psi_m}{\psi_2} \text{ for } m > 2\]
\[\psi_{2m+1} = \psi_{m+2} \psi_{m}^3 - \psi_{m-1} \psi_{m+1}^3 \text{ for } m \geq 2.\]

\[g_m - g_n = -\frac{\psi_{m+n} \psi_{m-n}}{\psi_m^2 \psi_n^2}\]. Putting \(n = 1\) gives \(g_m = x - \frac{\psi_{m+1} \psi_{m-1}}{\psi_m^2}\).

\[h_m = \frac{\psi_{m+2} \psi_{m-1}^2 - \psi_{m-2} \psi_{m+1}^2}{2 \psi_2 \psi_m^3} - \frac{1}{2} (a_1 g_m + a_3)\]
\[= y + \frac{\psi_{m+2} \psi_{m-1}^2}{\psi_2 \psi_m^3} + (3x^2 + 2a_2 x + a_4 - a_1 y) \frac{\psi_{m-1} \psi_{m+1}}{\psi_2 \psi_m^2}.\]
Size and Structure of $E_q$

**Hasse’s Theorem:** $|E_q| = q + 1 - t$ with $-2\sqrt{q} \leq t \leq 2\sqrt{q}$.

$t$ is called the **trace of Frobenius** at $q$.

The Frobenius endomorphism satisfies $\varphi \circ \varphi - [t] \circ \varphi + [q] = O'$.

Let $L = \mathbb{F}_{q^k}$ be an extension of $K = \mathbb{F}_q$.

Let $W^2 - tW + q = (W - \alpha)(W - \beta)$ with $\alpha, \beta \in \mathbb{C}$.

**Weil’s Theorem:** $|E_{q^k}| = q^k + 1 - (\alpha^k + \beta^k)$.

**Example:** Consider $E : Y^2 = X^3 + X + 1$ defined over $\mathbb{F}_5$. $E_5$ contains the nine points $\mathcal{O}$, $(0, \pm 1)$, $(2, \pm 1)$, $(3, \pm 1)$ and $(4, \pm 2)$, so that $|E_5| = 9 = (5 + 1) - t$, that is, $t = -3$.

Consider $(W - \alpha)(W - \beta) = W^2 - tW + q = W^2 + 3W + 5$, that is, $\alpha + \beta = -3$ and $\alpha\beta = 5$. But then $\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = 9 - 10 = -1$. Therefore, $|E_{25}| = 25 + 1 - (-1) = 27$.

**Structure Theorem for $E_q$:**

$E_q$ is either cyclic or isomorphic to $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ with $n_1, n_2 \geq 2$, $n_1 | n_2$, and $n_1 | (q - 1)$.
More on Divisors

\[
\text{Div}(L_P, Q) = [P] + [Q] + [R] - 3[\mathcal{O}].
\]
\[
\text{Div}(L_R, -R) = [R] + [-R] - 2[\mathcal{O}].
\]
\[
\text{Div}(L_P, Q/L_R, -R) = [P] + [Q] - [-R] - [\mathcal{O}] = [P] + [Q] - [P + Q] - [\mathcal{O}].
\]
\[
[P] - [\mathcal{O}] \text{ is equivalent to } [P + Q] - [Q].
\]
\[
([P] - [\mathcal{O}]) + ([Q] - [\mathcal{O}]) \text{ is equivalent to } [P + Q] - [\mathcal{O}].
\]

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 $\text{Div}(f)$ are disjoint. Define

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

$\text{Div}(f) = \text{Div}(g)$ 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 $\text{Div}(f)$ and $\text{Div}(g)$ have disjoint supports, then

$$f(\text{Div}(g)) = g(\text{Div}(f)).$$
**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 $p = \text{char } K$.

Let $\mu_m$ denote the $m$-th roots of unity in $\bar{K}$.

We have $\mu_m \subseteq \mathbb{F}_{q^k}$, where $k = \text{ord}_m(q)$ 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

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

defined as follows.

Take $P_1, P_2 \in E[m]$.

Let $D_1$ be a divisor equivalent to $[P_1] - [O]$. Since $mP_1 = O$, there exists a rational function $f_1$ such that $\text{Div}(f_1) = mD_1 = m[P_1] - m[O]$.

Similarly, let $D_2$ be a divisor equivalent to $[P_2] - [O]$. There exists a rational function $f_2$ such that $\text{Div}(f_2) = mD_2 = m[P_2] - m[O]$.

$D_1$ and $D_2$ are chosen to have disjoint supports.

Define $e_m(P_1, P_2) = f_1(D_2)/f_2(D_1)$. 
Weil Pairing is Well-defined

- \( f_1 \) and \( f_2 \) are unique up to multiplication by non-zero elements of \( \bar{K}^* \). So \( f_1(D_2) \) and \( f_2(D_1) \) are independent of the choices of \( f_1 \) and \( f_2 \).

- Let \( D_1' = D_1 + \text{Div}(g) \) have disjoint support from \( D_2 \). But then

\[
mD_1' = mD_1 + m \text{Div}(g) = \text{Div}(f_1) + \text{Div}(g^m) = \text{Div}(f_1g^m).
\]

Therefore,

\[
f_1g^m(D_2)/f_2(D_1 + \text{Div}(g)) = \frac{f_1(D_2)g^m(D_2)}{f_2(D_1)f_2(\text{Div}(g))} = \frac{f_1(D_2)g(mD_2)}{f_2(D_1)f_2(\text{Div}(g))} = \frac{f_1(D_2)g(\text{Div}(f_2))}{f_2(D_1)f_2(\text{Div}(g))} = \frac{f_1(D_2)g(\text{Div}(f_2))}{f_2(D_1)g(\text{Div}(f_2))} = \frac{f_1(D_2)}{f_2(D_1)}.
\]

So \( e_m(P_1, P_2) \) is independent of the choice of \( D_1 \) and likewise of \( D_2 \) too.

- It is customary to choose \( D_2 = [P_2] - [\mathcal{O}] \) and \( D_1 = [P_1 + T] - [T] \) for a point \( T \) different from \(-P_1, P_2, P_2 - P_1, \) and \( \mathcal{O} \). \( T \) need not be in \( E[m] \).

One can take \( T \) randomly from \( E \).

- \( e_m(P_1, P_2)^m = f_1(mD_2)/f_2(mD_1) = f_1(\text{Div}(f_2))/f_2(\text{Div}(f_1)) = 1 \) (by Weil reciprocity), that is, \( e_m(P_1, P_2) \) is indeed an \( m \)-th root of unity.
Properties of Weil Pairing

Let \( P, Q, R \) be arbitrary points in \( E[m] \).

**Bilinearity:**

\[
e_m(P + Q, R) = e_m(P, R)e_m(Q, R),
\]
\[
e_m(P, Q + R) = e_m(P, Q)e_m(P, R).
\]

**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
\[
\text{Div}(f_{n,P}) = n[P] - [nP] - (n - 1)[\mathcal{O}].
\]
$f_{n,P}$ are unique up to multiplication by elements of $\overline{K}^*$. We may choose the unique monic polynomial for $f_{n,P}$.

$f_{n,P}$ satisfy the recurrence relation:
\[
\begin{align*}
  f_{0,P} &= f_{1,P} = 1, \\
  f_{n+1,P} &= \left( \frac{L_{P,nP}}{L_{(n+1)P, -(n+1)P}} \right) f_{n,P} \text{ for } n \geq 1, \\
  f_{-n,P} &= \frac{1}{f_{n,P}} \text{ for } n \geq 1.
\end{align*}
\]

If $P \in E[m]$, then $\text{Div}(f_{m,P}) = m[P] - [mP] - (m - 1)[\mathcal{O}] = m[P] - m[\mathcal{O}]$.

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 $n = (n_sn_{s-1} \ldots n_1n_0)_2$ 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 $e_m(P_1, P_2) = \frac{f_{m,P_2}(T) f_{m,P_1}(P_2 - T)}{f_{m,P_1}(-T) f_{m,P_2}(P_1 + T)}$.

If $P_1 \neq P_2$, then we also have $e_m(P_1, P_2) = (-1)^m \frac{f_{m,P_1}(P_2)}{f_{m,P_2}(P_1)}$.

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.
Tate Pairing

Let $E$ be an elliptic curve defined over $K = \mathbb{F}_q$ with $p = \text{char } K$.
Let $m$ be a positive integer coprime to $p$.
Let $k = \text{ord}_m(q)$ (the embedding degree), and $L = \mathbb{F}_{q^k}$.
Let $E_L[m] = \{ P \in E_L \mid mP = \mathcal{O} \}$, and $mE_L = \{ mP \mid P \in E_L \}$.
Let $(L^*)^m = \{ a^m \mid a \in L^* \}$ be the set of $m$-th powers in $L^*$.

Let $P$ be a point in $E_L[m]$, and $Q$ a point in $E_L$.

Since $mP = \mathcal{O}$, there is a rational function $f$ with $\text{Div}(f) = m[P] - m[\mathcal{O}]$.

Let $D$ be any divisor equivalent to $[Q] - [\mathcal{O}]$ with disjoint support from $\text{Div}(f)$. It is customary to choose a point $T$ different from $-P, Q, Q - P, \mathcal{O}$ and take $D = [Q + T] - [T]$.

The Tate pairing $\langle , \rangle_m : E_L[m] \times E_L/mE_L \to L^*/(L^*)^m$ of $P$ and $Q$ is

$$\langle P, Q \rangle_m = f(D).$$

$Q$ should be regarded as a point in $E_L/mE_L$.

The value of $\langle P, Q \rangle_m$ is unique up to multiplication by an $m$-th power of a non-zero element of $L$, that is, $\langle P, Q \rangle_m$ is unique in $L^*/(L^*)^m$. 
Properties of Tate Pairing

Bilinearity:

\[
\langle P + Q, R \rangle_m = \langle P, R \rangle_m \langle Q, R \rangle_m,
\]

\[
\langle P, Q + R \rangle_m = \langle P, Q \rangle_m \langle P, R \rangle_m.
\]

Non-degeneracy: For every \( P \in E_L[m], P \neq O \), there exists \( Q \) with \( \langle P, Q \rangle_m \neq 1 \). For every \( Q \notin mE_L \), there exists \( P \in E_L[m] \) with \( \langle P, Q \rangle_m \neq 1 \).

The Weil pairing is related to the Tate pairing as

\[
e_m(P, Q) = \frac{\langle P, Q \rangle_m}{\langle Q, P \rangle_m}
\]

up to \( m \)-th powers.

Let \( k = \text{ord}_m(q) \) be the embedding degree. The Tate pairing can be made unique by exponentiation to the power \((q^k - 1)/m\):

\[
\hat{e}_m(P, Q) = \left( \langle P, Q \rangle_m \right)^{q^k - 1 \over m}
\]

\( \hat{e}_m(P, Q) \) is called the reduced Tate pairing. The reduced pairing continues to exhibit bilinearity and non-degeneracy.
Computing the Tate Pairing

- Take $D = [Q + T] - [T]$, where $T \neq P, -Q, P - Q, O$.
- We have $\langle P, Q \rangle_m = \frac{f_{m,P}(Q + T)}{f_{m,P}(T)}$.
- Miller’s algorithm is used to compute $\langle P, Q \rangle_m$.
- A single double-and-add loop suffices.
- For efficiency, the numerator and the denominator in $f$ may be updated separately. After the loop, a single division is made.
- If the reduced pairing is desired, then a final exponentiation to the power $(q^k - 1)/m$ is made on the value returned by Miller’s algorithm.
Weil vs. Tate Pairing

- The Miller loop for Tate pairing is more efficient than that for Weil pairing.
- The reduced Tate pairing demands an extra exponentiation.
- Let \( k = \text{ord}_m(q) \) be the embedding degree, and \( L = \mathbb{F}_{q^k} \).
- Tate pairing requires working in the field \( L \).
- Let \( L' \) be the field obtained by adjoining to \( L \) all the coordinates of \( E[m] = E_K[m] \).
- Weil pairing requires working in the field \( L' \).
- \( L' \) is potentially much larger than \( L \).
- **Special case:** \( m \) is a prime divisor of \( |E_K| \) with \( m \nmid q \) and \( m \nmid (q - 1) \). Then, \( L' = L \). So it suffices to work in the field \( L \) only.
- For cryptographic applications, Tate pairing is used more often than Weil pairing.
- One takes \( \mathbb{F}_q \) with \( |q| \) about 160–300 bits and \( k \leq 12 \). Larger embedding degrees are impractical for implementation.
Distortion Maps

Let $m$ be a prime divisor of $|E_K|$.
Let $P$ be a generator of a subgroup $G$ of $E_K$ of order $m$.

**Goal:** To define a pairing of the points in $G$.

- If $k = 1$ (that is, $L = K$), then $\langle P, P \rangle_m \neq 1$.
- **Bad news:** If $k > 1$, then $\langle P, P \rangle_m = 1$.
  But then, by bilinearity, $\langle Q, Q' \rangle_m = 1$ for all $Q, Q' \in G$.

- **A way out:** If $k > 1$ and $Q \in L$ is linearly independent of $P$ (that is, $Q \notin G$), then $\langle P, Q \rangle_m \neq 1$.

- Let $\phi : E_L \to E_L$ be an endomorphism of $E_L$ with $\phi(P) \notin G$.
  $\phi$ is called a **distortion map**.

Define the **distorted Tate pairing** of $P, Q \in G$ as $\langle P, \phi(Q) \rangle_m$.
- Since $\phi(P)$ is linearly independent of $P$, we have $\langle P, \phi(P) \rangle_m \neq 1$.
- Since $\phi$ is an endomorphism, bilinearity is preserved.

**Symmetry:** We have $\langle Q, \phi(Q') \rangle_m = \langle Q', \phi(Q) \rangle_m$ for all $Q, Q' \in G$.

Distortion maps exist only for supersingular curves.
Twists

Let $E$ be defined by the short Weierstrass equation $Y^2 = X^3 + aX + b$. Let $d \geq 2$, and $v \in \mathbb{F}_q^*$ a $d$-th power non-residue.

Consider the curve $E' : Y^2 = X^3 + v^{4/d}aX + v^{6/d}b$ (defined over $\mathbb{F}_{q^d}$).

If $d = 2$, then $E'$ is defined over $\mathbb{F}_q$ itself.

$E'$ is called a twist of $E$ of degree $d$.

$E$ and $E'$ are isomorphic over $\mathbb{F}_{q^d}$. An explicit isomorphism is given by the map $\phi_d : E' \rightarrow E$ taking $(h, k) \mapsto (v^{-2/d}h, v^{-3/d}k)$.

Let $m$ be a prime divisor of $|E_q|$, $G$ a subgroup of order $m$ in $E_{q^k}$, and $G'$ a subgroup of order $m$ in $E'_{q^k}$. Let $P, P'$ be generators of $G$ and $G'$. Suppose that $\phi_d(P')$ is linearly independent of $P$.

For $d = 2$ (quadratic twist), a natural choice is $G \subseteq E_q$ and $G' \subseteq E'_q$.

Define a pairing of points $Q \in G$ and $Q' \in G'$ as $\langle Q, \phi_d(Q') \rangle_m$.

This is called the twisted Tate pairing.
Pairing-friendly Curves

- **Requirement for efficient computation:** Small embedding degree $k$.
- For general curves, $k$ is quite high ($|k| \approx |m|$).
- Only some specific types of curves qualify as pairing-friendly.

**Supersingular curves**

- By Hasse’s Theorem, $|E_q| = q + 1 - t$ with $|t| \leq 2\sqrt{q}$.
- If $p|t$, we call $E$ a **supersingular curve**.
- Curves of the form $Y^2 + aY = X^3 + bX + c$ are supersingular over fields of characteristic 2.
- All supersingular curves over a finite field $K$ of characteristic 2 have $j$-invariant equal to 0, and so are isomorphic over $\bar{K}$. The same result holds for $p = 3$.
- Supersingular curves have small embedding degrees. The only possibilities are 1, 2, 3, 4, 6.
- If $\mathbb{F}_q$ is a prime field with $q \geq 5$, the only possibility is $k = 2$.
- Non-supersingular curves are called **ordinary curves**.
- It is difficult to locate ordinary curves with small embedding degrees.
How to Find Pairing-friendly Curves

Let \( k \) be a positive integer, and \( \Delta \) a small positive square-free integer.

Search for integer-valued polynomials \( t(x), m(x), q(x) \in \mathbb{Q}[x] \) to represent a family of elliptic curves of embedding degree \( k \) and discriminant \( \Delta \). The triple \((t, m, q)\) should satisfy the following:

1. \( q(x) = p(x)^n \) for some \( n \in \mathbb{N} \) and \( p(x) \in \mathbb{Q}[x] \) representing primes.
2. \( m(x) \) is irreducible with a positive leading coefficient.
3. \( m(x) \mid q(x) + 1 - t(x) \).
4. \( m(x) \mid \Phi_k(t(x) - 1) \), where \( \Phi_k \) is the \( k \)-th cyclotomic polynomial.
5. There are infinitely many integers \((x, y)\) satisfying \( \Delta y^2 = 4q(x) - t(x)^2 \).

If \( y \) in Condition 5 can be parameterized by a polynomial \( y(x) \in \mathbb{Q}[x] \), the family is called \textbf{complete}, otherwise it is called \textbf{sparse}.

For obtaining ordinary curves, we require \( \gcd(q(x), m(x)) = 1 \).

The \textbf{complex multiplication method} is used to obtain specific examples of elliptic curves \( E \) over \( \mathbb{F}_q \) with \( E_q \) having a subgroup of order \( m \).
Some sparse families of ordinary pairing-friendly curves are:

- **MNT (Miyaji-Nakabayashi-Takano) curves:** These are curves of prime orders with embedding degrees 3, 4 or 6.
- **Freeman curves:** These curves have embedding degree 10.

Some complete families of ordinary pairing-friendly curves are:

- **BN (Barreto-Naehrig) curves:** These curves have embedding degree 12 and discriminant 3.
- **SB (Scott-Barreto) curves**
- **BLS (Barreto-Lynn-Scott) curves**
- **BW (Brezing-Weng) curves**
Efficient Implementation

**Denominator elimination:** Let $k$ be even. Take $d = k/2$.

$f_{n,P}(Q)$ is computed by Miller’s algorithm, where $Q = (h, k)$ with $h \in \mathbb{F}_{q^d}$.

The denominators $L_{2U,-2U}(Q)$ and $L_{U+P,-(U+P)}(Q)$ correspond to vertical lines, evaluate to elements of $\mathbb{F}_{q^d}$, and can be discarded.

The final exponentiation guarantees correct computation of $\hat{e}_m(P, Q)$.

---

**BMX (Blake-Murty-Xu) refinements** use 2-bit windows in Miller’s loop.

---

**Loop reduction:** With clever modifications to Tate pairing, the number of iterations in the Miller loop can be substantially reduced.

A typical reduction is by a factor of 2.

**Examples**

- $\eta$ and $\eta_T$ pairings
- Ate pairing
- R-ate pairing
References for Part II


DAS, A., Computational Number Theory, Manuscript under preparation.


Part III

Hyperelliptic Curves

Representation of the Jacobian
References for Part III
