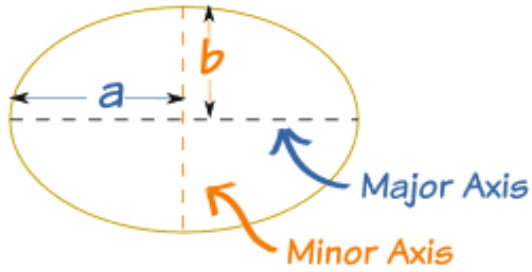
18.783 Elliptic Curves
Lecture 1

Andrew Sutherland

January 31, 2022

What is an elliptic curve?

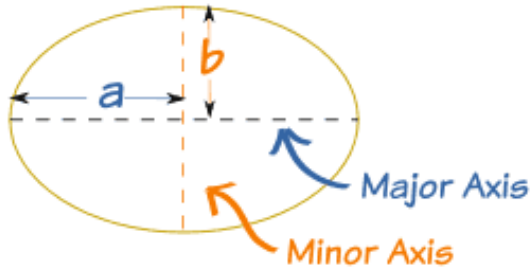
The equation $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ defines an **ellipse**.



Like all conic sections, an ellipse is a curve of genus 0.
Elliptic curves have genus 1, so **an ellipse is not an elliptic curve**.

What is an elliptic curve?

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



Like all conic sections, an ellipse is a curve of genus 0.
Elliptic curves have genus 1, so **an ellipse is not an elliptic curve**.

The area of this ellipse is πab. What is its circumference?

A. $\pi(a+b)$

B. $2\pi(a+b)$

C. $2\pi\sqrt{ab}$

D. It's complicated...

The circumference of an ellipse

Let $f(x) = b\sqrt{1 - x^2/a^2}$ and put $r = b/a$.

By 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.

The circumference of an ellipse

Let $f(x) = b\sqrt{1 - x^2/a^2}$ and put $r = b/a$.

By 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 $u = u(t)$ satisfies

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

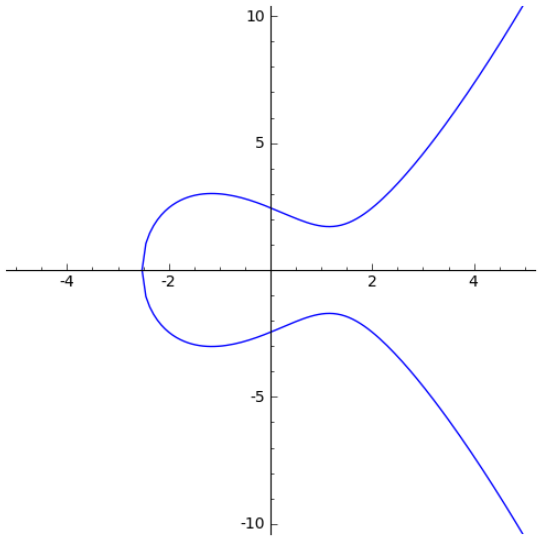
This equation defines an **elliptic curve**.

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

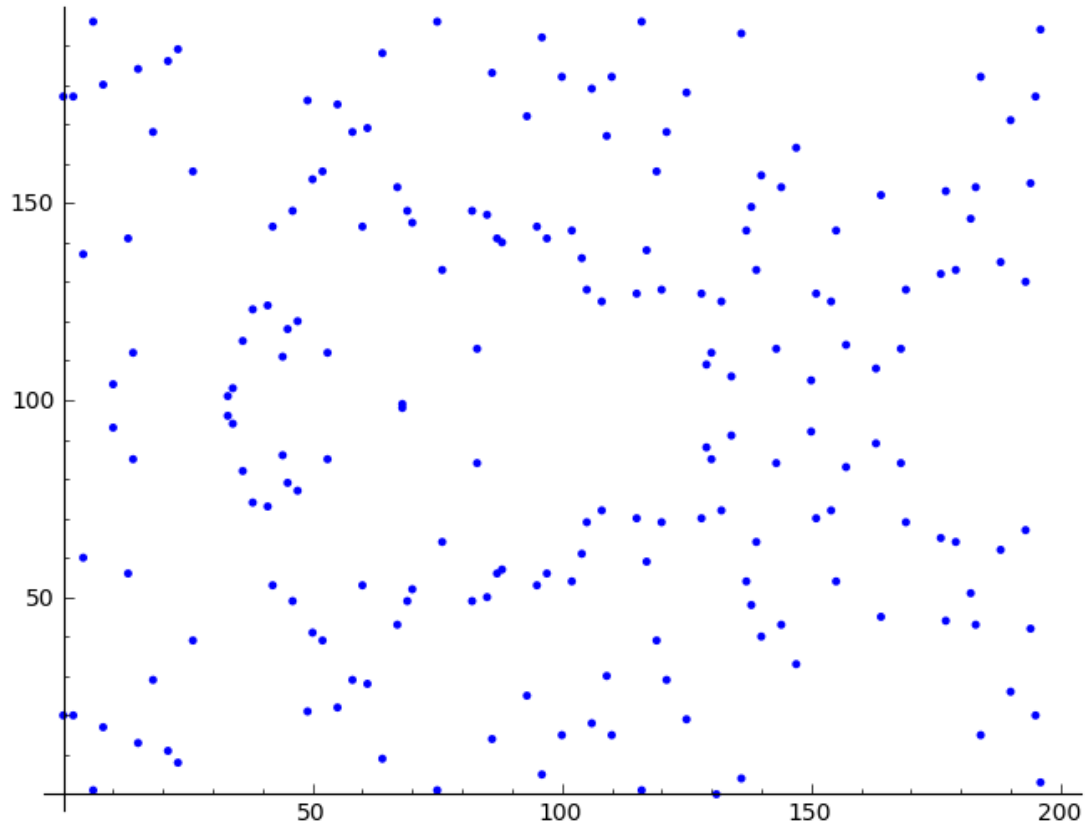
$$y^2 = x^3 + Ax + B,$$

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



$y^2 = x^3 - 4x + 6$
over $\mathbb{R}$

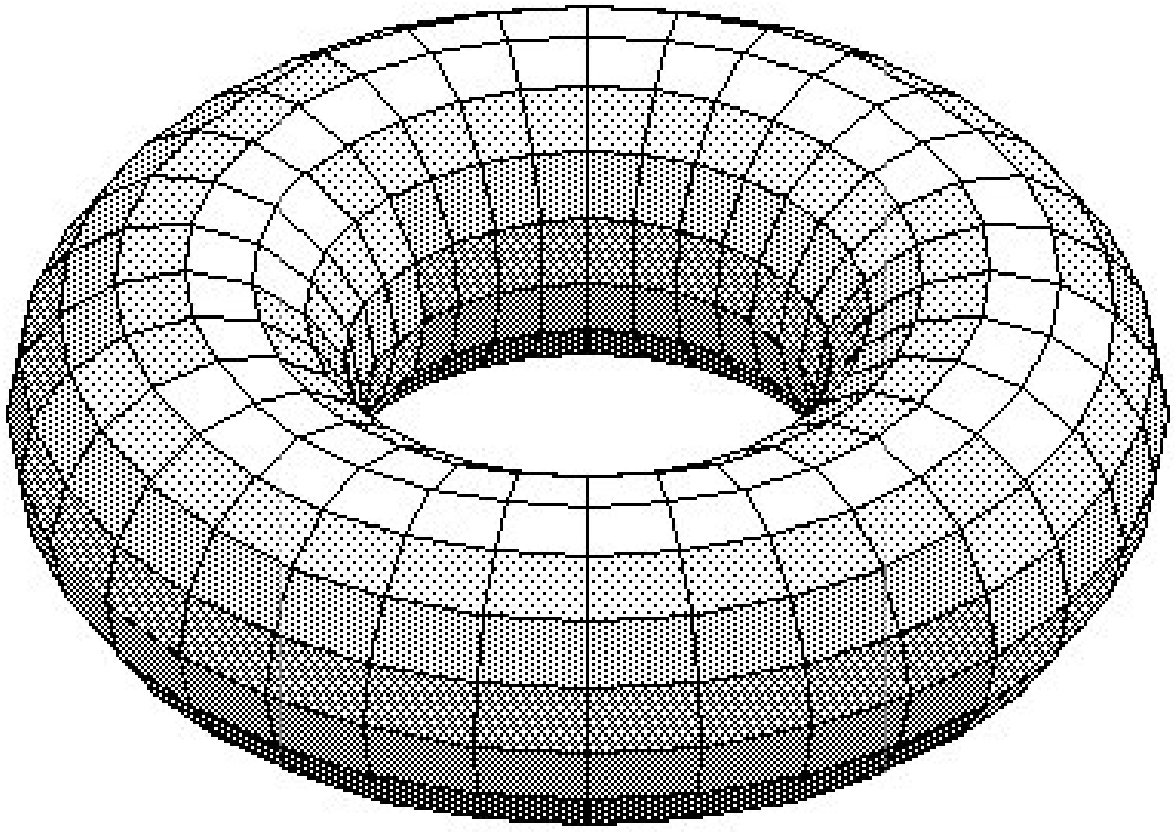
An elliptic curve over a finite field



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

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

An elliptic curve over the complex numbers



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

Definitions

Definition

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

Definitions

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 $y^2 = -x^4 - 1$ over $\mathbb{Q}$ is a smooth projective curve of genus 1 with no rational points.

The projective plane

Definition

The **projective plane** is the set $\mathbb{P}^2(k)$ of all nonzero triples (x, y, z) in k^3 modulo the equivalence relation $(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$.

The **projective point** $(x : y : z)$ is the equivalence class of (x, y, z).

Points of the form $(x : y : 1)$ are called **affine points**.
They form an affine (Euclidean) plane $\mathbb{A}^2(k)$ embedded in $\mathbb{P}^2(k)$.

Points of the form $(x : y : 0)$ are called **points at infinity**.
These consist of the points $(x : 1 : 0)$ and the point $(1 : 0 : 0)$, which form the **line at infinity**: this is a copy of $\mathbb{P}^1(k)$ embedded in $\mathbb{P}^2(k)$.

This is just a convention, we could have chosen $(1 : y : z)$ to be our affine plane and called $(0 : y : z)$ the line at infinity.

Plane projective curves

Definition

A **plane projective curve** C_f/k is a homogeneous polynomial $f(x, y, z)$ with coefficients in k.[1] The **degree** of C_f is the degree of $f(x, y, z)$.

For any field K containing k, the K-**rational points** of C_f form the set

$$C_f(K) = \{(x : y : z) \in \mathbb{P}^2(K) \mid f(x, y, z) = 0\}.$$

A point $P \in C_f(K)$ is **singular** if $\frac{\partial f}{\partial x}$, $\frac{\partial f}{\partial y}$, $\frac{\partial f}{\partial z}$ all vanish at P.
C_f is **smooth** (or **nonsingular**) if there are no singular points in $C_f(\bar{k})$.

Every polynomial equation $g(x, y) = h(x, y)$ of total degree d determines a projective curve C_f of degree d with $f(x, y, 1) = g(x, y) - h(x, y)$.

We often specify projective curves with affine equations,
but we always mean to define a **projective curve**.

[1] Fine print: up to scalar equivalence and with no repeated factors in $\bar{k}[x, y, z]$.

Examples of plane projective curves over $\mathbb{Q}$

affine equation	$f(x,y,z)$	points at ∞
$y = mx + b$	$y - mx - bz$	$(1 : m : 0)$
$x^2 + y^2 = 1$	$x^2 + y^2 - z^2$	none
$x^2 - y^2 = 1$	$x^2 - y^2 - z^2$	$(1 : 1 : 0)$, $(1, -1, 0)$
$y^2 = x^3 + Ax + B$	$y^2z - x^3 - Axz^2 - Bz^3$	$(0 : 1 : 0)$
$x^2 + y^2 = 1 - x^2y^2$	$x^2z^2 + y^2z^2 - z^4 + x^2y^2$	$(1 : 0 : 0), (0 : 1 : 0)$

The first four curves are smooth (provided that $4A^3 + 27B^2 \neq 0$).
The last curve is singular (both points at infinity are singular).

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.

genus 0 genus 1 genus 2 genus 3

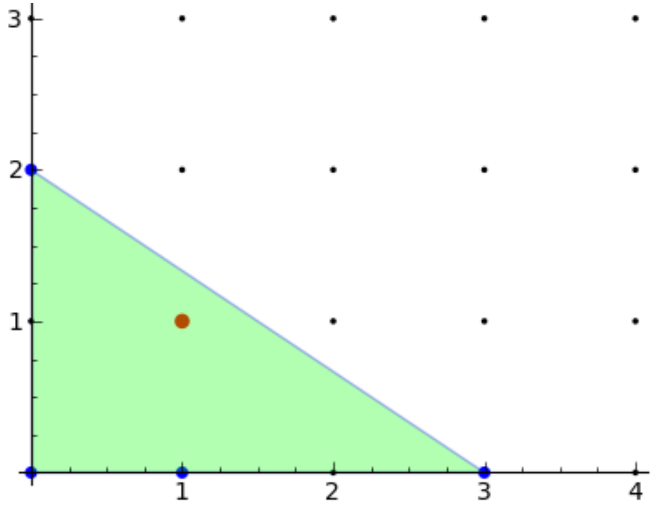
In fact, the genus can be defined algebraically over any field, not just $\mathbb{C}$.

Newton polytopes

Definition

The **Newton polytope** of a polynomial $f(x,y) = \sum a_{ij}x^i y^j$ is the convex hull of the set $\{(i,j) : a_{ij} \neq 0\}$ in $\mathbb{R}^2$.

An easy way to compute the genus of a (sufficiently general) irreducible curve defined by an affine equation $f(x,y) = 0$ is to count the integer lattice points in the interior of its Newton polytope:



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

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.

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

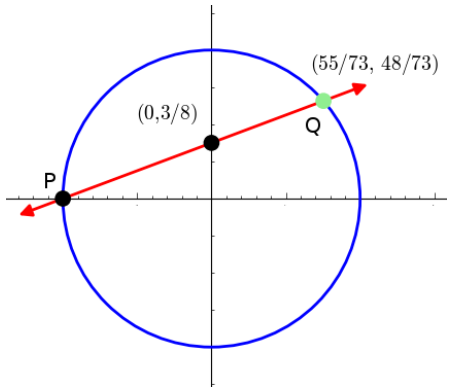
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

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

Rational points in genus 0

Let C be a smooth projective curve over $\mathbb{Q}$ of genus 0 with a rational point P, for example, consider the unit circle with $P = (-1 : 0 : 1)$.

Any line ℓ with rational slope t that passes through P intersects C in exactly one "other" point $Q \in C(\mathbb{Q})$ (when ℓ is a tangent, $Q = P$). Conversely, for $Q \in C(\mathbb{Q})$ the line $\overline{PQ}$ is vertical or has rational slope t.



Treating the vertical line as the point at infinity on the projective line $\mathbb{P}^1(\mathbb{Q})$, there is a rational map from $C(\mathbb{Q})$ and $\mathbb{P}^1(\mathbb{Q})$, and vice versa.

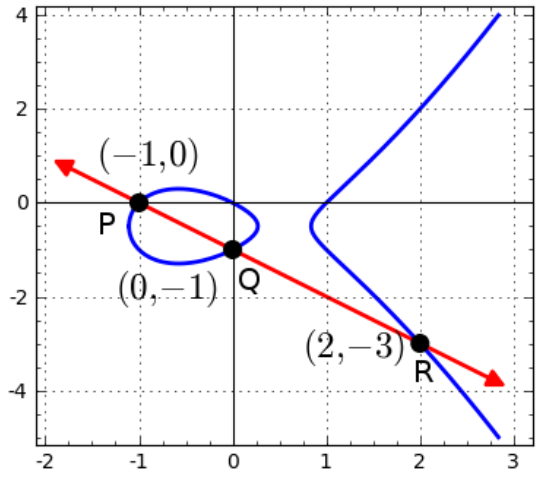
This applies to any conic, and in fact every genus 0 curve with a rational point is isomorphic to $\mathbb{P}^1(\mathbb{Q})$, in other words, they are all the same curve!

Rational points in genus 1

Now let E be an elliptic curve over $\mathbb{Q}$ defined by a Weierstrass equation.

If P is a rational point and ℓ is a line through P with rational slope, it is not necessarily true that ℓ intersects E in another rational point.

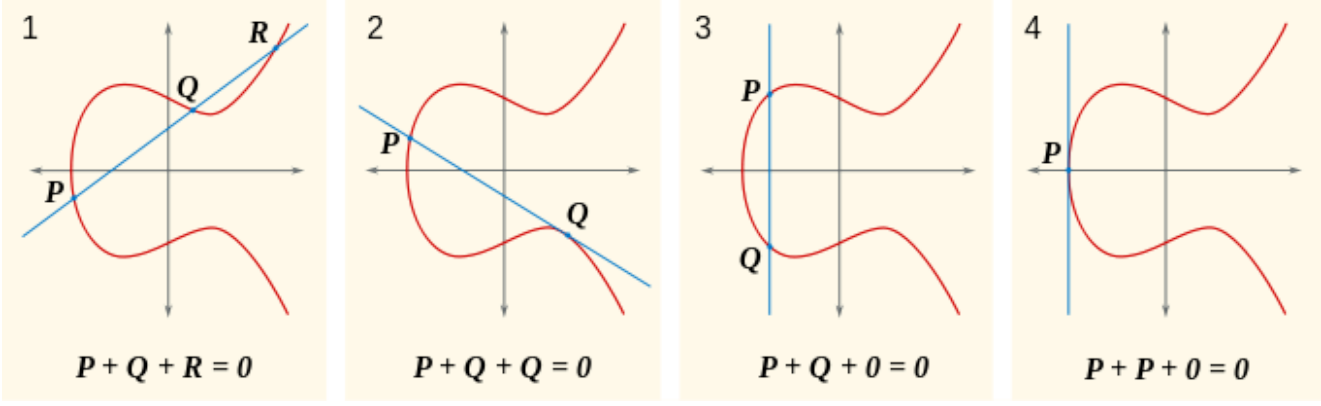
However, if P and Q are two rational points on E, then the line $\overline{PQ}$ intersects E in a third rational point R (by Bezout's theorem).

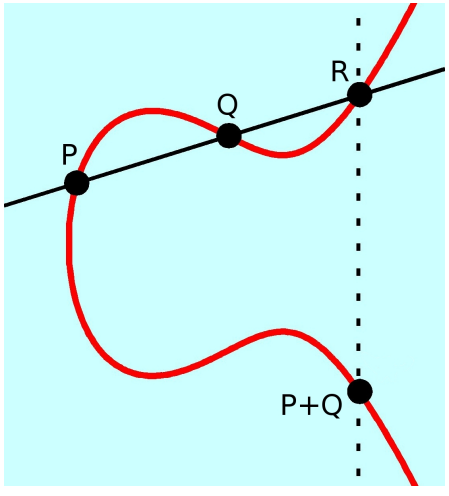


Even better, it allows us to define a group operation on $E(\mathbb{Q})$, or on $E(k)$, for any elliptic curve E defined over a field k.

The elliptic curve group law

Three points on a line sum to zero.





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 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 $(-n)P = -nP$.

We can thus perform **scalar multiplication** by any integer n.
In other words, $E(k)$ is a $\mathbb{Z}$-module (just like any abelian group).

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 (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.

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

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

Theorem (Mazur 1977)

The torsion subgroup of $E(\mathbb{Q})$ is isomorphic to one of the following:

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

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

Barry Mazur receiving the National Medal of Science

Ranks of elliptic curves over $\mathbb{Q}$

The rank r of $E(\mathbb{Q})$ is **not** well understood. Things we do not know:

1. Is there an effective algorithm 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 know a few things, and we can usually compute r when it is small.
When r is large often the best we can do is a lower bound.
The largest r known occurs for a curve with $r \geq 28$ due to Elkies (2006).

Noam Elkies

Ranks of elliptic curves over $\mathbb{Q}$

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

Theorem (Bhargava, Shankar 2010-2012)

The average rank of all elliptic curves over $\mathbb{Q}$ is less than 1.

In fact, we 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).

Manjul Bhargava

Arul Shankar

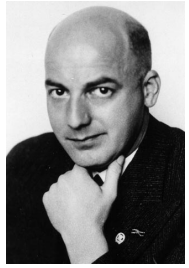
The group $E(\mathbb{F}_p)$

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 (Hasse 1933)

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

Emil Artin



Helmut Hasse

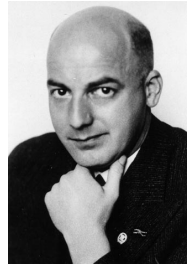
The group $E(\mathbb{F}_p)$

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 (Hasse 1933)

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

Emil Artin



Helmut Hasse

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.

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.

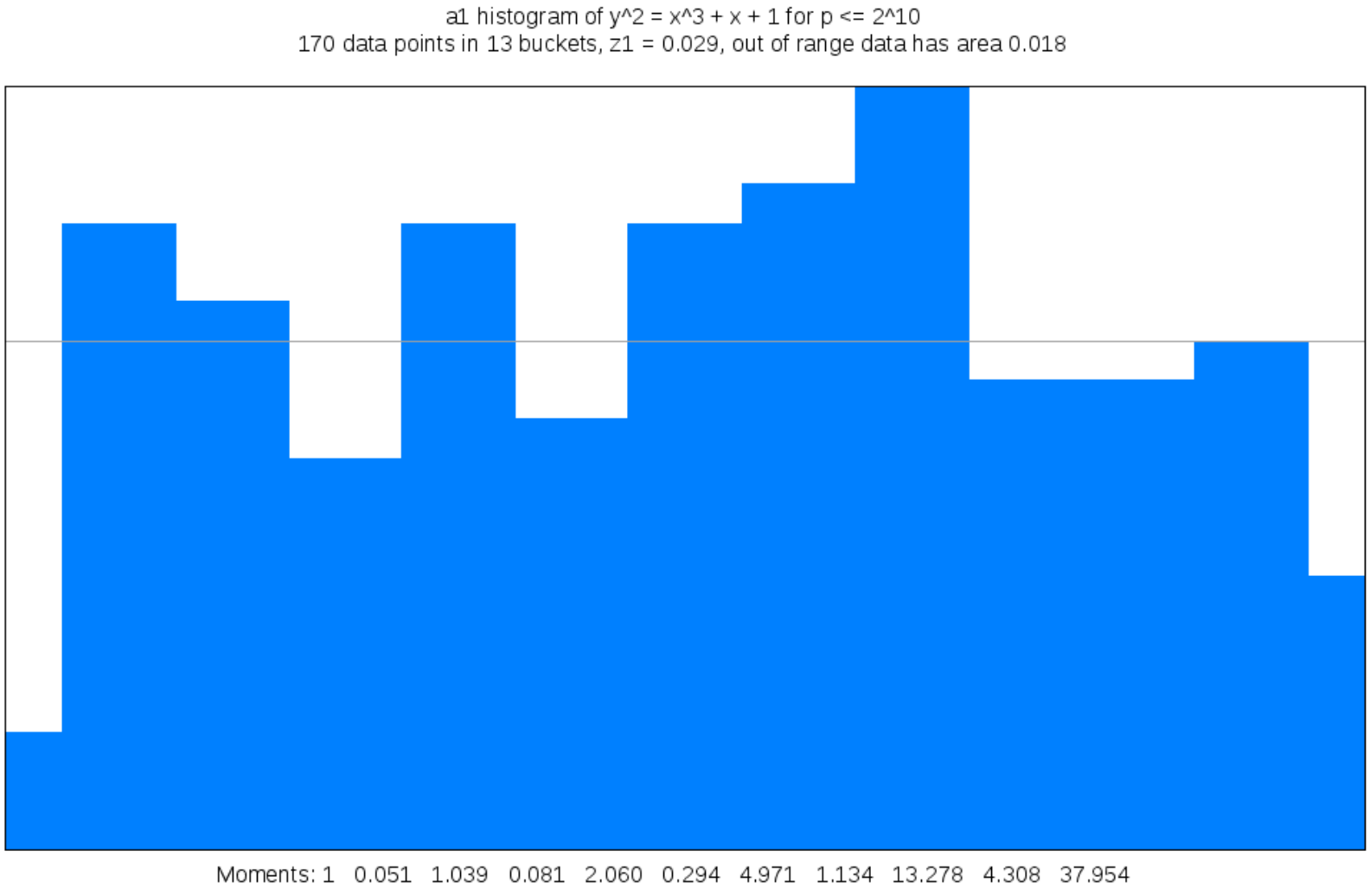
If we reduce A and B modulo p, we obtain an elliptic curve $E_p := E \bmod p$ defined over the finite field $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$.

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?



(click to animate – requires Adobe reader)

The Sato-Tate conjecture

The Sato-Tate conjecture, open for nearly 50 years, was recently proved.

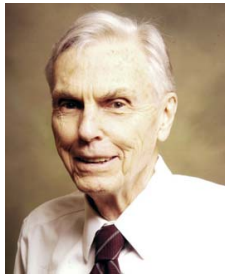
Richard Taylor received the 2014 Breakthrough Prize in Mathematics for work that led to this the proof (and other results).

Theorem (Taylor et al., 2006 and 2008)

Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Then the x_p have a semi-circular distribution.

Mikio Sato

Richard Taylor



John Tate

The Birch and Swinnerton-Dyer conjecture

There is believed to be a relationship between the infinite sequence of integers a_p associated to an elliptic curve $E/\mathbb{Q}$ and the rank r.

The L-**function** $L(E,s)$ of an elliptic curve $E/\mathbb{Q}$ is a function of a complex variable s that "encodes" the infinite sequence of integers a_p.

For the "bad" primes that divide $\Delta(E)$, one defines a_p to be $0, 1$, or -1, depending on the type of singularity E has when reduced mod p.

$$L(E,s) = \prod_{\text{bad } p} (1 - a_p p^{-s})^{-1} \prod_{\text{good } p} (1 - a_p p^{-s} + p^{1-2s})^{-1} = \sum_{n=0}^{\infty} a_n n^{-s}$$

The Birch and Swinnerton-Dyer conjecture

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

Conjecture (Birch and Swinnerton-Dyer)

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.*

Byran Birch

EDSAC-2

Sir Peter Swinnerton-Dyer

They later made a more precise conjecture that also specifies the constant coefficient a_0 of $g(s) = \sum_{n \geq 0} a_n (s-1)^n$.

Fermat's Last Theorem

Theorem (Wiles et al. 1995)

$x^n + y^n = z^n$ has no positive integer solutions for $n > 2$.

It suffices to consider n prime.

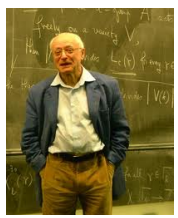
Suppose $a^n + b^n = c^n$ with $a, b, c > 0$ and $n > 3$ (the case $n = 3$ was proved by Euler). Consider the elliptic curve $E_{a,b,c}/\mathbb{Q}$ defined by

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

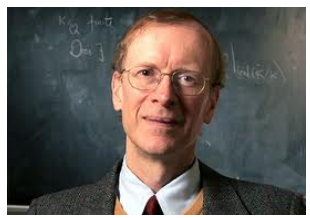
Serre and Ribet proved that $E_{a,b,c}$ **is not modular**.

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.


J.-P. Serre


Ken Ribet


Sir Andrew Wiles


Richard Taylor

Instant poll

Which of the following statements do you think is most likely to be true?

A. Ranks of elliptic curves over $\mathbb{Q}$ are bounded.

B. Ranks of elliptic curves over $\mathbb{Q}$ are unbounded.

C. BSD is true.

D. BSD is false.

E. Fermat had a proof of his last theorem.

Applications of elliptic curves over finite fields

There are several features that make elliptic curves over finite fields particularly well suited to practical applications:

- There are many groups available, even when the finite field is fixed.
- The underlying group operation can be made very efficient.
- There are techniques to construct a group of any desired size.
- The representation of group elements appears to be opaque, making $E(\mathbb{F}_q)$ a good candidate for a "black box group", one to which only **generic group algorithms** apply.

There are three particular applications that we will explore in some detail:

1. factoring integers
2. primality proving
3. cryptography

The discrete log problem

Problem: Given a point $P \in E(\mathbb{F}_q)$ and $Q = nP$, determine n.

This is known as the **discrete log problem**, a term that originates from the analogous problem in the multiplicative group $\mathbb{F}_q^\times$: given $a \in \mathbb{F}_q^\times$ and $b = a^n$, determine $n = \log_a b$.

In the group $\mathbb{F}_q^\times$, this problem can be solved in subexponential time, but no comparable result is known for the group $E(\mathbb{F}_q)$.

In fact, the best known algorithm for solving the discrete log problem in $E(\mathbb{F}_q)$ takes time $\Omega(\sqrt{q})$, which is fully exponential in $\log q$.

This allows cryptographic systems based on the elliptic curve discrete log problem (DLP) to use smaller key sizes than other systems.

Of course we do not have any proof that the elliptic curve discrete log problem is hard, just as we have no proof that factoring integers is hard, (and we know that for quantum computers, both problems are easy).

Diffie-Hellman key exchange

Diffie and Hellman proposed a method for two parties to establish a secret key over a public network, based on the discrete log problem. Their method is generic, it works in a cyclic subgroup of any given group.

Let $E/\mathbb{F}_p$ be an elliptic curve with a point $P \in E(\mathbb{F}_p)$.

Alice and Bob, who both know E and P, establish a secret S as follows:

1. Alice chooses a random integer a and sends aP to Bob.
2. Bob choses a random integer b and sends bP to Alice.
3. Alice computes $abP = S$ and Bob computes $baP = S$.

[2] As written, this protocol is vulnerable to a man-in-the-middle attack.

Diffie-Hellman key exchange

Diffie and Hellman proposed a method for two parties to establish a secret key over a public network, based on the discrete log problem. Their method is generic, it works in a cyclic subgroup of any given group.

Let $E/\mathbb{F}_p$ be an elliptic curve with a point $P \in E(\mathbb{F}_p)$.

Alice and Bob, who both know E and P, establish a secret S as follows:

1. Alice chooses a random integer a and sends aP to Bob.
2. Bob choses a random integer b and sends bP to Alice.
3. Alice computes $abP = S$ and Bob computes $baP = S$.

The coordinates of S depend on the random integer ab and can be hashed to yield a shared secret consisting of $\log_2 ab$ random bits.[2]

An eavesdropper may know E, P, aP and bP, but not a, b, or S.
It is believed that computing S from these values is as hard as computing discrete logarithms in $E(\mathbb{F}_p)$ (but this is not proven).

[2] As written, this protocol is vulnerable to a man-in-the-middle attack.

Ephemeral Diffie-Hellman (ECDHE) and ECDSA

With **ephemeral** Diffie-Hellman (**ECDHE**) the elliptic curve E is fixed, but a new base point P is chosen for each key exchange.

This provides what is known as **perfect forward secrecy**, which compartmentalizes the security of each communication session (breaking one session should not make it easier to break others).

ECDHE was adopted by Google in late 2011 and has become the most widely used key exchange protocol. It is the default protocol in TLS 1.2 and later, which is now used to secure the majority of all internet traffic.

If you look at the security details of your web browsers connection to your favorite internet site, you are very likely to find ECDHE listed as the key exchange protocol, with either RSA, DSA, or ECDSA used for authentication (this protects against man-in-the-middle attacks).

ECDSA is a digital signature scheme based on the elliptic curve discrete logarithm problem; it is used by Bitcoin and many other cryptocurrencies.

Pairing-based cryptography

Elliptic curves also support bilinear **pairings** $\varepsilon\colon E(\overline{\mathbb{F}}_p) \times E(\overline{\mathbb{F}}_p) \to \overline{\mathbb{F}}_p^\times$, which satisfy $\varepsilon(aP, bQ) = \varepsilon(P, Q)^{ab}$. Pairings facilitate some more sophisticated cryptographic protocols.

For **pairing friendly** elliptic curves $E/\mathbb{F}_p$, one can define a pairing $\varepsilon\colon E(\mathbb{F}_p) \times E(\mathbb{F}_p) \to \mathbb{F}_{p^k}$, where $\#E(\mathbb{F}_p)$ divides $p^k - 1$ with k small.

As an example, here is how Alice, Bob, and Carol can establish a shared secret using a single round of communication (as proposed by Joux).

1. Alice chooses a random a and sends aP to Bob and Carol,
   Bob chooses a random b and sends bP to Alice and Carol,
   Carol chooses a random c and sends cP to Alice and Bob.
2. Alice computes $\varepsilon(bP, cP)^a = \varepsilon(P, P)^{bca} = S$,
   Bob computes $\varepsilon(aP, cP)^b = \varepsilon(P, P)^{acb} = S$,
   Carol computes $\varepsilon(aP, bP)^c = \varepsilon(P, P)^{abc} = S$.

An eavesdropper may know E, P, aP, bP, cP, but not a, b, c or S.

Pairing-based cryptography

Now the security of the system depends **both** on the difficulty of the discrete log problem in $E(\mathbb{F}_p)$, and the discrete log problem in $\mathbb{F}_{p^k}$.

The complexity of the discrete log problem in $E(\mathbb{F}_p)$ is believed to be $\Omega(\sqrt{p})$, whereas the fastest known algorithm for computing discrete logarithms in $\mathbb{F}_{p^k}$ has complexity

$$L[1/3, c] = \exp\big((c + o(1))(\log n)^{1/3}(\log\log n)^{2/3}\big),$$

where $n = p^k$ and c is a constant that may be as small as about 1.4 (for binary fields).

If $p \approx 2^{256}$ and $k = 12$, then $p^k \approx 2^{3072}$ and the two complexities are roughly comparable.

Pairings make it possible to implement more sophisticated cryptographic protocols that go far beyond Diffie-Hellman key exchange. In addition to multiparty key exchange, this includes identity based cryptography and zero knowledge proofs (both are relevant to cryptocurrency applications).

Isogeny-based cryptography

Both factoring and the discrete logarithm problem can be solved in polynomial-time on a quantum computer.

SIDH is a variant of the Diffie Hellman protocol that replaces scalar multiplication with a walk on a **supersingular isogeny graph**:

Alice and Bob, who both know a public **supersingular** elliptic curve $E/\mathbb{F}_{p^2}$, establish a secret S as follows:

1. Alice chooses a random a encoded in base-2 and computes E_a by taking an a-walk in the 2-isogeny graph; she sends E_a to Bob.[3]
2. Bob choses a random b encoded in base-3 and computes E_b by taking a b-walk in the 3-isogeny graph; he sends E_b to Alice.[4]
3. Alice computes $(E_b)_a$ and Bob computes $(E_a)_b$.
   The j-**invariant** $j((E_b)_a) = j((E_a)_b) \in \mathbb{F}_{p^2}$ is their shared secret S.

No efficient algorithm is known for computing $j((E_b)_a) = j((E_a)_b)$ given E, E_a, E_b, not even on an quantum computer.

---

[3] Alice/Bob also sends the images of two points on E under the isogeny.

Instant poll

Which of the following statements do you think is most likely to be true?

A. DLP can be solved classically in sub-exponential time.

B. Quantum computers will break 256-bit DLP within 20 years.

C. Someone will access Satoshi's bitcoin in the next 20 years.

D. Lattice-based crypto is not quantum-secure.

E. Isogeny-based crypto is not quantum-secure.