IAS/Park City Mathematics Series
Volume XX, XXXX

Introduction to Elliptic Curves

Alice Silverberg

Introduction

Why study elliptic curves?

Solving equations is a classical problem with a long history. Starting with the simplest equations, we know that linear and quadratic equations are easy to solve. However, there are still have many interesting unanswered questions about cubic equations.

In addition, there are important applications of elliptic curves to cryptography. There are also important applications of elliptic curves within mathematics, most notably to the proof of Fermat's Last Theorem. By studying about elliptic curves, one learns about deep connections among arithmetic, algebra, geometry, and complex analysis.

Some suggested reading is [**4, 5, 1, 3**].

1. Definitions

Definition 1.1. An *elliptic curve* E over a field F is a smooth projective curve with an affine equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

where the a_i's are in F.

An equation of the above form (1) is called a *generalized Weierstrass equation*.

Recall that the points in projective space $\mathbb{P}^n(F)$ correspond to the equivalence classes in $F^{n+1} - \{(0, \ldots, 0)\}$ under the equivalence relation $(x_0, \ldots, x_n) \approx (\lambda x_0, \ldots, \lambda x_n)$ with $\lambda \in F^\times$.

The projective equation corresponding to the affine equation (1) is the homogeneous equation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Smooth means that there is no point on the curve at which all partial derivatives vanish.

If $\mathrm{char}(F) \neq 2$ or 3, then a change of variables puts E in the form

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

with $a, b \in F$. Such an equation is called a *Weierstrass equation*.

A projective curve $y^2z = x^3 + axz^2 + bz^3$ is smooth if and only if $2(4a^3 + 27b^2) \neq 0$.

Department of Mathematics, University of California, Irvine, CA 92697-3875
E-mail address: asilverb@math.uci.edu

The points (x, y, z) on the projective curve

$$y^2z = x^3 + axz^2 + bz^3$$

are the points $(x, y, 1)$ where (x, y) in a solution to $y^2 = x^3 + ax + b$ along with the point $(0, 1, 0)$.

The point $(0, 1, 0)$ is called the *point at infinity*. It can be viewed as the point where all vertical lines meet. Denote it by O_E or O.

Exercise 1.2. Over which fields F is $y^2 = x^3 - x$ an elliptic curve?

Next we give some equivalent definitions.

Definition 1.3. An *elliptic curve* E over a field F is a smooth projective plane cubic over F with a point whose coordinates are in F.

Definition 1.4. An *elliptic curve* E over a field F is a smooth projective curve of genus one with a point whose coordinates are in F.

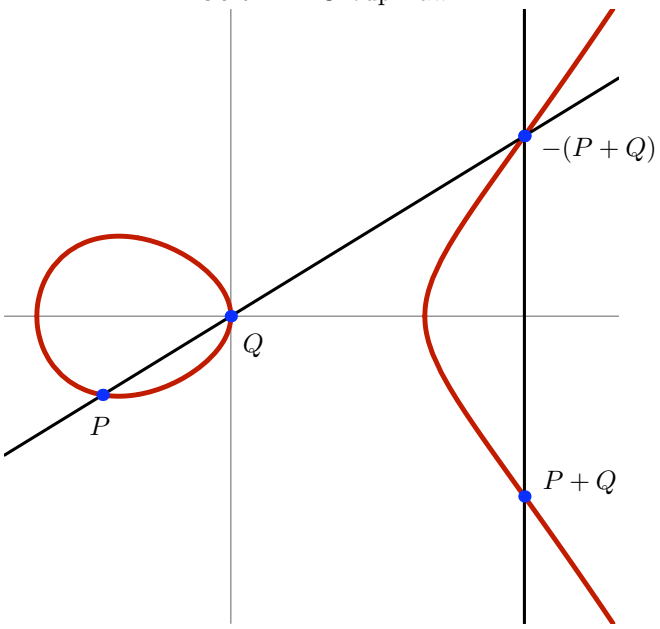
Definition 1.5. If E is $y^2 = x^3+ax+b$, then the discriminant $\Delta(E)$ and j-invariant $j(E)$ are defined as follows:

$$\Delta(E) = -16(4a^3 + 27b^2), \qquad j(E) = \frac{(-48a)^3}{\Delta}.$$

2. Group Law

Figure 2 illustrates the group law on an elliptic curve.

FIGURE 1. Group Law



This can be expressed algebraically, as follows.

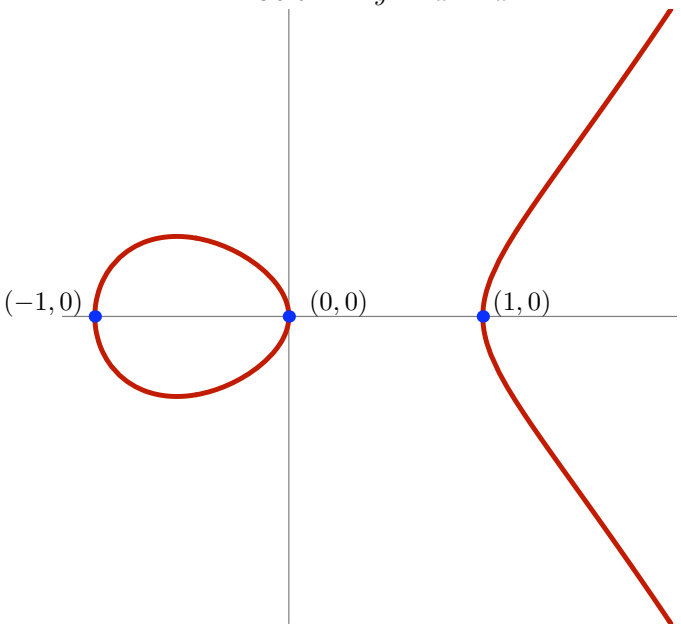
If E is $y^2 = x^3+ax+b$, and $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, then $P+Q = (x_3, y_3)$ where

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$
$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } P \neq Q, \\ (3x_1^2 + a)/2y_1 & \text{if } P = Q. \end{cases}$$

The point $O_E = (0, 1, 0)$ is the identity element for the group law.

With this group law, the points on E with coordinates in F, along with the point at ∞, form an abelian group. This group is denoted $E(F)$. When F is a number field, $E(F)$ is called the *Mordell-Weil group* of E over F.

FIGURE 2. $y^2 = x^3 - x$



$$E(\mathbb{Q}) = \{(0,0), (1,0), (-1,0), O\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

3. N-torsion

Let ($\overline{F}$ denote an algebraic closure of the field F.

Definition 3.1. If E is an elliptic curve over F, then

$$E[N] := \{P \in E(\overline{F}) : NP = O_E\}.$$

Fact 3.2. $E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ if $\mathrm{char}(F) \nmid N$.

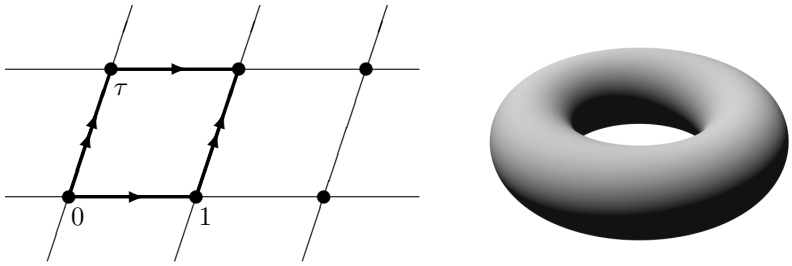
Example 3.3. If E is the elliptic curve $y^2 = x^3 - x$ over $\mathbb{Q}$, then

$$E[2] = \{(0,0), (1,0), (-1,0), O\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$
$$E[4] = \langle (i, i-1), (1-\sqrt{2}, 2-\sqrt{2}) \rangle \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

4. Elliptic Curves over $\mathbb{C}$

If E is an elliptic curve over $\mathbb{C}$, then $E(\mathbb{C})$ is isomorphic to $\mathbb{C}/L$ for a lattice $L = \mathbb{Z}\tau + \mathbb{Z}$ for some τ in the complex upper half plane.

FIGURE 3. Elliptic curves over $\mathbb{C}$



It easily follows that

$$E[N] \cong \tfrac{1}{N}L/L \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z},$$

which agrees with Fact 3.2.

5. Elliptic Curves over Number Fields

Mordell-Weil Theorem. *If E is an elliptic curve over a number field F, then the abelian group $E(F)$ is finitely generated.*

Therefore:

$$E(F) \cong \mathbb{Z}^r \times \text{ finite group.}$$

The finite group is called the *torsion subgroup* of $E(F)$ and is denoted $E(F)_{\text{tors}}$. The non-negative integer r is called the *rank* of $E(F)$.

5.1. The Torsion Subgroup

Nagell-Lutz Theorem (1930's)**.** *If $E : y^2 = x^3 + ax + b$ is an elliptic curve with $a, b \in \mathbb{Z}$, and $O_E \neq (x, y) \in E(\mathbb{Q})_{\text{tors}}$, then x and y are integers, and either $y = 0$ or y^2 is a divisor of $4a^3 + 27b^2$.*

Exercise 5.1. Show that for $E : y^2 = x^3 + 4x$,

$$E(\mathbb{Q})_{\text{tors}} = \{O, (0,0), (2,4), (2,-4)\} \cong \mathbb{Z}/4\mathbb{Z}.$$

Exercise 5.2. Show that for $E : y^2 = x^3 + 1$,

$$E(\mathbb{Q})_{\text{tors}} = \{O, (-1,0), (0,1), (0,-1), (2,3), (2,-3)\} \cong \mathbb{Z}/6\mathbb{Z}.$$

Mazur Theorem (1977)**.** *If E is an elliptic curve over $\mathbb{Q}$, then $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following 15 groups:*

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z} & \text{for} \quad N = 1, \ldots, 10 \text{ or } 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} & \text{for} \quad N = 1, 2, 3, \text{ or } 4. \end{array}$$

Each of these groups occurs infinitely often.

Theorem 5.3 (Merel-Oesterlé-Parent, 1990's)**.** *Suppose E is an elliptic curve defined over a number field F, and $m = [F : \mathbb{Q}]$. Then $\#E(F)_{\text{tors}}$ is bounded above by a constant depending only on m. More precisely, if $E(F)$ has a point of order p^n where p is a prime number, then*

$$p^n \leq 129(5^m - 1)(3m)^6.$$

5.2. Ranks

In 1901, Henri Poincaré stated that the rank is obviously very important in the classification of rational cubics. In 1922, Mordell stated, "Mathematicians have been familiar with very few questions for so long a period with so little accomplished in the way of general results, as that of finding the rational [points on elliptic curves]."

Most major open questions about elliptic curves today have something to do with the rank.

Example 5.4. If E is the elliptic curve $y^2 = x^3 - x$ over $\mathbb{Q}$, then

$$E(\mathbb{Q}) = \langle (1,0), (0,0) \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

so the rank is 0.

Example 5.5. If E is the elliptic curve $y^2 = x^3 - 2x$ over $\mathbb{Q}$, then

$$E(\mathbb{Q}) = \langle (-1,1), (0,0) \rangle \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

so the rank is 1.

Example 5.6. If E is the elliptic curve $y^2 = x^3 - 17x$ over $\mathbb{Q}$, then

$$E(\mathbb{Q}) = \langle (-1,4), (9,24), (0,0) \rangle \cong \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

so the rank is 2.

Some open questions about ranks are:

- We still do not know an algorithm that is guaranteed to find the rational points on elliptic curves over $\mathbb{Q}$.
- In particular, there is no known algorithm guaranteed to determine the rank.
- It is not known which integers can occur as ranks.
- It is not known if ranks are unbounded.

Figure 5.2 gives the year that an elliptic curve was first written down with rank $\geq n$ for various values of n up to 28.

The Parity Conjecture, which is a consequence of the Conjecture of Birch and Swinnerton-Dyer, says that half of the elliptic curves over $\mathbb{Q}$ have even rank and half have odd rank.

Some people believe the stronger statement that density $\frac{1}{2}$ (in a suitable sense) of the elliptic curves over $\mathbb{Q}$ have rank 0, density $\frac{1}{2}$ have rank 1, and the density of elliptic curves over $\mathbb{Q}$ with rank ≥ 2 is zero.

Many people believe that ranks of elliptic curves over $\mathbb{Q}$ are unbounded.

There are similar questions about elliptic curves over other number fields.

6. Elliptic Curves over Finite Fields

Fact 6.1. If E is an elliptic curve over a finite field $\mathbb{F}_q$, then

$$E(\mathbb{F}_q) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

where m is a divisor of n.

Hasse Bound. *If E is an elliptic curve over $\mathbb{F}_q$, then*

$$(\sqrt{q} - 1)^2 \leq \#E(\mathbb{F}_q) \leq (\sqrt{q} + 1)^2.$$

FIGURE 4. Rank Records

Rank $\geq$	**Year**	**Discoverers**
3	1945	Billing
4	1945	Wiman
6	1974	Penney & Pomerance
7	1975	Penney & Pomerance
8	1977	Grunewald & Zimmert
9	1977	Brumer & Kramer
12	1982	Mestre
14	1986	Mestre
15	1992	Mestre
17	1992	Nagao
19	1992	Fermigier
20	1993	Nagao
21	1994	Nagao-Kouya
22	1997	Fermigier
23	1998	Martin-McMillen
24	2000	Martin-McMillen
28	2006	Elkies

Elliptic Curves over finite fields are used in elliptic curve cryptography and pairing-based cryptography. The security of elliptic curve and pairing-based cryptosystems depends on the difficulty of certain problems about elliptic curves and their Weil and Tate pairings. An important open problem in cryptography is to understand how difficult these "hard problems" are.

7. Homomorphisms

Definition 7.1. A *homomorphism* $f : E_1 \to E_2$ of elliptic curves over the same field F is a morphism that takes O_{E_1} to O_{E_2}.

It follows that the induced map $f : E_1(F) \to E_2(F)$ is a group homomorphism.

Write $\mathrm{Hom}_F(E_1, E_2)$ for the homomorphisms defined over F and $\mathrm{Hom}(E_1, E_2)$ for the homomorphisms defined over $\overline{F}$.

Definition 7.2. An *endomorphism* is a homomorphism from E to itself.

$$\mathrm{End}(E) := \mathrm{Hom}(E, E)$$

Fact 7.3. $\mathrm{End}(E)$ is either:

(i) $\mathbb{Z}$,
(ii) an order in an imaginary quadratic field, or
(iii) a maximal order in a definite quaternion algebra over $\mathbb{Q}$.

The third doesn't happen in characteristic 0. The first doesn't happen over finite fields.

Example 7.4. The map $P \mapsto NP$ is always an endomorphism, and this gives an injection

$$\mathbb{Z} \hookrightarrow \mathrm{End}(E).$$

Example 7.5. If E is an elliptic curve over $\mathbb{F}_q$, then

$$\phi_q : (x, y) \mapsto (x^q, y^q)$$

is an endomorphism, called the *Frobenius endomorphism*.

Example 7.6. Suppose E is $y^2 = x^3 - x$. Then $I : (x, y) \mapsto (-x, \sqrt{-1}y)$ is an automorphism.

Over $\mathbb{Q}$ or $\mathbb{F}_p$ with a prime $p \equiv 1 \pmod 4$:

$$\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}I \cong \mathbb{Z}[i].$$

Over $\mathbb{F}_p$ with a prime $p \equiv 3 \pmod 4$, we have $\phi_p^2 = -p$, $\phi_p \circ I = -I \circ \phi_p$, and

$$\begin{aligned}\mathrm{End}(E) &= \mathbb{Z} + \mathbb{Z}I + \mathbb{Z}(\frac{1+\phi_p}{2}) + \mathbb{Z}(\frac{1+\phi_p}{2}) \circ I \\ &\cong \mathbb{Z}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + \mathbb{Z}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} + \mathbb{Z}\begin{pmatrix}\frac{1+\sqrt{-p}}{2} & 0\\ 0 & \frac{1-\sqrt{-p}}{2}\end{pmatrix} + \mathbb{Z}\begin{pmatrix}0 & \frac{1-\sqrt{-p}}{2}\\ \frac{-1-\sqrt{-p}}{2} & 0\end{pmatrix}.\end{aligned}$$

Definition 7.7. *Isogeny* can be defined using any of the following equivalent definitions:

(i) An *isogeny* of elliptic curves is a non-zero homomorphism.
(ii) An *isogeny* of elliptic curves is a surjective homomorphism.
(iii) An *isogeny* of elliptic curves is a homomorphism with finite kernel.

If there is an isogeny from E_1 to E_2 then there is an isogeny from E_2 to E_1. We say that E_1 and E_2 are *isogenous*. Being isogenous is an equivalence relation.

Two elliptic curves over F are isomorphic over $\overline{F}$ if and only if they have the same j-invariant.

A stronger statement is the following. If E is $y^2 = x^3 + ax + b$ and E' is $y^2 = x^3 + a'x + b'$, then an isomorphism $f : E \to E'$ is of the form

$$f(x, y) = (\lambda^2 x, \lambda^3 y)$$

where $a' = \lambda^4 a$ and $b' = \lambda^6 b$.

8. Supersingular and Ordinary

Definition 8.1. Suppose E is an elliptic curve over $\mathbb{F}_{p^r}$ with p prime. Then E is *supersingular* if and only if any of the following equivalent statements holds:

(i) $\#E(\mathbb{F}_{p^r}) \equiv 1 \pmod p$,
(ii) $E[p] = \{O\}$,
(iii) $\mathrm{End}(E)$ is non-commutative,
(iv) $\mathrm{End}(E)$ is an order in a quaternion algebra over $\mathbb{Q}$.

Otherwise, E is called *ordinary*.

Example 8.2. Suppose $p \equiv 3 \pmod 4$. By Example 7.6, the curve $y^2 = x^3 - x$ is supersingular over $\mathbb{F}_{p^r}$. Further, $\#E(\mathbb{F}_{p^r}) = \begin{cases} p^r + 1 & \text{if } r \text{ is odd} \\ ((-p)^{r/2} - 1)^2 & \text{if } r \text{ is even.}\end{cases}$

If E is an elliptic curve over $\mathbb{F}_{p^r}$ with p prime, then E is ordinary if and only if any of the following equivalent statements holds:

(i) $\#E(\mathbb{F}_{p^r}) \not\equiv 1 \pmod p$,
(ii) $E[p] \cong \mathbb{Z}/p\mathbb{Z}$,

(iii) $\mathrm{End}(E)$ is commutative,
(iv) $\mathrm{End}(E)$ is an order in an imaginary quadratic field.

Example 8.3. By Example 7.6, the curve $y^2 = x^3 - x$ is ordinary over $\mathbb{F}_{p^r}$ if $p \equiv 1 \pmod 4$.

9. Mod N representations

Let F^s be a separable closure of F and let $G_F = \mathrm{Gal}(F^s/F)$. If E is defined over F, then G_F acts on $E[N]$, and this action induces the mod N representation

$$\rho_{E,N} : G_F \to \mathrm{Aut}(E[N]).$$

Note that $\mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ if $\mathrm{char}(F) \nmid N$.

Example 9.1. If E is $y^2 = x^3 - x$ over $\mathbb{Q}$, then

$$\rho_{E,2}(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

for all $\sigma \in G_F$, since $E[2] \subseteq E(\mathbb{Q})$.

Exercise 9.2. Suppose E is $y^2 = x^3 - x$ over $\mathbb{Q}$. Since $E[4] \subset \mathbb{Q}(i, \sqrt{2})$, the mod 4 representation

$$\rho_{E,4} : G_{\mathbb{Q}} \to \mathrm{Aut}(E[4])$$

factors through $\mathrm{Gal}(\mathbb{Q}(i, \sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. This Galois group is generated by σ and τ such that $\sigma(i) = -i$, $\sigma(\sqrt{2}) = \sqrt{2}$, $\tau(i) = i$, and $\tau(\sqrt{2}) = -\sqrt{2}$. Show that:

$$\rho_{E,4}(\sigma) = \begin{pmatrix} -1 & 0 \\ 2 & 1 \end{pmatrix}, \quad \rho_{E,4}(\tau) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$$

with respect to the basis $\{(i, i-1), (1-\sqrt{2}, 2-\sqrt{2})\}$ for $E[4]$.

10. Tate modules

For ℓ prime, with respect to the maps

$$E[\ell^{n+1}] \to E[\ell^n], \quad P \mapsto \ell P$$

define

$$T_\ell(E) := \varprojlim_n E[\ell^n], \qquad V_\ell(E) := T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Then $T_\ell(E)$ is a free $\mathbb{Z}_\ell$-module and $V_\ell(E)$ is a $\mathbb{Q}_\ell$-vector space.

If E is defined over F, then G_F acts on $V_\ell(E)$, and this action induces the ℓ-adic representation:

$$\rho_{E,\ell^\infty} : G_F \to \mathrm{Aut}(V_\ell(E)).$$

Note that if $\mathrm{char}(F) \neq \ell$, then $V_\ell(E) \cong \mathbb{Q}_\ell^2$ (as groups) and $\mathrm{Aut}(V_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Q}_\ell)$.

Isogeny Theorem (Tate, Parshin, Faltings,...). *Suppose F is a finitely generated extension of a number field or of a finite field, and E_1 and E_2 are elliptic curves defined over F. Then the following are equivalent:*

- *E_1 and E_2 are isogenous over F,*
- *ρ_{E_1,ℓ^∞} and ρ_{E_2,ℓ^∞} are isomorphic for every $\ell \neq \mathrm{char}(F)$,*
- *ρ_{E_1,ℓ^∞} and ρ_{E_2,ℓ^∞} are isomorphic for one $\ell \neq \mathrm{char}(F)$.*

In other words, elliptic curves over F are determined (up to isogeny) by their ℓ-adic representations.

11. Reduction of Elliptic Curves

If E is an elliptic curve over a number field F, then E can be reduced modulo a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$, where $\mathcal{O}_F$ is the ring of integers of F. If $\mathfrak{p} \nmid \Delta(E)$, this gives an elliptic curve $\tilde{E}$ over the finite field $\mathcal{O}_F/\mathfrak{p}$.

Exercise 11.1. Take the elliptic curve $y^2 = x^3 - x$ over $\mathbb{Q}$ and reduce the coefficients modulo 7. This gives an elliptic curve $\tilde{E}$ over $\mathbb{F}_7$. Compute $\tilde{E}(\mathbb{F}_7)$.

12. Conjecture of Birch and Swinnerton-Dyer

The Conjecture of Birch and Swinnerton-Dyer tells us that an analytic object, namely the L-function of an elliptic curve over a number field, encodes certain arithmetic information about the Mordell-Weil group.

In particular, the Birch and Swinnerton-Dyer Conjecture relates the size of the Mordell-Weil group of an elliptic curve over a number field with the numbers of points on the reductions of the curve.

See [**2**] for more.

13. Abelian varieties

Abelian varieties are higher-dimensional generalizations of elliptic curves.

Definition 13.1. An *abelian variety* is a connected projective group variety.

Remark 13.2. Note the the definition doesn't say that abelian varieties are *abelian* groups. The fact that abelian varieties are abelian is a theorem.

Examples 13.3.
(i) The one-dimensional abelian varieties are exactly the elliptic curves.
(ii) Products of abelian varieties are abelian varieties.
(iii) Jacobian varieties of curves of genus g are abelian varieties of dimension g.
(iv) For example, if C is a smooth plane curve of degree n, then C has genus $(n-1)(n-2)/2$ and its Jacobian variety has dimension $\frac{(n-1)(n-2)}{2}$.
(v) In particular, the Jacobian variety of $x^n + y^n = z^n$ is an abelian variety of dimension $\frac{(n-1)(n-2)}{2}$.

Mordell-Weil Theorem. *The group of points on an abelian variety over a number field is a finitely generated abelian group.*

Many of the facts we know about elliptic curves are open questions for higher-dimensional abelian varieties. The Torsion Conjecture is one example:

Torsion Conjecture. *If A is an abelian variety of dimension d defined over a number field F, then $\#A(F)_{\text{tors}}$ is bounded above by a constant depending only on d and F.*

For every dimension greater than one, the Torsion Conjecture is open even when $F = \mathbb{Q}$.

Strong Torsion Conjecture. *If A is an abelian variety of dimension d defined over a number field F of degree m, then $\#A(F)_{\text{tors}}$ is bounded above by a constant depending only on d and m.*

The Strong Torsion Conjecture is sometimes called the Uniform Boundedness Conjecture.

Many open questions about elliptic curves make sense and are open (though sometimes different) for abelian varieties.

Open Questions. Here are just a small number of examples of other open questions about abelian varieties:

(i) Distributions of ranks, including boundedness or unboundedness.
(ii) Conjecture of Birch and Swinnerton-Dyer.
(iii) Difficulty of the Discrete Log Problem (cryptography).

Bibliography

[1] J. P. Buhler, *Elliptic curves, modular forms, and applications*, in Arithmetic algebraic geometry (Park City, UT, 1999), 5–81, IAS/Park City Math. Ser. **9**, Amer. Math. Soc., Providence, RI, 2001.
[2] B. Gross, *Introduction to the Birch and Swinnerton-Dyer Conjecture*, Lecture Series in this Summer School.
[3] A. Silverberg, *Open questions in arithmetic algebraic geometry*, in Arithmetic algebraic geometry (Park City, UT, 1999), 83–142, IAS/Park City Math. Ser. **9**, Amer. Math. Soc., Providence, RI, 2001.
[4] J. H. Silverman, The arithmetic of elliptic curves, Corrected reprint of the 1986 original, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1992.
[5] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics **151**, Springer-Verlag, New York, 1994.