1.12 26/07/02 - The Name "Elliptic Curves" and Torsion Points on Elliptic Curves

I want to start today by addressing the pressing question of

1.12.A Why are elliptic curves called "elliptic" when they are not ellipses?

The story starts from the attempts by geometers going back to the 18^{th} century to find a formula for the perimeter of an ellipse. For this, suppose that we are given $a, b \in \mathbb{R}$ with $a > b > 0$, and let $C_{a,b} : (x/a)^2 + (y/b)^2 = 1$ be the ellipse with semi-major axis a and semi-minor axis b. We can parametrize the ellipse via $(x(t), y(t)) = (a\cos t, b\sin t)$, and this allows us to express the perimeter of $C_{a,b}$ as the integral

$$P = 4\int_0^{\pi/2} \sqrt{x'(t)^2 + y'(t)^2}\,\mathrm{d}t = 4\int_0^{\pi/2} \sqrt{a^2\sin^2 t + b^2\sin^2 t}\,\mathrm{d}t.$$

Pulling out the a and expressing in terms of the eccentricity $e := \sqrt{1-(b/a)^2} \in [0,1)$ (and a minor resubstitution) gives us the integral

$$P = 4a\int_0^{\pi/2} \sqrt{1 - e^2\sin^2 t}\,\mathrm{d}t.$$

As a sanity check, if $e = 0$, then this is just $P = 2\pi a$. In general, the trigonometric substitution $u = \sin t$ gives us the expression

$$P = 4a\int_0^1 \sqrt{\frac{1-e^2u^2}{1-u^2}}\mathrm{d}u = 4a\int_0^1 \frac{1-e^2u^2}{\sqrt{(1-u^2)(1-e^2u^2)}}\mathrm{d}u.$$

This is the integral people could not figure out how to evaluate (where by evaluation we mean finding a formula in terms of elementary functions or constants). It turns out that this is for good reason–it's essentially because there is no expression for the antiderivative in terms of elementary functions. Proving this would take us very far afield, but the basic reason behind that is that if you look at the curve

$$C : v^2 = (1-u^2)(1-e^2u^2),$$

then P amounts to evaluating the integral

$$\int_\gamma \frac{1-e^2u^2}{v}\mathrm{d}u$$

for a suitable path γ on C. And the point is, that this curve C (after a suitable compatification), is a smooth projective geometrically integral genus one curve with a rational point, i.e., an elliptic curve in the sense of 1.9.2 (see 1.9.5(b)). Indeed, you don't need any fancy machinery to check that the change of coordinates

$$(x, y) = \left(\frac{\beta}{u-1}, \frac{\beta^2 v}{(u-1)^2}\right)$$

for $\beta = 1/(2(e^2-1))$ transforms C into a curve of the form

$$E_0 : y^2 = f(x)$$

for a suitable monic cubic $f(x) \in \mathbb{R}[x]$ with distinct roots (2.1.12), i.e., an elliptic curve. In fact, we can go one step further and put E_0 into shortest Weierstrass form to get a model of the form

$$E : y^2 = (x - 6(1+e^2))(x + 3(1+6e+e^2))(x + 3(1-6e+e^2)).$$

As you can check, this last curve E has discriminant $\Delta = 2^8 3^{12} e^2(1-e^2)^4$, and hence *for* $e \in (0,1)$ defines an elliptic curve. The reason there isn't an expression of P in terms of elementary functions is ultimately because of the fact that E has genus one (1.8.17). This is ultimately the reason people got interested in curves of the form $y^2 = f(x)$ for $f(x)$ a cubic, and this is why such curves are called *elliptic* curves–the name comes from *elliptic integrals*, which are so because such integrals arise naturally when you try to solve for the perimeter for an ellipse.

1.12.B Torsion in Abelian Groups

Let's quickly review the terminology surrounding torsion.

Definition 1.12.1. Let A be an abelian group, with group operation written additively.

(a) An element $a \in A$ is said to be a *torsion element* if there is an $n \in \mathbb{Z}_{\geq 1}$ such that $n \cdot a = 0$ in A; the least such n is called the *order* of a, and this case a is said to be an n-torsion element.
(b) For each $n \in \mathbb{Z}_{\geq 1}$, the subset $A[n] := \{a \in A : na = 0\}$ of elements of order dividing n is the kernel of the multiplication-by-n homomorphism $A \to A$, and is hence a subgroup of A, and is called the *n-torsion subgroup* of A. Similarly, the subset $\operatorname{Tors}(A) = \bigcup_{n \in \mathbb{Z}_{\geq 1}} A[n] \subset A$ of all torsion elements is a subgroup of A, and is called the *torsion subgroup* of A.

We can easily do other things of this sort. For instance, for any prime p, we can define the subgroup $A[p^\infty] := \bigcup_{m \geq 1} A[p^m] \subset A$ consisting of all elements annihilated by some power of p; this is known as the *p-power-torsion* or *p-primary* subgroup of A.

Example 1.12.2.

(a) We have $\operatorname{Tors} \mathbb{Z} = \{0\}$.
(b) If A is a finite group, then $\operatorname{Tors} A = A$.
(c) If $A = \mathbb{Q}/\mathbb{Z}$, then also $\operatorname{Tors} A = A$.
(d) If $A = \mathbb{Z} \oplus \mathbb{Z}/3$, then $\operatorname{Tors} A = 0 \oplus \mathbb{Z}/3 \cong \mathbb{Z}/3$. In fact, we have $A[m] = \{0\}$ if $3 \nmid m$, and $A[m] = \operatorname{Tors} A \cong \mathbb{Z}/3$ if $3 \mid m$.

The goal for us now is to study torsion points on elliptic curves. Why might we want to do that? If we look back at Bachet's example from 1.1.6, we see that Bachet's procedure is given exactly by sending $P \mapsto -2P$ in the group law on the elliptic curve $y^2 = x^3 + c$. Therefore, the sequence $\{P_0, P_1, P_2, P_3, \dots\}$ produced from a seed point $P = P_0$ is precisely $\{P, -2P, 4P, -8P, \dots\}$. When does this sequence contain only finitely many distinct terms? You can check that this happens iff $P \in E(K)$ is a torsion point.

Exercise 1.12.3. Let A be an abelian group, and let $a \in A$. Show that the sequence of elements $\{a, -2a, 4a, -8a, \dots\}$, i.e., given by $a_k = (-2)^k a$ for $k \in \mathbb{Z}_{\geq 0}$, contains only finitely many distinct elements iff a is a torsion point, i.e., if there is an $n \in \mathbb{Z}_{\geq 1}$ such that $na = 0$.

Therefore, studying when Bachet-like procedures give rise to infinitely many points is exactly equivalent to studying torsion points on elliptic curves. If we have a good understanding of which points are torsion, and which are not, then we can use this as a tool towards studying rational points on curves.

1.12.C Two Torsion on Elliptic Curves and Supersingularity

Let K be a field, and let $\overline{K}$ be an alegbraic closure of K. Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over K. Since $\mathscr{O} \in E(K)$ is an inflection point, we know from §1.7.B that to find the negative of a $P \in E(K) \smallsetminus \{\mathscr{O}\}$ say $P = (x_0, y_0)$, we just do $-P = \mathscr{O} * P$. For this, we have to draw the line $L_{\mathscr{O}P}$ joining P and $\mathscr{O}$, and take its third intersection point with E. This line is just the vertical line through P which has the equation $x = x_0$. Substituting this into the equation for E and using that $P \in E(K)$ gives us the quadratic equation for y of the form

$$y^2 + a_1x_0y + a_3y = y_0^2 + a_1x_0y_0 + a_3y_0,$$

which factors as

$$(y - y_0)(y + y_0 + a_1x_0 + a_3) = 0.$$

One root is the expected $y = y_0$ corresponding to P, and the other root is therefore

$$-P = (x_0, -y_0 - a_1x_0 - a_3). \tag{1.12.4}$$

Note that this formula is valid in all characteristics, including characteristic 2. However, if $\operatorname{ch} K \neq 2$ and we use the short Weierstrass form with $a_1 = a_3 = 0$, then the formula becomes the much easier $-P = (x_0, -y_0)$: you negate the point by negating the y-coordinate.

Now suppose we are trying to study the 2-torsion points on E, i.e., the subgroup $E[2](K) = E(K)[2]$. Note that a point $P \in E(K)$ satisfies $2P = \mathscr{O}$ iff $P = -P$. Now if $P \neq \mathscr{O}$, then $P = (x_0, y_0)$ is an affine point, and all we have to do is equate the formulae for P and $-P$ from 1.12.4, which amounts to the single equation

$$2y_0 + a_1x_0 + a_3 = 0. \tag{1.12.5}$$

As you can see from this, things proceed differently from here depending on whether $\operatorname{ch} K = 2$.

Case 1. Suppose first that $\operatorname{ch} K \neq 2$. Then if $P = (x_0, y_0) \in E[2](K)$, we get an expression for y_0 in terms of x_0 as

$$y_0 = -\frac{a_1x_0 + a_3}{2}.$$

We can plug this expression for y back into the Weierstrass equation to get a cubic equation for x, the roots of which correspond precisely to the 2-torsion points on E. The fact that $\Delta \neq 0$ actually implies that the resulting cubic polynomial is separable, i.e., has no repeated roots over an algebraic closure. This is not hard to check, but let's not bother with it in the general case, and just focus on the case of short Weierstrass equations in which $a_1 = a_3 = 0$. In this case, if $P = (x_0, y_0) \in E[2](K)$, then in fact $y_0 = 0$ and so x_0 is a root of $f(x) = x^3 + a_2x^4 + a_4x + a_6 = x^3 + ax^2 + bx + c$; we have seen in §1.10.A that nonvanishing of Δ is equivalent to the fact that $f(x)$ has three distinct roots over an algebraic closure. However, if we are only looking for roots in K, then exactly one of the following three things happens:

Case 1.a. The polynomial $f(x)$ is irreducible, and so there are no 2-torsion K-points other than $\mathscr{O}$, i.e., $E[2](K) = \{\mathscr{O}\}$. This happens, for instance, if $K = \mathbb{Q}$ and $f(x) = x^3 + 3x + 1$ (c.f. 2.2.5).

Case 1.b. The polynomial $f(x)$ factors into a linear and an irreducible quadratic factor. In this case, there is precisely one nontrivial 2-torsion K-point $T = (x_0, 0)$, where $x_0 \in K$ satisfies $f(x_0) = 0$. In this case, we have $E[2](K) = \{\mathscr{O}, T\}$, with group structure $\mathbb{Z}/2$. This happens, for instance, if $K = \mathbb{Q}$ and $f(x) = x^3 + 1 = (x + 1)(x^2 - x + 1)$.

Case 1.c. The polynomial $f(x)$ splits completely over K. In this case, there are three nontrivial 2-torsin K-points, say T_1, T_2, T_3, where for $i = 1, 2, 3$ we have $T_i = (x_i, 0)$, where the x_i are the roots of $f(x)$. In this case, $E[2](K) = \{\mathscr{O}, T_1, T_2, T_3\}$ is a group of size 4 in which every nontrivial element has order 2, and this forces $E[2](K)$ to be isomorphic to $\mathbb{Z}/2 \oplus \mathbb{Z}/2$. This happens, for instance, if $K = \mathbb{Q}$ and $f(x) = x(x + 1)(x + 4)$.

Of course, only Case 1.c occurs if K is algebraically closed (of characteristic not two). Therefore, in all subcases of Case 1, we have that $E[2](\overline{K}) \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$.

Case 2. Finally, suppose that $\operatorname{ch} K = 2$. Here the defining equation for 2-torsion just because $a_1x_0 + a_3 = 0$, and we see that things behave very differently depending on whether or not $a_1 = 0$.

Case 2.a. Suppose that $a_1 \neq 0$. Then the only allowable x-coordinate for a 2-torsion point on E is $x_0 = -a_3/a_1 = a_3/a_1$. Plugging this back into the equation for the elliptic curve tells us that the y-coordinate must satisfy

$$y_0^2 = \frac{a_3^3 + a_1a_2a_3^2 + a_1^2a_3a_4 + a_1^3a_6}{a_1^3}. \tag{1.12.6}$$

If we're looking for roots over an algebraically closed field (or even perfect field!), then then this equation *has a unique* solution; this is because if one solution is $y_0 = \alpha$, then the equation 1.12.6 factors as $(y_0 - \alpha)^2 = 0$, since we're in characteristic two. However, if we are only looking for roots in K, then again exactly one of the following two things happens:

Case 2.a.i The unique root y_0 of 1.12.6 lies in K. In this case, there is precisely one nontrivial 2-torsion K-point $T = (-a_1^{-1}a_3, y_0)$, so $E[2](K) = \{\mathscr{O}, T\}$ with group structure $\mathbb{Z}/2$. This happens, for instance if $K = \mathbb{F}_2$ and $E : y^2 + xy = x^3 + 1$, in which $E[2](\mathbb{F}_2) = \{\mathscr{O}, (0, 1)\}$.

Case 2.a.ii The unique root y_0 of 1.12.6 in $\overline{K}$ *does not* lie in K. In this case, there are no 2-torsion K-points other than $\mathscr{O}$, i.e., $E[2](K) = \{\mathscr{O}\}$. In this case, the "remaining" 2-torsion point is not visible over K, but only over a purely inseparable extension of K. This happens, for instance, if $K = \mathbb{F}_2(t)$ and $E : y^2 + xy = x^3 + t$; the point $T = (0, t^{1/2}) \in E[2](\overline{K}) \smallsetminus \{\mathscr{O}\}$ is the other two-torsion point visible over $L = \mathbb{F}_2(t^{1/2})$, and so $E[2](L) = [2](\overline{K}) = \{\mathscr{O}, T\}$, which is isomorphic to $\mathbb{Z}/2$.

Again, if K is a perfect field (e.g., if K is finite, or if K is algebraically closed of characteristic two), then only Case 2.a.i occurs.

Case 2.b. Suppose finally that $a_1 = 0$. In this case, from the smoothness $\Delta \neq 0$ and the expression for Δ in characteristic two (1.9.13), we see immediately that $a_3 \neq 0$. In this case, there is *no solution* to $a_3 = 0$, even if K is algebraically closed. Therefore, in this case, there are no 2-torsion K-points other than $\mathscr{O}$, and $E[2](K) = E[2](\overline{K}) = \{\mathscr{O}\}$. This happens, for instance, when $K = \mathbb{F}_2$ and $E : y^2 + y = x^3$.

These six cases cover all the possibilities for what 2-torsion K-points on an elliptic curve E over a field K can look like. We summarize our discussion in

Theorem 1.12.7 (2-Torsion on Elliptic Curves)**.** Let K be a field, $\overline{K}$ an algebraic closure of K, and E/K an elliptic curve.

(a) If $\operatorname{ch} K \neq 2$, then $E[2](\overline{K}) \cong_{\mathsf{Ab}} \mathbb{Z}/2 \oplus \mathbb{Z}/2$. The subgroup $E[2](K) \subset E[2](\overline{K})$ is either trivial, $\mathbb{Z}/2$, or $\mathbb{Z}/2 \oplus \mathbb{Z}/2$, and all possibilities occur in general (e.g., over $K = \mathbb{Q}$).
(b) If $\operatorname{ch} K = 2$, then $E[2](\overline{K})$ is isomorphic to either $\mathbb{Z}/2$, which happens iff $a_1 \neq 0$, or trivial, which happens iff $a_1 = 0$. In the former case, $E[2](K) \subset E[2](\overline{K})$ is either trivial or $\mathbb{Z}/2$, and only the latter can happen if K is perfect (e.g., finite or algebraically closed).

In characteristic 2, the cases $a_1 \neq 0$ and $a_1 = 0$ are thus genuinely different (this was foreshadowed in 1.10.3). These have different names:

Definition 1.12.8 (Supersingularity in Characteristic Two)**.** Let K be a field of characteristic two. An elliptic curve E/K is said to be *supersingular* if the following equivalent conditions hold:

(a) In some Weierstrass equation for E, we have $a_1 = 0$.
(b) In *every* Weierstrass equation for E, we have $a_1 = 0$ (c.f. 1.10.3).
(c) For every field L/K, we have that $E[2](L) = \{\mathscr{O}\}$.
(d) If $\overline{K}$ is an algebraic closure of K, then $E[2](\overline{K}) = \{\mathscr{O}\}$.

The elliptic curve E is said to be *ordinary* otherwise.

Therefore, 1.12.7 says that if $\operatorname{ch} K = 2$ and $\overline{K}/K$ as above, then an elliptic curve E/K is ordinary iff $E[2](\overline{K}) \cong_{\mathsf{Ab}} \mathbb{Z}/2$ and supersingular iff $E[2](\overline{K}) \cong_{\mathsf{Ab}} \{0\}$.

Example 1.12.9. Let $K = \mathbb{F}_2$.

(a) If $E : y^2 + xy = x^3 + 1$, then $E(\mathbb{F}_2) = \{\mathscr{O}, (0,1), (1,0), (1,1)\}$. This is a group of size 4 with only one 2-torsion point, and hence $E(\mathbb{F}_2) \cong_{\mathsf{Ab}} \mathbb{Z}/4$, with generators $(1,0)$ and $(1,1)$. The curve E is ordinary and $j(E) = 1$.
(b) If $E : y^2 + y = x^3$, then $E(\mathbb{F}_2) = \{\mathscr{O}, (0,0), (0,1)\}$. This is a group of size 3, and hence $E(\mathbb{F}_2) \cong_{\mathsf{Ab}} \mathbb{Z}/3$. The curve E is supersingular and $j(E) = 0$.

Unimportant Remark 1.12.10. Note that when $\operatorname{ch} K = 2$, then the formula for c_4 in 1.11.14 simplifies drastically to $c_4 = a_1^4$, and similarly the j-invariant is simply $j(E) = a_1^{12}/\Delta$. This tells us that in characteristic two, supersingularity is equivalent to the vanishing of the j-invariant. This is true also in characteristics 3 and 5, but the reason I want to de-emphasize this is because this should be thought of as an accident: this equivalence is not true for general $p > 0$. We will define supersingularity for a field of any positive characteristic p below, and 1.12.30 gives an example of supersingular elliptic curve $E/\mathbb{F}_7$ with $j(E) = -1$.

There are many other equivalent definitions of supersingularity, and we will meet some of them on the next Exercise Sheet; see also [7, §IV.4] and [8, Theorem V.3.1].

Unimportant Remark 1.12.11. Note that this is really unfortunate terminology, since an elliptic curve is always smooth and hence "nonsingular", i.e., doesn't have any singular points. (This is partly why I like to avoid the term "nonsingular" altogether.) The clashing nomenclature comes from the unrelated facts that singular points on curves behave strangely and different than other (i.e., smooth) points and that supersingular elliptic curves are very strange (super = very, singular = strange).

So far, we have avoided developing explicit formulae for the group law on an elliptic curve. However, we do really need at least a general form of these formulae when discussing three-torsion, so

we might as well bite the bullet now.

1.12.D Explicit Formulae for the Group Law

Let K be any field, and let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over K. For $i = 1, 2, 3$, let $P_i = (x_i, y_i) \in E(K) \smallsetminus \{\mathscr{O}\}$ be points. Suppose that $P_1 + P_2 = P_3$; in particular, we are assuming that $P_1 + P_2 \neq \mathscr{O}$. In this case, we can easily find an expression relating the coordinates of the P_i.

Indeed, let $L_{P_1P_2}$ denote the line joining P_1 and P_2. (The case $P_1 = P_2$ is allowed, in which case $L_{P_1P_2} = \mathrm{T}_{P_1}E$ is the tangent line to E at P_1 as usual.) The hypothesis $P_1 + P_2 \neq \mathscr{O}$ tells us that $L_{P_1P_2}$ has an equation of the form

$$L_{P_1P_2} : y = \lambda x + \nu,$$

where

$$\lambda := \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{if } x_1 \neq x_2, \\ \dfrac{3x^2 + 2a_2x + a_4 - a_1y}{2y + a_1x + a_3}, & \text{if } x_1 = x_2, \end{cases}$$

and where

$$\nu := y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

To intersect $L_{P_1P_2}$ with E, we plug in the equation for y into the equation for E to get a cubic equation in x of the form

$$x^3 - (\lambda^2 + a_1\lambda - a_2)x^2 + \cdots = 0.$$

The three roots of this equation are $x = x_1, x_2, x_3$, and so these are related by

$$x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2.$$

In particular, if we know x_1 and x_2, we can recover x_3 as $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$. The y-coordinate of the third intersection point of $L_{P_1P_2}$ with E is the $\lambda x_3 + \nu$; to get y_3, we then simply apply the negation formula 1.12.4 to get $y_3 = -(\lambda x_3 + \nu) - a_1x_3 - a_3$. In this way, we have found an explicit formula for adding two points on an elliptic curve: the formula is

$$(x_3, y_3) = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(\lambda x_3 + \nu) - a_1x_3 - a_3),$$

where λ, ν are as above.

In particular, we can take $P_1 = P_2$ to get (after a little algebraic simplification),

Proposition 1.12.12 (The Duplication Formula)**.** Let K be a field, $E : y^2 + a_1xy + a_3x = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over K, and let $P = (x, y) \in E(K)$. If $2P \neq \mathscr{O}$, then the x-coordinate of $2P$ can be expressed in terms of that of P as

$$x(2P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6},$$

where the polynomials b_i are defined by

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6, \text{ and} \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

Let me emphasize that there is nothing mysterious going on here; this is just algebra. For instance, it is clear from the formula for λ when $x_1 = x_2$ that the denominator of x_3 will look like $(2y + a_1x + a_3)^2$. We can expand this out to get

$$4(y^2 + a_1xy + a_3y) + a_1^2x^2 + 2a_1a_3 + a_3^2.$$

If P lies on the elliptic curve, then we can replace the quantity $y^2 + a_1xy + a_3y$ by $x^3 + a_2x^2 + a_4x + a_6$, and the polynomials b_k essentially come from giving names to the resulting quantities. Similarly, it is clear from the general form of the equation that the numerator will be a quartic polynomial in x and y (of "total weight 8"), and to make it into a polynomial in x only, you again replace every occurence of $y^2 + a_1xy + a_3y$ by $x^3 + a_2x^2 + a_4x + a_6$.

Remark 1.12.13.

(a) Let me remark here, for future use, the polynomial equalities

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \tag{1.12.14}$$

and

$$4b_8 = b_2b_6 - b_4^2, \tag{1.12.15}$$

both of which from straightforward algebraic checks.

(b) If $\operatorname{ch} K \neq 2$ and we work with the shorter Weierstrass form with $a_1 = a_3 = 0$ and use the labels $(a_2, a_4, a_6) = (a, b, c)$, so the curve E has the form $y^2 = f(x) = x^3 + ax^2 + bx + c$, then the duplication formula can be expressed more succinctly as

$$x(2P) = \frac{f'(x)^2}{4f(x)} - a - 2x = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4f(x)}. \tag{1.12.16}$$

1.12.E Three Torsion on Elliptic Curves

Let's now study three-torsion on elliptic curves. There are two perspectives we could take here: the geometric perspective, and the algebraic perspective. For the geometric perspective, note that the group law on an elliptic curve can be summarized by the

Observation 1.12.17. Let K be a field, and $E \subset \mathbb{P}^2_K$ be an elliptic curve in Weierstrass form. Then for $P, Q, R \in E(K)$, we have that $P + Q + R = \mathscr{O}$ in the group law iff P, Q, R are collinear.

In particular, applying this to $P = Q = R$ immediately gives us that $3P = \mathscr{O}$ in the group law iff P is an inflection point of E. In other words, the 3-torsion points on E are precisely the inflection points on E. This is really cool relationship between the algebraic and geometric perspectives. If we have a good way of getting all the inflection points on E, then we have a handle on 3-torsion, and vice-versa. When $\operatorname{ch} K \neq 2$, there is in fact a good way of getting a handle on all inflection points; this proceeds by calculating something known as the Hessian divisor of the curve. I will not tell this story here, but you can find it, for instance, in [6, Problem 5.23]. See also 1.12.26.

The algebraic perspective is much more direct and mechanical. Suppose that $P = (x_0, y_0) \in E(K) \smallsetminus \{\mathscr{O}\}$ and that $3P = \mathscr{O}$. Then $2P = -P \neq \mathscr{O}$, and so

$$x(2P) = x(-P) = x(P).$$

Conversely, if $x(2P) = x(P)$, then the line $x = x(P)$ intersects E in the points $\mathscr{O}, P$ and $2P$. This means that $2P = \pm P$, but $2P = P$ can't be true since $P \neq \mathscr{O}$, and so we must have $2P = -P$, i.e., $3P = \mathscr{O}$. We summarize this in

Proposition 1.12.18. Let K be a field (of any characteristic), and let $E \subset \mathbb{P}^2_K$ be an elliptic curve in Weierstrass form. Let $P \in E(K) \smallsetminus \{\mathscr{O}\}$. The following conditions are equivalent:

(a) We have $3P = \mathscr{O}$ in the group $E(K)$.
(b) The point P is an inflection point on E.
(c) We have that $x(2P) = x(P)$.

Now, the duplication formula 1.12.12 gives us an easy way to check when $x(2P) = x(P)$. Indeed, simply cross-multiplying and subtracting, we see that $x(2P) = x(P)$ is equivalent to saying that $x = x(P)$ is a root of the polynomial

$$f_3(x) := 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8. \tag{1.12.19}$$

The polynomial $f_3(x)$, whose roots correspond to the x-coordinates of the three-torsion points on E, is called the *third division polynomial* of E. To study how many roots $f_3(x)$ has, let's first see if it has any repeated roots, which can be checked by computing its discrimimant:

$$\operatorname{disc}(f_3) = -81\Delta^2.$$

You don't have to–and shouldn't–take my word on faith; you can just compute the discriminant yourself, or get a computer algebra software to do it for you. Again, different things happen when $\operatorname{ch} K \neq 3$ and when $\operatorname{ch} K = 3$.

Case 1. Suppose first that $\operatorname{ch} K \neq 3$. Then smoothness $\Delta \neq 0$ implies that $\operatorname{disc}(f_3) \neq 0$. This means that over an algebraic closure $\overline{K}$, the polynomial f_3 factors completely as

$$f_3(x) = 3\prod_{i=1}^{4}(x - \beta_i)$$

for four distinct $\beta_i \in \overline{K}$. For each $i = 1, \dots, 4$, we can plug $x = \beta_i$ into the equation for E to get the corresponding quadratic equation

$$y^2 + (a_1\beta_i + a_3)y - (\beta_i^3 + a_2\beta_i^2 + a_4\beta_i + a_6) = 0. \tag{1.12.20}$$

Can this quadratic equation 1.12.20 for y have a repeated root? Well, if it does, then then this repeated root y_0 is also a root of its derivative

$$2y + (a_1\beta_i + a_3) = 0.$$

But this was precisely our condition (1.12.5) for (β_i, y_0) to be a 2-torsion point! Since we're assuming it's a 3-torsion point, it *cannot* be 2-torsion (since it is not $\mathcal{O}$), and this tells us that y_0 is not a repeated root of the quadratic equation 1.12.20. Therefore, for each $i = 1, \dots, 4$, we get two different roots $y = \delta_i^{\pm}$ of this equation, giving us the 8 nontrivial 3-torsion points $(\beta_i, \delta_i^{\pm})$ for $i = 1, \dots, 4$. In particular, $\#E[3](\overline{K}) = 9$. Up to isomorphism, there are two abelian groups of size 9, and only one of them has the property that every nontrivial element has order 3. This is sufficient to conclude that $E[3](\overline{K}) \cong_{\mathsf{Ab}} \mathbb{Z}/3 \oplus \mathbb{Z}/3$.

Case 2. Finally, suppose that $\operatorname{ch} K = 3$. In this case, $f_3(x)$ becomes

$$f_3(x) = b_2x^3 + b_8.$$

Therefore, we see that things behave very differently depending on whether or not $b_2 = 0$.

Case 2.a. Suppose that $b_2 \neq 0$. Then the only allowable x-coordinate for a three-torsion point on E is $x = (-b_2^{-1}b_8)^{1/3} \in \overline{K}$. (Why is this? Well, if β solves $b_2\beta^3 + b_8 = 0$, then in the equation $b_2x^3 + b_8$ actually factors completely as $b_2(x-\beta)^3 = 0$, since we are in characteristic 3.) Again, plugging this in above gives us a quadratic equation for y, which doesn't have repeated roots for the same reason as in Case 1. We conclude that in this case, $E[3](\overline{K}) \cong_{\mathsf{Ab}} \mathbb{Z}/3$. (Again, we don't need K to be algebraically closed; we only need it to be perfect for this to be true. In particular, something like $K = \mathbb{F}_3$ works just fine.)

Case 2.b. Suppose finally that $b_2 = 0$. In this case, the formula 1.12.14 when $\operatorname{ch} K = 3$ simplifies drastically to $\Delta = b_4^3$, so smoothness $\Delta \neq 0$ implies that $b_4 \neq 0$. But now the relation (1.12.15) along with $b_2 = 0$ forces $b_8 = -b_4^2$, from which we conclude that $b_8 \neq 0$. In particular, the equation $f_3(x) = 0$ has no roots whatsoever, and we conclude that $E[3](\overline{K}) = \{\mathcal{O}\}$.

Remark 1.12.21. Suppose that $\operatorname{ch} K \neq 2, 3$, and we are working with the short Weierstrass form with $a_1 = a_3 = 0$. Then either by using the formula 1.12.16 or by plugging in $a_1 = a_3 = 0$ into 1.12.19, we get the formula

$$f_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 2f(x)f'(x) - f'(x)^2,$$

where $E : y^2 = f(x)$ with $f(x) = x^3 + ax^2 + bx + c$. To check if $f_3(x)$ has any repeated roots, we need to check if it shares any roots with its derivative

$$f_3'(x) = 2f(x)f'''(x) = 12f(x).$$

But any common root of f_3 and f_3', would then be a common root of f and f', which does not exist by smoothness (1.10.A). This is again enough to conclude that the polynomial $f_3(x)$ is separable, i.e., has distinct roots over an algebraic closure $\overline{K}$. This is basically the argument given in [2, Theorem 2.1]. The only disadvantage of this approach is that it does not work when $\operatorname{ch} K = 2$, whereas our proof above does.

We have proven

Theorem 1.12.22 (3-Torsion on Elliptic Curves)**.** Let K be a field, $\overline{K}$ an algebraic closure of K, and E/K an elliptic curve.

(a) If $\operatorname{ch} K \neq 3$, then $E[3](\overline{K}) \cong_{\mathsf{Ab}} \mathbb{Z}/3 \oplus \mathbb{Z}/3$.
(b) If $\operatorname{ch} K = 3$, then $E[3](\overline{K})$ is isomorphic to either $\mathbb{Z}/3$, which happens iff $b_2 \neq 0$, or trivial, which happens iff $b_2 = 0$.

An analysis similar to 1.12.7 (but more complicated) can be done to figure out what the subgroup $E[3](K) \subset E[3](\overline{K})$ looks like in general; this is an exercise on the Exercise Sheet for next week. Finally, as in 1.12.7, we see from the proof that if K is perfect (e.g., finite) and E has $b_2 \neq 0$, then in fact $E[2](K) \cong_{\mathsf{Ab}} \mathbb{Z}/3$; we don't need to go to $\overline{K}$. Finally, we have

Definition 1.12.23 (Supersingularity in Characteristic Three)**.** Let K be a field of characteristic three. An elliptic curve E/K is said to be *supersingular* if the following equivalent conditions hold:

(a) In some Weierstrass equation for E, we have $b_2 = 0$.
(b) In *every* Weierstrass equation for E, we have $b_2 = 0$.
(c) For every field L/K, we have that $E[3](L) = \{\mathscr{O}\}$.
(d) If $\overline{K}$ is an algebraic closure of K, then $E[3](\overline{K}) = \{\mathscr{O}\}$.

The elliptic curve E is said to be *ordinary* otherwise.

Note that when $\operatorname{ch} K = 3$ and we're in short Weierstrass form with $a_1 = a_3 = 0$, then $b_2 = a_2$. In other words, a curve of the form $y^2 = x^3 + ax^2 + bx + c$ in characteristic 3 is supersingular iff $a = 0$ (c.f. 1.11.7).

Example 1.12.24. Let $K = \mathbb{F}_3$.

(a) If $E : y^2 = x^3 + x^2 + 1$, then $\Delta(E) = j(E) = -1$. It is easy to see that

$$E(\mathbb{F}_3) = \{\mathscr{O}, (0, \pm 1), (-1, \pm 1), (1, 0)\},$$

so that $\#E(\mathbb{F}_3) = 6$. Up to isomorphism, there is a unique abelian group of order six, and so we must have $E(\mathbb{F}_3) \cong_{\mathsf{Ab}} \mathbb{Z}/2 \oplus \mathbb{Z}/3 \cong_{\mathsf{Ab}} \mathbb{Z}/6$. The points $(0, \pm 1)$ are easily seen to have order six, and hence must be the two generators. Note that $x^3 + x^2 + 1 = (x-1)(x^2 - x - 1) \in \mathbb{F}_3[x]$; therefore, we are in Case 1.b of §1.12.C. Correspondingly,

$$E[2](\mathbb{F}_3) = \{\mathscr{O}, (1, 0)\} \cong_{\mathsf{Ab}} \mathbb{Z}/2,$$

whereas

$$E[2](\overline{\mathbb{F}}_3) = \{\mathscr{O}, (1, 0), (-1 \pm i, 0)\} \cong_{\mathsf{Ab}} \mathbb{Z}/2 \oplus \mathbb{Z}/2.$$

Finally, we have that

$$E[3](\mathbb{F}_3) = E[3](\overline{\mathbb{F}}_3) = \{\mathscr{O}, (-1, \pm 1)\}.$$

The curve E is therefore ordinary.

(b) If $E : y^2 = x^3 + x$, then $\Delta(E) = -1$ and $j(E) = 0$. It is easy to see that

$$E(\mathbb{F}_3) = \{\mathscr{O}, (0, 0), (-1, \pm 1)\},$$

so that $\#E(\mathbb{F}_3) = 4$. Since $x^3 + x = x(x^2 + 1) \in \mathbb{F}_3[x]$, we are in Case 1.b of §1.12.C. Correspondingly,

$$E[2](\mathbb{F}_3) = \{\mathscr{O}, (0, 0)\} \cong_{\mathsf{Ab}} \mathbb{Z}/2.$$

This is enough to conclude that $E(\mathbb{F}_3) \cong_{\mathsf{Ab}} \mathbb{Z}/4$, and also

$$E[2](\overline{\mathbb{F}}_3) = \{\mathscr{O}, (0,0), (\pm i, 0)\} \cong_{\mathsf{Ab}} \mathbb{Z}/2 \oplus \mathbb{Z}/2.$$

Finally, we see that

$$E[3](\mathbb{F}_3) = E[3](\overline{\mathbb{F}}_3) = \{\mathscr{O}\},$$

i.e., the curve E is supersingular.

Unimportant Remark 1.12.25. Note that when $\operatorname{ch} K = 3$, the formula for c_4 in 1.11.14 simplifies drastically to $c_4 = b_2^2$ (check!), and similarly the j-invariant is simply $j(E) = b_2^6/\Delta$. This tells us that in characteristic three, supersingularity is again equivalent to the vanishing of the j-invariant. See 1.12.10.

Unimportant Remark 1.12.26. If $F_3 = 3X^4 + b_2X^3Z + 3b_4X^2Z^2 + 3b_6XZ^3 + b_8Z^4$ is the homogenization of the third division polynomial, then the Hessian H of the curve $E = \mathbb{V}(F)$, where

$$F = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3,$$

satisfies the very simple identity

$$HZ = (2b_2Z + 24X)F + 8F_3.$$

It follows from this formula (check!) that $\mathbb{V}(H)$ always contains $\mathscr{O} = [0:1:0]$, and further in characteristic not two, the ideal (F, H) contains F_3, telling us again that all the 3-torsion points other than $\mathscr{O}$ must have x-coordinates which are roots of $f_3(x) = F_3(x, 1)$. When $\operatorname{ch} K = 3$, the Hessian satisfies

$$H = -b_2F - (b_2X^3 + b_8Z^3).$$

In this case, the Hessian divisor on E is the vanishing locus of

$$b_2X^3 + b_8Z^3.$$

As before, if $b_2 \neq 0$ (i.e., when E is not supersingular), and we let $\beta := (-b_2^{-1}b_8)^{1/3} \in \overline{K}$, then

$$b_2X^3 + b_8Z^3 = b_2(X - \beta Z)^3,$$

which tells us that the reason for the existence of only 3 inflection points is because the Hessian divisor is nonreduced and has multiplicity 3 at each of the three inflection points (over $\overline{K}$). Finally, if $b_2 = 0$ (i.e., if E *is* supersingular), then $b_8 \neq 0$ as above, and the Hessian divisor is the vanishing locus of Z^3, which is just $9(\mathscr{O})$; in this case, the Hessian divisor is *even more* nonreduced, and is supported only at $\mathscr{O}$ with multiplicity 9, explaining the existence of a unique inflection point on E. Note finally also that when $\operatorname{ch} K = 2$, we have $H \equiv 0$, corresponding to the fact that the vanishing of the Hessian only gives us inflection points when $\operatorname{ch} K \neq 2$.

1.12.F Supersingularity in General

At this point, based on what we have seen already, the following results shouldn't be too surprising.

Theorem 1.12.27. Let K be a field of characterstic zero, and $\overline{K}$ an algebraic closure of K. Then for any elliptic curve E/K and $n \in \mathbb{Z}_{\geq 1}$, we have that

$$E[n](\overline{K}) \cong_{\mathsf{Ab}} \mathbb{Z}/n \oplus \mathbb{Z}/n.$$

Theorem 1.12.28. Let K be a field of characteristic $p > 0$, and $\overline{K}$ be an algebraic closure of K. Then for any given elliptic curve E/K, exactly one of the following holds:

(a) For all $n \in \mathbb{Z}_{\geq 1}$, if we write $n = p^r m$ for $r, m \in \mathbb{Z}_{\geq 0}$ with $p \nmid m$, then

$$E[n](\overline{K}) \cong_{\mathsf{Ab}} \mathbb{Z}/m \oplus \mathbb{Z}/m \oplus \mathbb{Z}/p^r.$$

(b) For all $n \in \mathbb{Z}_{\geq 1}$, if we write $n = p^r m$ for $r, m \in \mathbb{Z}_{\geq 0}$ with $p \nmid m$, then

$$E[n](\overline{K}) \cong_{\mathsf{Ab}} \mathbb{Z}/m \oplus \mathbb{Z}/m.$$

Curves satisfying (a) are known as *ordinary*, and curves satisfying (b) are called *supersingular*.

Note that in either case, if $\operatorname{ch} K \nmid n$, then we always have $E[n](\overline{K}) \cong_{\mathsf{Ab}} \mathbb{Z}/n \oplus \mathbb{Z}/n$; the difference comes when trying to analyze p-power torsion. For instance, in the ordinary case for any $r \geq 0$ we have $E[p^r](\overline{K}) \cong_{\mathsf{Ab}} \mathbb{Z}/p^r$, whereas in the supersingular case, we have $E[p^r](\overline{K}) \cong_{\mathsf{Ab}} \{0\}$. We won't prove these results here, although one proof of a special case can be found in (the double-starred exercise) 2.2.10. The general algebraic proof of these results can be given by studying the *invariant differential* on elliptic curves; material along these lines can be found in [8]. However, the *real* reason for why we should expect results of this sort (at least 1.12.27) to be true (I think) comes from the picture over $K = \mathbb{C}$, which we will see next time. We end with a couple of

Example 1.12.29. Let $K = \mathbb{F}_5$, and consider the elliptic curve $E : y^2 = x^3 - x$. This has $\Delta(E) = -1$ and $j(E) = -2$. An easy check shows that

$$E(\mathbb{F}_4) = \{\mathscr{O}, (0,0), (\pm 1, 0), (2, \pm 1), (-2, \pm 2)\}.$$

In particular, $\#E(\mathbb{F}_5) = 8$. Now $x^3 - x = x(x+1)(x-1) \in \mathbb{F}_5[x]$ tells us that we are in Case 1.c of §1.12.C, and hence

$$E[2](\mathbb{F}_5) = \{\mathscr{O}, (0,0), (\pm 1, 0)\} \cong_{\mathsf{Ab}} \mathbb{Z}/2 \oplus \mathbb{Z}/2.$$

This is enough to conclude (check!) that $E(\mathbb{F}_5) \cong_{\mathsf{Ab}} \mathbb{Z}/4 \oplus \mathbb{Z}/2$, with the four points $(2, \pm 1)$ and $(-2, \pm 2)$ each having order 4.

Next, we note that $f_3(x) = 3x^4 - 6x^2 - 1 = -2(x^4 - 2x^2 - 2) \in \mathbb{F}_5[x]$ is irreducible, which agrees with out observation that $E[3](\mathbb{F}_5) = \{\mathscr{O}\}$. Now a careful study of the general theory above guarantees (check!) that there is an extension $L/\mathbb{F}_5$ of degree at most $4 \cdot 2 = 8$ such that $E[3](L) \cong \mathbb{Z}/3 \oplus \mathbb{Z}/3$, and indeed one can check that we do really need L to be $\mathbb{F}_{5^8} = \mathbb{F}_{390625}$ here: for $i = 0, 1, \ldots, 7$, we have that $E[3](\mathbb{F}_{5^i}) = \{\mathscr{O}\}$ but in fact $E[3](\mathbb{F}_{390625}) \cong_{\mathsf{Ab}} \mathbb{Z}/3 \oplus \mathbb{Z}/3$.

Finally, we see by Lagrange's Theorem that $\#E[5](\mathbb{F}_5) = \{\mathscr{O}\}$, but this is not enough to conclude that E is supersingular over $\mathbb{F}_5$. Indeed, we have $\#E[5](\mathbb{F}_{625}) \cong_{\mathsf{Ab}} \mathbb{Z}/5$ (check!), which proves that E is ordinary.

Example 1.12.30. Let $K = \mathbb{F}_7$, and consider the elliptic curve $E : y^2 = x^3 - x$. This has $\Delta(E) = 1$ and $j(E) = -1$. An easy check shows that

$$E(\mathbb{F}_7) = \{\mathscr{O}, (0,0), (\pm 1, 0), (-2, \pm 1), (-3, \pm 2)\}.$$

In particular, $\#E(\mathbb{F}_7) = 8$. Now $x^3 - x = x(x+1)(x-1) \in \mathbb{F}_7[x]$ tells us that we are in Case 1.c of §1.12.C, and hence

$$E[2](\mathbb{F}_7) = \{\mathscr{O}, (0,0), (\pm 1, 0)\} \cong_{\mathsf{Ab}} \mathbb{Z}/2 \oplus \mathbb{Z}/2.$$

This is enough to conclude as above that in fact $E(\mathbb{F}_7) \cong_{\mathsf{Ab}} \mathbb{Z}/4 \oplus \mathbb{Z}/2$, with the four points $(-2, \pm 1)$ and $(-3, \pm 2)$ each having order 4. Next, we note that $f_3(x) = 3x^4 - 6x^2 - 1 \in \mathbb{F}_7[x]$, which factors as

$$f_3(x) = 3(x^2 + x + 3)(x^2 - x + 3) \in \mathbb{F}_7[x].$$

In particular, $E[3](\mathbb{F}_7) = \{\mathscr{O}\}$ (we knew this already), but over $\mathbb{F}_{2401} \cong \mathbb{F}_7[\alpha] := \mathbb{F}_7[x]/(x^4 - 2x^2 - 3x + 3)$, we have $\#E[3](\mathbb{F}_{2401}) = 9$ with $\#E[3](\mathbb{F}_{2401}) \cong_{\mathsf{Ab}} \mathbb{Z}/3 \oplus \mathbb{Z}/3$ (as you can check with Sage). Finally, it follows from $\#E(\mathbb{F}_7) = 8$ and Lagrange's Theorem that $E[7](\mathbb{F}_7) = \{\mathscr{O}\}$. However, this is again not sufficient to conclude that $E/\mathbb{F}_7$ is supersingular. In fact, it turns out that E *is* supersingular.

There are a few ways of proving this, but none within the reach of the tools in this course. One can argue that if $E/\mathbb{F}_p$ is an elliptic curve, then E is supersingular iff $\#E[p](\mathbb{F}_{p^i}) = 1$ for all $i = 1, \ldots, p-1$; this reduces the question to a finite check which can be performed on Sage. Another way to proceed would be to use [7, Proposition IV.4.21] to reduce to checking the coefficient of $x^6 y^6$ in $(y^2 - x^3 + x)^6 \in \mathbb{F}_7[x, y]$, which happens to be zero–this implies supersingularity. Finally, using [7, IV.4.22, IV.4.23.3], we see that $h_7(\lambda) = \lambda^3 + 9\lambda^2 + 9\lambda + 1$, which does have $\lambda = -1$ as a root; again, this is sufficient to conclude that E is supersingular.