24.1 Isogenies of elliptic curves

Definition 24.1. Let E_1/k and E_2/k be elliptic curves with distinguished rational points O_1 and O_2, respectively. An *isogeny* $\varphi\colon E_1 \to E_2$ of elliptic curves is a surjective morphism that maps O_1 to O_2.

As an example, the negation map that send $P \in E(\bar{k})$ to its additive inverse is an isogeny from E to itself; as noted in Lecture 23, it is an automorphism, hence a surjective morphism, and it clearly fixes the identity element (the distinguished rational point O).

Recall that a morphism of projective curves is either constant or surjective, so any nonconstant morphism that maps O_1 to O_2 is automatically an isogeny. The composition of two isogenies is an isogeny, and the set of elliptic curves over a field k and the isogenies between them form a category; the identity morphism in this category is simply the identity map from an elliptic curve to itself, which is is clearly an isogeny. Given that the set of rational points on an elliptic curve form a group, it would seem natural to insist that, as morphisms in the category of elliptic curves, isogenies should preserve this group structure. But there is no need to put this requirement into the definition, it is necessarily satisfied.

Theorem 24.2. *Let E_1/k and E_2/k be elliptic curves and let $\varphi\colon E_1 \to E_2$ be an isogeny defined over k. Then φ is a group homomorphism from $E_1(L)$ to $E_2(L)$, for any algebraic extension L/k.*

Proof. This is essentially immediate (just consider the pushforward map on divisors), but let us spell out the details.

By base extension to L, it suffices to consider the case $L = k$. For $i = 1, 2$, let O_i be the distinguished rational point of E_i and let $\phi_i\colon E_i(k) \to \operatorname{Pic}^0_k E_i$ be the group isomorphism that sends $P \in E_i(k)$ to the divisor class $[P - O_i]$. Let $\varphi_*\colon \operatorname{Pic}^0_k E_1 \to \operatorname{Pic}^0_k E_2$ be the pushforward map on divisor classes of degree zero. For any $P \in E_1(k)$ we have $\varphi_*([P]) = [\varphi(P)]$, since P and $\varphi(P)$ both have degree one, and

$$\varphi_*(\phi_1(P)) = \varphi_*([P - O_1]) = [\varphi_*(P - O_1)] = [\varphi(P) - \varphi(O_1)] = [\varphi(P) - O_2] = \phi_2(\varphi(P)).$$

For any $P, Q \in E_1(k)$ with $P \oplus Q = R$ we have

$$\begin{aligned} P \oplus Q &= R \\ \phi_1(P) + \phi_1(Q) &= \phi_1(R) \\ \varphi_*(\phi_1(P) + \phi(Q)) &= \varphi_*(\phi_!(R)) \\ \varphi_*(\phi_1(P)) + \varphi_*(\phi_1(Q)) &= \varphi_*(\phi_1(R)) \\ \phi_2(\varphi(P)) + \phi_2(\varphi(Q)) &= \phi_2(\varphi(R)) \\ \varphi(P) \oplus \varphi(Q) &= \varphi(R), \end{aligned}$$

where $\oplus$ denotes the group operation on both $E_1(k)$ and $E_2(k)$. □

Now that we know that an isogeny $\varphi\colon E_1 \to E_2$ is a group homomorphism, we can speak of its kernel $\varphi^{-1}(O_2)$. One can view $\ker \varphi$ as a set of closed points of E_1/k, but it is more useful to view it as a subgroup of $E_1(\bar{k})$.

Definition 24.3. Let $\varphi\colon E_1 \to E_2$ be an isogeny of elliptic curves over k. The *kernel* of φ, denoted $\ker\varphi$ is the kernel of the group homomorphism $\varphi\colon E_1(\bar{k}) \to E_2(\bar{k})$.

Recall the translation-by-Q automorphism $\tau_Q\colon E \to E$ that sends P to $P \oplus Q$. The induced map $\tau_Q^*\colon \bar{k}(E) \to \bar{k}(E)$ is an automorphism of the function field $\bar{k}(E)$.

Lemma 24.4. *Let $\varphi\colon E_1 \to E_2$ be an isogeny of elliptic curves. For each $P \in \ker\varphi$, the automorphism τ_P^* fixes $\varphi^*(\bar{k}(E_2))$, and the map $\ker\varphi \to \mathrm{Aut}(\bar{k}(E_1)/\varphi^*(\bar{k}(E_2)))$ defined by $P \mapsto \tau_P^*$ is an injective group homomorphism.*

Proof. Let $P \in \ker\varphi$ and let $f \in \bar{k}(E_2)$. Then

$$\tau_P^*(\varphi^*(f))(Q) = (f \circ \varphi \circ \tau_P)(Q) = f(\varphi(P \oplus Q)) = f(\varphi(Q)) = (f \circ \varphi)(Q) = \varphi^*(f)(Q),$$

since φ is a group homomorphism and P lies in its kernel. Thus τ_P fixes $\varphi^*(\bar{k}(E_2))$.

For any $P, Q \in \ker\varphi$ and $f \in \bar{k}(E_1)$ we have

$$\tau_{P\oplus Q}^*(f) = f \circ \tau_{P\oplus Q} = f \circ \tau_Q \circ \tau_P = \tau_P^*(f \circ \tau_Q) = \tau_P^*(\tau_Q^*(f)),$$

so $\tau_{P\oplus Q}^* = \tau_P^* \circ \tau_Q^*$, and the map $P \mapsto \tau_P^*$ is a group homomorphism. It is clearly injective, since if $P \neq Q$ then $P \ominus Q \neq O$ and $\tau_{P\ominus Q}^* = \tau_P^* \circ (\tau_Q^*)^{-1}$ is not the identity map (apply it to any nonconstant $f \in \bar{k}(E_1)$). □

Corollary 24.5. *For any isogeny $\varphi\colon E_1 \to E_2$ of elliptic curves, $\#\ker\varphi$ divides $\deg\varphi$. In particular, the kernel of an isogeny is finite.*

Proof. By definition, $\deg\varphi = [\bar{k}(E_1) : \varphi^*(\bar{k}(E_2))]$, and we know from Galois theory that the order of the automorphism group of a finite extension divides the degree of the extension. Since $\ker\varphi$ injects into $\mathrm{Aut}(\bar{k}(E_1)/\varphi^*(\bar{k}(E_2)))$, its order must divide $\deg\varphi$. □

Remark 24.6. In fact, the homomorphism in Lemma 24.4 is an isomorphism, and the corollary implies that when φ is separable we have $\#\ker\varphi = \deg\varphi$; see [1, III.4.10].

24.2 Torsion points on elliptic curves

Definition 24.7. Let E/k be an elliptic curve and let n be a positive integer. The *multiplication-by-n* map $[n]\colon E(\bar{k}) \to E(\bar{k})$ is the group homomorphism defined by

$$nP = P \oplus P \oplus \cdots \oplus P.$$

The points $P \in E(\bar{k})$ for which $nP = O$ are called *n-torsion points*. They form a subgroup of $E(\bar{k})$ denoted $E[n]$.

If $\varphi\colon E_1 \to E_2$ is an isogeny, then we know from Corollary 24.5 that $n = \deg\varphi$ is a multiple of the order of $\ker\varphi$. It follows that every point in $\ker\varphi$ is an n-torsion point. By definition, $[n]$ is a group homomorphism. We now show that $[n]$ is an isogeny.

Theorem 24.8. *The multiplication-by-n map on an elliptic curve E/k is an isogeny.*

Proof assuming $\mathrm{char}(k) \neq 2$*:* The case $n = 1$ is clear, and for $n = 2$ the map $P \mapsto P \oplus P$ is a rational map, hence a morphism (by Theorem 18.6, a rational map from a smooth projective curve is a morphism), since it can be defined in terms of rational functions of the coordinates of P via the algebraic formulas for the group operation on $E(\bar{k})$. More

generally, given any morphism $\phi\colon E \to E$, plugging the coordinate functions of ϕ into the formulas for the group law yields a morphism that sends P to $\phi(P) \oplus P$. It follows by induction that $[n]$ is a morphism, and it clearly fixes the identity element O.

It remains to show that $[n]$ is surjective. For this it suffices to show that it does not map every point to O, since a morphism of smooth projective curves is either surjective or constant (by Corollary 18.7). We have already seen that there are exactly 4 points in $E(\bar{k})$ that are fixed by the negation map, three of which have order 2 (in short Weierstrass form, these are the point at infinity and the 3 points whose y-coordinate is zero). For n odd, $[n]$ cannot map a point of order 2 to O, so $[n]$ is surjective for n odd. For $n = 2^k m$ with m odd we may write $[n] = [2] \circ \cdots \circ [2] \circ [m]$. We already know that $[m]$ is surjective, so it suffices to show that [2] is. But [2] cannot map any of the infinitely many points in $E(\bar{k})$ that are not one of the 4 points fixed by the negation map to O, so [2] must be surjective. □

Remark 24.9. Note that in characteristic 2 there are not four 2-torsion points, in fact there may be none. But one can modify the proof above to use 3-torsion points instead.

Corollary 24.10. *Let E/k be an elliptic curve. For any positive integer n, the number of n-torsion points in $E(\bar{k})$ is finite.*

Remark 24.11. In fact one can show that the number of n-torsion points divides n^2, and for n not divisible by $\mathrm{char}(k)$, is equal to n^2.

24.3 Torsion points on elliptic curves over $\mathbb{Q}$

Let E be an elliptic curve $\mathbb{Q}$, which we may assume is given by a short Weierstrass equation

$$E\colon y^2 = x^3 + a_4 x + a_6,$$

with $a_4, a_6 \in \mathbb{Q}$. Let d be the LCM of the denominators of a_4 and a_6. After multiplying both sides by d^6 and replacing y by $d^{3n}y$ and x by $d^{2n}x$, we may assume $a_4, a_6 \in \mathbb{Z}$. Since E is non-singular, we must have $\Delta = \Delta(E) := -16(4a_4^3 + 27a_6^2) \neq 0$.[1]

For each prime p the equation for E also defines an elliptic curve over $\mathbb{Q}_p$. For the sake of simplicity we will focus our attention on primes p that do not divide Δ, but everything we do below can be extended to arbitrary p (as we will indicate as we go along). Let E^0 denote the elliptic curve over $\mathbb{Q}_p$ obtained by base extension from $\mathbb{Q}$ to $\mathbb{Q}_p$. Let $\overline{E}/\mathbb{F}_p$ denote the curve over $\mathbb{F}_p$ obtained by reducing the equation for E modulo p. Here we are assuming $\Delta \not\equiv 0 \bmod p$ so that the reduced equation has no singular points, meaning that $\overline{E}$ is an elliptic curve. We say that E has *good reduction* at p when this holds.

The reduction map $E^0(\mathbb{Q}_p) \to \overline{E}(\mathbb{F}_p)$ is a group homomorphism, and we define $E^1(\mathbb{Q}_p)$ to be its kernel; these are the points that reduce to $(0:1:0)$ modulo p. In fact, $E^1(\mathbb{Q}_p)$ can be defined as the kernel of the reduction map regardless of whether E has good reduction at p or not and one can show that the points in $E^1(\mathbb{Q}_p)$ still form a group.

The points in $E^1(\mathbb{Q}_p)$ are precisely the points in $E^0(\mathbb{Q}_p)$ that can be represented as $(x:y:z)$, with $v_p(x), v_p(z) > 0$ and $v_p(y) = 0$; equivalently, the points with $v_p(x/y) > 0$ (note that $v_p(x/y)$ does not depend on how the coordinates are scaled). For all positive integers n we thus define

$$E^n(\mathbb{Q}_p) = \left\{(x:y:z) \in E^0(\mathbb{Q}_p) : v_p(x/y) \geq n\right\},$$

and note that this agrees with our previous definition of $E^1(\mathbb{Q}_p)$.

[1] The leading factor of -16 appears for technical reasons that we won't explain here, but it is useful to have a factor of 2 in Δ because a short Weierstrass equation always has singular points in characteristic 2.

Lemma 24.12. *For $n > 0$, each of the sets $E^{n+1}(\mathbb{Q}_p)$ is an index p subgroup of $E^n(\mathbb{Q}_p)$.*

Proof. Containment is clear from the definition, but we need to show that the sets $E^n(\mathbb{Q}_p)$ are actually groups. For $O = (0 : 1 : 0)$ we have $v_p(x/y) = \infty$, so $O \in E^n(\mathbb{Q}_p)$ for all n. Any affine point $P \in E^n(\mathbb{Q}_p) - E^{n+1}(\mathbb{Q}_p)$ has $v_p(x/y) = n$, and and after dividing through by z can be written as $(x : y : 1)$ with $v_p(y) < 0$. Since $a_4, a_6 \in \mathbb{Z}_p$, the equation $y^2 = x^3 + a_4x + a_6$ implies $3v_p(x) = 2v_p(y)$, so

$$n = v_p(x/y) = v_p(x) - v_p(y) = -v_p(y)/3,$$

and therefore $v_p(y) = -3n$ and $v_p(x) = -2n$. After multiplying through by p^{3n} we can write $P = (p^n x_0 : y_0 : p^{3n})$ with $x_0, y_0 \in \mathbb{Z}_p^\times$. We then have

$$\begin{aligned} p^{3n}y_0^2 &= p^{3n}x_0^3 + a_4p^{7n}x_0 + a_6p^{9n} \\ y_0^2 &= x_0^3 + a_4p^{4n}x_0 + a_6p^{6n}. \end{aligned}$$

After reducing mod p we obtain an affine point $(\overline{x_0} : \overline{y_0} : 1)$ whose coordinates are all nonzero and which lies on the singular variety $C_0/\mathbb{F}_p$ defined by

$$y^2z = x^3,$$

which also contains the reduction of $O = (0 : 1 : 0)$. If we consider the image of the group law on $E^0(\mathbb{Q}_p)$ on $C_0(\mathbb{F}_p)$, we still have an operation defined by the rule that three colinear points sum to zero. We claim that this makes the set S of nonsingular points in $C_0(\mathbb{F}_p)$ into a group of order p. To show this, we first determine S. We have

$$\begin{aligned} (\partial/\partial x)(y^2z - x^3) &= -3x^2, \\ (\partial/\partial y)(y^2z - x^3) &= 2yz, \\ (\partial/\partial z)(y^2z - x^3) &= y^2. \end{aligned}$$

It follows that a point in $C_0(\mathbb{F}_p)$ is singular if and only if its y-coordinate is zero. In particular all of the reductions of points in $E^n(\mathbb{Q}_p)$ are non-singular, for any $n \geq 1$. Every non-singular point in $C_0(\mathbb{F}_p)$ can be written as $(x : 1 : x^3)$, and this gives a bijection from $\mathbb{F}_p$ to S defined by $x \mapsto (x : 1 : x^3)$. Thus the set S has order p and it contains the identity element. It is clearly closed under negation, and we now show it is closed under addition. If P and Q are two elements of S not both equal to $(0 : 1 : 0)$, then at least one of them has non-zero z-coordinate and the line L defined by P and Q can be written in the form $z = ax + by$. Plugging this into the curve equation gives

$$y^2(ax + by) = x^3,$$

and it is then clear that the third point R in $C_0 \cap L$ must have nonzero y-coordinate, since $y_0 = 0 \Rightarrow x_0 = 0 \Rightarrow z_0 = 0$ for any $(x_0 : y_0 : z_0) \in C_0 \cap L$. Since P and Q are both in $C_0(\mathbb{F}_p)$, so is R, thus R lies in S, as does its negation, which is $P \oplus Q$. Therefore the reduction map $E^n(\mathbb{Q}_p) \to C_0(\mathbb{F}_p)$ defines a group homomorphism from $E^n(\mathbb{Q}_p)$ to S, and its kernel is $E^{n+1}(\mathbb{Q}_p)$, an index p subgroup of $E^n(\mathbb{Q}_p)$. □

Definition 24.13. The infinite chain of groups

$$E^0(\mathbb{Q}_p) \supset E^1(\mathbb{Q}_p) \supset E^2(\mathbb{Q}_p) \supset \cdots$$

is called the *p-adic filtration* of $E/\mathbb{Q}$.

Theorem 24.14. *Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime not dividing $\Delta(E)$. The p-adic filtration of E satisfies*

(1) $E^0(\mathbb{Q}_p)/E^1(\mathbb{Q}_p) \simeq \overline{E}(\mathbb{F}_p)$;

(2) $E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p) \simeq E(\mathbb{F}_p) \simeq \mathbb{Z}/p\mathbb{Z}$ *for all* $n > 0$;

(3) $\cap_n E^n = \{O\}$.

Proof. The group $E^1(\mathbb{Q}_p)$ is, by definition, the kernel of the reduction map from $E^0(\mathbb{Q}_p)$ to $\overline{E}(\mathbb{F}_p)$. To prove (1) we just need to show that the reduction map is surjective.

Let $P = (a_1 : a_2 : a_3)$ be a point in $\overline{E}(\mathbb{F}_p)$ with the $a_i \in \mathbb{Z}/p\mathbb{Z}$. The point P is non-singular, so at least one of the partial derivatives of the curve equation $f(x_1, x_2, x_3) = 0$ for E does not vanish. Without loss of generality, suppose $\partial f/\partial x_1$ does not vanish at P. If we pick an arbitrary point $\hat{P} = (\hat{a}_1 : \hat{a}_2 : \hat{a}_3)$ with coefficients $\hat{a}_i \in \mathbb{Z}_p$ such that $\hat{a}_i \equiv a_i \bmod p$, we can apply Hensel's to the polynomial $g(t) = f(t, \hat{a}_2, \hat{a}_3)$ using $a_1 \in \mathbb{Z}/p\mathbb{Z}$ as our initial solution, which satisfies $g'(a_i) \neq 0$. This yields a point in $E^0(\mathbb{Q}_p)$ that reduces to P, thus the reduction map is surjective, which proves (1).

Property (2) follows from the lemma above. For (3), note that $E^1(\mathbb{Q}_p)$ contains only points with nonzero y-coordinate, and the only such point with $v_p(x/y) = \infty$ is O; every other other point $(x : y : z) \in E^1(\mathbb{Q}_p)$ lies in $E^n(\mathbb{Q}_p) - E^{n+1}(\mathbb{Q}_p)$, where $n = v_p(x/y)$. □

Remark 24.15. Theorem 24.14 can be extended to all primes p by replacing $\overline{E}(\mathbb{F}_p)$ in (1) with the set S of non-singular points on the reduction of E modulo p. As in the proof of Lemma 24.12, one can show that S always contains O and is closed under the group operation, but there are now three different group structures that can arise:

1. A cyclic group of order p isomorphic to the additive group of $\mathbb{F}_p$; in this case E is said to as *additive reduction* at p.

2. A cyclic group of order $p-1$ isomorphic to the multiplicative group of $\mathbb{F}_p$; in this case E is said to have *split multiplicative reduction* at p.

3. A cyclic group of order $p+1$ isomorphic to the subgroup of the multiplicative group of a quadratic extension of $\mathbb{F}_p$ consisting of elements of norm one; in this case E is said to have *non-split multiplicative reduction* at p.

Parts (2) and (3) of the theorem remain true for all primes p (as we will now assume).

Corollary 24.16. *Suppose $P = (x : y : 1)$ is an affine point in $E^0(\mathbb{Q}_p)$ with finite order prime to p. Then $x, y \in \mathbb{Z}_p$.*

Proof. Suppose not. Then both x and y must have negative p-adic valuations in order to satisfiy $y^2 = x^3 + a_4x + a_6$ with $a_4, a_6 \in \mathbb{Z}_p$, and we must have $2v_p(x) = 3v_p(y)$, so $v_p(x/y) > 0$. Let $n = v_p(x/y)$. Then $P \in E^n(\mathbb{Q}_p) - E^{n+1}(\mathbb{Q}_p)$, and the image of P in

$$E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p) \simeq \mathbb{Z}/p\mathbb{Z}$$

is not zero, hence it has order p. The order m of P is prime to p, so the image of mP in $E^n(\mathbb{Q}_p)/E^{n+1}(\mathbb{Q}_p)$ is also nonzero. Thus $mP \notin E^{n+1}(\mathbb{Q}_p)$, but this is a contradiction, because $mP = O \in E^{n+1}(\mathbb{Q}_p)$. □

Lemma 24.17. *Suppose P_1, P_2, P_3 are colinear points in $E^n(\mathbb{Q}_p)$, for some $n > 0$, with $P_i = (x_i : 1 : z_i)$. Then $v_p(x_1 + x_2 + x_3) \geq 5n$.*

Proof. We have already seen that for $P_i \in E^n(\mathbb{Q}_p)$ we have $x_i \in p^n\mathbb{Z}_p$ and $z_i \in p^{3n}\mathbb{Z}_p$. Fixing $y = 1$, if $P_1 \neq P_2$ then the equation of the line through P_1 and P_2 in the x-z plane has the form $z = \alpha x + \beta$ with $\alpha = (z_2 - z_1)/(x_2 - x_1)$. Using the curve equation $z = x^3 + a_3xz^2 + z^3$ (with $y = 1$), we can rewrite α as

$$\begin{aligned}
\alpha &= \frac{z_2 - z_1}{x_2 - x_1} \\
&= \frac{z_2 - z_1}{x_2 - x_1} \cdot \frac{1 - a_4z_2^2 - a_6(z_2^2 + z_1z_2 + z_1^2)}{1 - a_4z_2^2 - a_6(z_2^2 + z_1z_2 + z_1^2)} \\
&= \frac{(z_2 - a_6z_2^3) - (z_1 - a_4x_1z_1^2 - a_6z_1^3) - a_4x_1z_2^2}{(x_1 - x_2)(1 - a_4z_2^2 - a_6(z_2^2 + z_1z_2 + z_1^2))} \\
&= \frac{(x_2^3 + a_4x_2z_2^2) - x_1^3 - a_4x_1z_2^2}{(x_1 - x_2)(1 - a_4z_2^2 - a_6(z_2^2 + z_1z_2 + z_1^2))} \\
&= \frac{(x_2 - x_1)(x_2^2 + x_1x_2 + x_1^2 + a_4z_2^2)}{(x_1 - x_2)(1 - a_4z_2^2 - a_6(z_2^2 + z_1z_2 + z_1^2))} \\
&= \frac{x_2^2 + x_1x_2 + x_1^2 + a_4z_2^2}{1 - a_4z_2^2 - a_6(z_2^2 + z_1z_2 + z_1^2)}.
\end{aligned}$$

The key point is that the denominator of α is then a p-adic unit. It follows that $\alpha \in p^{2n}\mathbb{Z}_p$, and then $\beta = z_1 - \alpha x_1 \in p^{3n}\mathbb{Z}_p$. Substituting $z = \alpha x + \beta$ into the curve equation gives

$$\alpha x + \beta = x^3 + a_4x(\alpha x + \beta)^2 + b(\alpha x + \beta)^3.$$

We know that x_1, x_2, x_3 are the three roots of the cubic defined by the equation above, thus $x_1 + x_2 + x_3$ is equal to the coefficient of the quadratic term divided by the coefficient of the cubic term. Therefore

$$x_1 + x_2 + x_3 = \frac{2a_4\alpha\beta + 3a_6\alpha^2\beta}{1 + a_4\alpha^2 + a_6\beta^3} \in p^{5n}\mathbb{Z}_p.$$

The case $P_1 = P_2$ is similar. □

Corollary 24.18. *The group $E^1(\mathbb{Q}_p)$ is torsion-free.*

Proof. By the previous corollary we only need to consider the case of a point of order p. So suppose $pP = 0$ for some $P \in E^n(\mathbb{Q}_p) - E^{n+1}(\mathbb{Q}_p)$. Consider the map

$$E^n(\mathbb{Q}_p) \to p^n\mathbb{Z}_p/p^{5n}\mathbb{Z}_p$$

that sends $P := (x : 1 : z)$ to the reduction of x in $p^n\mathbb{Z}_p/p^{5n}\mathbb{Z}_p$. By the lemma above, this is a homomorphism of abelian groups, so it sends pP to the reduction of $px \in p^{n+1}\mathbb{Z}_p - p^{n+2}\mathbb{Z}_p$ modulo $p^{5n}\mathbb{Z}_p$, which is not zero, a contradiction. □

Corollary 24.19. *Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime of good reduction. The torsion subgroup of $E(\mathbb{Q})$ injects into $\overline{E}(\mathbb{F}_p)$. in particular, the torsion subgroup is finite.*

Proof. The group $E(\mathbb{Q})$ is isomorphic to a subgroup of $E^0(\mathbb{Q}_p)$ and $\overline{E}(\mathbb{F}_p) = E^0(\mathbb{Q}_p)/E^1(\mathbb{Q}_p)$. But $E^1(\mathbb{Q}_p)$ is torison free, so the torsion subgroup of $E(\mathbb{Q})$ injects into $\overline{E}(\mathbb{F}_p)$. □

Now that we know that each elliptic curve over $\mathbb{Q}$ has a finite number of rational torsion points, one might ask whether there is a *uniform* upper bound that applies to every elliptic curve over $\mathbb{Q}$. It's not *a priori* clear that this should be the case; one might suppose that by varying the elliptic curve we could get an arbitrarily large number of rational torsion points. But this is not the case; an elliptic curve over $\mathbb{Q}$ can have at most 16 rational points of finite order. This follows from a celebrated theorem of Mazur that tells us exactly which rational torsion subgroups can (and do) arise for elliptic curves defined over $\mathbb{Q}$.

Theorem 24.20 (Mazur)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. The torsion subgroup of $E(\mathbb{Q})$ is isomorphic to one of the fifteen subgroups listed below:*

$$\mathbb{Z}/n\mathbb{Z} \quad (n = 1, 2, 3, \ldots, 9, 10, 12), \qquad\qquad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \quad (n = 1, 2, 3, 4).$$

The proof of this theorem is well beyond the scope of this course.[2] However, as a further refinement of our results above, we can prove the Nagell-Lutz Theorem.

Theorem 24.21 (Nagell-Lutz)**.** *Let $P = (x_0 : y_0 : 1)$ be an affine point of finite order on the elliptic curve $y^2 = x^3 + a_4x + a_6$ over $\mathbb{Q}$, with $a_4, a_6 \in Z$. Then $x_0, y_0 \in \mathbb{Z}$, and if $y_0 \neq 0$ then y_0^2 divides $4a_4^3 + 27a_6^2$.*

Proof. For any prime p, if $v_p(x_0) < 0$ then $2v_p(y_0) = 3v_p(x_0)$ and $v_p(x_0/y_0) > 0$. It follows that $P \in E_1(\mathbb{Q})$, but then P cannot be a torsion point. So $v_p(x) \geq 0$ for all primes p. Thus x_0 is an integer, and so is $y_0^2 = x_0^3 + a_4x_0 + a_6$, and therefore y.

If P has order 2 then $y_0 = 0$; otherwise, the x-coordinate of $2P$ is an integer equal to $\lambda^2 - 2x_0$, where $\lambda = (3x_0^2 + a_4)/(2y_0)$ is the slope of the tangent at P. Thus $4y_0^2$ and therefore y_0^2 divides $\lambda^2 = (3x_0^2 + a_4)^2$, as well as $x_0^3 + a_4x_0 + a_6$. We now note that

$$\begin{aligned}(3x_0^2 + 4a_4)(3x_0^2 + a_4)^2 &= 27x_0^6 + 54a_4x_0^4 + 27a_4^2x_0^2 + 4a_4^3\\ (3x_0^2 + 4a_4)(3x_0^2 + a_4)^2 &= 27(x_0^3 + a_4x_0)^2 + 4a_4^3\\ 0 &\equiv 27a_6^2 + 4a_4^3 \bmod y_0^2,\end{aligned}$$

since $(x_0^3 + a_4x_0) \equiv -a_6 \bmod y_0^2$, thus y_0 divides $4a_4^3 + 27a_6^2$. □

The Nagell-Lutz theorem gives an effective method for enumerating all of the torsion points in $E(\mathbb{Q})$ that is quite practical when the coefficients a_4 and a_6 are small. By factoring $D = 4a_4^3 + 27a_6^2$, one can determine all the squares y_0^2 that divide D. By considering each of these, along with $y_0 = 0$, one then checks whether there exists an integral solution x_0 to $y_0^2 = x_0^3 + ax_0 + a_6$ (note that such an x_0 must be a divisor of $a_6 - y_0^2$).

This yields a list of candidate torsion points $P = (x_0 : y_0 : 1)$ that are all points in $E(\mathbb{Q})$, but do not necessarily all have finite order. To determine which do, one computes multiples nP for increasing values of n (by adding the point P at each step, using the group law on E), checking at each step whether $nP = O$. If at any stage it is found that the affine coordinates of nP are not integers then nP, and therefore P, cannot be a torsion point, and in any case we know from Mazur's theorem that if $nP \neq O$ for any $n \leq 12$ then P is not a torsion point; alternatively, we also know that n must divide $\#\overline{E}(\mathbb{F}_p)$, where p is the least prime that does not divide $\Delta(E)$.

However, this method is not practical in general, both because it requires us to factor D, and because D might have a very large number of square divisors (if D is, say, the product

[2] There was recently a graduate seminar at Harvard devoted entirely to the proof of Mazur's theorem; see http://www.math.harvard.edu/~chaoli/MazurTorsionSeminar.html for notes and references.

of the squares of the first 100 primes, then we have 2^{100} values of y_0 to consider). But Cororllary 24.19 gives us a much more efficient alternative that can be implemented to run in quasi-linear time (roughly proportional to the number of bits it takes to represent a_4 and a_6 on a computer).

We first determine the least odd prime p that does not divide D; we don't need to factor D to do this and we will always have p bounded by $O(\log D) = O(\log \max(|a_4|, |a_6|)$. We then exhaustively compute the set $\overline{E}(\mathbb{F}_p)$, which clearly has cardinality at most $2p$ (in fact, at most $p + 1 + 2\sqrt{p}$). For each integer $m > 1$ there is an *m-division polynomial* $f_m \in \mathbb{Z}[x]$ with the property that $P = (x_0, y_0) \in E(\overline{\mathbb{Q}})$ satisfies $mP = 0$ if and only if $f_m(x_0) = 0$. The polynomials f_m can be explicitly computed using formulas for the group law on E and have integer coefficients that depend on the integer coefficients of E and degree bounded by m^2. If $\overline{P} = (\overline{x}_0, \overline{y}_0)$ is a point of order m in $\overline{E}(\mathbb{F}_p)$ then $f(\overline{x}_0) \equiv 0 \bmod p$, and we can use Hensel's lemma to efficiently "lift" the root $\overline{x}_0$ of f_m modulo p to a root x_0 of f_m modulo p^n, where n is chosen so that p^n is more than twice as large as the absolute value of the x-coordinate of any torsion point in $E(\mathbb{Q})$; the fact that y_0^2 must divide D gives us an upper bound on both y_0 and x_0. We choose a representative $x_0 \in \mathbb{Z}$ with $|x_0| < p^n/2$ and check whether $f_m(x_0) = 0$; if so then $x_0^3 + a_4x + a_6$ must be the square of an integer $y_0 \equiv \overline{y}_0 \bmod p$ (which we can also compute using Hensel lifting) and $(x_0, y_0) \in E(\mathbb{Q})$ is a torsion point. Repeating this process for each $P \in \overline{E}(\mathbb{F}_p)$ yields the torsion subgroup of $E(\mathbb{Q})$. But we know from Mazur's theorem that we only need to consider the points $\overline{P} \in \overline{E}(\mathbb{F}_p)$ of order $m \leq 12$, which means there at only $O(1)$ points to consider; here we are using the fact that $\overline{E}(\mathbb{F}_p)$ is generated by at most two elements, which we will not prove here. Provided we use fast algorithms for integer multiplication in our implementation of Hensel lifting, this yields a quasi-linear running time.

References

[1] J. H. Silverman, *The arithmetic of elliptic curves*, Springer, 2009.