An Introduction to the Theory of Elliptic Curves

Joseph H. Silverman

Brown University and
NTRU Cryptosystems, Inc.

Summer School on
Computational Number Theory and Applications to Cryptography
University of Wyoming

June 19 – July 7, 2006

Outline

- Introduction
- Elliptic Curves
- The Geometry of Elliptic Curves
- The Algebra of Elliptic Curves
- What Does $E(K)$ Look Like?
- Elliptic Curves Over Finite Fields
- The Elliptic Curve Discrete Logarithm Problem
- Reduction Modulo p, Lifting, and Height Functions
- Canonical Heights on Elliptic Curves
- Factorization Using Elliptic Curves
- L-Series, Birch–Swinnerton-Dyer, and \$1,000,000
- Additional Material
- Further Reading

The Discrete Logarithm Problem

Fix a group G and an element $g \in G$. The **Discrete Logarithm Problem** (**DLP**) for G is:

Given an element h in the subgroup generated by g, find an integer m satisfying $h = g^m$.

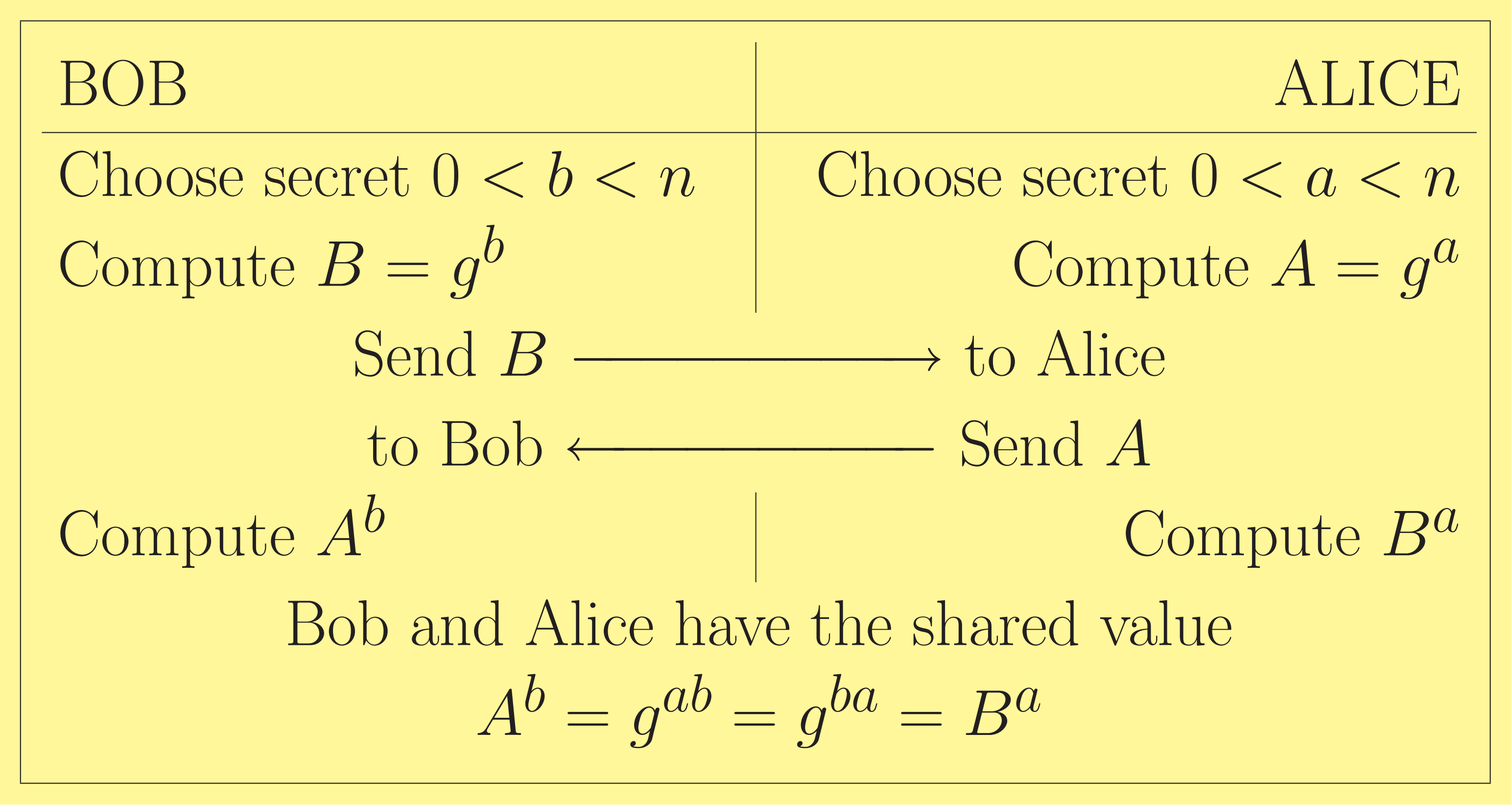
The smallest integer m satisfying $h = g^m$ is called the **logarithm** (or **index**) of h with respect to g, and is denoted

$$m = \log_g(h) \qquad \text{or} \qquad m = \operatorname{ind}_g(h).$$

The Discrete Logarithm Problem is used as the underlying hard problem in many cryptographic constructions, including key exchange, encryption, digital signatures, and hash functions.

Diffie-Hellman Key Exchange

Public Knowledge: Group G and element g of order n.



BOB	ALICE
Choose secret $0 < b < n$	Choose secret $0 < a < n$
Compute $B = g^b$	Compute $A = g^a$

Send B → to Alice

to Bob ← Send A

Compute A^b	Compute B^a

Bob and Alice have the shared value

$$A^b = g^{ab} = g^{ba} = B^a$$

And one hopes that computing g^{ab} from g^a and g^b requires solving the discrete logarithm problem.

How Hard is the Discrete Log Problem?

For some groups, DLP is very easy:

- $\mathbb{Z}/m\mathbb{Z}$ under addition (Euclidean algorithm)
- $\mathbb{R}^*$ or $\mathbb{C}^*$ under multiplication (analytic logarithm)

For some groups, DLP is difficult. The classical example is:

$$\mathbb{F}_p^* \text{ under multiplication}$$

The best known algorithm to solve DLP in $\mathbb{F}_p^*$ takes time

$$O\left(e^{c\sqrt[3]{(\log p)(\log\log p)^2}}\right)$$

This is called **subexponential**, since it is faster than exponential (in $\log p$), but slower than polynomial.
For cryptographic purposes, it would be better to use a group G for which solving DLP takes time that is exponential in the order of G.

Elliptic Curves

What is an Elliptic Curve?

- An elliptic curve is a curve that's also naturally a group.
- The group law is constructed geometrically.
- Elliptic curves have (almost) nothing to do with ellipses, so put ellipses and conic sections out of your thoughts.
- Elliptic curves appear in many diverse areas of mathematics, ranging from number theory to complex analysis, and from cryptography to mathematical physics.

Points on Elliptic Curves

- Elliptic curves can have points with coordinates in any field, such as $\mathbb{F}_p$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$.
- Elliptic curves with points in $\mathbb{F}_p$ are finite groups.
- **Elliptic Curve Discrete Logarithm Problem** (**ECDLP**) is the discrete logarithm problem for the group of points on an elliptic curve over a finite field.
- The best known algorithm to solve the ECDLP is exponential, which is why elliptic curve groups are used for cryptography.
- More precisely, the best known way to solve ECDLP for an elliptic curve over $\mathbb{F}_p$ takes time $O\bigl(\sqrt{p}\,\bigr)$.
- The goal of these talks is to tell you something about the theory of elliptic curves, with an emphasis on those aspects that are of interest in cryptography.

The Equation of an Elliptic Curve

An **Elliptic Curve** is a curve given by an equation of the form

$$\boxed{y^2 = x^3 + Ax + B}$$

There is also a requirement that the **discriminant**

$$\Delta = 4A^3 + 27B^2 \text{ is nonzero.}$$

Equivalently, the polynomial $x^3 + Ax + B$ has distinct roots. This ensures that the curve is nonsingular.

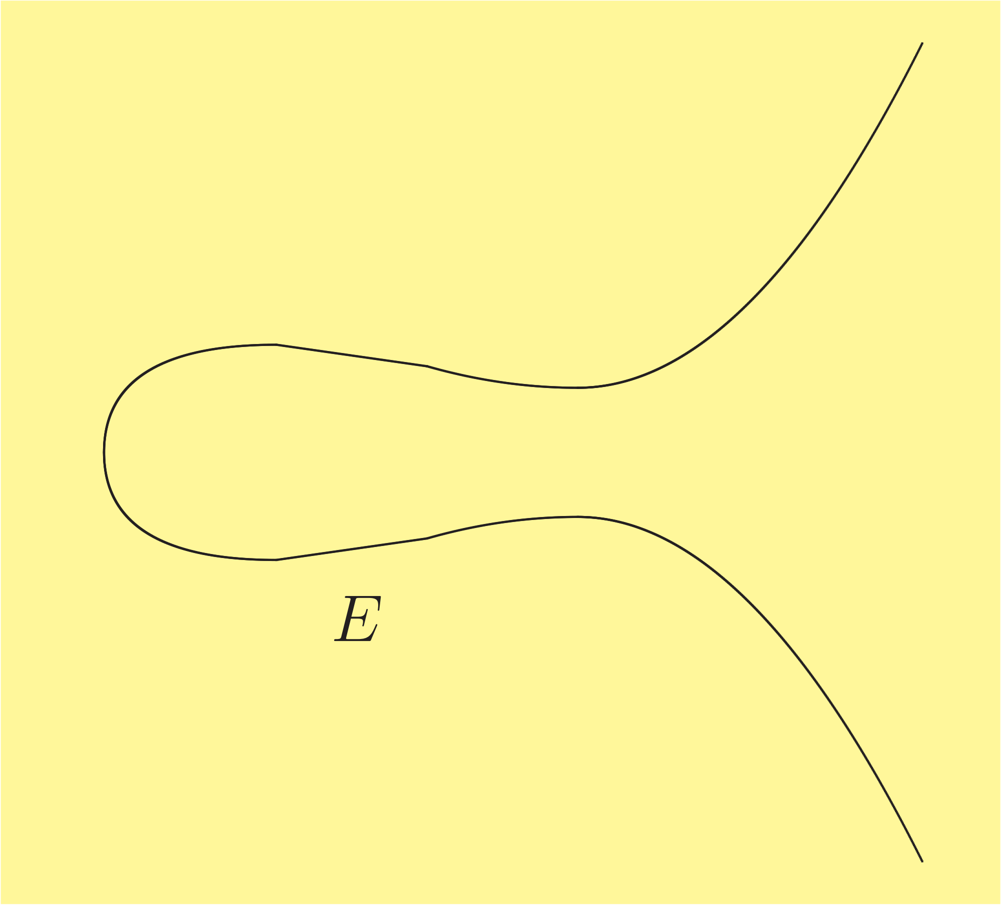
For reasons to be explained later, we also toss in an extra point, $\mathcal{O}$, that is “at infinity,” so E is the set

$$E = \{(x, y) : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

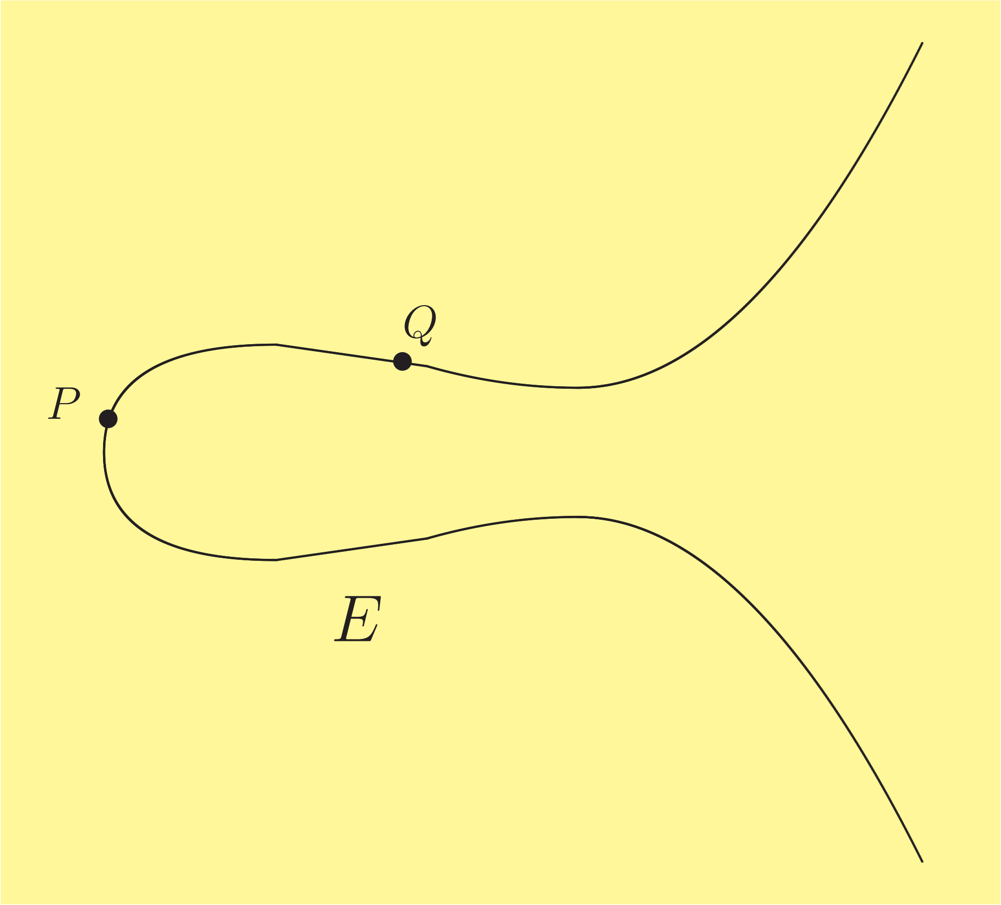
Amazing Fact: We can use **geometry** to make the points of an elliptic curve into a group. The next few slides illustrate how this is accomplished.

The Geometry of Elliptic Curves

The Elliptic Curve $E : y^2 = x^3 - 5x + 8$

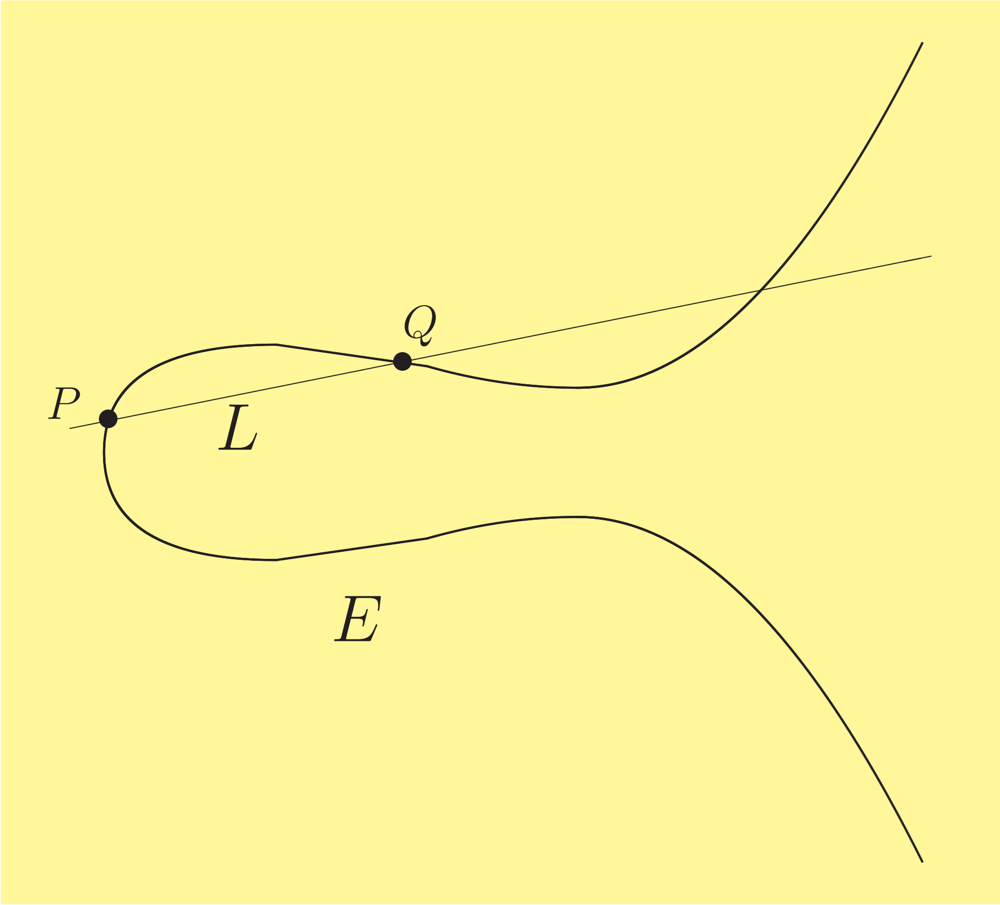


Adding Points on an Elliptic Curve



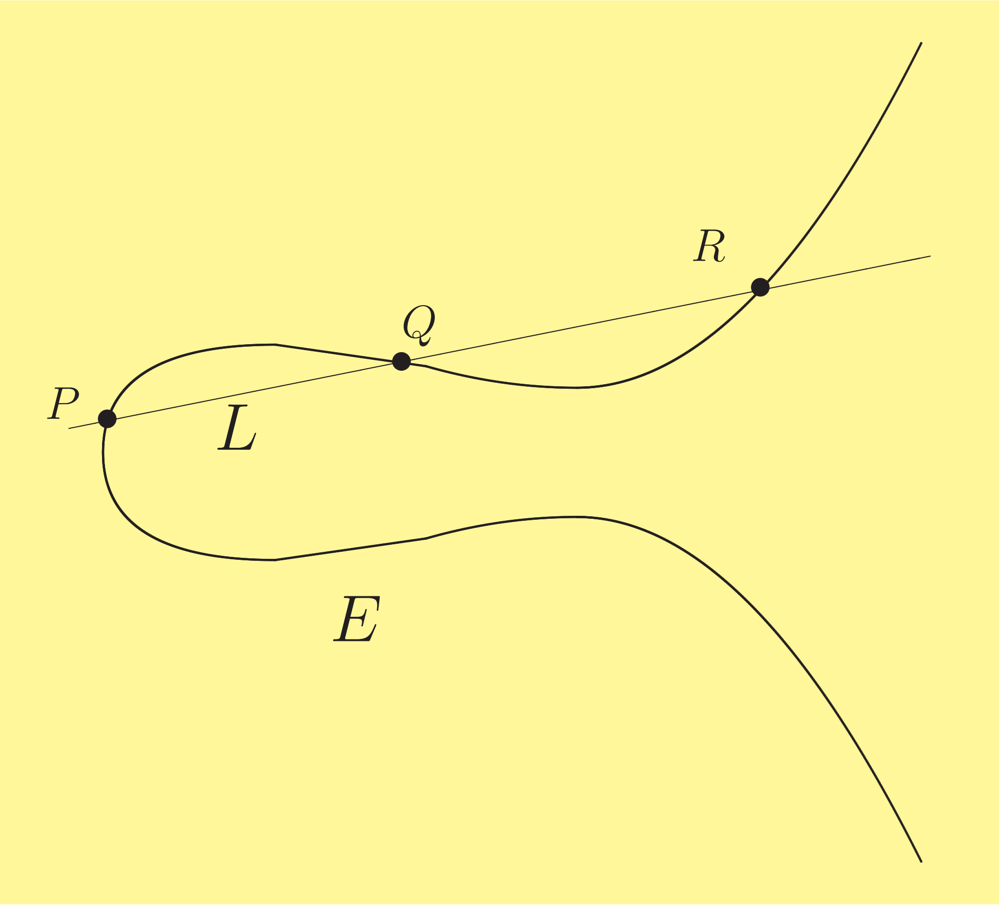
Start with two points P and Q on E.

Adding Points on an Elliptic Curve



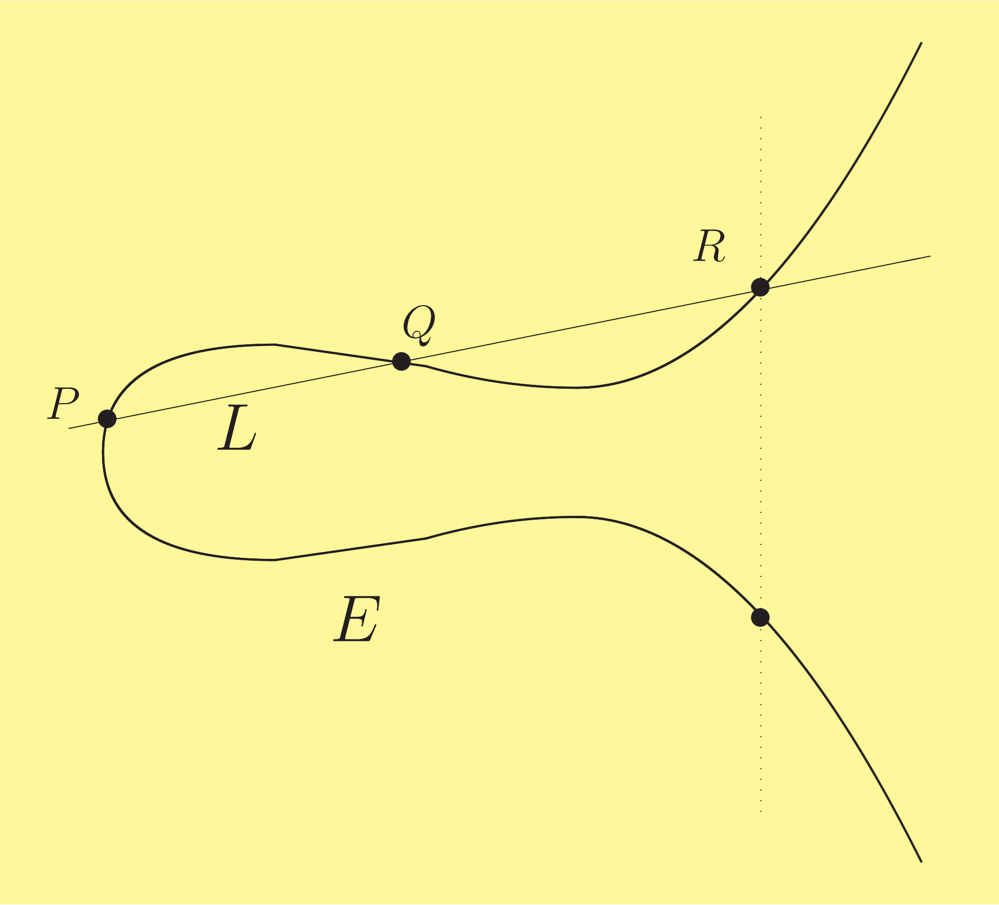
Draw the line L through P and Q.

Adding Points on an Elliptic Curve



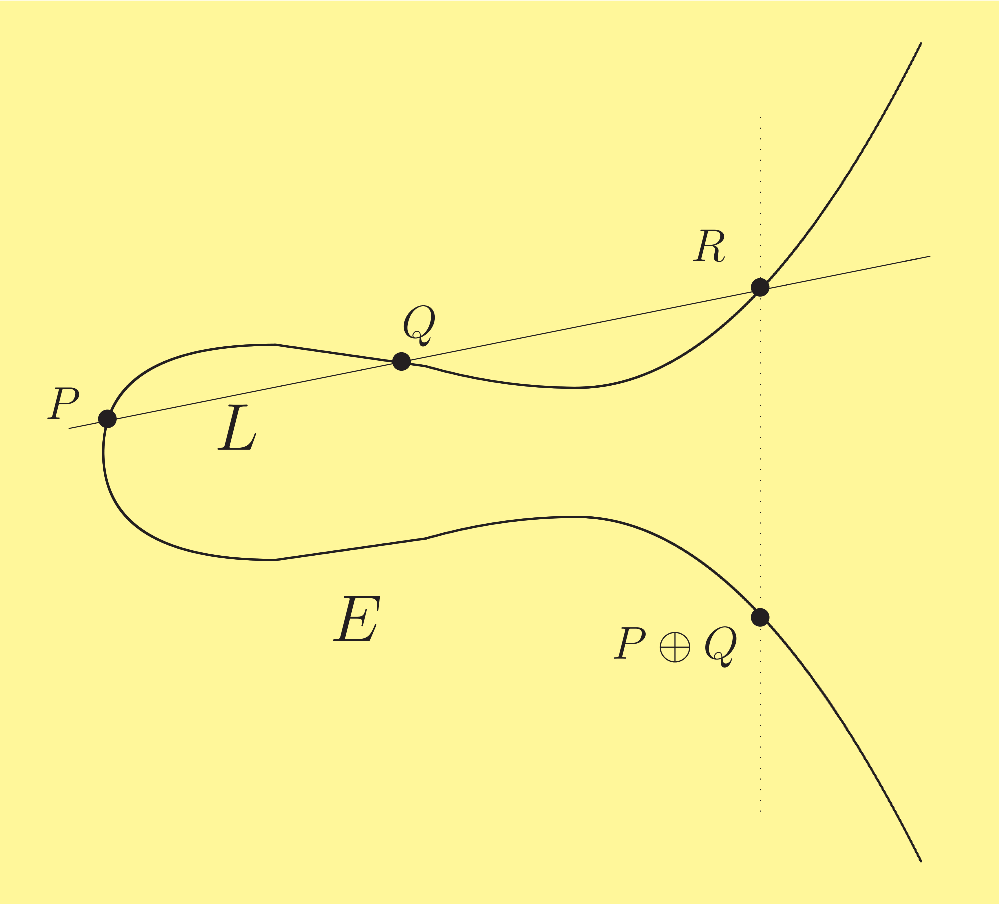
The line L intersects the cubic curve E in a third point. Call that third point R.

Adding Points on an Elliptic Curve



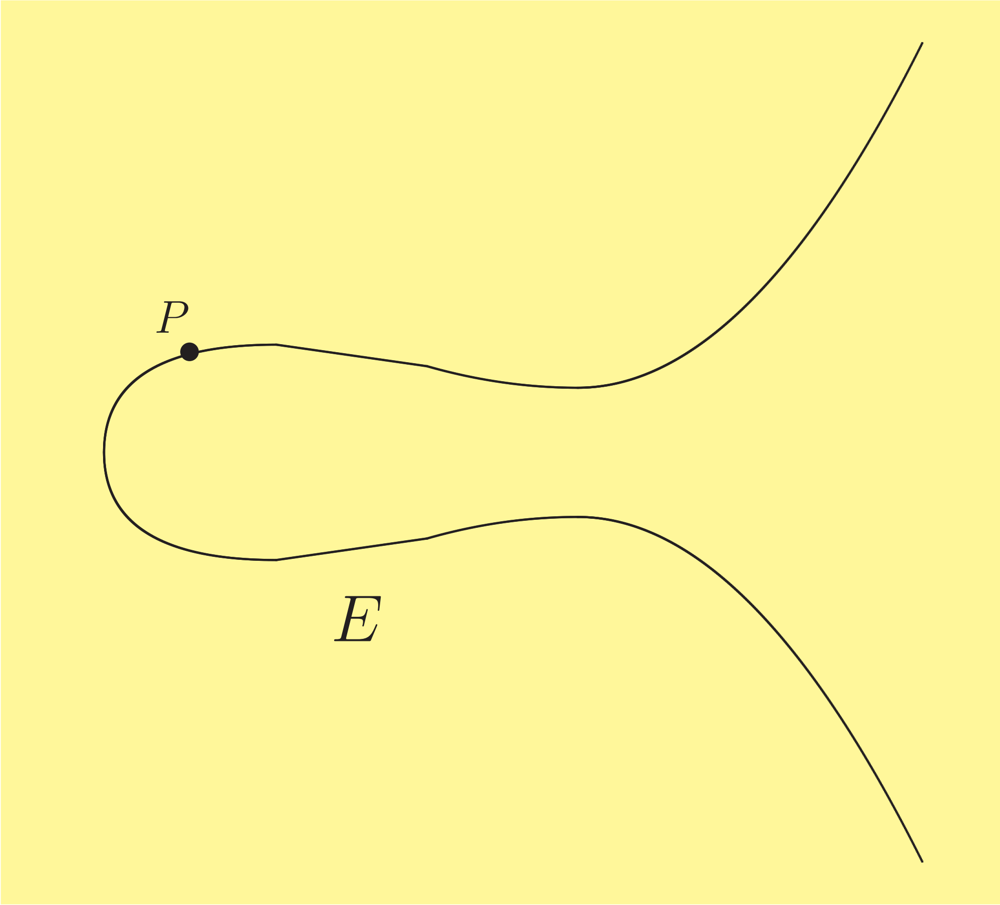
Draw the vertical line through R.
It hits E in another point.

Adding Points on an Elliptic Curve



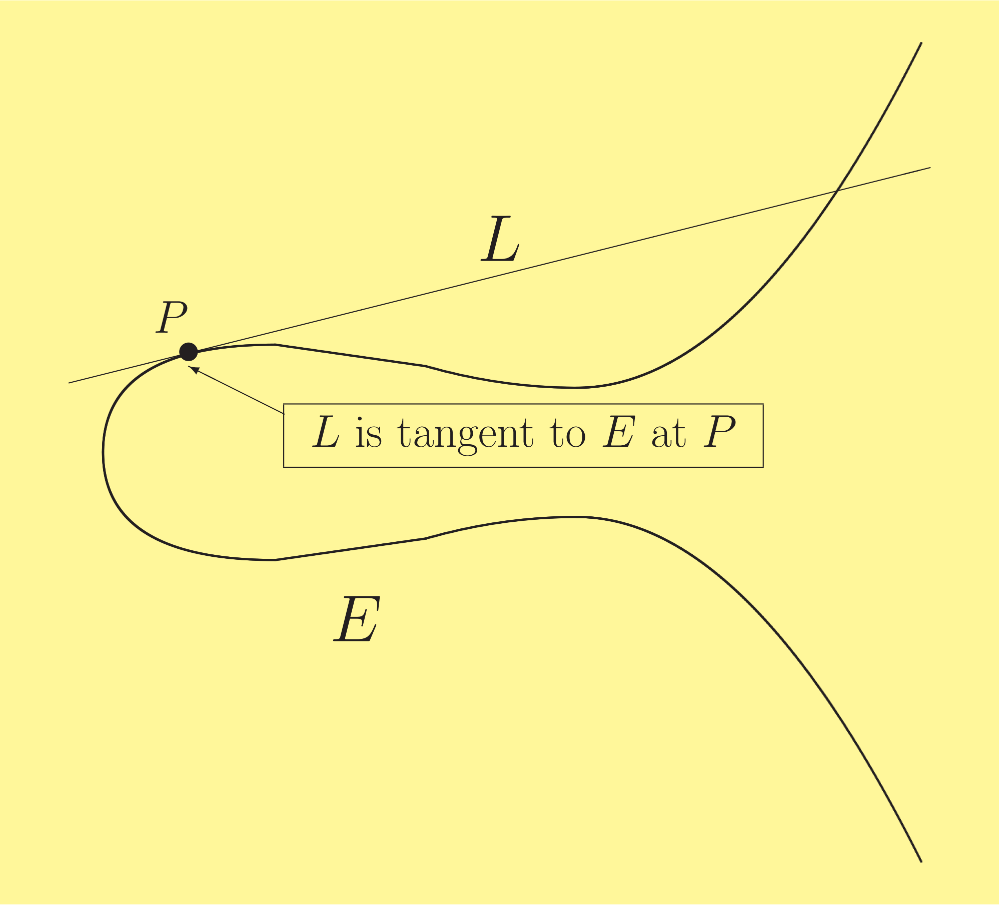
We define the **sum of P and Q on E** to be the reflected point. We denote it by $P \oplus Q$ or just $P + Q$.

Adding a Point To Itself on an Elliptic Curve



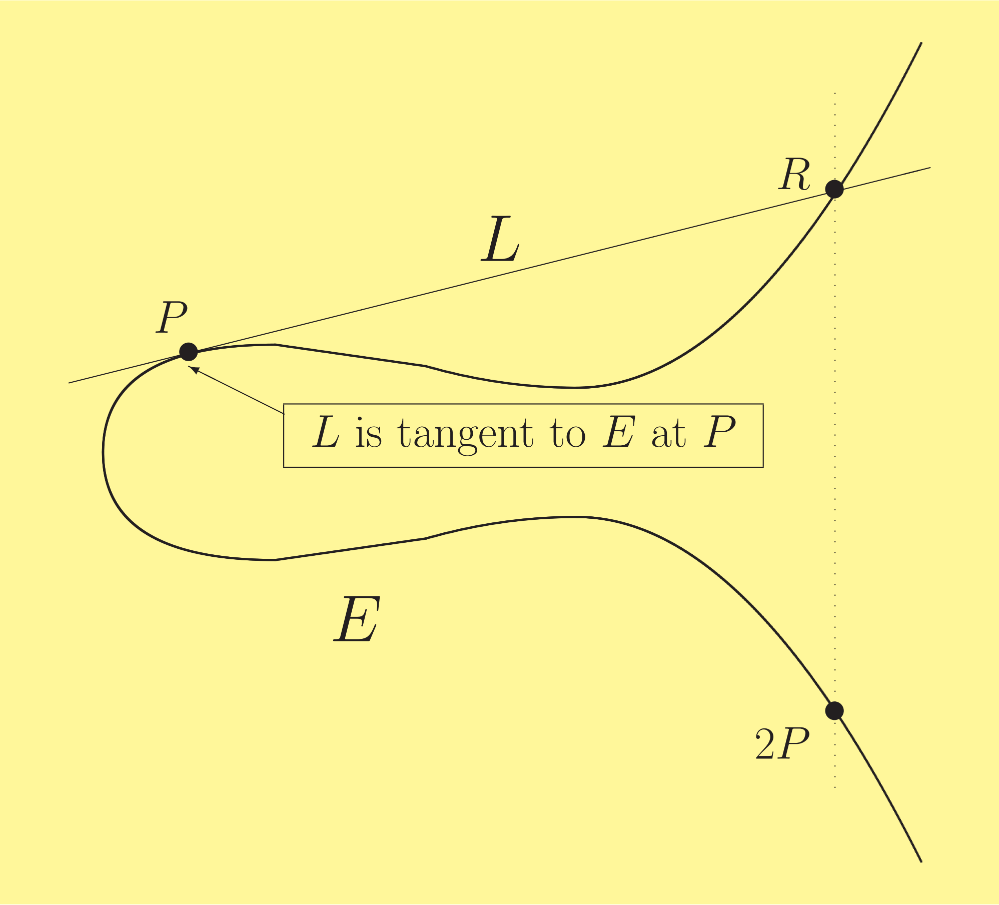
How do we add a point P to itself, since there are many different lines that go through P?

Adding a Point To Itself on an Elliptic Curve



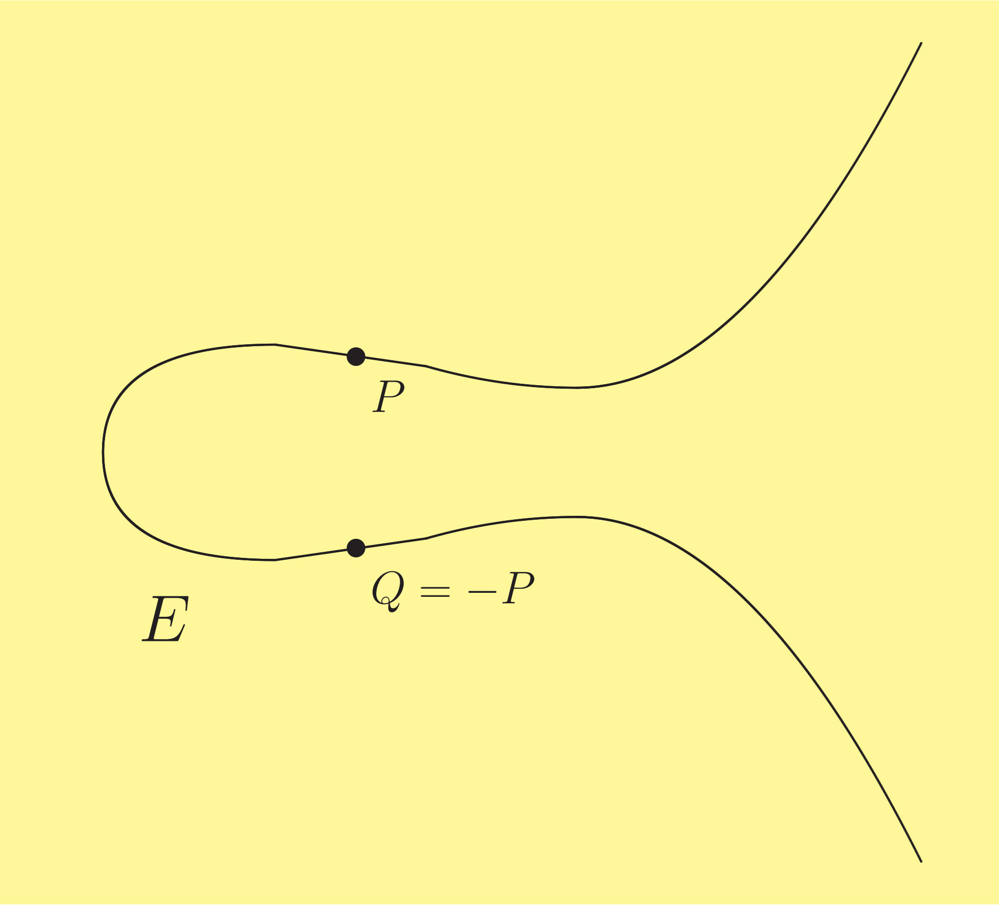
If we think of adding P to Q and let Q approach P, then the line L becomes the tangent line to E at P.

Adding a Point To Itself on an Elliptic Curve



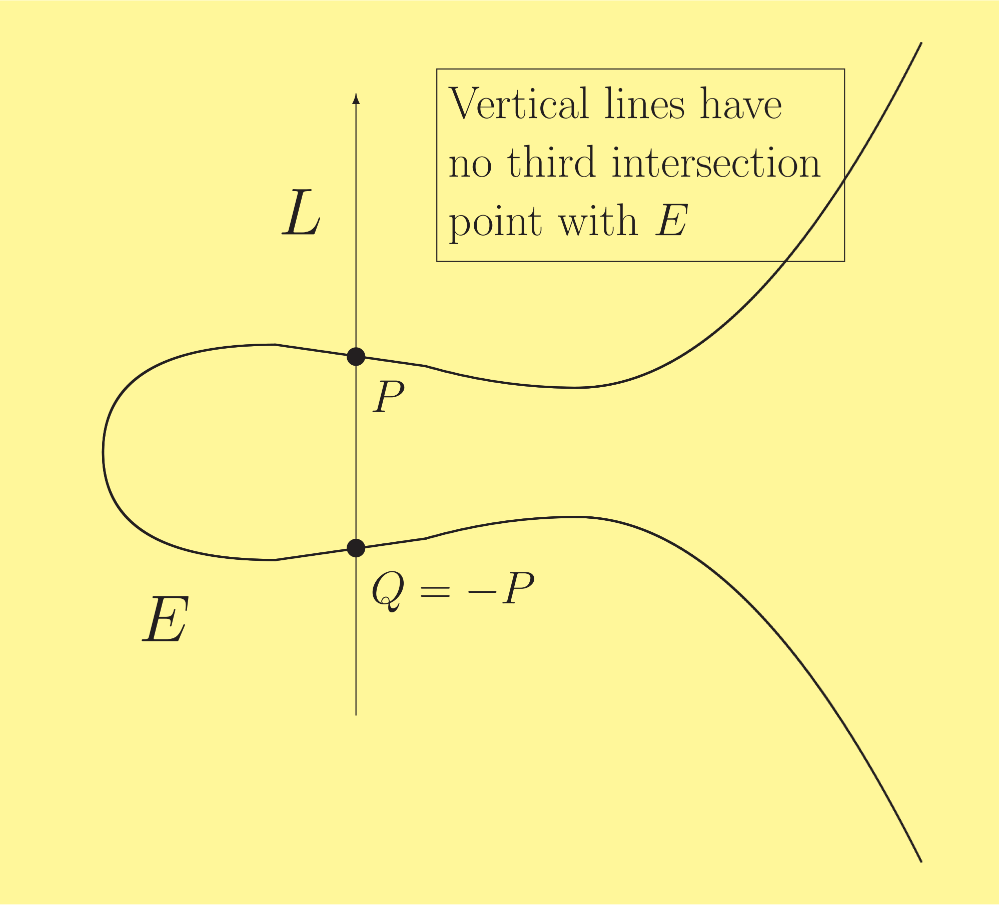
Then we take the third intersection point R, reflect across the x-axis, and call the resulting point $P \oplus P$ or $2P$.

Vertical Lines and the Extra Point "At Infinity"



Let $P \in E$. We denote the reflected point by $-P$.

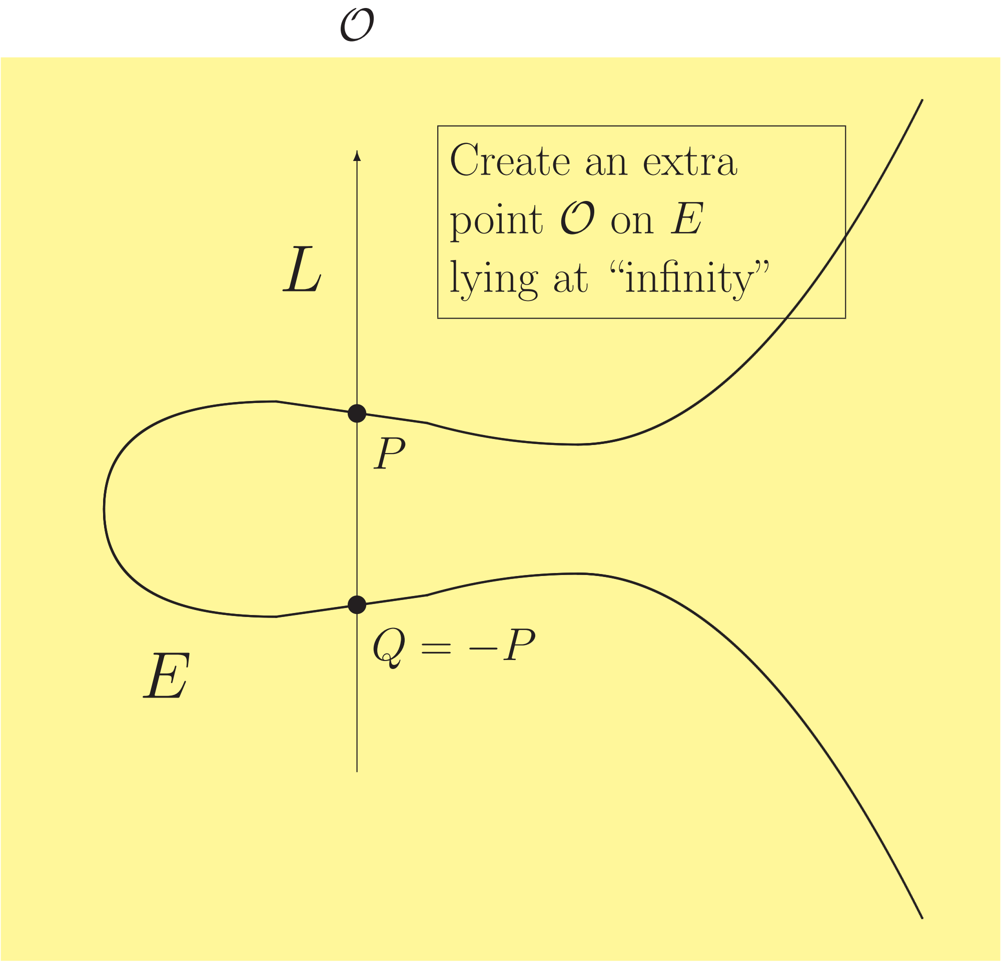
Vertical Lines and the Extra Point "At Infinity"



Vertical lines have no third intersection point with E

Big Problem: The vertical line L through P and $-P$ does not intersect E in a third point! And we need a third point to define $P \oplus (-P)$.

Vertical Lines and the Extra Point "At Infinity"



Create an extra point $\mathcal{O}$ on E lying at "infinity"

Solution: Since there is no point in the plane that works, we create an extra point $\mathcal{O}$ "at infinity."

Rule: $\mathcal{O}$ is a point on every <u>vertical</u> line.

The Algebra of Elliptic Curves

Properties of "Addition" on E

Theorem *The addition law on E has the following properties:*

(a) $P + \mathcal{O} = \mathcal{O} + P = P$ for all $P \in E$.
(b) $P + (-P) = \mathcal{O}$ for all $P \in E$.
(c) $P + (Q + R) = (P + Q) + R$ for all $P, Q, R \in E$.
(d) $P + Q = Q + P$ for all $P, Q \in E$.

In other words, the addition law $+$ makes the points of E into a commutative group.

All of the group properties are trivial to check **except** for the associative law (c). The associative law can be verified by a lengthy computation using explicit formulas, or by using more advanced algebraic or analytic methods.

A Numerical Example

$$\boxed{E : y^2 = x^3 - 5x + 8}$$

The point $P = (1, 2)$ is on the curve E.
Using the tangent line construction, we find that

$$2P = P + P = \left(-\frac{7}{4}, -\frac{27}{8}\right).$$

Let $Q = \left(-\frac{7}{4}, -\frac{27}{8}\right)$. Using the secant line construction, we find that

$$3P = P + Q = \left(\frac{553}{121}, -\frac{11950}{1331}\right).$$

Similarly,

$$4P = \left(\frac{45313}{11664}, -\frac{8655103}{1259712}\right).$$

As you can see, the coordinates are getting very large.

Formulas for Addition on E

Suppose that we want to add the points

$$P_1 = (x_1, y_1) \quad \text{and} \quad P_2 = (x_2, y_2)$$

on the elliptic curve

$$E : y^2 = x^3 + Ax + B.$$

Let the line connecting P to Q be

$$L : y = \lambda x + \nu$$

Explicitly, the slope and y-intercept of L are given by

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \ne P_2 \\ \dfrac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2 \end{cases} \qquad \text{and} \qquad \nu = y_1 - \lambda x_1.$$

Formulas for Addition on E (continued)

We find the intersection of

$$E : y^2 = x^3 + Ax + B \qquad \text{and} \qquad L : y = \lambda x + \nu$$

by solving

$$(\lambda x + \nu)^2 = x^3 + Ax + B.$$

We already know that x_1 and x_2 are solutions, so we can find the third solution x_3 by comparing the two sides of

$$\begin{aligned} &x^3 + Ax + B - (\lambda x + \nu)^2 \\ &\quad = (x - x_1)(x - x_2)(x - x_3) \\ &\quad = x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3. \end{aligned}$$

Equating the coefficients of x^2, for example, gives

$-\lambda^2 = -x_1 - x_2 - x_3,$ and hence $x_3 = \lambda^2 - x_1 - x_2.$

Then we compute y_3 using $y_3 = \lambda x_3 + \nu$, and finally

$$P_1 + P_2 = (x_3, -y_3).$$

Formulas for Addition on E (Summary)

Addition algorithm for $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$
on the elliptic curve $E : y^2 = x^3 + Ax + B$

- If $P_1 \neq P_2$ and $x_1 = x_2$, then $P_1 + P_2 = \mathcal{O}$.
- If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = 2P_1 = \mathcal{O}$.
- If $P_1 \neq P_2$ (and $x_1 \neq x_2$),

$$\text{let } \lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ and } \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$

- If $P_1 = P_2$ (and $y_1 \neq 0$),

$$\text{let } \lambda = \frac{3x_1^2 + A}{2y_1} \text{ and } \nu = \frac{-x^3 + Ax + 2B}{2y}.$$

Then

Formulas for Addition on E (Summary)

Addition algorithm for $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ on the elliptic curve $E : y^2 = x^3 + Ax + B$

- If $P_1 \neq P_2$ and $x_1 = x_2$, then $P_1 + P_2 = \mathcal{O}$.
- If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = 2P_1 = \mathcal{O}$.
- If $P_1 \neq P_2$ (and $x_1 \neq x_2$),
$$\text{let } \lambda = \frac{y_2 - y_1}{x_2 - x_1} \text{ and } \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}.$$
- If $P_1 = P_2$ (and $y_1 \neq 0$),
$$\text{let } \lambda = \frac{3x_1^2 + A}{2y_1} \text{ and } \nu = \frac{-x^3 + Ax + 2B}{2y}.$$

Then

$$P_1 + P_2 = (\lambda^2 - x_1 - x_2, -\lambda^3 + \lambda(x_1 + x_2) - \nu).$$

An Observation About the Addition Formulas

The addition formulas look complicated, but for example, if $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are distinct points, then

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2,$$

and if $P = (x, y)$ is any point, then

$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}.$$

Important Observation: If A and B are in a field K and if P_1 and P_2 have coordinates in K, then $P_1 + P_2$ and $2P_1$ also have coordinates in K.

The Group of Points on E with Coordinates in a Field K

The elementary observation on the previous slide leads to the important result that points with coordinates in a particular field form a subgroup of the full set of points.

Theorem. (Poincaré, $\approx$ 1900) Let K be a field and suppose that an elliptic curve E is given by an equation of the form

$$E : y^2 = x^3 + Ax + B \qquad \text{with} \quad A, B \in K.$$

Let $E(K)$ denote the set of points of E with coordinates in K,

$$E(K) = \bigl\{(x, y) \in E : x, y \in K\bigr\} \cup \{\mathcal{O}\}.$$

Then $E(K)$ is a **subgroup** of the group of all points of E.

A Finite Field Example

The formulas giving the group law on E are valid if the points have coordinates in any field, even if the geometric pictures don't make sense. For example, we can take points with coordinates in $\mathbb{F}_p$.

Example. The curve

$$E : y^2 = x^3 - 5x + 8 \pmod{37}$$

contains the points

$$P = (6,3) \in E(\mathbb{F}_{37}) \quad \text{and} \quad Q = (9,10) \in E(\mathbb{F}_{37}).$$

Using the addition formulas, we can compute in $E(\mathbb{F}_{37})$:

2P=(35,11), 3P=(34,25),

4P=(8,6), 5P=(16,19),. . .

P+Q=(11,10),. . .

3P+4Q=(31,28),. . .

A Finite Field Example (continued)

Substituting in each possible value $x = 0, 1, 2, \ldots, 36$ and checking if $x^3 - 5x + 8$ is a square modulo 37, we find that $E(\mathbb{F}_{37})$ consists of the following 45 points modulo 37:

$$
\begin{gathered}
(1, \pm 2), (5, \pm 21), (6, \pm 3), (8, \pm 6), (9, \pm 27), (10, \pm 25),\\
(11, \pm 27), (12, \pm 23), (16, \pm 19), (17, \pm 27), (19, \pm 1), (20, \pm 8),\\
(21, \pm 5), (22, \pm 1), (26, \pm 8), (28, \pm 8), (30, \pm 25), (31, \pm 9),\\
(33, \pm 1), (34, \pm 25), (35, \pm 26), (36, \pm 7), \mathcal{O}.
\end{gathered}
$$

There are nine points of order dividing three, so as an abstract group,

$$E(\mathbb{F}_{37}) \cong C_3 \times C_{15}.$$

Theorem. Working over a finite field, the group of points $E(\mathbb{F}_p)$ is always either a cyclic group or the product of two cyclic groups.

Computing Large Multiples of a Point

To use the finite group $E(\mathbb{F}_p)$ for Diffie-Hellman, say, we need p to be quite large ($p > 2^{160}$) and we need to compute multiples

$$mP = \underbrace{P + P + \cdots + P}_{m \text{ times}} \in E(\mathbb{F}_p)$$

for very large values of m.

We can compute mP in $O(\log m)$ steps by the usual **Double-and-Add Method**. First write

$$m = m_0 + m_1 \cdot 2 + m_2 \cdot 2^2 + \cdots + m_r \cdot 2^r \qquad \text{with } m_0, \ldots, m_r \in \{0, 1\}.$$

Then mP can be computed as

$$mP = m_0 P + m_1 \cdot 2P + m_2 \cdot 2^2 P + \cdots + m_r \cdot 2^r P,$$

where $2^k P = 2 \cdot 2 \cdots 2P$ requires only k doublings.

Computing Large Multiples of a Point (continued)

Thus on average, it takes approximately $\log_2(m)$ doublings and $\frac{1}{2}\log_2(m)$ additions to compute mP.

There is a simple way to reduce the computation time even further. Since it takes the same amount of time to subtract two point as it does to add two points, we can instead look at a “ternary expansion of m, which means writing

$$m = m_0 + m_1 \cdot 2 + m_2 \cdot 2^2 + \cdots + m_r \cdot 2^r \qquad \text{with } m_0, \ldots, m_r \in \{-1, 0, 1\}.$$

On average, this can be done with approximately $\frac{2}{3}$ of the m_i's equal to 0, which reduces the average number of additions to $\frac{1}{3}\log_2(m)$.

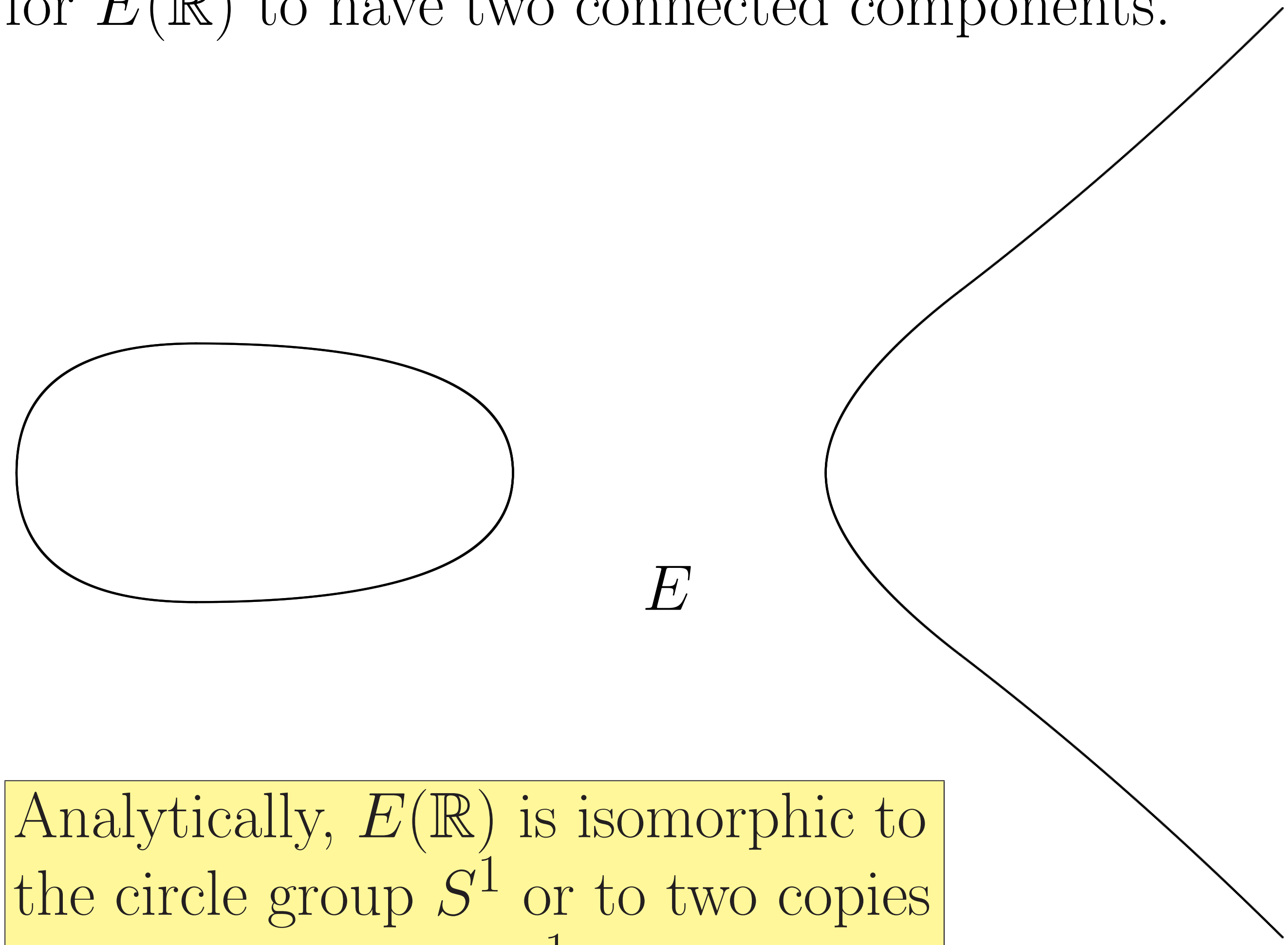
What Does $E(K)$ Look Like?

What Does $E(K)$ Look Like?

There's no single answer, it depends on the field K.

What Does $E(\mathbb{R})$ Look Like?

We have seen a picture of an $E(\mathbb{R})$. It is also possible for $E(\mathbb{R})$ to have two connected components.

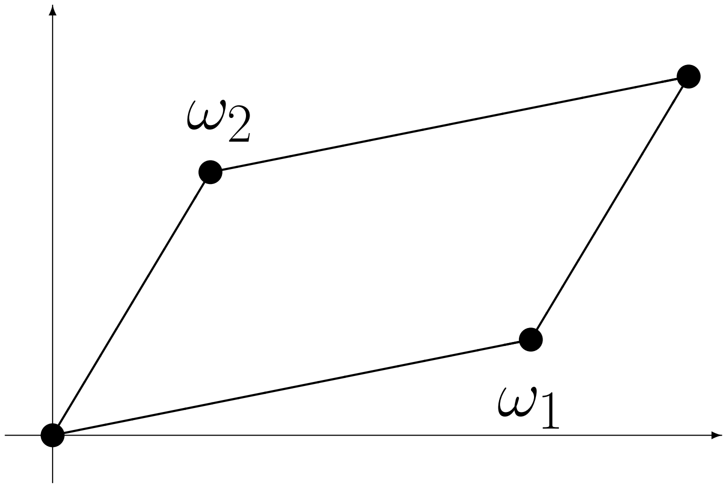


Analytically, $E(\mathbb{R})$ is isomorphic to the circle group S^1 or to two copies of the circle group $S^1 \times C_2$.

What Does $E(\mathbb{C})$ Look Like?

The points of an elliptic curve with coordinates in the complex numbers $\mathbb{C}$ form a **torus**, which is the mathematical term for the surface of a donut.

We can form a torus by choosing two complex numbers $\omega_1, \omega_2 \in \mathbb{C}$, using them as two sides of a parallelogram, and then identifying the opposite sides.

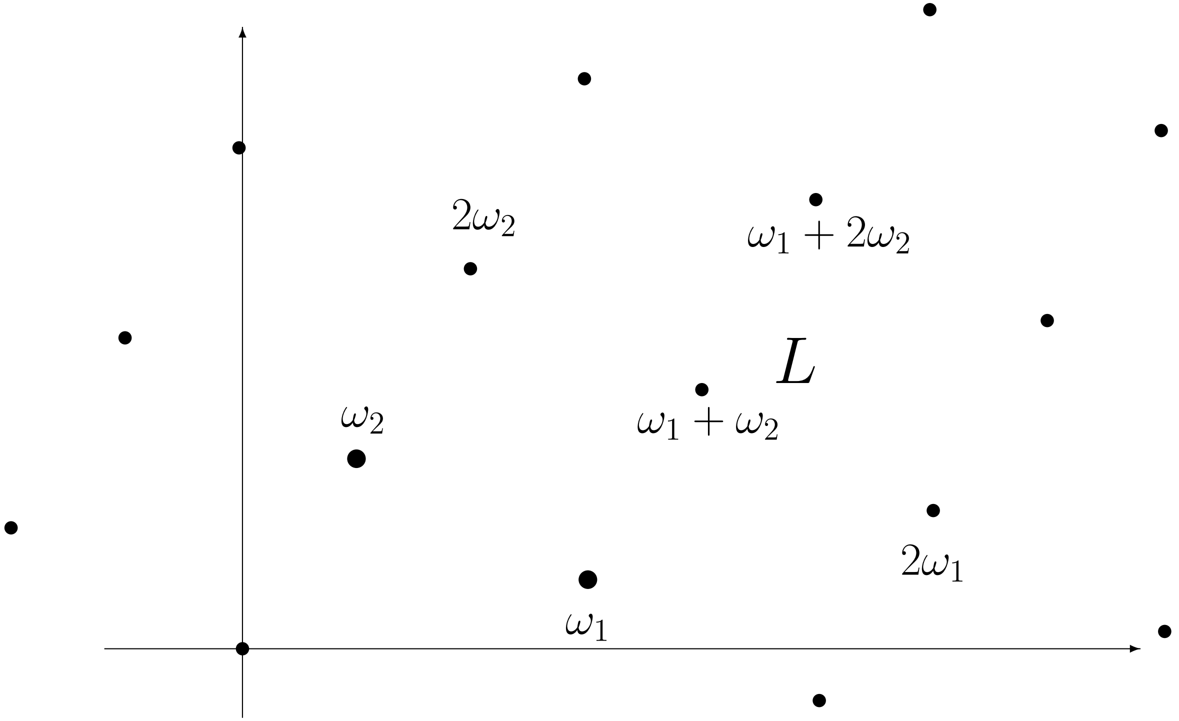


What Does $E(\mathbb{C})$ Look Like?

The complex numbers ω_1 and ω_2 are called **periods of E**. To describe the group law on $E(\mathbb{C})$, we look at

$$L = \{n_1\omega_1 + n_2\omega_2 : n_1, n_2 \in \mathbb{Z}\} \subset \mathbb{C},$$

the **lattice** spanned by ω_1 and ω_2.



The lattice L is a regularly spaced array of points in $\mathbb{C}$.

What Does $E(\mathbb{C})$ Look Like?

The lattice L is a subgroup of the complex numbers. The quotient is both a group and a complex manifold, and there is a a complex analytic isomorphism

$$\mathbb{C}/L \xrightarrow{\left(\wp(z),\frac{1}{2}\wp'(z)\right)} E(\mathbb{C}),$$

where the **Weierstrass $\wp$-function** is defined by the Laurent series

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in L\\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right).$$

It satisfies $\wp(z+\omega) = \wp(z) \qquad \text{for all } \omega \in L.$

Thus $\wp(z)$ is a **doubly periodic function**, since it has two independent periods ω_1 and ω_2. It generalizes the classical function e^z that has the single period $2\pi i$.

Points of Finite Order in $E(\mathbb{C})$

As an abstract group, the group $E(\mathbb{C})$ looks like

$$E(\mathbb{C}) \cong \mathbb{C}/L \cong S^1 \times S^1.$$

It is very easy to describe the points of finite order on the torus $S^1 \times S^1$.

For any integer $N \geq 1$, we write

$$E(\mathbb{C})_N = \{P \in E(\mathbb{C}) : NP = \mathcal{O}\}$$

for the set of elements of $E(\mathbb{C})$ of order dividing N.

Exercise If G is an *abelian* group, prove that G_N is a subgroup of G. Also find a nonabelian counterexample.

Proposition. For all $N \geq 1$,

$$E(\mathbb{C})_N \cong C_N \times C_N$$

is the product of two cyclic groups of order N.

What Does $E(\mathbb{Q})$ Look Like?

The group of rational points $E(\mathbb{Q})$ is a subgroup of the group of real points $E(\mathbb{R})$, but we can no more draw a nice picture of $E(\mathbb{Q})$ sitting inside $E(\mathbb{R})$ than we can draw a nice picture of the rational numbers $\mathbb{Q}$ sitting inside the real numbers $\mathbb{R}$.

Study of the group $E(\mathbb{Q})$ has played and continues to play a fundamental role in the development of many areas of number theory.

The modern theory of **Diophantine equations**, the solution of polynomial equations using integers or rational numbers, was initiated in 1922 when L.J. Mordell proved a landmark result describing $E(\mathbb{Q})$.

What Does $E(\mathbb{Q})$ Look Like?

Theorem. (Mordell, 1922) Let E be an elliptic curve given by an equation

$$E : y^2 = x^3 + Ax + B \qquad \text{with } A, B \in \mathbb{Q}.$$

Then the group of rational points $E(\mathbb{Q})$ is a **finitely generated** abelian group. In other words, there is a finite set of points $P_1, \ldots, P_t \in E(\mathbb{Q})$ so that every point $P \in E(\mathbb{Q})$ can be written in the form

$$P = n_1P_1 + n_2P_2 + \cdots + n_tP_t$$

$$\text{for some } n_1, n_2, \ldots, n_t \in \mathbb{Z}.$$

A standard theorem about finitely generated abelian groups tells us that $E(\mathbb{Q})$ looks like

$$E(\mathbb{Q}) \cong (\text{Finite Group}) \times \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ copies}}.$$

What Does $E(\mathbb{Q})$ Look Like?

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ copies}}.$$

The finite group $E(\mathbb{Q})_{\text{tors}}$ is called the

Torsion Subgroup of $E(\mathbb{Q})$.

The integer r is called the **Rank of $E(\mathbb{Q})$**.

The *description* of all possible torsion subgroups for $E(\mathbb{Q})$ is very easy, although the *proof* is extremely difficult.

Theorem. (Mazur, 1977) The torsion subgroup of the group of rational points $E(\mathbb{Q})$ on an elliptic curve must be one of the following 15 groups:

$$\begin{array}{cl} C_N & \text{with } 1 \le N \le 10 \text{ or } N = 12, \\ C_2 \times C_{2N} & \text{with } 1 \le N \le 4. \end{array}$$

In particular, $E(\mathbb{Q})_{\text{tors}}$ has order at most 16.

What Does $E(\mathbb{Q})$ Look Like?

The rank is a far more mysterious quantity, although there is a folklore conjecture.

Conjecture. There exist elliptic curve groups $E(\mathbb{Q})$ of arbitrarily large rank.

The evidence for this conjecture is fragmentary at best. An example of rank at least 24 (Martin-McMillen 2000):

$$\begin{aligned} y^2 + xy + y = x^3 &- 120039822036992245303534619191166796374x \\ &+ 504224992484910670010801799168082726759443756222911415116 \end{aligned}$$

And here is the only example known of higher rank. It has rank at least 28 (Elkies 2006):

$$\begin{aligned} y^2 + xy + y = x^3 &- 20067762415575526585033208209338542750930230312178956502x \\ &+ 3448161179503055646703298569039072037485594435931918036126600829629193944873224 3429 \end{aligned}$$

Slightly more convincing is the fact that there do exist elliptic curves with coefficients in the field $\mathbb{F}_p(T)$ such that the rank of $E(\mathbb{F}_p(T))$ is arbitrarily large.

What Does $E(\mathbb{Z})$ Look Like?

The ring $\mathbb{Z}$ is not a field, so the set

$$E(\mathbb{Z}) = \{(x,y) \in E(\mathbb{Q}) : x, y \in \mathbb{Z}\} \cup \{\mathcal{O}\}$$

is usually **not** a subgroup of $E(\mathbb{Q})$.

Indeed, even if P_1 and P_2 have integer coordinates, the formula for $P_1 + P_2$ is so complicated, it seems unlikely that the point $P_1 + P_2$ will have integer coordinates.

Complementing Mordell's Theorem describing $E(\mathbb{Q})$ is a famous finiteness result for $E(\mathbb{Z})$.

Theorem. (Siegel, 1928) Let E be an elliptic curve given by an equation

$$E : y^2 = x^3 + Ax + B \qquad \text{with } A, B \in \mathbb{Z}.$$

Then E has only finitely many points $P = (x,y)$ with integer coordinates $x, y \in \mathbb{Z}$, i.e., $E(\mathbb{Z})$ is a finite set.

What Does $E(\mathbb{Z})$ Look Like?

Siegel actually proves something much stronger.

For each point $P \in E(\mathbb{Q})$, write

$$x(P) = \frac{a(P)}{b(P)} \in \mathbb{Q} \quad \text{as a fraction in lowest terms.}$$

Theorem. (Siegel, 1928)

$$\lim_{\substack{P\in E(\mathbb{Q})\\ \max\{|a(P)|,|b(P)|\}\to\infty}} \frac{\log|a(P)|}{\log|b(P)|} = 1.$$

Roughly speaking, Siegel's result says that the numerator and the denominator of $x(P)$ tend to have approximately the same number of digits.

What Does $E(\mathbb{F}_p)$ Look Like?

The group $E(\mathbb{F}_p)$ is obviously a finite group. Indeed, it clearly has no more than $2p+1$ points.

For each $x \in \mathbb{F}_p$, there is a "50% chance" that the value of $f(x) = x^3 + Ax + B$ is a square in $\mathbb{F}_p^*$. And if $f(x) = y^2$ is a square, then we (usually) get two points $(x, \pm y)$ in $E(\mathbb{F}_p)$. Plus there's the point $\mathcal{O}$.

Thus we might expect $E(\mathbb{F}_p)$ to contain approximately

$$\#E(\mathbb{F}_p) \approx \tfrac{1}{2} \cdot 2 \cdot p + 1 = p + 1 \text{ points}$$

A famous theorem of Hasse makes this precise:

Theorem. (Hasse, 1922) Let E be an elliptic curve

$$y^2 = x^3 + Ax + B \quad \text{with } A, B \in \mathbb{F}_p.$$

Then
$$\bigl|\#E(\mathbb{F}_p) - (p+1)\bigr| \le 2\sqrt{p}.$$

Elliptic Curves
Over Finite Fields

The Order of the Group $E(\mathbb{F}_p)$

The **Frobenius Map** is the function

$$\tau_p : E(\bar{\mathbb{F}}_p) \longrightarrow E(\bar{\mathbb{F}}_p), \qquad \tau_p(x,y) = (x^p, y^p).$$

One can check that τ_p is a **group homomorphism**.

The quantity
$$a_p = p + 1 - \#E(\mathbb{F}_p)$$
is called the **Trace of Frobinius**, because one way to calculate it is to use the Frobenius map to get a linear transformation on a certain vector space $V_\ell(E)$. Then a_p is the trace of that linear transformation.

Hasse's Theorem says that
$$|a_p| \le 2\sqrt{p}.$$

For cryptography, we need $E(\mathbb{F}_p)$ to contain a subgroup of large **prime** order. How does $\#E(\mathbb{F}_p)$ vary for different E?

The Distribution of the Trace of Frobenius

There are approximately $2p$ different elliptic curves defined over $\mathbb{F}_p$.

If the $a_p(E)$ values for different E were uniformly distributed in the interval from $-2\sqrt{p}$ to $2\sqrt{p}$ then we would expect each value to appear approximately $\frac{1}{2}\sqrt{p}$ times.

This is not quite true, but it is true that the values a_p between (say) $-\sqrt{p}$ and $\sqrt{p}$ appear quite frequently. The precise statement says that the a_p values follow a Sato-Tate distribution:

Theorem. (Birch)

$$\#\{E/\mathbb{F}_p : \alpha \le a_p(E) \le \beta\} \approx \frac{1}{\pi}\int_\alpha^\beta \sqrt{4p - t^2}\, dt.$$

Computing the Order of $E(\mathbb{F}_p)$

If p is small, we can compute $x^3 + Ax + B$ for each $p = 0, 1, \ldots, p-1$ and use quadratic reciprocity to check if it is a square modulo p. This takes time $O(p \log p)$.

Schoof found a deterministic polynomial-time algorithm that computes $E(\mathbb{F}_p)$ in time $O(\log p)^6$.

Elkies and Atkin made Schoof's algorithm more efficient (but probabilistic), so it is now called the

SEA Algorithm.

The details of SEA are somewhat complicated. Roughly, one studies the set of all maps of a fixed degree ℓ from E to other elliptic curves. These correspond to quotient curves E/Φ for finite subgroups $\Phi \subset E$ of order ℓ. One deduces information about a_p modulo ℓ, from which a_p can be reconstructed.

Elliptic Curves in Characteristic 2

As a practical matter, computers tend to work more efficiently with fields of characteristic 2 than they do with fields of (large) prime characteristic.

For this reason, cryptographers often use elliptic curves defined over a field $\mathbb{F}_q$ having $q = 2^k$ elements.

In characteristic 2, the curve $y^2 = x^2 + Ax + B$ is always singular, so a more general equation is needed:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The formulas giving the group law are a little more complicated, but have the same general form.

A number of people (Sato, Kedlaya, Lauder, Wan, Denef, Vercauteren,...) have worked on methods more efficient than SEA to count $\#E(\mathbb{F}_q)$ when $q = p^k$ and p is a small prime.

Koblitz Curves

For maximum efficiency, a **Koblitz curve** is used:

$$E : y^2 + xy = x^3 + ax^2 + 1 \quad \text{with } a = 0 \text{ or } a = 1.$$

The Koblitz curve E has coefficients in $\mathbb{F}_2$. For cryptographic purposes, one takes points in $E(\mathbb{F}_q)$ with $q = 2^k$ and k large, say $k \geq 160$.

There are security reasons why one might insist that k be prime. But there are certain efficiency gains available if k is composite.

A nice feature of the Koblitz curves is that it is easy to count their points:

$$\#E(\mathbb{F}_{2^k}) = 2^k - \left(\frac{-1+\sqrt{-7}}{2}\right)^k - \left(\frac{-1-\sqrt{-7}}{2}\right)^k + 1.$$

Computing Multiples on Koblitz Curves

The computational advantage of the Koblitz curves lies in the existence of the group homomorphism

$$\tau : E(\mathbb{F}_q) \longrightarrow E(\mathbb{F}_q), \qquad \tau(x,y) = (x^2, y^2).$$

Exercise Use the fact that squaring is a field automorphism of $\mathbb{F}_2$ to prove that $\tau(P+Q) = \tau(P) + \tau(Q)$.

The map τ also satisfies: $\tau^2(P) + \tau(P) + 2P = \mathcal{O}$

Using this relation, every integer m has a "τ-adic" expansion (similar to its binary expansion):

$$m = m_0 + m_1\tau + m_2\tau^2 + \cdots + m_r\tau^r \qquad \text{with } m_0, m_1, \ldots, m_r \in \{0, \pm 1\}.$$

Then mP can be computed without doubling maps as:

$$mP = m_0P + m_1\tau(P) + m_2\tau^2(P) + \cdots + m_r\tau^r(P).$$

The Elliptic Curve Discrete Logarithm Problem

Elliptic Curve Discrete Logarithm Problem ECDLP

Let E be an elliptic curve defined over a finite field $\mathbb{F}_p$.

$$E : y^2 = x^3 + Ax + B \qquad A, B \in \mathbb{F}_p.$$

Let S and T be points in $E(\mathbb{F}_p)$. Find an integer m so that

$$T = mS.$$

Recall that the (smallest) integer m with this property is called the **Discrete Logarithm** (or **Index**) of T with respect to S and is denoted:

$$m = \log_S(T) = \mathrm{ind}_S(T).$$

Let n be the order of S in the group $E(\mathbb{F}_p)$. Then

$$\log_S : (\text{Subgroup of } E \text{ generated by } S) \longrightarrow \mathbb{Z}/n\mathbb{Z}.$$

is a group isomorphism, the inverse of $m \mapsto mS$.

How To Solve the ECDLP

Exhaustive Search Method

Compute $m_1S, m_2S, m_3S, \ldots$ for randomly chosen values m_1, m_2, m_3 until you find a multiple with $mS = T$. Expected running time is $O(p)$, since $\#E(\mathbb{F}_p) = O(p)$.

Collision Search Method

Compute two lists for randomly chosen values $m_1, m_2, \ldots$

List 1: $m_1S,\ m_2S,\ m_3S, \ldots$

List 2: $T - m_1S,\ T - m_2S,\ T - m_3S \ldots$

until finding a collision

$$m_iS = T - m_jS.$$

Expected running time is $O(\sqrt{p}\,)$ by the birthday paradox.

How To Solve the ECDLP

Pollard's ρ Method

- The collision method has running time $O(\sqrt{p})$, but it takes about $O(\sqrt{p})$ space to store the two lists.
- Pollards ρ method for discrete logs achieves the same $O(\sqrt{p})$ running time while only requiring a very small amount of storage.
- The idea is to traverse a "random" path through the multiples $mS + nT$ until finding a collision. This path will consist of a loop with a tail attached (just like the letter ρ!!).
- It takes $O(\sqrt{p})$ steps to arrive on the loop part. Then we can detect a collision in $O(\sqrt{p})$ steps by storing only a small proportion of the visited points. We choose which points to store using a criterion that is independent of the underlying group law.

How Else Can DLP Be Solved?

Pollard's ρ method works for most discrete log problems.

For an abstract finite group G whose group law is given by a black box, one can **prove** that the fastest solution to the DLP has running time $O(\sqrt{\#G}\,)$.

But for specific groups with known structure, there are often faster algorithms.

- For $\mathbb{Z}/N\mathbb{Z}$, the DLP is inversion modulo N. It takes $O(\log N)$ steps by the Euclidean algorithm.
- For $\mathbb{R}^*$, the DLP can be solved using the standard logarithm,

$$\text{if } \beta = \alpha^m, \text{ then } m = \log(\beta)/\log(\alpha).$$

- For $\mathbb{F}_p^*$, there is a subexponential algorithm called the **Index Calculus** that runs in (roughly)

$$O\left(e^{c\sqrt[3]{\log p}}\right) \text{ steps.}$$

Does ECDLP Have a Faster Solution?

The principal reason that elliptic curve groups are used for cryptography is:

For general elliptic curves, the fastest known method to solve ECDLP is Pollard's ρ Method!!

This means that it is not currently feasible to solve ECDLP in $E(\mathbb{F}_q)$ if (say) $q > 2^{160}$.

A DLP of equivalent difficulty in $\mathbb{F}_q^*$ requires $q \approx 2^{1000}$. Similarly, ECDLP with $q \approx 2^{160}$ is approximately as hard as factoring a 1000 bit number.

Hence cryptographic constructions based on ECDLP have smaller keys, smaller message blocks, and may also be faster.

Solving ECDLP in Special Cases

For "most" elliptic curves, the best known solution to ECDLP has running time $O(\sqrt{p})$. But for certain special classes of curves, there are faster methods.

It is important to know which curves have fast ECDLP algorithms so that we can avoid using them.

Elliptic Curves $E(\mathbb{F}_p)$ With Exactly p Points

If $\#E(\mathbb{F}_p) = p$, then there is a "p-adic logarithm map" that gives an easily computed homomorphism

$$\log_{p\text{-adic}} : E(\mathbb{F}_p) \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

It is easy to solve the discrete logarithm problem in $\mathbb{Z}/p\mathbb{Z}$, so if $\#E(\mathbb{F}_p) = p$, then we can solve ECDLP in time $O(\log p)$.

The Weil Pairing

An important tool for studying elliptic curves E over any field is the **Weil Pairing**. Let

$$E_N = \{P \in E : NP = \mathcal{O}\} \quad \text{and} \quad \boldsymbol{\mu}_N = \{\zeta : \zeta^N = 1\}.$$

The Weil pairing is a non-degenerate alternating bilinear form

$$e_N : E_N \times E_N \longrightarrow \boldsymbol{\mu}_N$$

The alternating property means that $e_N(P,P) = 1$.

In order to work with the Weil pairing over a finite field $\mathbb{F}_q$, it is necessary that $E_N \subset E(\mathbb{F}_q)$. (This also ensures that $\boldsymbol{\mu}_N \subset \mathbb{F}_q$.)

The Weil pairing has important applications in both cryptanalysis and in the construction of certain cryptosystems. There are various equivalent ways to define the Weil pairing and various algorithms to compute it.

Divisors and a Definition of the Weil Pairing

If E is an elliptic curve, then any function $f(x,y)$ that does not vanish identically on E will have zeros and poles, each of which may occur with multiplicity one or larger. The **divisor of f** is the formal sum

$$\operatorname{div}(f) = n_1(P_1) + n_2(P_2) + \cdots + n_r(P_r),$$

where f has a zero at P_i of order n_i (if $n_i > 0$) and a pole at P_i of order $-n_i$ (if $n_i < 0$).

Given two points $P, Q \in E_N$, choose any two points $R, S \in E$ and find functions f_P and f_Q satisfying

$$\begin{aligned}\operatorname{div}(f_P) &= N(P+R) - N(R),\\ \operatorname{div}(f_Q) &= N(Q+S) - N(S).\end{aligned}$$

Then

$$e_N(P,Q) = \frac{f_P(Q+S)}{f_P(S)} \cdot \frac{f_Q(R)}{f_Q(P+R)}.$$

The Tate Pairing

The Weil pairing is alternating. It is often more efficient to use the Tate pairing, which is symmetric.

The **Tate Pairing** is a non-degenerate **symmetric** bilinear form

$$E(\mathbb{F}_q)_N \times \frac{E(\mathbb{F}_q)}{NE(\mathbb{F}_q)} \longrightarrow \frac{\mathbb{F}_q^*}{(\mathbb{F}_q^*)^N}, \qquad (P, Q) \longmapsto \langle P, Q\rangle_{\text{Tate}}.$$

We assume that $\boldsymbol{\mu}_N \subset \mathbb{F}_q^*$, so $\mathbb{F}_q^*/(\mathbb{F}_q^*)^N$ is cyclic of order N, since $\mathbb{F}_q^*$ is a cyclic group.

To compute $\langle P, Q\rangle_{\text{Tate}}$, find a function f_P with divisor

$$\operatorname{div}(f_P) = N(P) - N(\mathcal{O})$$

and choose any point $S \in E$. Then

$$\langle P, Q\rangle_{\text{Tate}} = f_P(Q+S)/f_P(S).$$

Reducing ECDLP in $E(\mathbb{F}_p)$ to DLP in $\mathbb{F}_p^*$

The Tate pairing can be used to reduce ECDLP in $E(\mathbb{F}_p)$ to DLP in $\mathbb{F}_q^*$ for a power $q = p^t$. (MOV method)

Precisely, let $q = p^t$ be the smallest power of p satisfying

$$p^t \equiv 1 \pmod{N}, \qquad \text{where } N = \#E(\mathbb{F}_p).$$

Then the field $\mathbb{F}_q$ contains a primitive N^{th} root of unity.

Reduction of ECDLP in $E(\mathbb{F}_p)$ to DLP in $\mathbb{F}_p^*$

- Suppose that $S, T \in E(\mathbb{F}_p)$ satisfy $T = mS$.
- Compute $\langle S, S\rangle_{\text{Tate}}$ and $\langle S, T\rangle_{\text{Tate}}$ as elements of $\mathbb{F}_q^*$.
- By linearity, $\langle S, T\rangle_{\text{Tate}} = \langle S, mS\rangle_{\text{Tate}} = \langle S, S\rangle_{\text{Tate}}^m$.
- Solving DLP in $\mathbb{F}_q^*$ reveals m and solves ECDLP.

Moral: Don't use curves with small p^t (say $p^t < 2^{1000}$).

Tripartite Diffie-Hellman Key Exchange

The Tate pairing is used in a number of important cryptographic constructions. The first was Joux's method to do Diffie-Hellman key exchange with **three** people. (No four person method is known!)

We begin by fixing:

- A prime $p > 2^{1000}$ and an elliptic curve $E/\mathbb{F}_p$.
- A point $S \in E(\mathbb{F}_p)$ of order N with $p \equiv 1 \pmod{N}$.

Three Person Diffie-Hellman Key Exchange

Alice	**Bob**	**Carl**
Choose secret a	Choose secret b	Choose secret c
Publish $A = aS$	Publish $B = bS$	Publish $C = cS$
Do $\langle B, C\rangle_{\text{Tate}}^{a}$	Do $\langle A, C\rangle_{\text{Tate}}^{b}$	Do $\langle A, B\rangle_{\text{Tate}}^{c}$
Alice, Bob, and Carl share the value $\langle S, S\rangle_{\text{Tate}}^{abc}$		

Reduction Modulo p, Lifting, and ECDLP

Reduction of an Elliptic Curve Modulo p

Let E be an elliptic curve given by an equation

$$E : y^2 = x^3 + Ax + B \qquad \text{with } A, B \in \mathbb{Z}$$

We can reduce the coefficients of E modulo a prime p to get an elliptic curve $\tilde{E}$ with coefficients in $\mathbb{F}_p$,

$$\tilde{E} : y^2 = x^3 + \tilde{A}x + \tilde{B} \qquad \text{with } \tilde{A}, \tilde{B} \in \mathbb{F}_p.$$

However, remember we must check that $\tilde{E}$ is not singular, which means that we need the discriminant

$$\tilde{\Delta} = 4\tilde{A}^3 + 27\tilde{B}^2 \neq 0 \quad \text{in } \mathbb{F}_p \quad (\text{also } p \neq 2).$$

We say that E has **Good Reduction at p** if p does not divide the discrimiannt $\Delta = 4A^3 + 27B^2$ and we say that E has **Bad Reduction at p** if p does divide Δ.

When we talk about reduction modulo p, we will generally assume that we have good reduction at p.

Reduction of Points Modulo p

Let $P = (x, y) \in E(\mathbb{Q})$ be a rational point on an elliptic curve. We can reduce the coordinates of P modulo p to get a point

$$\tilde{P} = (\tilde{x}, \tilde{y}) \in \tilde{E}(\mathbb{F}_p).$$

If x and y are in $\mathbb{Z}$, this is fine, but what if they have denominators? Suppose $x = \frac{a}{b} \in \mathbb{Q}$. If $p \nmid b$, then $\tilde{b}$ has an inverse in $\mathbb{F}_p$, so we set

$$\tilde{x} = \tilde{a}\tilde{b}^{-1} \quad \text{in } \mathbb{F}_p.$$

And $\tilde{y}$ is defined similarly.

What happens if p divides the denominator of x or y? In that case, it divides both denominators and we set

$$\tilde{P} = \tilde{\mathcal{O}} = \text{point at infinity on } \tilde{E}.$$

We have defined a **Reduction Modulo p Map**

$$E(\mathbb{Q}) \longrightarrow \tilde{E}(\mathbb{F}_p), \qquad P \longmapsto \tilde{P}.$$

The Reduction Modulo p Homomorphism

It is hard to overstate the importance of reduction modulo p. A first indication is:

Theorem. If E has good reduction, then the reduction modulo p map

$$E(\mathbb{Q}) \longrightarrow \tilde{E}(\mathbb{F}_p), \qquad P \longmapsto \tilde{P},$$

is a group homomorphism.

Example Let E be the elliptic curve

$$E : y^2 = x^3 + 2x + 4.$$

Some points in $E(\mathbb{Q})$ are

$$P = (2,4), \quad Q = \left(\frac{1}{4}, \frac{17}{8}\right), \quad P + Q = \left(-\frac{54}{49}, -\frac{232}{343}\right).$$

The reduction modulo 11 map $E(\mathbb{Q}) \to \tilde{E}(\mathbb{F}_{11})$ gives

$$\tilde{P} = (2,4), \quad \tilde{Q} = (3,9), \quad \tilde{P} + \tilde{Q} = (9,5) = \widetilde{P+Q}.$$

Reduction Modulo p and Torsion Points

If $E(\mathbb{Q})$ is infinite, then obviously the homomorphism

$$E(\mathbb{Q}) \longrightarrow \tilde{E}(\mathbb{F}_p)$$

cannot be one-to-one.

Theorem. If $\gcd(N,p) = 1$ and E has good reduction, then

$$E(\mathbb{Q})_N \longrightarrow \tilde{E}(\mathbb{F}_p) \quad \text{is one-to-one.}$$

A similar statement holds if $\mathbb{Q}$ is replaced by a number field. It is difficult to overemphasize the importance of this theorem.

The theorem gives an efficient way to find $E(\mathbb{Q})_{\text{tors}}$.

Example. $E : y^2 = x^3 - 5x + 2$. We compute

$$\Delta = -392 = -2^3 \cdot 7^2, \quad \#E(\mathbb{F}_3) = 4, \quad \#E(\mathbb{F}_{11}) = 14.$$

Hence $\#E(\mathbb{Q})_{\text{tors}}$ is at most 2. Since $(2,0) \in E(\mathbb{Q})_{\text{tors}}$ is a point of order 2, this proves that $E(\mathbb{Q})_{\text{tors}} = C_2$.

Reduction Modulo p, Lifting, and ECDLP

Here is a possible approach to solving ECDLP:

(1) Start with points $\tilde{S}, \tilde{T} \in \tilde{E}(\mathbb{F}_p)$.
(2) Choose an elliptic curve E whose reduction is $\tilde{E}$.
(3) Lift $\tilde{S}, \tilde{T}$ to points $S, T \in E(\mathbb{Q})$.
(4) Find a relation $nT = mS$ in $E(\mathbb{Q})$.
(5) Reduce modulo p to get $n\tilde{T} = m\tilde{S}$.

- It is easy to find a lift E of $\tilde{E}$ so that $\tilde{S}$ and $\tilde{T}$ have lifts $S, T \in E(\mathbb{Q})$.
- If S and T are linearly dependent in $E(\mathbb{Q})$, then there are efficient methods for finding a relation.

So what makes it hard to solve ECDLP?

- For some E, it is easy to find S and T, but S and T are almost always independent.
- For some E, the lifts S and T exist and are always dependent, but S and T are very hard to find.

Height Functions On Elliptic Curves

Height Functions

In order to understand lifting (and for many other purposes), it is important to answer the question:

How complicated are the points in $E(\mathbb{Q})$?

The answer is provided by the **Theory of Heights**. The **Height** of a rational number is defined to be

$$H\left(\frac{a}{b}\right) = \max\bigl\{|a|, |b|\bigr\}, \quad \text{for } \frac{a}{b} \in \mathbb{Q},\ \gcd(a,b) = 1.$$

Note. There are only finitely many rational numbers with height less than a given bound.

On elliptic curves, it is convenient to take the logarithm, so the **Height of a Point** on an elliptic curve is

$$h(P) = \log H(x_P) \qquad \text{for } P = (x_P, y_P) \in E(\mathbb{Q}).$$

(If $P = \mathcal{O}$, we set $h(P) = 0$.)

Intuition. It takes $O(h(P))$ bits to store P.

Properties of the Height Function on an Elliptic Curve

The reason that the height function plays an important role in studying $E(\mathbb{Q})$ is due to its dual role:

(1) h measures the arithmetic complexity of points.

(2) h's transformations reflect the group law on E

Theorem. There are constants $c_1, c_2, \ldots$ so that for all points $P, Q, \ldots \in E(\mathbb{Q})$:

(a) $\bigl|h(nP) - n^2 h(P)\bigr| \le c_1$.

(b) $\bigl|h(P+Q) + h(P-Q) - 2h(P) - 2h(Q)\bigr| \le c_2$.

(c) For any c, the set

$$\bigl\{P \in E(\mathbb{Q}) : h(P) \le c\bigr\} \quad \text{is finite.}$$

Property (a) may be written $h(nP) = n^2 h(P) + O(1)$. Remember that $h(P)$ is the logarithm, so this says that the numerator or denominator of x_{nP} should have approximately n^2 digits.

The Quadratic Growth of the Height on Elliptic Curves

We illustrate with the elliptic curve and point

$$E : y^2 = x^3 + x + 1 \qquad \text{and} \qquad P = (0,1).$$

Here is a table of $H(x_{nP})$ for $n = 1, 2, \ldots, 25$.

1	1
2	2
3	13
4	36
5	685
6	7082
7	196249
8	9781441
9	645430801
10	54088691834
11	23545957758733
12	3348618159624516
13	3438505996705270765
14	2389279734043328028530
15	3568842156502352911081681
16	9147174028201584695660404993
17	40437302897155037003168469209281
18	144041052884595077187155035625188225
19	4077551427539061268365818617070082487981
20	29247742836717181569573123126609380958628633
21	1644662183623605030943992459758717959368038089933
22	76795559807444450146033952048248025474377706486132570
23	6037390795706541540397642739132383429233648456214266105001
24	816297679393916005694837838808362431503501229559444925278681793
25	242513738949178952234806483689465816559631390124939658301320990605073
26	47803232530993255659471421491008524334965293857886857075847338386784976289
27	67559659782039617237841184516992302782851604142385500859648938761010393239431661
28	32014345486637038681521545788678891610665676156825092102996356573331436095404542962201
29	75366079100860358183774143789438882594269554344230013075428451465317687946832468865183904333
30	2355960977134663307380989725524222422374156906907547045290688341377958875910979032848694872594995042
31	949929776724866709094954536710367778326401614961417743163923974793524931042092311077415673676701373662241
32	6939337780803547166840419022721964472182663632045063388197164628060008767530358928827755424306465309623700644865
33	138560009627230805680861712729089150246171433367872626810509092219015283874452951868081163892328387927559567336088640513
34	1470496183658794212496122961743692131111461785062102204982019653166220314029845380022856443720777836633186409902489575338782721
35	107010592458999940561955702180302050658481740392774624430340775789803872514791716886258854994198364978765941985457904860326401460918221

Notice the parabolic shape, reflecting the quadratic growth in the number of digits.

Canonical Heights on Elliptic Curves

Canonical Heights

Taking a limit gets rid of those pesky $O(1)$'s.

Theorem. (*Néron, Tate*). The limit

$$\boxed{\hat{h}(P) = \lim_{n\to\infty} \frac{1}{n^2} h([n]P)}$$

exists and has the following properties:

- $\hat{h}(P) = h(P) + O(1)$.
- $\hat{h}([n]P) = n^2\hat{h}(P)$.
- $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$.
- $\hat{h}(P) = 0$ if and only if $P \in E(\mathbb{Q})_{\text{tors}}$.
- More generally, the canonical height $\hat{h}$ induces a positive definite quadratic form on the real vector space

$$E(\mathbb{Q}) \otimes \mathbb{R} \cong \mathbb{R}^r, \qquad \text{where } r = \operatorname{rank} E(\mathbb{Q}).$$

The Height Regulator

The inner product

$$\langle P, Q\rangle := \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$$

gives $E(\mathbb{Q}) \otimes \mathbb{R} \cong \mathbb{R}^r$ the structure of a Euclidean space, and $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}^r$ is a lattice in $\mathbb{R}^r$. The volume of a fundamental domain of this lattice is

$$\mathcal{R}_E = \textbf{Elliptic Regulator of } E.$$

Concretely, let $P_1, \ldots, P_r \in E(K)$ be a basis for the quotient $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}}$. Then

$$\mathcal{R}_E = \det\bigl(\langle P_i, P_j\rangle\bigr)_{1\le i,j\le r}.$$

Efficient methods to compute $\hat{h}(P)$ to high accuracy (e.g., to 10^{-100}), even for elliptic curves whose coefficients have hundreds of digits, use a local decomposition

$$\hat{h}(P) = \hat{\lambda}_\infty(P) + \sum \hat{\lambda}_p(P).$$

Using Heights To Compute Relations

Here is an initially plausible way to solve ECDLP via lifting. Let $\tilde{S}, \tilde{T} \in \tilde{E}(\mathbb{F}_p)$.

(1) Lift $\tilde{E}$ and $\tilde{T}$ to a curve $E/\mathbb{Q}$ and point $T \in E(\mathbb{Q})$.

(2) Do this in such a way that $E(\mathbb{Q})$ has rank 1. (This can probably be done.)

(3) Lift $\tilde{S}$ to a point $S \in E(\mathbb{Q})$.

(4) Compute $\hat{h}(S)/\hat{h}(T)$. This is the square of a rational number, since S and T are both multiples of a generator of $E(\mathbb{Q})$. Find that rational number m^2/n^2. (In practice, n will be small.)

(5) Then $nT = mS$, so $n\tilde{T} = m\tilde{S}$.

The problem is Step (3), because usually $m = O(p)$. Thus the point $S \in E(\mathbb{Q})$ satisfies $\hat{h}(S) = O(p^2)$. Remember that $\hat{h}(S)$ is the amount of memory it takes to store S. Since typically $p \approx 2^{160}$, we cannot even store the point S.

Using Heights To Compute Relations

Here is an initially plausible way to solve ECDLP via lifting. Let $\tilde{S}, \tilde{T} \in \tilde{E}(\mathbb{F}_p)$.

(1) Lift $\tilde{E}$ and $\tilde{T}$ to a curve $E/\mathbb{Q}$ and point $T \in E(\mathbb{Q})$.

(2) Do this in such a way that $E(\mathbb{Q})$ has rank 1. (This can probably be done.)

(3) Lift $\tilde{S}$ to a point $S \in E(\mathbb{Q})$.

(4) Compute $\hat{h}(S)/\hat{h}(T)$. This is the square of a rational number, since S and T are both multiples of a generator of $E(\mathbb{Q})$. Find that rational number m^2/n^2. (In practice, n will be small.)

(5) Then $nT = mS$, so $n\tilde{T} = m\tilde{S}$.

Indeed, Neal Koblitz's talk at the Elliptic Curve Cryptography Conference in 2000 was entitled:

Miracles of the Height Function:
A Golden Shield Protecting ECC

Descent and the Mordell-Weil Theorem

Recall that Mordell's Theorem (which was later generalized by André Weil) says:

Mordell-Weil Theorem. The group of rational points $E(\mathbb{Q})$ is a finitely generated abelian group.

The proof proceeds in two steps. The first uses reduction modulo p to limit the ramification in the field extension $\mathbb{Q}\big([m]^{-1}E(K)\big)$ and deduce the

Weak Mordell-Weil Theorem. For some $m \geq 2$, the group $E(\mathbb{Q})/mE(\mathbb{Q})$ is a finite.

The second step is prove the implication

$$\text{Weak Mordell-Weil} \Longrightarrow \text{Mordell-Weil.}$$

This descent argument uses height functions and is an elegant application of the theory of canonical heights.

Weak Mordell-Weil Theorem $\Longrightarrow$ Mordell-Weil Theorem

Let $P_1, \ldots, P_n \in E(\mathbb{Q})$ be representatives for the finite set $E(\mathbb{Q})/mE(\mathbb{Q})$.

Claim: $E(\mathbb{Q})$ is generated by the finite set

$$G = \left\{ R \in E(\mathbb{Q}) : \hat{h}(R) \le \max_i \hat{h}(P_i) \right\}.$$

Proof. Suppose not. Let $P \in E(\mathbb{Q})$ be a point of smallest height not in $\operatorname{Span}(G)$. Write $P = mQ + P_j$ for some index j. Then

$$\begin{aligned} m^2\hat{h}(Q) &= \hat{h}(mQ) \\ &= \hat{h}(P - P_j) \\ &\le 2\hat{h}(P) + 2\hat{h}(P_j) \\ &< 4\hat{h}(P) \qquad \text{since } P_j \in G \text{ and } P \notin G. \end{aligned}$$

Since $m \ge 2$, we conclude $\hat{h}(Q) < \hat{h}(P)$. Therefore $Q \in \operatorname{Span}(G)$, contradicting $P \notin \operatorname{Span}(G)$. QED

Factorization Using Elliptic Curves

Pollard's $p-1$ Factorization Algorithm

Let $N = p_1 p_2 \cdots p_r$ be a number to be factored.

Pollard's $p-1$ Factorization Algorithm works if one of the primes p_k dividing N has the property that $p_k - 1$ itself factors as

$$p_k - 1 = \ell_1^{e_1} \ell_2^{e_2} \cdots \ell_r^{e_r} \quad \text{with } \ell_1, \ldots, \ell_r \text{ small.}$$

If $\ell_1, \ldots, \ell_r \le B$, then there is a good chance that

$$\gcd\left(2^{\mathrm{LCM}(1,2,\ldots,B)} - 1, N\right) \quad \text{will equal } p_k.$$

The idea underlying Pollard's $p-1$ Algorithm is the fact that every element of $(\mathbb{Z}/p\mathbb{Z})^*$ has order dividing $p-1$.

Unfortunately, if no $p-1$ is "B-smooth", then Pollard's method does not work.

Using Elliptic Curves for Factorization

Hendrik Lenstra observed that one can replace the multiplicative group $\mathbb{F}_p^*$ with an elliptic curve group $E(\mathbb{F}_p)$.

More precisely, choose an elliptic curve modulo N and a point on the curve:

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}/N\mathbb{Z}, \quad S \in E(\mathbb{Z}/N\mathbb{Z}).$$

Suppose that there is a prime p dividing N for which the number of points in $E(\mathbb{F}_p)$ is B-smooth.

Then there is a good chance that during the computation of

$$\mathrm{LCM}(1, 2, \ldots, B)S \bmod N,$$

some inverse $(x_2 - x_1)^{-1} \bmod N$ will not exist, yielding

$$\gcd(x_2 - x_1, N) = p.$$

Properties of Lenstra's Algorithm

The advantage of Lenstra's Elliptic Curve Algorithm over Pollard's $p - 1$ Algorithm is the introduction of many finite groups $E(\mathbb{F}_p)$ with many different orders.

The theoretical running time of Lenstra's Algorithm can be calculated using a reasonable assumption about the distribution of B-smooth numbers in short intervals:

> Let p the **smallest** prime dividing N. Then the expected running time of Lenstra's algorithm is
>
> $$O\left(e^{c\sqrt{(\log p)(\log\log p)}}\right).$$

The fact that the running time depends on the smallest prime divisor of N makes Lenstra's algorithm especially good for factoring "random" numbers, but it is slower than sieve methods for "RSA-type" numbers $N = pq$.

L-Series, the Conjecture of Birch and Swinnerton-Dyer, and a Million Dollar Prize

The L-Series of an Elliptic Curve

Let E be an elliptic curve given as usual by an equation

$$y^2 = x^3 + Ax + B \qquad \text{with } A, B \in \mathbb{Z}.$$

For each prime p, we can reduce E modulo p, count its points, and compute the trace of Frobenius:

$$a_p = p + 1 - \#\tilde{E}(\mathbb{F}_p).$$

The **L-Series of E** encodes all of the a_p values into a single function:

$$L(E,s) = \prod_{p \text{ prime}} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}.$$

The variable s is a complex variable $s \in \mathbb{C}$. Using Hasse's estimate $|a_p| \le 2\sqrt{p}$, it is easy to prove that the product defining $L(E,s)$ converges for $\mathrm{Re}(s) > \frac{3}{2}$.

The Analytic Continuation of $L(E, s)$

Wiles' Theorem. The function $L(E, s)$ extends to an analytic function on all of $\mathbb{C}$. Further, there is an integer N (the **Conductor of E**) so that the function

$$\xi(E, s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E, s)$$

satisfies the functional equation

$$\xi(E, 2 - s) = \pm\xi(E, s).$$

A more precise form of Wiles' Theorem says to write

$$L(E, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \quad \text{and set} \quad f(E, \tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i n \tau}.$$

Then $f(E, \tau)$ is a modular form (weight 2 cusp form) for $\Gamma_0(N)$. This statement combined with ideas of Frey and Serre and a theorem of Ribet are used to prove Fermat's Last Theorem.

The Behavior of $L(E,s)$ Near $s=1$

It is a truth universally acknowledged that L-series satisfying a functional equation have interesting behavior at the center of their critical strip. For elliptic curves, this is at the point $s=1$.

A formal (and completely unjustified) calculation yields

$$L(E,1) = \prod_p \left(1 - \frac{a_p}{p} + \frac{1}{p}\right)^{-1} = \prod_p \frac{p}{\#E(\mathbb{F}_p)}.$$

This suggests that if $\#E(\mathbb{F}_p)$ is large, then $L(E,1)=0$.

Birch and Swinnerton-Dyer observed that if $E(\mathbb{Q})$ is infinite, then the reduction of the points in $E(\mathbb{Q})$ tend to make $\#E(\mathbb{F}_p)$ larger than usual. So they conjectured

$$L(E,1) = 0 \quad \text{if and only if} \quad \#E(\mathbb{Q}) = \infty.$$

The Conjecture of Birch and Swinnerton-Dyer

More generally, as the group $E(\mathbb{Q})$ gets “larger”, the size of $\#E(\mathbb{F}_p)$ seems to get larger, too.

Birch–Swinnerton-Dyer Conjecture.

$$\operatorname{ord}_{s=1} L(E,s) = \operatorname{rank} E(\mathbb{Q}).$$

This amazing conjecture says that the order of vanishing of the function $L(E,s)$, which recall is created entirely from information about the elliptic curve modulo various primes p, governs how many rational points are needed to generate the full group $E(\mathbb{Q})$.

The BSwD conjecture is one of the Clay Millenium Problems, so its solution is worth \$1,000,000.

There is a refined conjecture $L(E,s) \sim c(s-1)^r$. The constant c depends, among other things, on the elliptic regulator $\mathcal{R}_E$.

Epilogue

The preceding slides have barely touched the vast and rich mathematical theory of elliptic curves.

And even in the small stream of cryptography, we have merely skimmed the surface of the subject.

In the vaster realm of mathematics, the theory of elliptic curves appears and reappears in contexts too numerous to list, ranging from Wiles' proof of Fermat's Last Theorem to rings formed from cohomology groups to noncommutative quantum algebras and beyond.

The annotated bibliography includes a few references to assist you in learning more about the number theory and cryptographic applications of elliptic curves.

Additional Material

The Galois Representation Attached to E

Let E be an elliptic curve defined over $\mathbb{Q}$. Then the points in the N-torsion subgroup

$$E_N = \{P \in E(\mathbb{C}) : NP = \mathcal{O}\}$$

have coordinates in the algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$. Each element σ of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on E_N as a homomorphism. Thus we obtain a map

$$R_{E,N} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \{\text{homomorphisms } E_N \to E_N\}.$$

Exercise Verify that $R_{E,N}$ is a homomorphism.

The group of homomorphisms from $E_N \cong C_N \times C_N$ to itself is $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the group of 2-by-2 invertible matrices with coefficients in $\mathbb{Z}/N\mathbb{Z}$.

The map

$$R_{E,N} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}),$$

is the **Mod N Representation Attached to E**.

Why is the "Trace of Frobenius" a Trace?

Let p be a prime. Then there are Frobenius elements $\sigma_p \in \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ characterized by the property that

$$\sigma_p(\alpha) \cong \alpha^p \pmod{\mathfrak{p}},$$

where $\alpha \in \bar{\mathbb{Q}}$ and $\mathfrak{p}$ is a prime ideal lying above p.

Evaluating the representation $R_{E,N}$ at σ_p yields a matrix

$$R_{E,N}(\sigma_p) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Of course, the particular matix depends on the choice of a basis for E_N. But the determinant and trace of this matrix are independent of the choice of basis.

Theorem. For all $N \geq 1$,

$$\operatorname{Trace}\bigl(R_{E,N}(\sigma_p)\bigr) \equiv a_p \pmod{N}.$$

This explains why a_p is the **Trace of Frobenius**.

Miller's Algorithm to Compute the Tate Pairing

1. Choose a random point $S \in E(\mathbb{F}_q)$ and compute $Q' = Q + S \in E(\mathbb{F}_q)$.

2. Set

$$n = \lfloor \log_2 N \rfloor - 1, \qquad T_1 = P, \qquad f_1 = 1.$$

3. While $n \geq 1$ do:

   - Calculate equations of the straight lines L_1 and L_2 that arise in doubling T_1 and set

$$T_1 = 2T_1 \qquad \text{and} \qquad f_1 = \frac{f_1^2 L_1(Q') L_2(S)}{L_2(Q') L_1(S)}.$$

   - If the n^{th} bit of N is 1 then calculate the equations of the straight lines L_1 and L_2 that arise when adding T_1 to P and set

$$T_1 = T_1 + P \qquad \text{and} \qquad f_1 = \frac{f_1 L_1(Q') L_2(S)}{L_2(Q') L_1(S)}.$$

   - Decrement n by 1.

4. Return f_1, which is equal to $\langle P, Q \rangle_{\text{Tate}}$.

A Fancy Construction of the Tate Pairing

Let G denote the Galois group of $\bar{\mathbb{F}}_q$ over $\mathbb{F}_q$, and let

$$E_N = \{P \in E(\bar{\mathbb{F}}_q) : NP = \mathcal{O}\}.$$

Take Galois invariants of the short exact sequence

$$0 \longrightarrow E_N \longrightarrow E(\bar{\mathbb{F}}_q) \xrightarrow{P \to NP} E(\bar{\mathbb{F}}_q) \longrightarrow 0.$$

Since $H^1(G, E(\bar{\mathbb{F}}_q)) = 0$, this gives

$$E(\mathbb{F}_q)/NE(\mathbb{F}_q) \cong H^1(G, E_N)$$

Let $P \in E(\mathbb{F}_q)_N$ and $Q \in E(\mathbb{F}_q)/NE(\mathbb{F}_q)$. Identify Q with some $\xi_Q \in H^1(G, E_N)$ and use the Weil pairing to create an element of $H^1(G, \boldsymbol{\mu}_N)$ via the map

$$e_N(P, \xi_Q) : G \longrightarrow \boldsymbol{\mu}_N, \qquad \sigma \longmapsto e_N(P, \xi_Q(\sigma)).$$

This gives an element of $H^1(G, \boldsymbol{\mu}_N)$. A similar argument shows that $H^1(G, \boldsymbol{\mu}_N) \cong \mathbb{F}_q^*/\mathbb{F}_q^{*N}$.

Further Reading

Further Reading

- Blake, I. F.; Seroussi, G.; Smart, N. P. Elliptic curves in cryptography. London Mathematical Society Lecture Note Series, 265. Cambridge University Press, Cambridge, 2000. [A good introduction to the subject.]
- Certicom tutorials and white papers <www.certicom.com>. [Certicom is a company that markets products using elliptic curve cryptography.]
- Cohen, Henri. A course in computational algebraic number theory. Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993. [A basic resource for many algorithms, covers lattice algorithms (LLL) and elliptic curve algorithms.]
- Cohen, H.. Elliptic and Hyperelliptic Curve Cryptography: Theory and Practice, Chapman & Hall/CRC, 2005. [Comprehensive study of ECC and beyond.]
- Cremona, J. E. Algorithms for modular elliptic curves. Cambridge University Press, Cambridge, 1997. [Extensive coverage of mathematical algorithms for elliptic curves, although not specifically for cryptography.]
- Garrett, Paul. Making, Breaking Codes: An Introduction to Cryptology. Prentice-Hall, 2001. [An undergraduate textbook on cryptography, includes descriptions of ECC and NTRU.]
- Hankerson, D., Menezes, A.J., Vanstone, S. Guide to Elliptic Curve Cryptography Springer-Verlag, 2004. [A practical guide to ECC.]

Further Reading

- Koblitz, Neal. Elliptic curve cryptosystems. Mathematics of Computation 48 (1987), 203-209. [One of the original articles that proposed the use of elliptic curves for cryptography. The other is by Victor Miller.]
- Koblitz, Neal. A course in number theory and cryptography. Graduate Texts in Mathematics, 114. Springer-Verlag, New York, 1994. [Covers basic cryptography.]
- Koblitz, Neal. Algebraic aspects of cryptography. Algorithms and Computation in Mathematics, 3. Springer-Verlag, Berlin, 1998. [Cryptography from an algebraic viewpoint.]
- Koblitz, Neal. Miracles of the Height Function — A Golden Shield Protecting ECC, 4th workshop on Elliptic Curve Cryptography (ECC 2000). [Slides from a talk.] `www.cacr.math.uwaterloo.ca/conferences/2000/ecc2000/koblitz.ps`
- Menezes, Alfred J.; Van Oorschot, Paul C.; Vanstone, Scott A.. Handbook of Applied Cryptography (CRC Press Series on Discrete Mathematics and Its Applications), 1996. [Encyclopedic description of cryptography.]
- Menezes, Alfred. Elliptic curve public key cryptosystems. The Kluwer International Series in Engineering and Computer Science, 234. Communications and Information Theory. Kluwer Academic Publishers, Boston, MA, 1993. [An early description of ECC with implementation methods.]

Further Reading

- Miller, Victor. Use of elliptic curves in cryptography. Advances in cryptology CRYPTO '85 (Santa Barbara, CA, 1985), 417–426, Lecture Notes in Comput. Sci., 218, Springer, Berlin, 1986. [One of the original articles proposing the use of elliptic curves for crypto. The other is by Neal Koblitz.]
- Silverman, Joseph H. The arithmetic of elliptic curves. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986. [The number theory of elliptic curves at a level suitable for advanced graduate students.]
- Silverman, Joseph H. Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994. [Additional topics in the number theory of elliptic curves.]
- Silverman, Joseph H.; Tate, John. Rational points on elliptic curves. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992. [An introduction to the number theoretic properties of elliptic curves at an advanced undergraduate level.]
- Stinson, Douglas R. Cryptography. Theory and practice. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1995. [An excellent introduction to cryptography at the advanced undergraduate or beginning graduate level, includes a description of ECC.]
- Washington, Lawrence. Elliptic Curves: Number Theory and Cryptography Chapman & Hall/CRC, 2003. [An introduction to elliptic curves and ECC at an advanced undergraduate/beginning graduate level.]