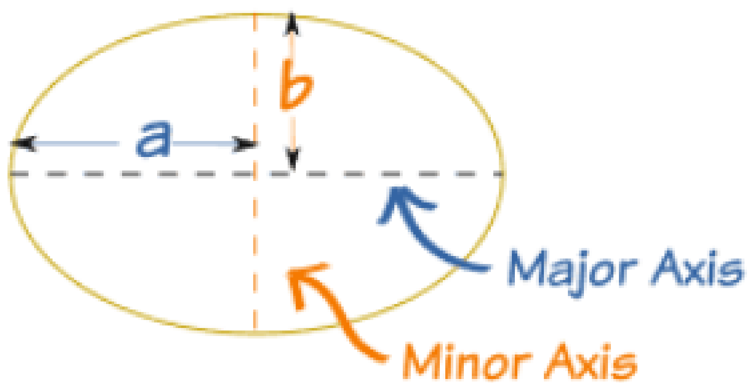
Number theory and Cryptography June 11, 2024

Lecture 11 : Introduction to Elliptic Curves

Instructor: Chao Qin *Notes written by: Wenhao Tong and Yingshu Wang*

1 What is an elliptic curve?

The equation $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ defines an ellipse.



An ellipse,like all conic sections, is a curve of genus 0.
It is not an elliptic curve. Elliptic curves have genus 1.
The area of this ellipse is πab. What is its circumference?

1.1 The circumference of an ellipse

Let $y = f(x) = b\sqrt{1 - x^2/a^2}$.
Then $f'(x) = -rx/\sqrt{a^2 - x^2}$,where $r = b/a < 1$.

Applying the arc length formula, the circumference is

$$4\int_0^a \sqrt{1 + f'(x)^2}\, dx = 4\int_0^a \sqrt{1 + r^2x^2/(a^2 - x^2)}\, dx$$

With the substitution $x = at$ this becomes

$$4a\int_0^1 \sqrt{\frac{1 - e^2t^2}{1 - t^2}}\, dt,$$

where $e = \sqrt{1 - r^2}$ is the eccentricity of the ellipse.
This is an elliptic integral. The integrand $u(t)$ satisfies

$$u^2(1 - t^2) = 1 - e^2t^2.$$

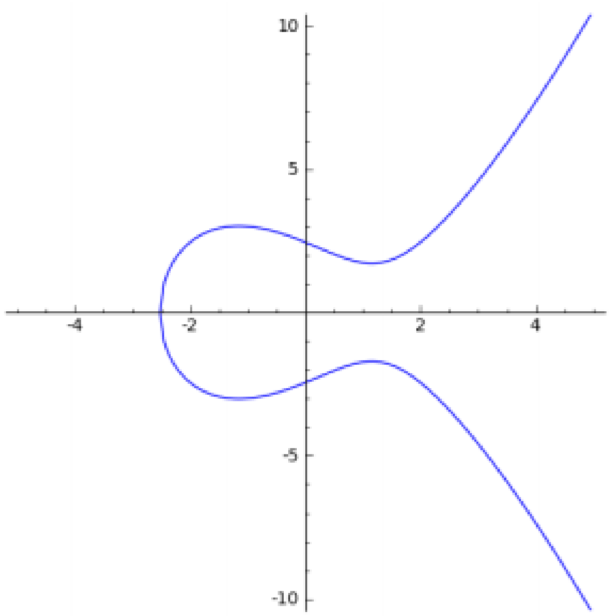
This equation defines an elliptic curve.

1.2 An elliptic curve over the real numbers

With a suitable change of variables, every elliptic curve with real coefficients can be put in the standard form

$$y^2 = x^3 + Ax + B,$$

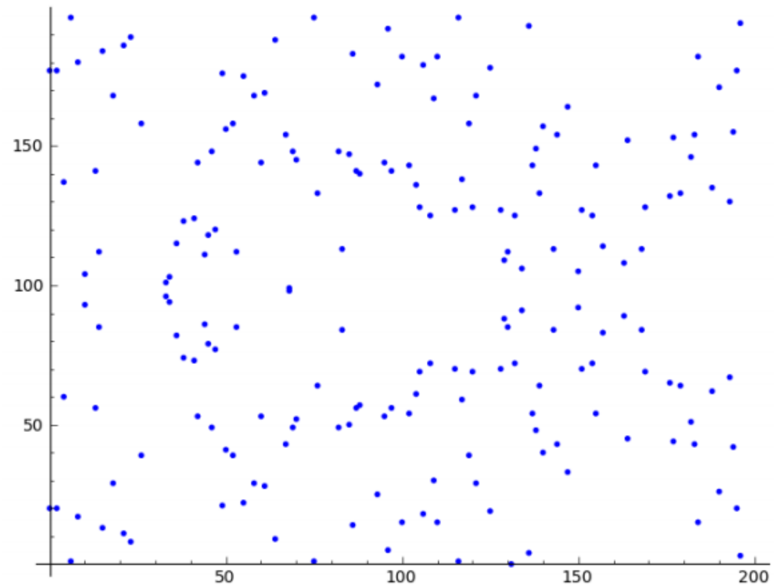
for some constants A and B. Below is an example of such a curve.



$$y^2 = x^3 - 4x + 6$$

over $\mathbb{R}$

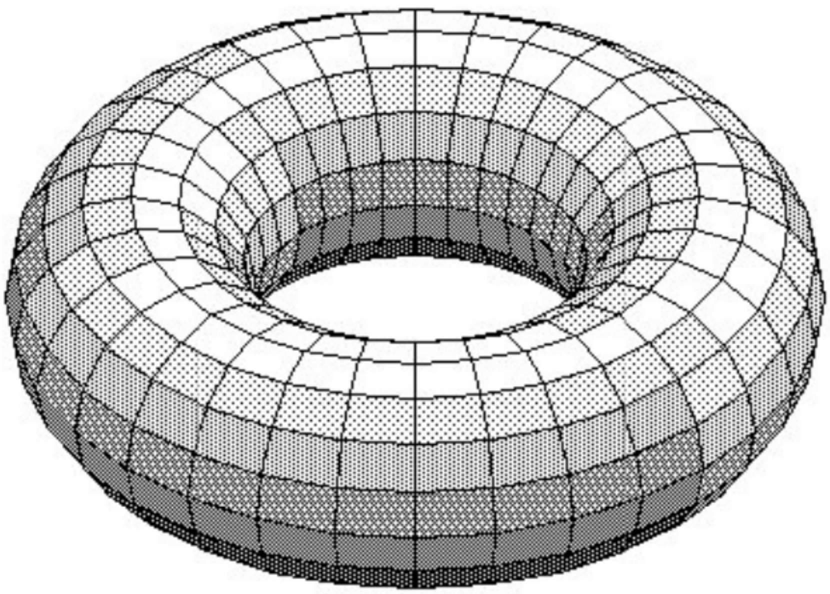
1.3 An elliptic curve over a finite field



$$y^2 = x^3 - 4x + 6$$

over $\mathbb{F}_{197}$

1.4 An elliptic curve over the complex numbers



An elliptic curve over C is a compact manifold of the form C/L, where $L = \mathbb{Z} + \omega\mathbb{Z}$ is a lattice in the complex plane.

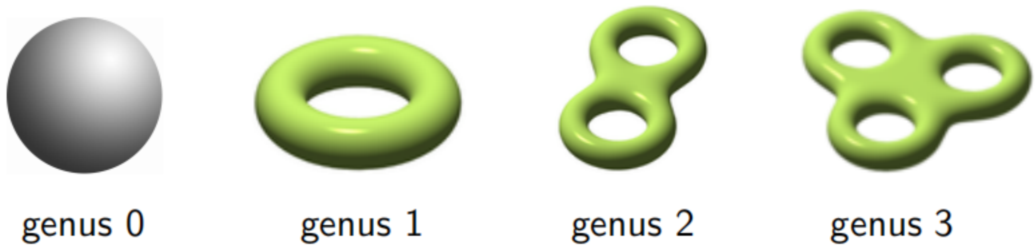
Definition. *An elliptic curve is a smooth projective curve of genus 1 with a distinguished point.*

Definition (more precise)**.** *An elliptic curve (over a field k) is a smooth projective curve of genus 1 (defined over k) with a distinguished (k-rational) point.*

Not every smooth projective curve of genus 1 corresponds to an elliptic curve, it needs to have at least one rational point!
For example, the (desingularization of) the curve defined by $y^2 = -x^4 - 1$ is a smooth projective curve of genus 1 with no rational points.

1.5 Genus

Over $\mathbb{C}$, an irreducible projective curve is a connected compact manifold of dimension one. Topologically, it is a sphere with handles.The number of handles is the genus.



In fact, the genus can be defined algebraically over any field, not just $\mathbb{C}$.

1.6 Weierstrass equations

Let $A, B \in k$ with $4A^3 + 27B^2 \neq 0$,and assume $\mathrm{char}(k) \neq 2, 3$.
The (short/narrow) Weierstrass equation $y^2 = x^3 + Ax + B$ defines a smooth projective genus 1 curve over k with the rational point (0:1:0).

In other words, an elliptic curve!

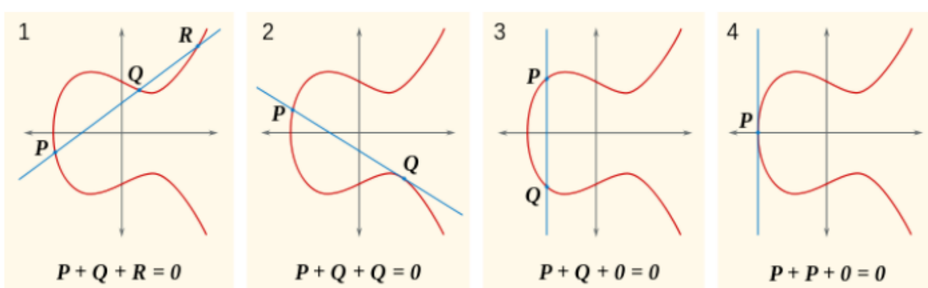
Up to isomorphism, every elliptic curve over k can be defined this way. The general Weierstrass equation

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

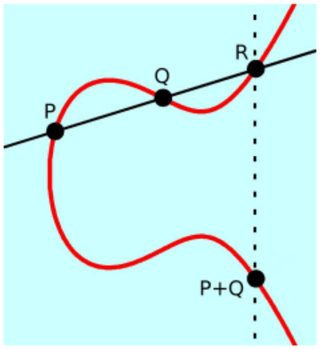
works over any field, including those of characteristic 2 and 3

1.7 The elliptic curve group law

Three points on a line sum to zero.



Zero is the point at infinity.



1.8 The elliptic curve group law

With addition defined as above, the set $E(k)$ becomes an abelian group.

- The point (0:1:0) at infinity is the identity element 0.
- The inverse of $P = (x : y : z)$ is the point $-P = (x : -y : z)$.
- Commutativity is obvious: $P + Q = Q + P$.
- Associativity is not so obvious: $P + (Q + R) = (P + Q) + R$.

The computation of $P + Q = R$ is purely algebraic. The coordinates of R are rational functions of the coordinates of P and Q,and can be computed over any field.
By adding a point to itself repeatedly, we can compute $2P = P + P$, $3P = P + P + P$,and in general,$nP = P + \cdots + P$ for any positive n.
We also define $0P = 0$ and $(-n)P = -nP$.
Thus we can perform scalar multiplication by any integer n.

1.9 The group E(k)

When $k = \mathbb{C}$,the group operation on $E(\mathbb{C}) \simeq \mathbb{C}/L$ is just addition of complex numbers, modulo the lattice L.
When $k = \mathbb{Q}$ things get much more interesting. The group $E(\mathbb{Q})$ may be finite or infinite, but in every case it is finitely generated.

theorem 1 (Mordell 1922)**.** *The group $E(\mathbb{Q})$ is a finitely generated abelian group. Thus*

$$E(\mathbb{Q}) \simeq T \oplus \mathbb{Z}^r,$$

where the torsion subgroup T is a finite abelian group corresponding to the elements of $E(\mathbb{Q})$ with finite order, and r is the rank of $E(\mathbb{Q})$.

It may happen (and often does) that $r = 0$ and T is the trivial group. In this case the only element of $E(\mathbb{Q})$ is the point at infinity.

1.10 The group E($\mathbb{Q}$)

The torsion subgroup of E($\mathbb{Q}$) is well understood.

theorem 2 (Mazur 1977)**.** *The torsion subgroup of $E(\mathbb{Q})$ is isomorphic to one of the following.*

$$\mathbb{Z}/n\mathbb{Z} \quad \text{or} \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z},$$

where $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$ and $m \in \{1, 2, 3, 4\}$.

1.11 The ranks of elliptic curves over $\mathbb{Q}$

The rank r of $E(\mathbb{Q})$ is not well understood. Here are some of the things we do not know about r :

1. Is there an algorithm that is guaranteed to compute r?
2. Which values of r can occur?
3. How often does each possible value of r occur, on average?
4. Is there an upper limit, or can r be arbitrarily large?

We do know a few things about r. We can compute r in most cases where r is small. When r is large often the best we can do is a lower bound; the largest example is a curve with $r \geq 28$ due to Elkies (2006).

1.12 The ranks of elliptic curves over $\mathbb{Q}$

The most significant thing we know about r is a bound on its average value over all elliptic curves (suitably ordered).

theorem 3 (Bhargava, Shankar 2010-2012)**.** *The average rank of all elliptic curves over $\mathbb{Q}$ is less than 1.*

In fact we now know the average rank is greater than 0.2 and less than 0.9; it is believed to be exactly 1/2 (half rank 0,half rank 1).
Manjul Bhargava received the Fields Medal in 2016 for the work that led to this theorem (and which has many other applications).

1.13 The group E($\mathbb{F}_p$)

Over a finite field $\mathbb{F}_p$, the group $E(\mathbb{F}_p)$ is necessarily finite.
On average, the size of the group is $p+1$, but it varies, depending on E.
The following theorem of Hasse was originally conjectured by Emil Artin.

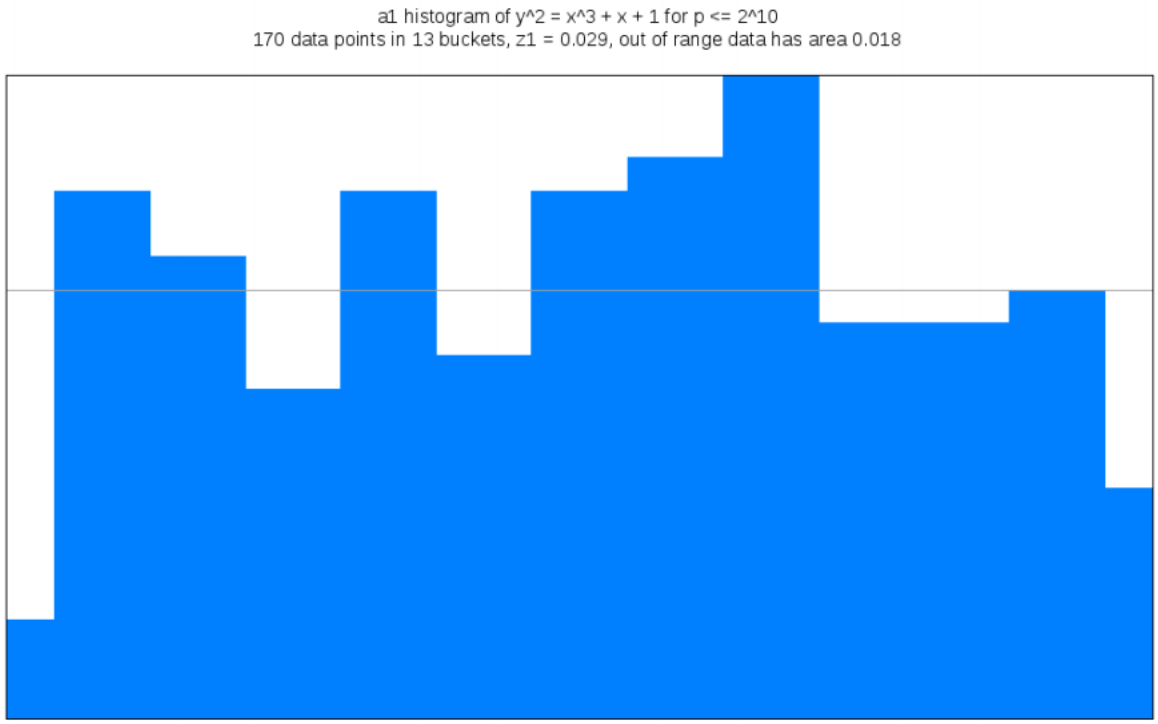
theorem 4 (Hasse 1933)**.** *The cardinality of* $E(\mathbb{F}_p)$ *satisfies* $\#E(\mathbb{F}_p) = p+1-t, with|t| \leq 2\sqrt{p}$.

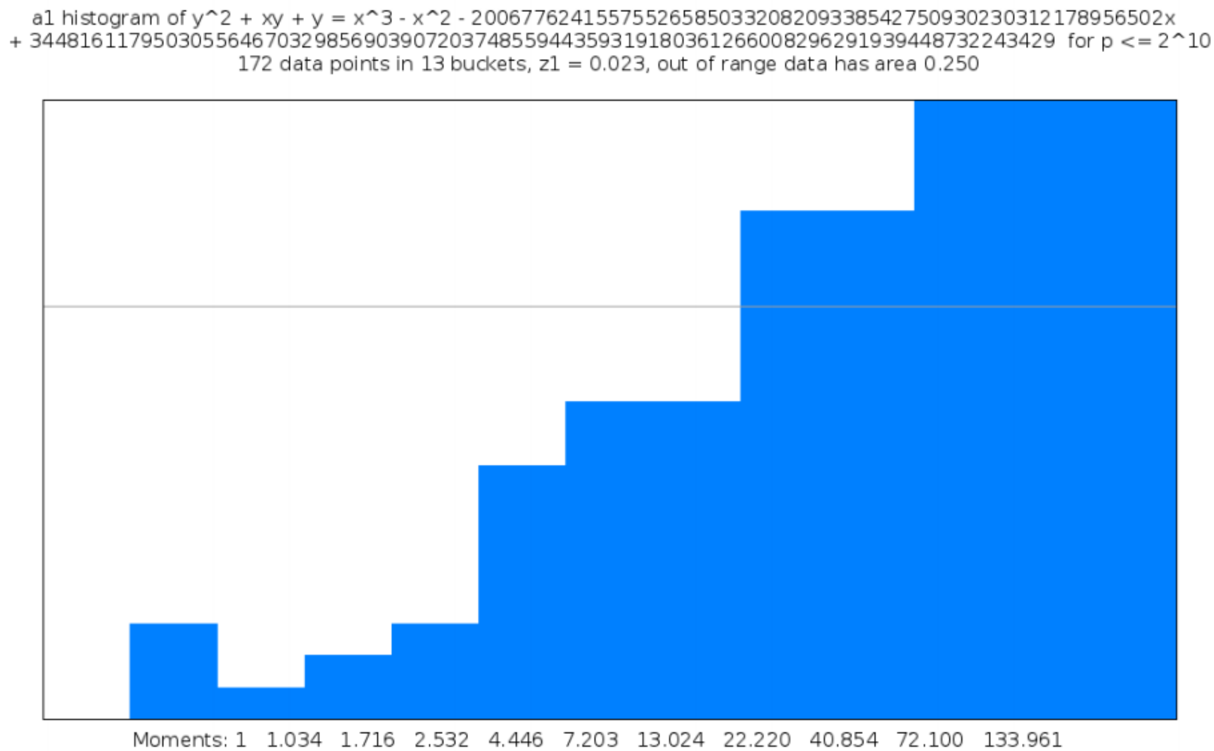
The fact that $E(\mathbb{F}_p)$ is a group whose size is not fixed by p is unique to genus 1 curves. This is the basis of many useful applications.
For curves C of genus $g = 0$, we always have $\#C(\mathbb{F}_p) = p+1$.
For curves C of genus $g > 1$, the set $C(\mathbb{F}_p)$ does not form a group.

1.14 Reducing elliptic curves over $\mathbb{Q}$ modulo p

Let $E/\mathbb{Q}$ be an elliptic curve defined by $y^2 = x^3 + Ax + B$,and let p be a prime that does not divide the discriminant $\Delta(E) = -16(4A^3 + 27B^2)$.
The elliptic curve E is then said to have good reduction at p.
If we reduce A and B modulo p, we obtain an elliptic curve $E_p := E \bmod p$ defined over the finite field $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$.
Thus from a single curve $E/\mathbb{Q}$ we get an infinite family of curves, one for each prime p where E has good reduction.
Now we may ask, how does $\#E_p(\mathbb{F}_p)$ vary with p?
We know $\#E_p(\mathbb{F}_p) = p+1-a_p$ for some integer a_p with $|a_p| \leq 2\sqrt{p}$.
So let $x_p := a_p/\sqrt{p}$. Then x_p is a real number in the interval [-2,2].

What is the distribution of x_p as p varies?


a1 histogram of y^2 = x^3 + x + 1 for p <= 2^10
170 data points in 13 buckets, z1 = 0.029, out of range data has area 0.018



1.15 The Birch and Swinnerton-Dyer conjecture

Based on extensive computer experiments (back in the 1960s!),
Bryan Birch and Pețter Swinnerton-Dyer made the following conjecture

Let$E/\mathbb{Q}$ be an elliptic curve with rank r. Then

$$L(E,s) = (s-1)^r g(s),$$

for some complex analytic function $g(s)$ with $g(1) \neq 0, \infty$. In other words, r is equal to the order of vanishing of $L(E,s)$ at 1.
They later made a more precise conjecture that also specifies the constant coefficient a_0 of $g(s) = \sum_{n \geq 0} a_n (s-1)^n$.

1.16 Fermat's Last Theorem

theorem 5 (Wiles et al. 1995). *$x^n + y^n = z^n$ has no positive integer solutions for $n > 2$.*

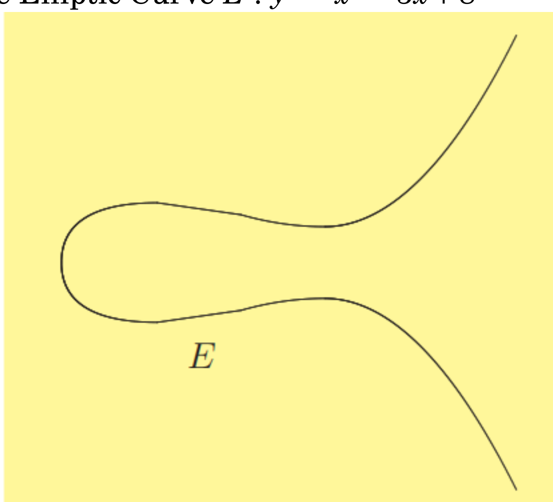
It suffices to consider n prime.
Suppose $a^n + b^n = c^n$ with $a, b, c > 0$ and $n > 3$ (the case $n = 3$ was proved by Euler). Consider the elliptic curve $E_{a,b,c}/\mathbb{Q}$ defined by

$$y^2 = x(x - a^n)(x - b^n).$$

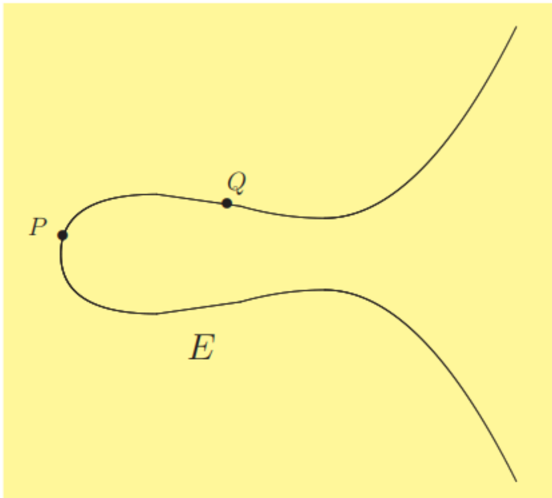
Serre and Ribet proved that $E_{a,b,c}$ is not modular.
Wiles (with assistance from Taylor) proved that every semistable elliptic curve over $\mathbb{Q}$, including E,is modular. Fermat's Last Theorem follows. We now know that all elliptic curves $E/\mathbb{Q}$ are modular.

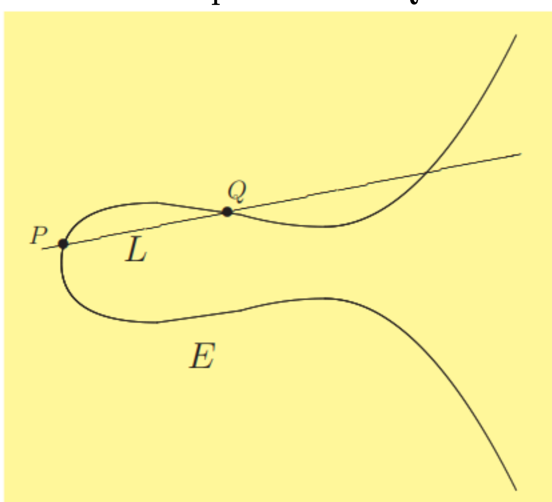
2 The Geometry of Elliptic Curves

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

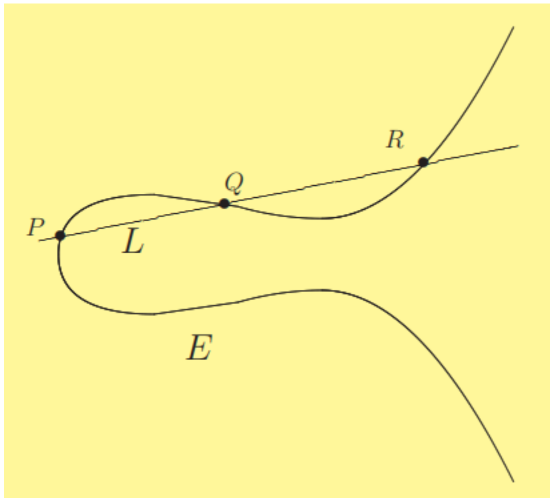


Adding Points on an Elliptic Curve

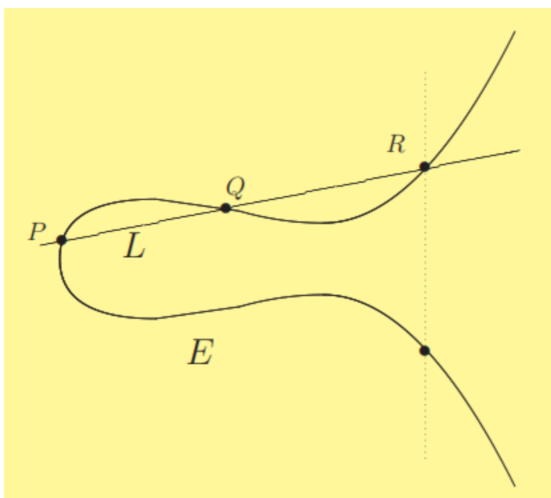


Start with two points P and Q on E.


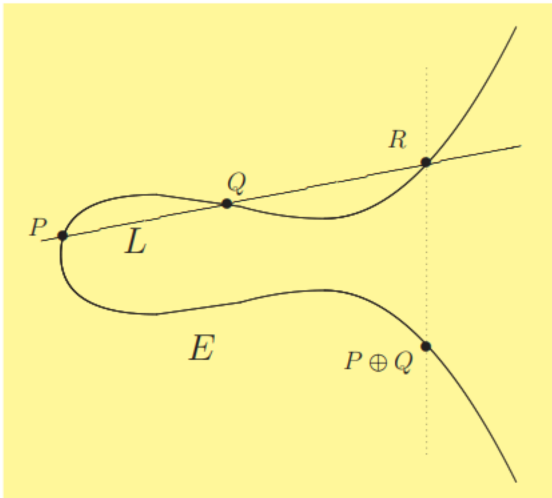
Draw the line L through P and Q.



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

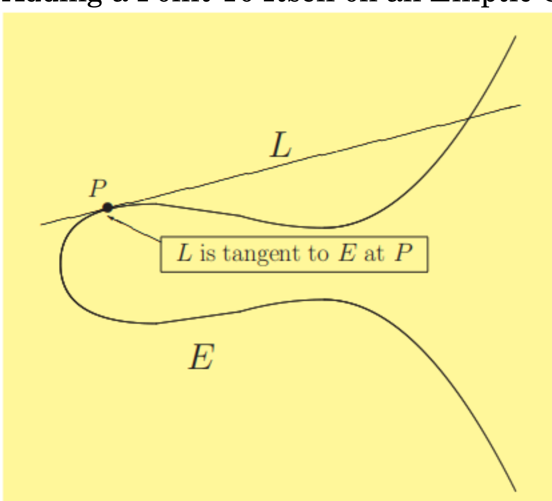


Draw the vertical line through R.It hits E in another point.

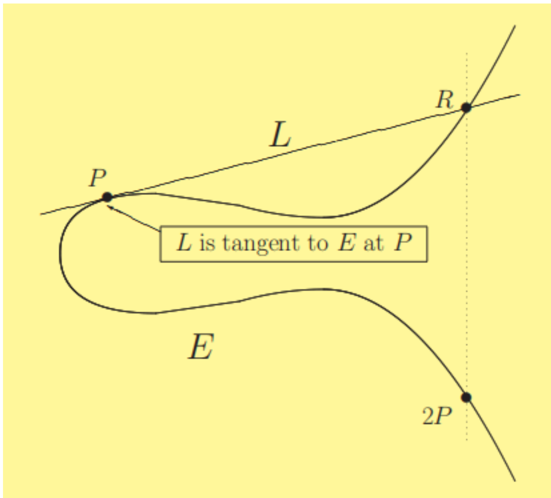


We define the sum of P and Q on E to be the reflected point.We denote it by $P \oplus Q$ or just $P + Q$.

Adding a Point To Itself on an Elliptic Curve



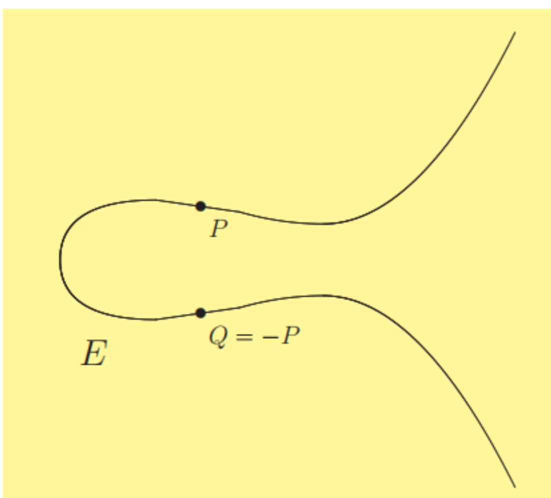
If we think of adding P to Q and let Q approach P, then the line L becomes the tangent line to E at P.



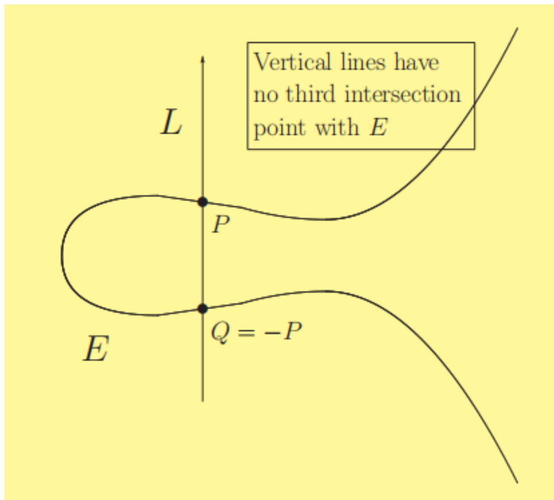
Then we take the third intersection point R, reflect across the x-axis, and call the resulting point

$$P \oplus P \text{ or } 2P.$$

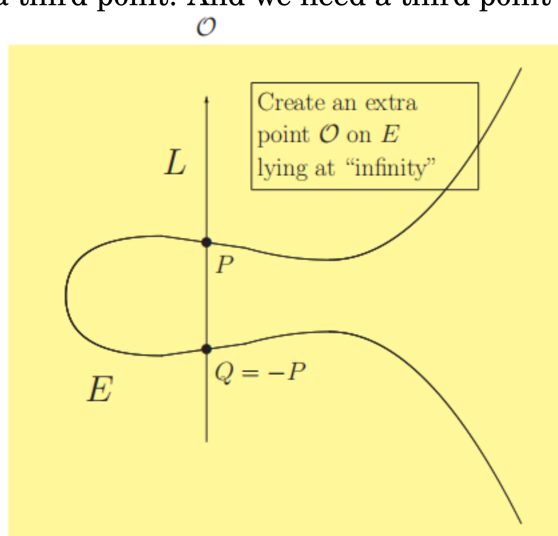
Vertical Lines and the Extra Point “At Infinity”



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



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 $P \oplus (-P)$.



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

Rule: O is a point on every vertical line.

3 The Algebra of Elliptic Curves

3.1 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.

3.2 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

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

We find the intersection of

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

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

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

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

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

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$P_1 + P_2 = O$.
- If $P_1 = P_2$ and $y_1 = 0$,then $P_1 + P_2 = 2P_1 = O$.
- If $P_1 \neq P_2$ (and $x_1 \neq x_2$),
  let $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ and $\nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$.
- If $P_1 = P_2$(and $y_1 \neq 0$),
  let $\lambda = \frac{3x_1^2 + A}{2y_1}$ and $\nu = \frac{-x^3 + Ax + 2B}{2y}$.

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

3.3 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.

3.4 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 6 (Poincareé, ≈ 1900)**.** *Let K be a field and suppose that an elliptic curve E is given by an equation of the form*

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

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

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

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

3.5 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 1. *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),....
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* $E(\bar{\mathbb{F}}_{37})$ *consists of the following 45 points modulo 37:*
$(1,\pm2), (5,\pm21), (6,\pm3), (8,\pm6), (9,\pm27), (10,\pm25),$
$(11,\pm27), (12,\pm23), (16,\pm19), (17,\pm27), (19,\pm1), (20,\pm8)$
$(21,\pm5), (22,\pm1), (26,\pm8), (28,\pm8), (30,\pm25), (31,\pm9),$
$(33,\pm1), (34,\pm25), (35,\pm26), (36,\pm7), O.$

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

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

theorem 7. *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.*

3.6 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

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

Then mP can be computed as

$$mP = m_0P + m_1 \cdot 2P + m_2 \cdot 2^2P + \cdots + m_r \cdot 2^rP,$$

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