Algorithmic Number Theory
MSRI Publications
Volume **44**, 2008

# Elliptic curves

BJORN POONEN

ABSTRACT. This is an introduction to some aspects of the arithmetic of elliptic curves, intended for readers with little or no background in number theory and algebraic geometry. In keeping with the rest of this volume, the presentation has an algorithmic slant. We also touch lightly on curves of higher genus. Readers desiring a more systematic development should consult one of the references for further reading suggested at the end.

CONTENTS



## 1. Plane curves

Let $k$ be a field. For instance, $k$ could be the field $\mathbb{Q}$ of rational numbers, the field $\mathbb{R}$ of real numbers, the field $\mathbb{C}$ of complex numbers, the field $\mathbb{Q}_p$ of $p$-adic numbers (see [Koblitz 1984] for an introduction), or the finite field $\mathbb{F}_q$ of $q$ elements (see Chapter I of [Serre 1973]). Let $\bar{k}$ be an algebraic closure of $k$.

A (geometrically integral, affine) *plane curve* $X$ over $k$ is defined by an equation $f(x, y) = 0$ where $f(x, y) = \sum a_{ij} x^i y^j \in k[x, y]$ is irreducible over $\bar{k}$.

The writing of this article was supported by NSF grant DMS-9801104, and a Packard Fellowship.

One defines the degree of $X$ and of $f$ by

$$\deg X = \deg f = \max\{i + j : a_{ij} \neq 0\}.$$

A *$k$-rational point* (or simply *$k$-point*) on $X$ is a point $(a, b)$ with coordinates in $k$ such that $f(a, b) = 0$. The set of all $k$-rational points on $X$ is denoted $X(k)$.

EXAMPLE. The equation $x^2y - 6y^2 - 11 = 0$ defines a plane curve $X$ over $\mathbb{Q}$ of degree 3, and $(5, 1/2) \in X(\mathbb{Q})$.

Already at this point we can state an open problem, one which over the centuries has served as motivation for the development of a huge amount of mathematics.

QUESTION. Is there an algorithm, that given a plane curve $X$ over $\mathbb{Q}$, determines $X(\mathbb{Q})$, or at least decides whether $X(\mathbb{Q})$ is nonempty?

Although $X(\mathbb{Q})$ need not be finite, we will see later that it always admits a finite description, so this problem of determining $X(\mathbb{Q})$ can be formulated precisely using the notion of *Turing machine*: see [Hopcroft and Ullman 1969] for a definition. For the relationship of this question to Hilbert's Tenth Problem, see the survey [Poonen 2002].

The current status is that there exist computational methods that often answer the question for a particular $X$, although it has never been proved that these methods work in general. Even the following are unknown:

(1) Is there an algorithm that given a degree 4 polynomial $f(x) \in \mathbb{Q}[x]$, determines whether $y^2 = f(x)$ has a rational point?
(2) Is there an algorithm that given a polynomial $f(x, y) \in \mathbb{Q}[x, y]$ of degree 3, determines whether $f(x, y) = 0$ has a rational point?

In fact, problems (1) and (2) are equivalent, although this is by no means obvious! (For the experts: both (1) and (2) are equivalent to

(3) Is there an algorithm to compute the rank of an elliptic curve over $\mathbb{Q}$?

If the answer to (1) is yes, then one can compute the rank of any elliptic curve over $\mathbb{Q}$, by 2-descent. Conversely, if the answer to (3) is yes, the answer to (1) is also yes, since the only difficult case of (1) is when $y^2 = f(x)$ is a locally trivial principal homogeneous space of an elliptic curve $E$ over $\mathbb{Q}$, hence represented by an element of the 2-Selmer group of $E$, and knowledge of the rank of $E(\mathbb{Q})$ lets one decide whether its image in $Ш(E)$ is nontrivial. Similarly (2) and (3) are equivalent, via 3-descent.)

## 2. Projective geometry

**2.1. The projective plane.** The affine plane $\mathbb{A}^2$ is the usual plane, with $\mathbb{A}^2(k) = \{(a, b) : a, b \in k\}$ for any field $k$. One "compactifies" $\mathbb{A}^2$ by adjoining some points "at infinity" to produce the projective plane $\mathbb{P}^2$. One of the main reasons for doing this is to make intersection theory work better: see Bézout's Theorem in Section 2.3.

The set of $k$-points on the projective plane $\mathbb{P}^2$ can be defined directly as $\mathbb{P}^2(k) := (k^3 - 0)/k^*$. In other words, a $k$-rational point on $\mathbb{P}^2$ is an equivalence class of triples $(a, b, c)$ with $a, b, c \in k$ not all zero, under the equivalence relation $\sim$, where $(a, b, c) \sim (\lambda a, \lambda b, \lambda c)$ for any $\lambda \in k^*$. The equivalence class of $(a, b, c)$ is denoted $(a : b : c)$. One can also identify $\mathbb{P}^2(k)$ with the set of lines through 0 in $(x, y, z)$-space.

The injection $\mathbb{A}^2(k) \hookrightarrow \mathbb{P}^2(k)$ mapping $(a, b)$ to $(a : b : 1)$ is almost a bijection: the points of $\mathbb{P}^2(k)$ not in the image, namely those of the form $(a : b : 0)$, form a projective line $\mathbb{P}^1(k)$ of "points at infinity". Viewing $\mathbb{P}^2(k)$ as lines through 0 in $(x, y, z)$-space, $\mathbb{A}^2(k)$ is the set of such lines passing through $(a, b, 1)$ for some $a, b \in k$, and the complement $\mathbb{P}^1(k)$ is the set of (horizontal) lines through 0 in the $(x, y)$-plane.

Also, $\mathbb{P}^2$ can be covered by three copies of $\mathbb{A}^2$, namely $\{(x : y : z) \mid x \neq 0\}$, $\{(x : y : z) \mid y \neq 0\}$, and $\{(x : y : z) \mid z \neq 0\}$.

**2.2. Projective closure of curves.** The *homogenization* of a polynomial $f(x, y)$ of degree $d$ is $F(X, Y, Z) := Z^d f(X/Z, Y/Z)$. In other words, one changes $x$ to $X$, $y$ to $Y$, and then appends enough factors of $Z$ to each monomial to bring the total degree of each monomial to $d$. One can recover $f$ as $f(x, y) = F(x, y, 1)$.

If $f(x, y) = 0$ is a plane curve $C$ in $\mathbb{A}^2$, its *projective closure* is the curve $\widetilde{C}$ in $\mathbb{P}^2$ defined by the homogenized equation $F(X, Y, Z) = 0$. The curve $\widetilde{C}$ equals $C$ plus some points "at infinity".

EXAMPLE. If $f(x, y) = y^2 - x^3 + x - 7$, then

$$F(X, Y, Z) = Y^2Z - X^3 + XZ^2 - 7Z^3$$

and

$$\begin{aligned}\widetilde{C}(\mathbb{Q}) &= \frac{\{\text{zeros of } F\}}{\mathbb{Q}^*} \\ &= \{\text{zeros of } F(X, Y, 1)\} \cup \frac{\{\text{zeros of } F(X, Y, 0)\} - 0}{\mathbb{Q}^*} \\ &= C(\mathbb{Q}) \cup \{P\},\end{aligned}$$

where $P$ is the point $(0 : 1 : 0)$ "at infinity".

**2.3. Bézout's Theorem.** As mentioned earlier, one of the primary reasons for working in the projective plane is to obtain a good intersection theory. Let $F(X, Y, Z) = 0$ and $G(X, Y, Z) = 0$ be curves in $\mathbb{P}^2$ over $k$, of degree $m$ and $n$, respectively. Bézout's Theorem states that they intersect in exactly $mn$ points of $\mathbb{P}^2$, provided that

(i) $F$ and $G$ have no nontrivial common factor,
(ii) one works over an algebraically closed field, and
(iii) one counts intersection points with multiplicity (in case of singularities, or points of tangency).

We have given condition (i) in a form that yields a correct statement of Bézout's Theorem even without our assumption that plane curves are defined by irreducible polynomials. Of course, if $F$ and $G$ *are* irreducible, condition (i) states simply that the curves do not coincide.

## 3. Determining $X(\mathbb{Q})$: subdivision by degree

We return to the problem of determining the set of rational points $X(\mathbb{Q})$, where $X$ is an affine plane curve $f(x, y) = 0$ over $\mathbb{Q}$ or its projective closure. Let $d = \deg f$. We will look at the problem for increasing values of $d$.

**3.1. $d = 1$: lines.** We know how to parameterize the rational points on $ax + by + c = 0$!

**3.2. $d = 2$: conics.** Legendre proved that conics satisfy the *Hasse Principle*. This means: $X$ has a $\mathbb{Q}$-point if and only if $X$ has an $\mathbb{R}$-point and a $\mathbb{Q}_p$-point for each prime $p$. Since a projective conic is described by a quadratic form in three variables, Legendre's result can be viewed as a special case of the Hasse–Minkowski Theorem [Serre 1973, Chapter IV, § 3.2], which states that a quadratic form in $n$ variables over $\mathbb{Q}$ represents 0 (in other words, takes the value 0 on some arguments in $\mathbb{Q}$ not all zero) if and only if it represents 0 over $\mathbb{R}$ and $\mathbb{Q}_p$ for all $p$.

Legendre's Theorem leads to an algorithm to determine the existence of a $\mathbb{Q}$-point on a conic $X$. Here is one such algorithm: complete the square, multiply by a constant, and absorb squares into the variables, to reduce to the case of $aX^2 + bY^2 + cZ^2 = 0$ in $\mathbb{P}^2$, where $a, b, c$ are nonzero, squarefree, pairwise relatively prime integers. Then one can show that there exists a $\mathbb{Q}$-point if and only if $a, b, c$ are not all of the same sign and the congruences

$$ax^2 + b \equiv 0 \pmod{c},$$
$$by^2 + c \equiv 0 \pmod{a},$$
$$cz^2 + a \equiv 0 \pmod{b}$$

are solvable in integers. Moreover, in this case, $aX^2 + bY^2 + cZ^2 = 0$ has a nontrivial solution in integers $X, Y, Z$ satisfying $|X| \le |bc|^{1/2}$, $|Y| \le |ac|^{1/2}$, and $|Z| \le |ab|^{1/2}$. See [Mordell 1969].

In the case where the conic $X$ has a $\mathbb{Q}$-point $P_0$, there remains the problem of describing the set of *all* $\mathbb{Q}$-points. For this there is a famous trick: for each $P \in X(\mathbb{Q})$ draw the line through $P_0$ and $P$, and let $t$ be its slope, which will be in $\mathbb{Q}$ (or maybe $\infty$). Conversely, given $t \in \mathbb{Q}$, Bézout's Theorem guarantees that the line through $P_0$ with slope $t$ will intersect the conic in one other point (provided that this line is not tangent to the conic at $P_0$), and this will be a rational point.

For example, if $X$ is the circle $x^2 + y^2 = 1$ and $P_0 = (-1, 0)$, then

$$t \longrightarrow \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right),$$
$$\frac{y}{x+1} \longleftarrow (x, y)$$

define *birational maps* from $\mathbb{A}^1$ to $X$ and back: this means that, ignoring finitely many subsets of smaller dimension (a few points), they are maps given by rational functions of the variables that induce a bijection between the $\overline{\mathbb{Q}}$-points on each side. These birational maps are defined over $\mathbb{Q}$; that is, the coefficients of the rational functions are in $\mathbb{Q}$, so they also induce a bijection between $\mathbb{Q}$-points (ignoring the same subsets as before). In particular, the complete set of rational solutions to $x^2 + y^2 = 1$ is

$$\left\{\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) : t \in \mathbb{Q}\right\} \cup \{(-1, 0)\}.$$

**3.3. $d = 3$: plane cubics.** Lind [1940] and Reichardt [1942] discovered that the Hasse Principle can fail for plane curves of degree 3. Here is a counterexample due to Selmer [1951; 1954]: the curve $3X^3 + 4Y^3 + 5Z^3 = 0$ in $\mathbb{P}^2$ has an $\mathbb{R}$-point $(((-4/3)^{1/3} : 1 : 0)$ is one) and a $\mathbb{Q}_p$-point for each prime $p$, but it has no $\mathbb{Q}$-point. (For $p > 5$, the existence of $\mathbb{Q}_p$-points can be proved by combining Hensel's Lemma [Koblitz 1984, Theorem 3] with a counting argument to prove the existence of solutions modulo $p$. For $p = 2, 3, 5$, a more general form of Hensel's Lemma can be used [Koblitz 1984, Chapter I, Exercise 6]. The nonexistence of $\mathbb{Q}$-points is more difficult to establish.)

As mentioned at the beginning of this article, deciding whether a plane cubic curve has a rational point is currently an unsolved problem. For the time being, we will restrict attention to those plane cubic curves that *do* have a rational point. These are called *elliptic curves*, and are birational to curves defined by a equation of a simple form. This leads to the first of the official definitions of elliptic curves that we present in the next section.

## 4. Elliptic curves

**4.1. Equivalent definitions.** Let $k$ be a perfect field. An *elliptic curve* over $k$ can be defined as any one of the following:

(i) The projective closure of a nonsingular curve defined by a "Weierstrass equation"
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
with $a_1, a_2, a_3, a_4, a_6 \in k$. If the characteristic of $k$ is not 2 or 3, one may restrict attention to projective closures of curves
$$y^2 = x^3 + Ax + B.$$
One can show that this is nonsingular if and only if $x^3 + Ax + B$ has distinct roots in $\overline{k}$, and that this holds if and only if the quantity $\Delta := -16(4A^3 + 27B^2)$ is nonzero.

(ii) A nonsingular projective genus 1 curve over $k$ equipped with a $k$-rational point $O$.

(iii) A one-dimensional projective group variety over $k$.

We need to define several of the terms occurring here. (Even then it will not be obvious that the definitions above are equivalent.)

**4.2. Singularities.** If $(0, 0)$ is a point on the affine curve $f(x, y) = 0$ over $k$, then $(0, 0)$ is a *singular* point if $\partial f/\partial x$ and $\partial f/\partial y$ both vanish at $(0, 0)$. Equivalently, $(0, 0)$ is singular if $f = f_2 + f_3 + \cdots + f_d$ where each $f_i \in k[x, y]$ is a homogeneous polynomial of degree $i$. For instance $(0, 0)$ is singular on $y^2 = x^3$ and on $y^2 = x^3 + x^2$, but not on $y^2 = x^3 - x$. More generally, $(a, b)$ is singular on $f(x, y) = 0$ if and only if $(0, 0)$ is singular on $f(X + a, Y + b) = 0$.

An affine curve is *nonsingular* if it has no singular points. A projective curve $F(X, Y, Z) = 0$ is nonsingular if its "affine pieces" $F(x, y, 1) = 0$, $F(x, 1, z) = 0$, $F(1, y, z) = 0$ are nonsingular. (One can generalize these notions to curves in higher dimensional affine or projective spaces. This is important because although every plane curve $X$, singular or not, is birational to some nonsingular projective curve $Y$, sometimes such a $Y$ cannot be found in the plane.)

*Smooth* is a synonym for nonsingular, at least for curves over a perfect field $k$.

**4.3. Genus.** Let $X$ be a nonsingular projective curve over a perfect field $k$. The *genus* of $X$ is a nonnegative integer $g$ that measures the geometric complexity of $X$. It has the following equivalent definitions:

(A) $g = \dim_k \Omega$ where $\Omega$ is the vector space of regular differentials on $X$. (Regular means "no poles". If $k = \mathbb{C}$, then regular is equivalent to holomorphic.)

(B) $g$ is the topological genus (number of handles) of the compact Riemann surface $X(\mathbb{C})$. (This definition makes sense only if $k$ can be embedded in $\mathbb{C}$.)
(C) $g = \frac{1}{2}(d-1)(d-2) - (\text{terms for singularities of } Y)$, where $Y$ is a (possibly singular) plane curve birational to $X$ and $d$ is the degree of $Y$. For example, a nonsingular plane cubic curve has genus 1.

We will not prove the equivalence of these definitions.

**4.4. Group law: definition.** To say that an elliptic curve $E$ over $k$ is a group variety means roughly that there is an "addition" map $E \times E \to E$, given by rational functions, that induces a group structure on $E(L)$ for any field extension $L$ of $k$. We now explain what the group law on $E(k)$ is, for an elliptic curve $E$ presented as a plane cubic curve in Weierstrass form.

The group law is characterized by the following two rules:

(i) The point $O = (0:1:0)$ at infinity is the identity of the group.
(ii) If a line $L$ intersects $E$ in three $k$-points $P, Q, R \in E(k)$ (taking multiplicities into account), then $P + Q + R = O$ in the group law.

From these one deduces:

(a) Given $P \in E(k)$ not equal to 0, the vertical line through $P$ intersects $E$ in $P$, $O$, and a third point which is $-P$.
(b) Given $P, Q \in E(k)$ not equal to $O$, the line through $P$ and $Q$ (take the tangent to $E$ at $P$ if $P = Q$) intersects $E$ at $P$, $Q$, and a third point $R \in E(k)$. If $R = O$, then $P + Q = O$; otherwise $P + Q = -R$, where $-R$ can be constructed as in (a).

Note that $E(k)$ is an *abelian* group.

**4.5. Group law: formulas.** It is easy to see that, at least generically, the coordinates of $P + Q$ can be expressed as rational functions in the coordinates of $P$ and $Q$. Here we present explicit formulas that give an algorithm for computing $P + Q$. The existence of these formulas will be important in Section 7.5 as we develop the elliptic curve factoring method.

To compute the sum $R$ of points $P, Q \in E(k)$ on $y^2 = x^3 + Ax + B$ over $k$:

1. If $P = O$, put $R = Q$ and stop.
2. If $Q = O$, put $R = P$ and stop.
3. Otherwise let $P = (x_1 : y_1 : 1)$ and $Q = (x_2 : y_2 : 1)$. If $x_1 \neq x_2$, put

$$\begin{aligned} \lambda &= (y_1 - y_2)(x_1 - x_2)^{-1}, \\ x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1, \\ R &= (x_3 : y_3 : 1), \end{aligned}$$

and stop.

4. If $x_1 = x_2$ and $y_1 = -y_2$, put $R = O$ and stop.
5. If $x_1 = x_2$ and $y_1 \neq -y_2$ (so $P = Q$), put

$$\begin{aligned} \lambda &= (3x_1^2 + A)(y_1 + y_2)^{-1}, \\ x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1, \\ R &= (x_3 : y_3 : 1), \end{aligned}$$

and stop.

This requires $O(1)$ field operations in $k$. Using projective coordinates renders division unnecessary.

**4.6. Group law: examples.** Let $E$ be the elliptic curve $y^2 = x^3 - 25x$. (From now on, when we give a nonhomogeneous equation for an elliptic curve $E$, it is understood that we really mean for $E$ to be defined as the projective closure of this affine curve.) Since $x^3 - 25x$ has distinct roots, $E$ is nonsingular, so $E$ really is an elliptic curve. The line $L$ through $P := (-4, 6)$ and $Q := (0, 0)$ has the equation $y = (-3/2)x$. We compute $L \cap E$ by substitution:

$$\begin{aligned} ((-3/2)x)^2 &= x^3 - 25x \\ 0 &= (x + 4)x(x - 25/4) \end{aligned}$$

and find $L \cap E = \{P, Q, R\}$ where $R := (25/4, -75/8)$. Thus $P + Q + R = O$ in the group law, and $P + Q = -R = (25/4, 75/8)$.

The intersection of the line $X = 0$ in $\mathbb{P}^2$ with $E : Y^2Z = X^3 - 25XZ^2$ is $X = 0 = Y^2Z$, which gives $(0 : 1 : 0) = O$ and $(0 : 0 : 1) = Q$, the latter with multiplicity 2. (Geometrically, this corresponds to the vertical line $x = 0$ being tangent to $E$ at $Q$.) Thus $Q + Q + O = O$, and $2Q = O$; that is, $Q$ is a point of order 2, a *2-torsion point*. (In general, the nonzero 2-torsion points on $y^2 = x^3 + Ax + B$ are $(\alpha, 0)$ where $\alpha$ is a root of $x^3 + Ax + B$: they form a subgroup of $E(\bar{k})$ isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.)

## 5. Structure of $E(k)$ for various fields $k$

What kind of group is $E(k)$?

**5.1. Elliptic curves over the complex numbers.** On one hand $E(\mathbb{C})$ is a complex manifold, but on the other hand it is a group, and the coordinates of $P + Q$ are rational functions in the coordinates of $P$ and $Q$, so the group law is holomorphic. Hence $E(\mathbb{C})$ is a 1-dimensional Lie group over $\mathbb{C}$. Moreover, $E(\mathbb{C})$ is closed in $\mathbb{P}^2(\mathbb{C})$, which is compact, so $E(\mathbb{C})$ is compact. It turns out that it is also connected. By the classification of compact connected 1-dimensional Lie groups over $\mathbb{C}$, we must have $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ as Lie groups over $\mathbb{C}$, for some

lattice $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, where $\omega_1, \omega_2$ are an $\mathbb{R}$-basis of $\mathbb{C}$. The $\omega_i$ are called *periods*, because there is a meromorphic function $\wp(z)$ on $\mathbb{C}$ defined below such that $\wp(z+\omega) = \wp(z)$ for all $\omega \in \Lambda$. The lattice $\Lambda$ is not uniquely determined by $E$; scaling it by a nonzero complex number does not affect the isomorphism type of $\mathbb{C}/\Lambda$. But a particular $\Lambda$ can be singled out if a nonzero holomorphic differential on $E$ is also given (to be identified with $dz$ on $\mathbb{C}/\Lambda$).

Suppose conversely that we start with a discrete rank 2 lattice $\Lambda$ in $\mathbb{C}$. In other words, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ for an $\mathbb{R}$-basis $\omega_1, \omega_2$ of $\mathbb{C}$. We will show how to reverse the previous paragraph to find a corresponding elliptic curve $E$ over $\mathbb{C}$. Set $g_2 = 60 \sum'_{\omega\in\Lambda} \omega^{-4}$ and $g_3 = 140 \sum'_{\omega\in\Lambda} \omega^{-6}$ where the $'$ means "omit the $\omega = 0$ term". Let

$$\wp(z) = z^{-2} + \textstyle\sum'_{\omega\in\Lambda}((z-\omega)^{-2} - \omega^{-2}).$$

Then one can prove the following: $\wp(z)$ is meromorphic on $\mathbb{C}$ with poles in $\Lambda$, $\wp(z+\omega) = \wp(z)$ for all $\omega \in \Lambda$, and $z \mapsto (\wp(z), \wp'(z))$ defines an analytic isomorphism $\mathbb{C}/\Lambda \to E(\mathbb{C})$ where $E$ is the elliptic curve

$$y^2 = 4x^3 - g_2 x - g_3$$

over $\mathbb{C}$. (The poles of $\wp(z)$ correspond under the isomorphism to the point $O \in E(\mathbb{C})$ at infinity.) The differential $dx/y$ on $E$ pulls back to $dz$ on $\mathbb{C}/\Lambda$; hence the inverse map $E(\mathbb{C}) \to \mathbb{C}/\Lambda$ is given by

$$(a,b) \mapsto \int_O^{(a,b)} \frac{dx}{y} = \int_\infty^a \frac{dx}{\sqrt{4x^3 - g_2 x - g_3}}$$

(with suitable choice of path and branch).

More generally, Riemann proved that any compact Riemann surface is isomorphic as complex manifold to $X(\mathbb{C})$ for some nonsingular projective curve $X$ over $\mathbb{C}$.

**5.2. Elliptic curves over the real numbers.** Let $E$ be an elliptic curve $y^2 = f(x)$ over $\mathbb{R}$, where $f(x) = x^3 + Ax + B \in \mathbb{R}[x]$ is squarefree. This time $E(\mathbb{R})$ is a 1-dimensional compact commutative Lie group over $\mathbb{R}$. Considering the intervals where $f$ is nonnegative, we find that $E(\mathbb{R})$ has one or two connected components, according as $f$ has one real root, or three real roots. Since the circle group

$$\mathbb{R}/\mathbb{Z} \quad \simeq \quad \{z \in \mathbb{C} : |z| = 1\}$$

is the only *connected* 1-dimensional compact commutative Lie group over $\mathbb{R}$, it follows that

$$E(\mathbb{R}) \simeq \begin{cases} \mathbb{R}/\mathbb{Z} & \text{if } f \text{ has 1 real root,} \\ \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } f \text{ has 3 real roots.} \end{cases}$$

The group $E(\mathbb{R})$ can also be viewed as the subgroup of $E(\mathbb{C})$ fixed by complex conjugation. If $E$ is defined over $\mathbb{R}$, one can choose $\Lambda$ of the previous section to be stable under complex conjugation, and the coordinatewise action of complex conjugation on $E(\mathbb{C})$ corresponds to the natural action on $\mathbb{C}/\Lambda$. If a nonzero regular differential on $E$ (defined over $\mathbb{R}$) is fixed, then $\Lambda$ is determined, and in this situation one defines the *real period* as the positive generator of the infinite cyclic group $\Lambda \cap \mathbb{R}$.

**5.3. Elliptic curves over finite fields.** Let $E$ be an elliptic curve over the finite field $\mathbb{F}_q$ of $q$ elements. Since $E(\mathbb{F}_q)$ is a subset of $\mathbb{P}^2(\mathbb{F}_q)$, $E(\mathbb{F}_q)$ is a *finite* abelian group. Hasse proved

$$\#E(\mathbb{F}_q) = q + 1 - a,$$

where $|a| \leq 2\sqrt{q}$. This is a special case of the "Weil conjectures" (now proved). Moreover, an algorithm of Schoof [1985] computes $\#E(\mathbb{F}_q)$ in time $(\log q)^{O(1)}$ as follows: an algorithm we will not explain determines $\#E(\mathbb{F}_q)$ mod $\ell$ for each prime $\ell$ up to about $\log q$, and then the Chinese Remainder Theorem recovers $\#E(\mathbb{F}_q)$.

EXAMPLE 1. Let $E$ be the elliptic curve $y^2 = x^3 - x + 1$ over $\mathbb{F}_3$. Hasse's Theorem implies $1 \leq \#E(\mathbb{F}_3) \leq 7$. In fact,

$$E(\mathbb{F}_3) = \{(0,1), (0,2), (1,1), (1,2), (2,1), (2,2), O\},$$

and $E(\mathbb{F}_3) \simeq \mathbb{Z}/7\mathbb{Z}$. Here is an exercise for the reader, an instance of what is called the *elliptic discrete logarithm problem*: which multiple of $(0,1)$ equals $(1,1)$?

EXAMPLE 2. Let $E$ be the elliptic curve $y^2 = x^3 - x$ over $\mathbb{F}_3$. Then

$$E(\mathbb{F}_3) = \{(0,0), (1,0), (2,0), O\},$$

and $E(\mathbb{F}_3) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

## 6. Elliptic curves over the rational numbers

**6.1. Mordell's Theorem.** Let $E$ be an elliptic curve over $\mathbb{Q}$. Mordell proved that $E(\mathbb{Q})$ is a finitely generated abelian group:

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

where $r \in \mathbb{Z}_{\geq 0}$ is called the *rank*, and $T = E(\mathbb{Q})_{\text{tors}}$ is a finite abelian group called the *torsion subgroup*. (This is sometimes called the Mordell–Weil theorem, because Weil proved a generalization for *abelian varieties* over number fields. Abelian varieties are projective group varieties of arbitrary dimension.)

Although $T$ can be computed in polynomial time, it is not known whether $r$ is computable. We will say a little more about the latter at the end of Section 6.7.

EXAMPLE 1. Let $E$ be the elliptic curve $y^2 = x^3 - 25x$ over $\mathbb{Q}$. With work, one can show

$$E(\mathbb{Q}) \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

where $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$ is generated by $(-4, 6)$.

EXAMPLE 2. Let $E$ be the elliptic curve $y^2 + y = x^3 - x^2$ over $\mathbb{Q}$, also known as "the modular curve $X_1(11)$". Then

$$E(\mathbb{Q}) = \{(0,0), (0,-1), (1,0), (1,-1), O\} \simeq \mathbb{Z}/5\mathbb{Z}.$$

EXAMPLE 3. Let $E$ be the elliptic curve $1063y^2 = x^3 - x$. (This is not in Weierstrass form, but it is isomorphic to $y^2 = x^3 - 1063^2 x$.) Using "Heegner points on modular curves", Elkies [1994] computed that $E(\mathbb{Q}) \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$ is generated by a point with $x$-coordinate $q^2/1063$, where

$$q = \frac{1109186374182976967504702163571228176738233966743464 5}{3173426575447721807352079773209000125228079367778 87}.$$

EXAMPLE 4. Let $E$ be the elliptic curve $y^2 + xy + y = x^3 + ax + b$ where

$$a = -120039822036992245303534619191166796374, \text{ and}$$
$$b = 5042249924849106700108017991680827267594437562229114151 16.$$

Martin and McMillen [2000] showed that $E(\mathbb{Q}) \simeq \mathbb{Z}^r$, where $r \geq 24$.

A folklore conjecture predicts that as E varies over all elliptic curves over $\mathbb{Q}$, the rank $r$ can be arbitrarily large. But the present author does not believe this.

**6.2. One-dimensional affine group varieties over $k$.** One way to begin studying an elliptic curve over $\mathbb{Q}$ or another number field is to reduce its coefficients modulo a prime and to study the resulting curve over a finite field. Unfortunately, the result can be singular even if the original curve was nonsingular. It turns out that upon deleting the singularity, we obtain a one-dimensional group variety, but it is no longer an elliptic curve: it is affine instead of projective due to the deletion.

The one-dimensional affine group varieties $G$ over $k$ can be classified. For simplicity, we assume that $k$ is a perfect field of characteristic not 2. The table on the next page lists all possibilities.

| $G$ | variety | group law | $G(k)$ |
|---|---|---|---|
| $\mathbb{G}_a$ | $\mathbb{A}^1$ | $x_1, x_2 \mapsto x_1 + x_2$ | $k$, under $+$ |
| $\mathbb{G}_m$ | $xy = 1$ | $(x_1, y_1), (x_2, y_2) \mapsto (x_1x_2, y_1y_2)$ | $k^*$, under $\cdot$ |
| $\mathbb{G}_m^{(a)}$ | $x^2 - ay^2 = 1$ | $(x_1, y_1), (x_2, y_2) \mapsto$ $(x_1x_2 + ay_1y_2, x_1y_2 + x_2y_1)$ | $\ker\big(k(\sqrt{a})^* \xrightarrow{\text{norm}} k^*\big)$ |

The first column gives the group variety $G$, which is either the *additive group* $\mathbb{G}_a$, or the *multiplicative group* $\mathbb{G}_m$ or one of its *twists* $\mathbb{G}_m^{(a)}$ for some $a \in k^*$. The isomorphism type of $\mathbb{G}_m^{(a)}$ as a group variety is determined by the image of $a$ in $k^*/k^{*2}$. If $a \in k^{*2}$, then $\mathbb{G}_m^{(a)}$ is isomorphic to $\mathbb{G}_m$.

The second column describes $G$ as a variety; in each case, $G$ is either $\mathbb{A}^1$ or a plane curve in $\mathbb{A}^2$. The third column expresses the group law morphism $G \times G \to G$ in coordinates. The final column describes the group of rational points $G(k)$.

**6.3. Singular Weierstrass cubics.** If $E$ is a *singular* curve defined as the projective closure of

$$y^2 = x^3 + ax^2 + bx + c$$

then there is at most one singularity. (Otherwise the formula for the genus would produce a negative integer.) Let $P_0$ be the singularity. By a change of variables, we may assume that $P_0 = (0, 0)$. The equation then has the form $(y^2 - ax^2) - x^3 = 0$. The tangent line(s) to the branches at $(0, 0)$ are $y = \pm\sqrt{a}x$. The singularity is called a *node* or a *cusp* according as $a \neq 0$ or $a = 0$.

In either case, $E_{\text{ns}} := E - \{P_0\}$ becomes a one-dimensional affine group variety using the same geometric construction as in the nonsingular case. (A line $L$ through two nonsingular points cannot pass through $P_0$, because the intersection multiplicity at $P_0$ would be at least 2, and Bézout's Theorem would be violated.) In fact,

$$E_{\text{ns}} \simeq \begin{cases} \mathbb{G}_a & \text{if } a = 0 \text{ (cusp)}, \\ \mathbb{G}_m & \text{if } a \in k^{*2} \text{ (node)}, \\ \mathbb{G}_m^{(a)} & \text{if } a \text{ is a nonsquare (node)}. \end{cases}$$

EXAMPLE. If $E$ is the projective closure of $y^2 = x^3$, which has a cusp at $(0, 0)$, then the isomorphism is given by

$$\begin{aligned} E_{\text{ns}} &\longleftrightarrow \mathbb{G}_a, \\ (x, y) &\longrightarrow x/y, \\ (t : 1 : t^3) = (t^{-2}, t^{-3}) &\longleftarrow t. \end{aligned}$$

The isomorphism respects the group structures: one can check for example that $(t : 1 : t^3)$, $(u : 1 : u^3)$, and $(v : 1 : v^3)$ are collinear in $\mathbb{P}^2$ whenever $t + u + v = 0$.

**6.4. Reduction mod $p$.** For any $u \in \mathbb{Q}^*$, the elliptic curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{Q}$ is isomorphic to $Y^2 = X^3 + u^4 AX + u^6 B$. (Multiply the equation by $u^6$, and set $Y = u^3 y$ and $X = u^2 x$.) Therefore, we may assume that $A, B \in \mathbb{Z}$. Then one can reduce the equation modulo a prime $p$ to get a cubic curve $\overline{E}$ over $\mathbb{F}_p$. But $\overline{E}$ might be singular. This happens if and only if $p$ divides $\Delta$.

One says that $E$ has *good reduction* at $p$ if there is some Weierstrass equation for $E$ (obtained by change of coordinates) whose reduction modulo $p$ is nonsingular. Similarly if there is a Weierstrass equation for $E$ whose reduction modulo $p$ is a cubic curve with a node, one says that $E$ has *multiplicative reduction* at $p$; in this case one says that $E$ has *split multiplicative reduction* or *nonsplit multiplicative reduction* according as $\overline{E}_{\text{ns}}$ is $\mathbb{G}_m$ or a nontrivial twist. Otherwise, if $E$ has neither good nor multiplicative reduction, then all Weierstrass equations for $E$ reduce modulo $p$ to a cubic curve with a cusp, and one says that $E$ has *additive reduction*. Some of this is summarized in the following table.

| singularity | $\overline{E}_{\text{ns}}$ | terminology |
|---|---|---|
| none | $\overline{E}$ | good reduction |
| cusp | $\mathbb{G}_a$ | additive reduction |
| node | $\mathbb{G}_m$ or $\mathbb{G}_m^{(d)}$ | multiplicative reduction |

**6.5. Finiteness of $T := E(\mathbb{Q})_{\text{tors}}$.** Suppose that an elliptic curve $E$ over $\mathbb{Q}$ has good reduction at $p$. By scaling, any point in $E(\mathbb{Q})$ can be written as $(a : b : c)$ with $a, b, c \in \mathbb{Z}$ such that $\gcd(a, b, c) = 1$, and then $a, b, c$ can be reduced modulo $p$ to obtain a point on $\overline{E}(\mathbb{F}_p)$. This defines a homomorphism $E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_p)$.

THEOREM. *If $E$ has good reduction at a prime $p > 2$, then the torsion subgroup $T$ of $E(\mathbb{Q})$* injects *into $\overline{E}(\mathbb{F}_p)$.*

COROLLARY. *$T$ is finite.*

EXAMPLE. Let $E$ be the elliptic curve $y^2 = x^3 - 4x + 4$ over $\mathbb{Q}$. Then

$$\Delta = -16(4(-4)^3 + 27 \cdot 4^2) = -2^8 \cdot 11,$$

so $E$ has good reduction at $p$ at least when $p \neq 2, 11$. We compute $\#\overline{E}(\mathbb{F}_3) = 7$ and $\#\overline{E}(\mathbb{F}_5) = 9$. The only group that can inject into groups of order 7 and 9 is the trivial group, so $T = \{O\}$. In particular, $(0, 2) \in E(\mathbb{Q})$ is of infinite order, and $E(\mathbb{Q})$ has positive rank.

**6.6. Other theorems about the torsion subgroup $T$.**

THEOREM (LUTZ, NAGELL). *Let $A, B \in \mathbb{Z}$ be such that $E : y^2 = x^3 + Ax + B$ is an elliptic curve. If $P \in T$ and $P \neq O$, then $P = (x_0, y_0)$ where $x_0, y_0 \in \mathbb{Z}$ and $y_0^2 \mid 4A^3 + 27B^2$.*

This gives a slow algorithm to determine $T$. (It requires factoring the integer $4A^3 + 27B^2$.)

THEOREM (MAZUR). *If $E$ is an elliptic curve over $\mathbb{Q}$, then either $T \simeq \mathbb{Z}/N\mathbb{Z}$ for some $N \leq 12$, $N \neq 11$, or $T \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}\mathbb{Z}$ for some $N \leq 4$. In particular, $\#T \leq 16$.*

For each $m \geq 1$, one can use the group law to compute the polynomial $\phi_m(x) \in \mathbb{Q}[x]$ whose roots are the $x$-coordinates of the points of order $m$ in $E(\overline{\mathbb{Q}})$. Determining the points of order $m$ in $E(\mathbb{Q})$ is then a matter of finding the rational roots of $\phi_m$ and checking which of these give a rational $y$-coordinate. By Mazur's Theorem, only finitely many $m$ need be considered, so this gives a polynomial time algorithm for computing $T$.

**6.7. Height functions.** We next describe some of the ingredients which go into the proof of Mordell's Theorem. If $P = (a : b : c) \in \mathbb{P}^2(\mathbb{Q})$, we may scale to assume $a, b, c \in \mathbb{Z}$ and $\gcd(a, b, c) = 1$. Then define

$$H(P) := \max(|a|, |b|, |c|) \quad \text{and} \quad h(P) := \log H(P).$$

One calls $h(P)$ the *(logarithmic) height* of $P$. Roughly, $h(P)$ is the width of a sheet of paper needed to write down $P$.

It is easy to see that for any $B > 0$,

$$\#\{P \in \mathbb{P}^2(\mathbb{Q}) : H(P) \leq B\} \leq (2B + 1)^3,$$

so

$$\{P \in \mathbb{P}^2(\mathbb{Q}) : h(P) \leq B\} \quad \text{is finite.} \tag{6-1}$$

The latter is a special case of Northcott's Theorem [Serre 1989, § 2.4]. If $E \subset \mathbb{P}^2$ is an elliptic curve over $\mathbb{Q}$, then one can show that for $P, Q \in E(\mathbb{Q})$,

$$h(P + Q) + h(P - Q) = 2h(P) + 2h(Q) + O(1), \tag{6-2}$$

where the $O(1)$ depends on $E$ but not on $P$ or $Q$.

Define the *canonical height* or *Néron–Tate height* of a point $P \in E(\mathbb{Q})$ as $\hat{h}(P) := \lim_{n\to\infty} h(2^n P)/4^n$. The following are formal consequences of (6-1) and (6-2): for $P, Q \in E(\mathbb{Q})$ and $n \in \mathbb{Z}$,

(a) $h(2P) = 4h(P) + O(1)$;
(b) the limit defining $\hat{h}(P)$ exists;
(c) $\hat{h}(P) = h(P) + O(1)$;
(d) $\hat{h}(P + Q) + \hat{h}(P - Q) = 2\hat{h}(P) + 2\hat{h}(Q)$;
(e) $\hat{h}(nP) = n^2\hat{h}(P)$;
(f) $\hat{h}(P) \geq 0$, with equality if and only if $P \in E(\mathbb{Q})_{\text{tors}}$.

In particular, $\hat{h}$ is a quadratic form on $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$.

Moreover, (6-1) and (6-2) with the "Weak Mordell–Weil Theorem", which asserts the finiteness of $E(\mathbb{Q})/2E(\mathbb{Q})$, imply that $E(\mathbb{Q})$ is finitely generated. If generators of $E(\mathbb{Q})/2E(\mathbb{Q})$ could be found effectively, then the rank of $E(\mathbb{Q})$ and generators of $E(\mathbb{Q})$ could be found effectively. Unfortunately, the only known method for calculating $E(\mathbb{Q})/2E(\mathbb{Q})$, *descent*, requires a prime $p$ such that the $p$-primary part of a certain torsion group $Ш(E)$ associated to $E$ is finite. The group $Ш(E)$, called the *Shafarevich–Tate group*, is conjectured to be finite for all $E$, but this has been proved only in certain cases.

## 7. The elliptic curve factoring method

**7.1. An interpretation of factoring.** Suppose that $p$ and $q$ are unknown large primes, and $N = pq$ is given. One way to factor $N$ is to compute somehow an integer $m$ that is zero modulo $p$ but nonzero mod $q$. Then $\gcd(m, N)$, which can be computed quickly, yields $p$.

**7.2. Some factoring methods.** We outline various well-known factoring methods from the point of view of Section 7.1. (We use $\mathbb{Z}/N$ as an abbreviation for the quotient ring $\mathbb{Z}/N\mathbb{Z}$.)

Trial division: Try $m = 2$, $m = 3$, $m = 5 \ldots$.

Pollard $\rho$: Let $f$ be a function $\mathbb{Z}/N \to \mathbb{Z}/N$, compute a sequence $x_1, x_2, x_3, \ldots$ of elements of $\mathbb{Z}/N$ satisfying $x_{i+1} = f(x_i)$, and try $m = x_j - x_i$ for various $i, j$.

Quadratic sieve, number field sieve: After finding a nontrivial solution to $x^2 \equiv y^2 \pmod{n}$, try $m = x + y$.

Pollard $p-1$: Choose random $a$ mod $N$, take $K = k!$ for some $k \geq 1$, and try $m = a^K - 1$.

ECM (Lenstra's elliptic curve method): Instead of $a^K$ for $a \in (\mathbb{Z}/N)^*$, consider $K \cdot P$ for some $P \in E(\mathbb{Z}/N)$, for some elliptic curve $E$. Here $K \cdot P$ means $P + P + \cdots + P$, the sum of $K$ copies of $P$ in an abelian group $E(\mathbb{Z}/N)$ to be defined.

**7.3. The Pollard $p-1$ method.** The elliptic curve method can be viewed as an analogue of the Pollard $p-1$ method. As a warmup for the elliptic curve method, we describe the $p-1$ method here more fully, but still ignoring details and practical improvements.

To factor $N$:

1. Choose an integer $K > 1$ with a lot of factors, for instance, $K = k!$ for some $k \geq 1$.

2. Choose an arbitrary integer $a$ satisfying $1 < a < N-1$.
3. If $\gcd(a, N) > 1$, then we're done! Otherwise continue.
4. Use the binary expansion of $K$ to compute $a^K \bmod N$.
5. Compute $g = \gcd(a^K - 1, N)$. If $1 < g < N$, then we're done, since $g$ is a nontrivial factor of $N$. If $g = N$, try again with a different $a$, or with $K$ replaced by a divisor. If $g = 1$, try again with a larger $K$ (or if you're tired, give up).

If $K$ is a multiple of $p-1$ for some prime $p$ dividing $N$, then in Step 4, $(a^K \bmod p)$ is a power of $(a^{p-1} \bmod p)$, which is $(1 \bmod p)$ by Fermat's Little Theorem. Then in Step 5, $a^K - 1$ is divisible by $p$, so $g = p$, (unless by chance $a^K - 1$ is divisible also by another factor of $N$).

The problem with this method is that it is not easy to arrange for $K$ to be divisible by $p-1$, since we do not know what $p$ is! The best we can do is choose a $K$ with many factors, and hope that $p-1$ will be among the factors. If we choose $K = k!$, we are essentially hoping that $p-1$ will be *smooth*, that is, equal to a product of small primes. Thus the Pollard $p-1$ method is effective only for finding factors $p$ of $N$ such that $p-1$ is smooth.

**7.4. Variants of the $p-1$ method.** If instead of Fermat's Little Theorem in $\mathbb{F}_p^*$, one uses that every element of $\mathbb{F}_{p^2}^*/\mathbb{F}_p^*$ has order dividing $p+1$, one can develop a $p+1$ method by working in $A^*/(\mathbb{Z}/N)^*$, where $A = (\mathbb{Z}/N)[t]/(t^2 - b)$ for some $b \in \mathbb{Z}/N$. This will be effective for finding factors $p$ of $N$ such that $p+1$ is smooth.

Similarly one can use subgroups of $\mathbb{F}_{p^r}^*$ for other small $r$ to develop methods that work well when $p^2 + p + 1$ is smooth, when $p^2 + 1$ is smooth, ..., when $\Phi_r(p)$ is smooth, where $\Phi_r(z)$ is the $r$-th cyclotomic polynomial. These rapidly become useless, because $p^2 + p + 1$ and so on are much larger than $p-1$, and hence are much less likely to be smooth.

Lenstra's idea was instead to replace $\mathbb{F}_p^*$ by the group $E(\mathbb{F}_p)$ where $E$ is an elliptic curve! There are many different $E$ to try, of varying orders close to $p$.

**7.5. Elliptic curves over $\mathbb{Z}/N$.** The elliptic curve method requires working with elliptic curves over rings that are not fields. The theory of elliptic curves over rings is best expressed in the language of schemes, but this would take too many pages to develop. Fortunately, for the factoring application, we can make do with a more concrete development based on explicit formulas for the group law.

Let $N$ be a positive integer. To simplify the exposition, we assume that $\gcd(N, 6) = 1$. Define

$$\mathbb{P}^2(\mathbb{Z}/N) := \frac{\{(a : b : c) \mid a, b, c \in \mathbb{Z}/N,\ \gcd(a, b, c, N) = 1\}}{(\mathbb{Z}/N)^*}.$$

An *elliptic curve $E$ over $\mathbb{Z}/N$* is given by an homogeneous equation

$$Y^2Z = X^3 + AXZ^2 + BZ^3,$$

where $A, B \in \mathbb{Z}/N$ are such that the quantity $\Delta := -16(4A^3 + 27B^2)$ is in $(\mathbb{Z}/N)^*$. Then $E(\mathbb{Z}/N)$ denotes the subset of points $(a : b : c) \in \mathbb{P}^2(\mathbb{Z}/N)$ satisfying the cubic equation. For any prime $p$ dividing $N$, $E(\mathbb{Z}/p)$ denotes the set of points in $\mathbb{P}^2(\mathbb{Z}/p)$ satisfying the equation reduced modulo $p$.

For simplicity, suppose that $N = pq$ where $p$ and $q$ are distinct primes greater than 3. The Chinese Remainder Theorem implies

$$\begin{aligned}
\frac{\mathbb{Z}}{N} &\simeq \frac{\mathbb{Z}}{p} \times \frac{\mathbb{Z}}{q} && \text{(as rings)},\\
\left(\frac{\mathbb{Z}}{N}\right)^* &\simeq \left(\frac{\mathbb{Z}}{p}\right)^* \times \left(\frac{\mathbb{Z}}{q}\right)^* && \text{(as groups)},\\
\mathbb{P}^2\left(\frac{\mathbb{Z}}{N}\right) &\simeq \mathbb{P}^2\left(\frac{\mathbb{Z}}{p}\right) \times \mathbb{P}^2\left(\frac{\mathbb{Z}}{q}\right) && \text{(as sets)},\\
E\left(\frac{\mathbb{Z}}{N}\right) &\simeq E\left(\frac{\mathbb{Z}}{p}\right) \times E\left(\frac{\mathbb{Z}}{q}\right) && \text{(as groups)}.
\end{aligned}$$

Hence the set $E(\mathbb{Z}/N)$ inherits the structure of an abelian group. Most pairs of points in $E(\mathbb{Z}/N)$ can be added using the formulas of Section 4.5. (Use the extended GCD algorithm to compute inverses modulo $N$.) In fact, the formulas fail only if some calculated quantity in $\mathbb{Z}/N$ is zero mod $p$ and nonzero mod $q$ or vice versa, in which case $N$ is factored!

**7.6. The elliptic curve method.** Assume that the integer $N$ to be factored satisfies $\gcd(N, 6) = 1$ and that $N \neq n^r$ for any integers $n, r \geq 2$. (The latter can be tested very quickly, in $(\log N)^{1+o(1)}$ time [Bernstein 1998].) To search for factors of $N$ of size less than about $P$:

1. Fix a "smoothness bound" $y$ much smaller than $P$, and let $K$ be the LCM of all $y$-smooth integers less than or equal to $P$.
2. Choose random integers $A, x_1, y_1 \in [1, N]$.
3. Let $B = y_1^2 - x_1^3 - Ax_1 \in \mathbb{Z}/N$ and let $E$ be $y^2 = x^3 + Ax + B$, so $P_1 := (x_1, y_1) \in E(\mathbb{Z}/N)$. If $\gcd(4A^3 + 27B^2, N) \neq 1$, go back to Step 2.
4. Use the binary expansion of the factors of $K$ to attempt to compute $K \cdot P_1 \in E(\mathbb{Z}/N)$ using the group law formula.
5. If at some point the formula fails (that is, we try to use the extended GCD to invert a nonzero non-unit in $\mathbb{Z}/N$), then we have found a factor of $N$. Otherwise, go back to Step 2 and try a different elliptic curve.

Note that in Steps 2 and 3 we choose the point first and then find an elliptic curve through it. This is because it is algorithmically difficult to find a "random" point on a given elliptic curve over $\mathbb{Z}/N$: doing this in the naive way, by

choosing the $x$-coordinate first, would require taking a square root of an element of $\mathbb{Z}/N$, which is a problem known to be random polynomial time equivalent to factoring $N$!

**7.7. Partial analysis of the elliptic curve method.** If $\#E(\mathbb{Z}/p)$ divides $K$, then $K \cdot P_1$ will reduce mod $p$ to $O$. In this case, it is probable that $K \cdot P_1$ is not also $O$ modulo $N$, or at least that at some point of the computation of $K \cdot P_1$, one reaches a subproduct $K'$ of $K$ such that $K' \cdot P_1$ is $O$ mod $p$ but not $O$ mod $N$. (This can be made precise.) Hence it is essentially true that factoring $N$ requires only being lucky enough to choose $E$ such that $\#E(\mathbb{Z}/p)$ divides $K$.

Suppose that $N$ has a prime factor $p$ such that $p + 1 + 2\sqrt{p} \le P$. Let $s$ be the probability that for a random $E$ constructed by the algorithm, the order of $E(\mathbb{Z}/p)$ is $y$-smooth. If $\#E(\mathbb{Z}/p)$ is $y$-smooth, then $\#E(\mathbb{Z}/p) \mid K$, by definition of $K$ and by Hasse's Theorem (Section 5.3) that $\#E(\mathbb{Z}/p) \le p + 1 + 2\sqrt{p}$. Hence the number of elliptic curves that need to be tried during the algorithm is $O(1/s)$. Each trial involves $O(\log K)$ group law operations, each requiring $(\log N)^{O(1)}$ bit operations, making the total running time

$$R = O(s^{-1}(\log K)(\log N)^{O(1)}).$$

Let $L(x) = \exp(\sqrt{(\log x)(\log\log x)})$, so $\log x \ll L(x) \ll x$ as $x \to \infty$. Take $y = L(P)^a$ for some $a > 0$ to be optimized later. In order to express the running time $R$ in terms of the parameters of the algorithm, namely $N$, $P$, and $a$, we first bound $K$:

$$K \le \prod_{\ell \le y} \ell^{\lfloor \log_\ell P \rfloor} \le \prod_{\ell \le y} P \le P^y,$$
$$\log K \le y \log P = L(P)^{a+o(1)}.$$

Next we need an estimate of the smoothness probability $s$. A theorem of Canfield, Erdős, and Pomerance [1983] states that the probability that a random integer in $[1, x]$ is $L(x)^a$-smooth is $L(x)^{-1/(2a)+o(1)}$ as $x \to \infty$. Using a formula of Deuring for the number of elliptic curves of given order over $\mathbb{Z}/p$, one can show that $\#E(\mathbb{Z}/p)$ is close to uniformly distributed over most of the Hasse range

$$[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}].$$

To proceed, we assume the conjecture that the result of Canfield, Erdős, and Pomerance result holds for random integers in this much smaller range. Then $s = L(P)^{-1/(2a)+o(1)}$.

Under this assumption, the total running time for the elliptic curve method is

$$R = L(P)^{a+1/(2a)+o(1)}(\log N)^{O(1)}.$$

This is optimized at $a = 1/\sqrt{2}$, which makes $y = L(P)^{1/\sqrt{2}}$ and

$$R = L(P)^{\sqrt{2}+o(1)}(\log N)^{O(1)}.$$

To factor $N$ completely, we would take $P = \sqrt{N}$, which yields a running time of $L(N)^{1+o(1)}$. But one advantage of the elliptic curve method over most other factoring methods is that its running time depends on the size of the factor to be found: it is capable of finding small factors more quickly.

In practice, since the optimal choices of $y$ and hence $K$ depend on $P$, it is reasonable to run the elliptic curve method with $P$ small at first (to search for small factors) and then if no factor is found, try again and again, with an increasing sequence of values of $P$. Eventually, if no small factors are found, one should switch to the number field sieve, which is faster asymptotically if the factors are large.

**7.8. Elliptic curve method records.** The largest factor found by the elliptic curve method as of April 2008 is the 67-digit prime factor

4444349792156709907895752551798631908946180608768737946280238078881

(by Bruce Dodson in August 2006; see [Zimmerman 2008]).

Given Richard Brent's 2000 extrapolation [2000, § 3.4] that the elliptic curve method record will be a $D$-digit factor in year $Y(D) := 9.3\sqrt{D} + 1932.3$, the value $Y(67) = 2008.4$ shows that the method performs well in practice.

## 8. Curves of genus greater than 1

**8.1. Divisors.** Divisors can be used to produce higher dimensional analogues of elliptic curves, attached to higher genus curves. They also give a natural proof of the associativity for the group law of elliptic curves.

Let $X$ be a nonsingular projective curve over a perfect field $k$. The *group of $\bar{k}$-divisors* $\mathrm{Div}(X_{\bar{k}})$ is the set of formal sums of points in $X(\bar{k})$. The subgroup of *$k$-rational divisors* $\mathrm{Div}(X)$ is the subgroup of $\mathrm{Gal}(\bar{k}/k)$-stable divisors. The degree of a divisor $D = n_1(P_1) + \cdots + n_r(P_r)$ is the integer $n_1 + \cdots + n_r$. Then $\mathrm{Div}^0(X_{\bar{k}})$ denotes the group of $\bar{k}$-divisors of degree zero. Similarly define $\mathrm{Div}^0(X)$.

EXAMPLE. Let $E$ be the elliptic curve $y^2 = x^3 + 17$ over $\mathbb{Q}$. The points

$$P = (1 + \sqrt{-7}, -2 + \sqrt{-7}), \quad Q = (1 - \sqrt{-7}, -2 - \sqrt{-7}), \quad R = (-1, 4)$$

lie in $E(\overline{\mathbb{Q}})$. The divisor $D := 2(P) + 2(Q) - 7(R)$ is stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ even though $P$ and $Q$ individually are not fixed, so $D \in \mathrm{Div}(E)$. The degree of $D$ is $2 + 2 - 7 = -3$.

**8.2. Principal divisors and the Picard group.** If $f$ is a nonzero rational function on $X$ (that is, a "function" given as a ratio of polynomials in the coordinates), and $P \in X(\bar{k})$, let $\operatorname{ord}_P(f)$ denote the "order of vanishing" of $f$ at $P$ (positive if $f(P) = 0$, negative if $f$ has a pole at $P$). Then the *divisor of* $f$ is

$$(f) := \sum_{P \in X(\bar{k})} \operatorname{ord}_P(f) \cdot P \quad \in \operatorname{Div}^0(X_{\bar{k}}),$$

and if the coefficients of $f$ are in $k$, then $(f) \in \operatorname{Div}^0(X)$. The set of such $(f)$ form the subgroup $\operatorname{Princ}(X)$ of *principal divisors*. If $D, D' \in \operatorname{Div}(X)$, one writes $D \sim D'$ if $D - D' \in \operatorname{Princ}(X)$. Define the *Picard group* or *divisor class group* of $X$ as $\operatorname{Pic}(X) := \operatorname{Div}(X)/\operatorname{Princ}(X)$. Also define $\operatorname{Pic}^0(X) := \operatorname{Div}^0(X)/\operatorname{Princ}(X)$.

EXAMPLE. If $E, P, Q, R$ are as in the example of the previous section and $f = y - x + 3$, one has $(f) = (P) + (Q) + (R) - 3(O)$, so $(P) + (Q) + (R) \sim 3(O)$ in $\operatorname{Pic}(E)$.

THEOREM. *If $E$ is an elliptic curve over $k$, the map $E(k) \to \operatorname{Pic}^0(E)$ sending $P$ to the class of $(P) - (O)$ is a bijection.*

The group structure on $\operatorname{Pic}^0(E)$ thus induces a group structure on $E(k)$, which is the same as the one we defined earlier.

**8.3. Analogies.** It is helpful to keep in mind the following analogies when studying algebraic number fields or the geometry of curves (especially if they are over finite fields).

| Number field object | Function field analogue |
|---|---|
| $\mathbb{Z}$ | $k[t]$ |
| $\mathbb{Q}$ | $k(t)$ |
| $\mathbb{Q}_p$ | $k((t))$ |
| number field $F$ | finite extension of $k(t)$ (rational functions on curve $X$) |
| $\operatorname{Spec} \mathcal{O}_F$ (where $\mathcal{O}_F$ is the ring of integers of $F$) | smooth affine curve $X$ |
| finite extension $F'$ of $F$ | covering $X' \to X$ |
| fractional ideal | divisor |
| principal ideal | principal divisor |
| class group | $\operatorname{Pic}(X)$ |
| functional equation of $\zeta(s)$, Riemann Hypothesis, and Generalized Riemann Hypothesis | Weil conjectures (all proved!) |

**8.4. Rational points on curves.** We now turn briefly to the study of rational points on curves of arbitrary genus. (Recall that elliptic curves were curves of genus 1 equipped with a rational point.) A curve over $\mathbb{Q}$ of any genus can have $X(\mathbb{Q}) = \varnothing$: for example, if $X$ is birational to $y^2 = -(x^{2g+2} + 1)$, then $X$ has genus $g$ and has no rational points. In the table below, assume $X$ is a plane curve over $\mathbb{Q}$ with $X(\mathbb{Q}) \neq \varnothing$, and define

$$N_X(B) := \#\{P \in X(\mathbb{Q}) : h(P) \leq B\}.$$

The qualitative behavior of $X(\mathbb{Q})$, and in particular the rate of growth of the function $N_X(B)$, are roughly determined by the genus.

| Genus | $X(\mathbb{Q})$ | $N_X(B)$ |
|---|---|---|
| 0 | infinite | $(c_1 + o(1))e^{c_2 B}$ |
| 1 | finitely generated abelian group | $(c_3 + o(1))B^{c_4}$ |
| $\geq 2$ | finite | $O(1)$ |

In the third column, $c_1, c_2, c_3 > 0, c_4 \geq 0$ are constants depending on $X$, and the estimates hold as $B \to \infty$.

The fact that $X(\mathbb{Q})$ is finite when the genus is at least 2 was conjectured by Mordell [1922]. Proofs were given by Faltings [1983] and Vojta [1991], and a simplified version of Vojta's proof was given by Bombieri [1990]. All known proofs are ineffective: it is not known whether there exists an algorithm to determine $X(\mathbb{Q})$, although there probably is one.

**8.5. Jacobians: one tool for studying higher genus curves.** Recall that for elliptic curves $E$, we have a group isomorphism $E(k) \simeq \mathrm{Pic}^0(k)$. But if $X$ is a nonsingular projective curve of genus $g > 1$ over a field $k$, then there is no natural bijection between $X(k)$ and $\mathrm{Pic}^0(X)$, and in fact one can show that $X$ cannot be made into a group variety. (Here is one way to show this: if $X$ is a group variety, then one can create a global section of the tangent bundle of $X$ by choosing a nonzero tangent vector at the origin and moving it around by translations. But on a curve of genus $g > 1$, any nonzero meromorphic section of the tangent bundle has degree $2-2g < 0$, so it cannot be regular everywhere.)

Define an *abelian variety* to be a projective group variety, so that an elliptic curve is a one-dimensional abelian variety. Then for any $X$ of genus $g$ as above, there is an abelian variety $J$ of dimension $g$ called the *Jacobian* of $X$, with the property that $J(k) \simeq \mathrm{Pic}^0(X)$, (at least under the technical assumption that $X(k) \neq \varnothing$). It is only when $X$ is an elliptic curve that $J$ coincides with $X$.

If $P_0 \in X(k)$, then there is an embedding of varieties $X \to J$ mapping each point $P$ on $X$ to the class of the divisor $(P) - (P_0)$ in $\mathrm{Pic}^0(X)$.

EXAMPLE. Here we do a few computations in a Jacobian of a Fermat curve. Let $X$ be the projective closure of $x^{13} + y^{13} = 1$ over $\mathbb{Q}$. The genus of $X$ is $g = (13-1)(13-2)/2 = 66$. Let $P = (1, 0)$ and $Q = (0, 1)$, which are in $X(\mathbb{Q})$. Let $J$ be the Jacobian of $X$, so $J$ is a 66-dimensional abelian variety. The divisor of the function $(y-1)/(x-1)$ on $X$ is $13(Q)-13(P)$, so the class of $13(Q)-13(P)$ in $\mathrm{Pic}^0(X) = J(\mathbb{Q})$ is trivial. Thus the class of $(Q)-(P)$ is a 13-torsion point (a point of order 13) in $J(\mathbb{Q})$. (One can use the fact that $X$ has positive genus to show that no function on $X$ has divisor $(Q)-(P)$, so this point of $J(\mathbb{Q})$ is nonzero.)

Suppose that $X$ is a nonsingular projective curve over $\mathbb{Q}$ of genus $g \geq 2$ with $X(\mathbb{Q}) \neq \varnothing$. By the Mordell–Weil theorem, $J(\mathbb{Q})$ is a finitely generated abelian group. Moreover, $J(\mathbb{Q})/J(\mathbb{Q})_{\mathrm{tors}}$ can be equipped with a quadratic canonical height function $\hat{h}$. Vojta's proof of the finiteness of $X(\mathbb{Q})$ (following earlier ideas of Mumford) studies how points of $X(\mathbb{Q})$ can sit inside this lattice by applying diophantine approximation techniques.

Unfortunately the diophantine approximation techniques are ineffective: they give bounds on the number of rational points, but not bounds on their height. (Height bounds would reduce the problem of listing the points of $X(\mathbb{Q})$ to a finite computation.)

Nevertheless there exist techniques that often succeed in determining $X(\mathbb{Q})$ for particular curves $X$; some of these are discussed by Poonen [1996; 2002]. Also, there are many other conjectural approaches towards a proof that $X(\mathbb{Q})$ can be determined explicitly for all curves $X$ over $\mathbb{Q}$. (See [Hindry and Silverman 2000, Section F.4.2] for a survey of some of these.) But none have yet been successful. We need some new ideas!

## 9. Further reading

For the reader who wants more, we suggest a few other books and survey articles. Within each topic, references assuming less background are listed first. Of course, there are many other books on these topics; those listed here were chosen partly because they are the ones the author is most familiar with.

**9.1. Elliptic curves.** The book [Silverman and Tate 1992] is an introduction to elliptic curves at the advanced undergraduate level; among other things, it contains a treatment of the elliptic curve factoring method. The graduate level textbook [Silverman 1986] uses more algebraic number theory and algebraic geometry, but most definitions and theorems are recalled as they are used, so the book is readable even by those with minimal background. Cremona's book [1997] contains extensive tables of elliptic curves over $\mathbb{Q}$, and discusses many elliptic curve algorithms in detail.

**9.2. Algebraic geometry.** Fulton's text [1969] requires only a knowledge of abstract algebra at the undergraduate level; it develops the commutative algebra as it goes along. Shafarevich's text, now in two volumes [1994a; 1994b], is a extensive survey of the main ideas of algebraic geometry and its connections to other areas of mathematics. It is intended for mathematicians outside algebraic geometry, but the topics covered are so diverse that even specialists are likely to find a few things that are new to them. Finally, Hartshorne's graduate text [1977], although more demanding, contains a thorough development of the language of schemes and sheaf cohomology, as well as applications to the theory of curves and surfaces, mainly over algebraically closed fields.

**9.3. Surveys on arithmetic geometry.** Mazur's article [1986] is intended for a general mathematical audience: it begins with a discussion of various diophantine problems, and works its way up to a sketch of Faltings' proof of the Mordell conjecture. Lang's book [1991] is a detailed survey of the tools and results of arithmetic geometry, mostly without proofs (but it too sketches Faltings' proof).

## References

[Bernstein 1998] D. J. Bernstein, "Detecting perfect powers in essentially linear time", *Math. Comp.* **67**:223 (1998), 1253–1283.

[Bombieri 1990] E. Bombieri, "The Mordell conjecture revisited", *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **17**:4 (1990), 615–640. Errata in "The Mordell conjecture revisited", *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* **18**:3 (1991), 473.

[Brent 2000] R. P. Brent, "Recent progress and prospects for integer factorisation algorithms", pp. 3–22 in *Computing and combinatorics* (Sydney, 2000), edited by D.-Z. Du et al., Lecture Notes in Comput. Sci. **1858**, Springer, Berlin, 2000.

[Canfield et al. 1983] E. R. Canfield, P. Erdős, and C. Pomerance, "On a problem of Oppenheim concerning "factorisatio numerorum"", *J. Number Theory* **17**:1 (1983), 1–28.

[Cremona 1997] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, Cambridge, 1997.

[Elkies 1994] N. D. Elkies, "Heegner point computations", pp. 122–133 in *Algorithmic number theory* (Ithaca, NY, 1994), edited by L. M. Adleman and M.-D. Huang, Lecture Notes in Comput. Sci. **877**, Springer, Berlin, 1994.

[Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73**:3 (1983), 349–366. Translated in *Arithmetic geometry*, edited by G. Cornell and J. Silverman, Springer, New York-Berlin, 1986, 9–27.

[Fulton 1969] W. Fulton, *Algebraic curves: An introduction to algebraic geometry*, Addison-Wesley, Reading, MA, 1969. With the collaboration of Richard Weiss.

[Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics **52**, Springer, New York, 1977.

[Hindry and Silverman 2000] M. Hindry and J. H. Silverman, *Diophantine geometry: An introduction*, Graduate Texts in Mathematics **201**, Springer, New York, 2000.

[Hopcroft and Ullman 1969] J. E. Hopcroft and J. D. Ullman, *Formal languages and their relation to automata*, Addison-Wesley, Reading, MA, 1969.

[Koblitz 1984] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, 2nd ed., Graduate Texts in Mathematics **58**, Springer, New York, 1984.

[Lang 1991] S. Lang, *Number theory. III*, Encyclopaedia of Mathematical Sciences **60**, Springer, Berlin, 1991. Diophantine geometry.

[Lind 1940] C.-E. Lind, *Untersuchungen über die rationalen Punkte der ebenen kubischen Kurven vom Geschlecht Eins*, thesis, University of Uppsala, 1940.

[Martin and McMillen 2000] R. Martin and W. McMillen, "An elliptic curve over $\mathbb{Q}$ with rank at least 24", electronic announcement on the NMBRTHRY list server, posted May 2, 2000. Available at http://listserv.nodak.edu/archives/nmbrthry.html.

[Mazur 1986] B. Mazur, "Arithmetic on curves", *Bull. Amer. Math. Soc.* (*N.S.*) **14**:2 (1986), 207–259.

[Mordell 1922] L. J. Mordell, "On the rational solutions of the indeterminate equations of the third and fourth degrees", *Proc. Cambridge Phil. Soc.* **21** (1922), 179–192.

[Mordell 1969] L. J. Mordell, "On the magnitude of the integer solutions of the equation $ax^2 + by^2 + cz^2 = 0$", *J. Number Theory* **1** (1969), 1–3.

[Poonen 1996] B. Poonen, "Computational aspects of curves of genus at least 2", pp. 283–306 in *Algorithmic number theory* (Talence, 1996), edited by H. Cohen, Lecture Notes in Comput. Sci. **1122**, Springer, Berlin, 1996.

[Poonen 2002] B. Poonen, "Computing rational points on curves", pp. 149–172 in *Number theory for the millennium, III* (Urbana, IL, 2000), edited by M. A. Bennett et al., A K Peters, Natick, MA, 2002.

[Reichardt 1942] H. Reichardt, "Einige im Kleinen überall lösbare, im Grossen unlösbare diophantische Gleichungen", *J. Reine Angew. Math.* **184** (1942), 12–18.

[Schoof 1985] R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod $p$", *Math. Comp.* **44**:170 (1985), 483–494.

[Selmer 1951] E. S. Selmer, "The diophantine equation $ax^3 + by^3 + cz^3 = 0$", *Acta Math.* **85** (1951), 203–362.

[Selmer 1954] E. S. Selmer, "The diophantine equation $ax^3 + by^3 + cz^3 = 0$: Completion of the tables", *Acta Math.* **92** (1954), 191–197.

[Serre 1973] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics **7**, Springer, New York, 1973.

[Serre 1989] J.-P. Serre, *Lectures on the Mordell–Weil theorem*, Aspects of Mathematics **E15**, Friedr. Vieweg & Sohn, Braunschweig, 1989.

[Shafarevich 1994a] I. R. Shafarevich, *Basic algebraic geometry, 1: Varieties in projective space*, 2nd ed., Springer, Berlin, 1994.

[Shafarevich 1994b] I. R. Shafarevich, *Basic algebraic geometry, 2: Schemes and complex manifolds*, 2nd ed., Springer, Berlin, 1994.

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986.

[Silverman and Tate 1992] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer, New York, 1992.

[Vojta 1991] P. Vojta, "Siegel's theorem in the compact case", *Ann. of Math.* (2) **133**:3 (1991), 509–548.

[Zimmerman 2008] P. Zimmerman, "50 largest factors found by ECM", web page, 2008. Available at http://www.loria.fr/~zimmerma/records/top100.html.

BJORN POONEN
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALIFORNIA
BERKELEY, CA 94720-3840
UNITED STATES
poonen@math.berkeley.edu