Chapter 6

Points of Finite Order

6.1 The Torsion Subgroup

The elements of finite order in an abelian group A form a subgroup $F \subset A$, since

$$a, b \in F \Longrightarrow ma = 0, nb = 0 \Longrightarrow mn(a+b) = 0 \Longrightarrow a + b \in F.$$

This subgroup F is commonly called the *torsion* subgroup of A. (See Appendix A for further details.)

It turns out to be much easier to determine the torsion subgroup $F \subset \mathcal{E}(\mathbb{Q})$ of an elliptic curve than it is to determine the rank of the curve — that is, the number of copies of $\mathbb{Z}$ in

$$\mathcal{E}(\mathbb{Q}) = F \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}.$$

In effect the discussion below provides a simple algorithm for determining F, while there is no known algorithm for determining the rank.

Proposition 6.1 *The torsion subgroup of an elliptic curve $\mathcal{E}(\mathbb{Q})$ is finite, ie $\mathcal{E}$ has only a finite number of points of finite order.*

Proof ▶ Suppose $\mathcal{E}$ has equation

$$y^2 + c_1xy + c_3y = x^3 + c_2x^2 + c_4x + c_6,$$

where $c_i \in \mathbb{Q}$. Choose any odd prime p not appearing in the denominators of the c_i, and consider the p-adic curve $\mathcal{E}(\mathbb{Q}_p)$. Any point $P \in \mathcal{E}(\mathbb{Q})$ of finite order will still have finite order in $\mathcal{E}(\mathbb{Q}_p)$.

We know that $\mathcal{E}(\mathbb{Q}_p)$ has an open subgroup

$$\mathcal{E}_{(p)}(\mathbb{Q}_p) \cong \mathbb{Z}_p.$$

The only point of finite order in this subgroup is 0 (since $\mathbb{Z}_p$ has no other elements of finite order).

It follows that any coset

$$P + \mathcal{E}_{(p)}(\mathbb{Q}_p)$$

contains at most one element of finite order. For if there were two, say P, Q, then $P - Q$ would be a point of finite order in the subgroup.

But $\mathcal{E}(\mathbb{Q}_p)$ is compact, since it is a closed subspace of the compact space $\mathbb{P}^2(\mathbb{Q}_p)$. Hence it can be covered by a finite number of cosets

$$P_1 + \mathcal{E}_{(p)}(\mathbb{Q}_p), \ \ldots, P_r + \mathcal{E}_{(p)}(\mathbb{Q}_p).$$

Since each coset contains at most 1 point of finite order, the number of such points is finite. ◀

Remarks:

1. The finiteness of the torsion group of $\mathcal{E}(\mathbb{Q})$ follows at once from the Nagell-Lutz Theorem (Theorem 6.2), the most important result in this Chapter.

2. We shall prove in Chapter 8 the much deeper result that the group $\mathcal{E}(\mathbb{Q})$ of an elliptic curve over $\mathbb{Q}$ is *finitely-generated* (Mordell's Theorem), from which the finiteness of F follows (as shown in Appendix A). However, it would be more realistic to describe the finiteness of the torsion group as a small part of Mordell's Theorem rather than a consequence of it.

6.2 Lessons from the Real Case

Proposition 6.2 *Suppose F is the torsion subgroup of the elliptic curve $\mathcal{E}(\mathbb{Q})$. Then*

$$F \cong \mathbb{Z}/(n) \text{ or } F \cong \mathbb{Z}(2n) \oplus \mathbb{Z}/(2).$$

Proof ▶ We know that

$$\mathcal{E}(\mathbb{R}) \cong \mathbb{T} \text{ or } \mathbb{T} \oplus \mathbb{Z}/(2).$$

Since

$$\mathcal{E}(\mathbb{Q}) \subset \mathcal{E}(\mathbb{R}),$$

it follows that

$$F \subset \mathbb{T} \text{ or } \mathbb{T} \oplus \mathbb{Z}/(2).$$

Lemma *Every finite subgroup of $\mathbb{T}$ is cyclic; and there is just one such subgroup of each order n.*

Proof of Lemma $\triangleright$ The torsion subgroup of

$$\mathbb{T} = \mathbb{R}/\mathbb{Z}$$

is

$$F = \mathbb{Q}/\mathbb{Z}.$$

For if $\bar{t} \in \mathbb{T}$ is of order n then $nt \in \mathbb{Z}$, say $nt = m$, ie $t = m/n \in \mathbb{Q}$. Conversely, if $t \in \mathbb{Q}$, say $t = m/n$, then $n\bar{t} = 0$, and so $\bar{t} \in F$.

Suppose

$$A \subset \mathbb{Q}/\mathbb{Z}$$

is a finite subgroup $\neq 0$. Since each $\bar{t} \in \mathbb{T}$ has a unique representative $t \in [-1/2, 1/2)$, A has a smallest representative $t = m/n > 0$, where we may assume that $m, n > 0$, $\gcd(m, n) = 1$.

In fact $n = 1$; for we can find $u, v, \in \mathbb{Z}$ such that

$$um + vn = 1,$$

and then

$$\frac{1}{n} = u\frac{m}{n} + v,$$

ie

$$\frac{1}{n} \equiv u\frac{m}{n} \bmod \mathbb{Z}$$

Thus

$$\frac{1}{n} \in A.$$

Since $1/n \leq m/n$, this must be our minimal representative: $n = 1$.

Now every element $\bar{t} \in A$ must be of the form m/n; for otherwise we could find a representative

$$t - m/n \in (0, 1/n),$$

contradicting our choice of $1/n$ as minimal representative of A.

We conclude that

$$A = \left\{0, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}\right\} \cong \mathbb{Z}/(n).$$

Moreover, our argument shows that this is the only subgroup of A of order n. $\triangleleft$

Since this is the only subgroup of $\mathbb{T}$ of order n we can write

$$\mathbb{Z}/(n) \subset \mathbb{T}$$

without ambiguity, identifying

$$r \bmod n \longleftrightarrow r/n \bmod \mathbb{Z}$$

This establishes the result if $F \subset \mathbb{T}$. It remains to consider the case

$$A \subset \mathbb{T} \oplus \mathbb{Z}/(2).$$

By the Lemma, $A \cap \mathbb{T}$ is cyclic, say

$$A \cap \mathbb{T} = \mathbb{Z}/(n).$$

Thus

$$\mathbb{Z}/(n) \subset A \subset \mathbb{Z}/(n) \oplus \mathbb{Z}/(2).$$

Since $\mathbb{Z}/(n)$ is of index 2 in $\mathbb{Z}/(n) \oplus \mathbb{Z}/(n)$ it follows that

$$A = \mathbb{Z}/(n) \text{ or } A = \mathbb{Z}/(n) \oplus \mathbb{Z}/(2).$$

If n is odd then

$$\mathbb{Z}/(n) \oplus \mathbb{Z}/(2) \cong \mathbb{Z}/(2n)$$

by the Chinese Remainder Theorem. Thus either A is cyclic or else

$$A \cong \mathbb{Z}/(n) \oplus \mathbb{Z}/(2)$$

with n even. $\blacktriangleleft$

Mazur has shown that in fact the torsion group of an elliptic curve can only be one of a small number of groups, namely

$$\mathbb{Z}/(n)\ (n = 1 - 10, 12) \text{ and } \mathbb{Z}/(2n) \oplus \mathbb{Z}/(2)\ (n = 1 - 5).$$

6.2.1 Elements of order 2

We can distinguish between the two cases in Proposition 6.2 by considering the number of points of order 2. For $Z/(n)$ has no points of order 2 if n is odd, and just one point if n is even, say $n = 2m$, namely $m \bmod n$; while $\mathbb{Z}/(2n) \oplus \mathbb{Z}/(2)$ has three points of order 2, namely $(n \bmod 2n, 0 \bmod 2)$, $(n \bmod 2n, 1 \bmod 2)$, $(0 \bmod 2n, 1 \bmod 2)$.

Proposition 6.3 *The point $P = (x, y)$ on the elliptic curve*

$$\mathcal{E}(\mathbb{Q}) : y^2 = x^3 + ax^2 + bx + c \qquad (a, b, c \in \mathbb{Q})$$

has order 2 if and only if $y = 0$. There are either 0, 1 or 3 points of order 2.

Proof ▶ If $P = (x, y)$ then $-P = (x, -y)$. Thus $2P = 0$, ie $-P = P$, if and only if $y = 0$.

Thus there are as many elements of order 2 as there are roots of $f(x) = x^3 + ax^2 + bx + c$ in $\mathbb{Q}$. But if 2 roots $\alpha, \beta \in \mathbb{Q}$ then the third root $\gamma \in \mathbb{Q}$, since

$$\alpha + \beta + \gamma = -a.$$

◀

In determining whether

$$f(x) = x^3 + ax^2 + bx + c$$

has 0, 1 or 3 rational roots, one idea is very important: *if $a, b, c \in \mathbb{Z}$ then every rational root r of $f(x)$ is in fact integral, and $r \mid n$.* (For on substituting $r = m/n$ and multiplying by n^3, each term is divisible by n except the first.) This usually reduces the search for rational roots to a number of simple cases.

We may also note that if $a, b, c \in \mathbb{Z}$ then a necessary — but not sufficient — condition for $f(x)$ to have 3 rational roots is that the discriminant D should be a perfect square: $D = d^2$. For

$$D = [(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)]^2 .$$

6.2.2 Elements of order 3

In any abelian group, the elements of order p (where p is a prime), together with 0, form a subgroup; for

$$pa = 0,\ pb = 0 \Longrightarrow p(a + b) = 0.$$

We can consider this subgroup as a vector space over the finite field $\mathbb{F}_(p)$.

Proposition 6.4 *If p is an odd prime then there are either no points of order p on the elliptic curve $\mathcal{E}(\mathbb{Q})$, or else there are exactly $p - 1$ such elements, forming with 0 the group $\mathbb{Z}/(p)$.*

Proof ▶ An element of $\mathbb{T} \oplus \mathbb{Z}/(2)$ of odd order p is necessarily in $\mathbb{T}$. Thus the result follows from Proposition 6.2 and the Lemma in the proof of that Proposition. ◀

The elements of order 3 have a particularly simple geometric description.

Proposition 6.5 *A point $P \neq 0$ on the elliptic curve $\mathcal{E}(\mathbb{Q})$ has order 3 if and only if it is a point of inflexion. There are either 0 or 2 such points.*

Proof ▶ Suppose P has order 3, ie

$$P + P + P = 0.$$

From the definition of addition, this means that the tangent at P meets $\mathcal{E}$ in 3 coincident points P, P, P. In other words, P is a point of inflexion.

It follows from the previous Proposition that there are either 0 or 2 such flexes. ◀

Remark: The point 0 is of course a flex (by choice); so there are either 1 or 3 flexes on the elliptic curve $\mathcal{E}(\mathbb{Q})$ given by a general Weierstrass equation.

6.3 Points of Finite Order are Integral

Theorem 6.1 *Suppose $P = (x, y)$ is a point of finite order on the elliptic curve*

$$\mathcal{E}(\mathbb{Q}) : y^2 + c_1 xy + c_3 y = x^3 + c_2 x^2 + c_4 x + c_6,$$

where $c_1, c_2, c_3, c_4, c_6 \in \mathbb{Z}$. Then $x, y \in \mathbb{Z}$.

Proof ▶ The following Lemma shows that it is sufficient to prove that $y \in \mathbb{Z}$.

Lemma 1 *$\mathbb{Z}$ is integrally closed in $\mathbb{Q}$, ie if $x \in \mathbb{Q}$ satisfies an equation*

$$x^d + c_1 x^{d-1} + \cdots + c_d = 0,$$

where $c_1, \ldots, c_d \in \mathbb{Z}$, then $x \in \mathbb{Z}$.

Proof of Lemma ▷ For each prime p,

$$\|x\|_p \leq 1;$$

for otherwise x^d would dominate the equation.

Since this is true for all primes p.

$$x \in \mathbb{Z}.$$

◁

For an alternative — perhaps simpler — proof, suppose $x = m/n$, where $\gcd(m, n) = 1$. Multiplying out,

$$m^d + c_1 m^{d-1} n + \cdots c_d n^d = 0.$$

Since n divides all the terms but the first,

$$n \mid m^d.$$

Since $\gcd(m, n) = 1$, it follows that $n = \pm 1$, ie $x \in \mathbb{Z}$.

Now suppose $y \in \mathbb{Z}$. Then x satisfies the equation

$$x^3 + ax^2 + bx + (c - y^2) = 0.$$

Since all the coefficients of this cubic are integral, it follows by the Lemma that $x \in \mathbb{Z}$.

Suppose $\mathcal{E}(\mathbb{Q}_p)$ is an elliptic curve over the p-adic field. Recall that

$$\mathcal{E}_{(p)} = \{[X, 1, Z] : \|X\|_p < 1, \|Z\|_p < 1\}.$$

Lemma 2 *If $P = (x, y) \in \mathcal{E}(\mathbb{Q}_p)$ then either $x, y \in \mathbb{Z}_p$ or else $P \in \mathcal{E}_{(p)}$.*

Proof of Lemma ▷ The equation of the curve in (X, Z)-coordinates is

$$Z + c_1XZ + c_3Z^2 = X^3 + c_2X^2Z + c_4XZ^2 + c_6Z^3.$$

Suppose $P \notin \mathcal{E}_{(p)}$, ie

$$\|X\|_p \geq 1 \text{ or } \|Z\|_p \geq 1.$$

In fact

$$\|X\|_p \geq 1 \Longrightarrow \|Z\|_p \geq 1;$$

for if $\|X\|_p \geq 1$ but $\|Z\|_p < 1$ then X^3 would dominate the equation. Thus

$$\|Z\|_p \geq 1$$

in either case.

Since $y = 1/Z$

$$\|Z\|_p \geq 1 \Longrightarrow \|y\|_p \leq 1.$$

Hence

$$x, y \in \mathbb{Z}_p$$

by Lemma **??**. ◁

Lemma 3 *1. If p is odd then $\mathcal{E}_{(p)}$ is torsion-free (ie has no elements of finite order except 0).*

2. $\mathcal{E}_{(2^2)}$ is torsion-free.

Proof of Lemma ▷ This follows at once from the fact that

$$\mathcal{E}_{(p)} \cong \mathbb{Z}_p \ (p \text{ odd}), \qquad \mathcal{E}_{(2^2)} \cong \mathbb{Z}_2,$$

as we saw in Chapter 5. ◁

Lemma 4 *If $P \in \mathcal{E}_{(2)}$ then $2P \in \mathcal{E}_{(2^2)}$.*

Proof of Lemma ▷ Suppose $P = (X, Z)$. Recall that although $\mathcal{E}_{(2)}$ was defined as

$$\mathcal{E}_{(2)} = \left\{(X, Z) \in \mathcal{E} : \|X\|_2, \|Z\|_2 < 2^{-1}\right\},$$

in fact it follows from the equation

$$Z(1 + c_1X + c_2Z) = X^3 + c_2X^2Z + c_4XZ^2 + C_6Z^3$$

that

$$(X, Z) \in \mathcal{E}_{(2)} \Longrightarrow \|Z\|_2 \leq 2^{-3}.$$

(More generally, although $\mathcal{E}_{(p^e)}$ is defined as

$$\mathcal{E}_{(p^e)} = \left\{(X, Z) \in \mathcal{E} : \|X\|_p < p^{-e}, \|Z\| < 1\right\},$$

in fact

$$(X, Z) \in \mathcal{E}_{(p^e)} \Longrightarrow \|Z\|_p \leq p^{-3e}$$

by induction on e.)

The tangent at P is

$$Z = MX + D$$

where

$$\begin{aligned} M &= \frac{\partial F/\partial X}{\partial F/\partial Z} \\ &= \frac{c_1Z - (3X^2 + 2c_2XZ + 3c_4Z^2)}{1 + c_1X + 2c_3Z - (c_2X^2 + 2c_4XZ + 3c_6Z^2)}. \end{aligned}$$

The term $3X^2$ dominates the numerator, while the term 1 dominates the numerator. It follows that

$$\|M\|_2 \leq 2^{-2}.$$

Hence

$$\|D\|_2 = \|Z - MX\|_2 \leq 2^{-3}.$$

The tangent meets $\mathcal{E}$ where

$$\begin{aligned}(MX+D)&(1+c_1X+c_3(MX+D))\\ &= X^3+c_2X^2(MX+D)+c_4X(MX+D)^2+c_6(MX+D)^3.\end{aligned}$$

Thus if the tangent meets $\mathcal{E}$ again at (X_2, Z_2) then

$$\begin{aligned}2X+X_2 &= -\frac{\text{coeff of } X^2}{\text{coeff of } X^3}\\ &= \frac{c_1M+c_3M^2-(c_2+2c_4M+3c_6M^2)D}{1+c_2M+c_4M^2+c_6M^3}.\end{aligned}$$

Hence

$$\|X_2\|_2 \le 2^{-2}.$$

Since

$$\|Z_2\| = \|MX_2+D\| \le 2^{-4},$$

it follows that

$$(X_2, Z_2) \in \mathcal{E}_{(2^2)}.$$

We conclude that

$$2P = -(X_2, Z_2) \in \mathcal{E}_{(2^2)},$$

since $\mathcal{E}_{(2^2(}$ is a subgroup of $\mathcal{E}$. ◁

Now suppose $P = (x, y) \in \mathcal{E}(\mathbb{Q})$ is of finite order.

For each odd prime p,

$$P \notin \mathcal{E}_{(p)}$$

by Lemma 3. Thus

$$x, y \in \mathbb{Z}_p$$

by Lemma 2.

Since $2P$ is of finite order,

$$P \in \mathcal{E}_{(2)} \Longrightarrow 2P \in \mathcal{E}_{(2^2)} \Longrightarrow 2P = 0,$$

by Lemmas 4 and 3. Thus if $2P \neq 0$ then

$$x, y \in \mathbb{Z}_2,$$

by Lemma 2.

Putting these results together, we conclude that either $2P = 0$ or else

$$x, y \in \mathbb{Z}_p \text{ for all } p \Longrightarrow x, y \in \mathbb{Z}.$$

◀

Corollary *If $P = (x, y)$ is a point of finite order on the elliptic curve*

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

then $x, y \in \mathbb{Z}$.

Proof ▶ After the Proposition we need only consider the case

$$2P = 0 \Longrightarrow y = 0 \Longrightarrow x^3 + ax^2 + bx + c = 0.$$

Since a rational root of a monic polynomial with integral coefficients is necessarily integral, it follows that $x \in \mathbb{Z}$. ◀

Recall that if $P = (x, y)$ is a point of

$$\mathcal{E}(\mathbb{Q}) : y^2 + c_1xy + c_3y = x^3 + c_2x^2 + c_4x + c_6$$

then

$$-P = (x, -y - c_1x - c_3).$$

For by definition, $-P$ is the point where the line OP meets the curve again. But the lines through O are just the lines

$$x = c$$

parallel to the y-axis (together with the line $Z = 0$ at infinity). This is clear if we take the line in homogeneous form

$$lX + mY + nZ = 0.$$

This passes through $O = [0, 1, 0]$ if $m = 0$, giving

$$x = X/Z = -n/l.$$

Thus $-P$ is the point with the same x-coordinate as P, say

$$-P = (x, y_1).$$

But y, y_1 are the roots of the quadratic

$$y^2 + y(c_1x + c_3) - (x^3 + c_2x^2 + c_4x + c_6).$$

Hence

$$y + y_1 = -(c_1x + c_3),$$

ie

$$y_1 = -y - c_1 x - c_3.$$

It follows that

$$\begin{aligned} 2P = 0 &\iff -P = P \\ &\iff y = -y - c_1 x - c_3 \\ &\iff 2y + c_1 x + c_3 = 0. \end{aligned}$$

Example: Consider the curve

$$\mathcal{E}(\mathbb{Q}) : y^2 + xy = x^3 + 4x^2 + x.$$

If $P = (x, y)$ is of order 2 then

$$2y + x = 0.$$

This meets the curve where

$$x^2/4 - x^2/2 = x^3 + 4x^2 + x,$$

ie

$$4x^3 + 17x^2 + 4x = 0.$$

This has roots $0, -1/4, -4$. Thus the curve has three points of order 2, namely $(0, 0), (-1/4, 1/8), (4, 2)$.

6.4 Points of Finite Order are Small

Theorem 6.2 (Nagell-Lutz) *Suppose $P = (x, y)$ is a point of finite order on the elliptic curve*

$$\mathcal{E}(\mathbb{Q}) : y^2 = x^3 + ax^2 + bx + c \qquad (a, b, c \in \mathbb{Z}).$$

Then $x, y \in \mathbb{Z}$; and either $y = 0$ or

$$y^2 \mid 3D,$$

where

$$D = 4a^3c - a^2b^2 - 18abc + 4b^3 + 27c^2$$

is the discriminant of $f(x) = x^3 + ax^2 + bx + c$.

Moreover, if $3 \mid a$ (in particular if $a = 0$) then either $y = 0$ or

$$y^2 \mid D.$$

Proof ▶ Suppose $P = (x, y)$ has finite order. We know that $x, y \in \mathbb{Z}$.

We start by proving the weaker result (sometimes known as the *weak Nagell-Lutz Theorem*) that either $y = 0$ or

$$y \mid D,$$

since this brings out the basic idea in a simpler form.

Let $2P = (x_2, y_2)$. Since P is of finite order so is $2P$. Hence by Proposition ,

$$x_2, y_2 \in \mathbb{Z}.$$

Recall that the resultant $R(f, g)$ of two polynomials

$$f(x) = a_0 x^m + a_1 x^{m-1} + \cdots + a_m, \; g(x) = b_0 x^n + b_1 x^{n-1} + \cdots + b_n$$

is the determinant of the $(m + n) \times (m + n)$ matrix

$$\mathbf{R}(f, g) = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_m & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_{m-1} & a_m & \dots & 0 \\ & & & \dots & & & & \\ 0 & 0 & 0 & \dots & & \dots & a_{m-1} & a_m \\ b_0 & b_1 & b_2 & \dots & b_n & 0 & \dots & 0 \\ 0 & b_0 & b_1 & \dots & b_{n-1} & b_n & \dots & 0 \\ & & & \dots & & & & \\ 0 & 0 & 0 & \dots & & \dots & b_{n-1} & b_n \end{pmatrix}$$

We saw earlier that $R(f, g) = 0$ is a necessary and sufficient condition for $f(x), g(x)$ to have a root in common. Our present use of the resultant, though related, is more subtle.

Lemma 1 *Suppose $f(x), g(x) \in \mathbb{Z}[x]$. Then there exist polynomials $u(x), v(x) \in \mathbb{Z}[x]$ such that*

$$u(x)f(x) + v(x)g(x) = R(f, g).$$

Proof of Lemma ▷ Let us associate to the polynomials

$$u(x) = c_0 x^{n-1} + c_1 x^{n-2} + \cdots + c_{n-1}, \; v(x) = d_0 x^{m-1} + d_1 x^{m-2} + \cdots + d_{m-1}$$

(of degrees $< n$ and $< m$) the $(m+n)$-vector

$$\begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \\ d_0 \\ d_1 \\ \vdots \\ d_{m-1} \end{pmatrix}.$$

It is readily verified that if

$$u(x)f(x) + v(x)g(x) = e_0 x^{m_n - 1} + \cdots + e_{m+n-1},$$

then the e_k are given by the vector equation

$$\mathbf{R}(f,g) \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \\ d_0 \\ d_1 \\ \vdots \\ d_{m-1} \end{pmatrix} = \begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{m+n-1} \end{pmatrix}.$$

Thus we are looking for integers c_i, d_j such that

$$\begin{pmatrix} e_0 \\ e_1 \\ \vdots \\ e_{m+n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ R(f,g) \end{pmatrix}$$

The existence of such integers follows at once from the following Sublemma. (For simplicity we prove the result with $\det A$ as first coordinate rather than last; but it is easy to see that this does not matter.)

Sublemma *Suppose A is an $n \times n$-matrix with integer entries. Then we can find a vector v with integer entries such that*

$$A \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} \det A \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Proof of Lemma ▷ On expanding $\det A$ by its first column,

$$\det A = a_{11}A_{11} + a_{21}A_{21} + \cdots + a_{n1}A_{n1},$$

where the A_{i1}'s are the corresponding co-factors. On the other hand, if $i \neq n$ then

$$a_{1i}A_{11} + a_{2i}A_{21} + \cdots + a_{ni}A_{n1} = 0,$$

since this is the determinant of a matrix with two identical columns.

Thus the vector

$$v = \begin{pmatrix} A_{11} \\ A_{21} \\ \vdots \\ A_{n1} \end{pmatrix}$$

has the required property. ◁

◁

We apply this Lemma to the polynomials $f(x), f'(x)$, recalling that

$$R(f, f') = -D(f).$$

It follows that we can find polynomials $u(x), v(x) \in \mathbb{Z}[x]$ such that

$$u(x)f(x) + v(x)f'(x) = D.$$

Hence

$$y \mid f(x), f'(x) \Longrightarrow y \mid D.$$

Turning now to the full result, suppose as before that $P = (x, y)$ is of finite order, and that $2P = (x_2, y_2)$. We know that $x, y, x_2, y_2 \in \mathbb{Z}$.

Lemma 2 *The x-coordinate of $2P$ is*

$$\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4y^2}.$$

Proof of Lemma ▷ Let $x_2 = x(2P)$. Recall that

$$2x + x_2 = m^2 - a,$$

where

$$m = \frac{f'(x)}{2y}.$$

Thus

$$x_2 = \frac{f'(x)^2}{4y^2} - (2x + a).$$

Now

$$y^2 = f(x).$$

Hence

$$x_2 = \frac{g(x)}{4y^2},$$

where

$$\begin{aligned} g(x) &= f'(x)^2 - 4(2x + a)f(x) \\ &= (3x^2 + 2ax + b)^2 - 4(2x + a)(x^3 + ax^2 + bx + c) \\ &= x^4 - 2bx^2 - 8cx + (b^2 - 4ac). \end{aligned}$$

$\triangleleft$

It follows from the lemma that

$$y^2 \mid g(x);$$

Thus

$$y^2 \mid f(x), g(x)$$

since $y^2 = f(x)$.

Now let us assume that $a = 0$. In that case

$$f(x) = x^3 + ax^2 + bx + c, \; g(x) = x^4 - 2bx^2 - 8cx + b^2.$$

(Observe that $g(x) = (x^2 - b)^2 - 8cx$. This is an easy way to remember the formula for $x(2P)$ when $a = 0$; and it will also have some relevance later, in the proof of Mordell's Theorem.)

Lemma 3 *If $a = 0$ then there exist polynomials $u(x), v(x) \in \mathbb{Z}[x]$ of degrees $3, 2$ such that*

$$u(x)f(x) + v(x)g(x) = D.$$

Proof of Lemma $\triangleright$ Let us see if we can find $u(x), v(x) \in \mathbb{Q}[x]$ of the form

$$u(x) = x^3 + Bx + C, \qquad v(x) = x^2 + D$$

(with $B, C, D \in \mathbb{Q}$) such that

$$u(x)f(x) - v(x)g(x) = \text{const}.$$

The coefficients of x^6 and x^5 on the left both vanish. Equating the coefficients of x^4, x^3, x^2, x yields

$$\begin{array}{lll} x^4: & b + B = -2b + D & \Longrightarrow D = B + 3b \\ x^3: & c + C = -8c & \Longrightarrow C = -9c \\ x^2: & Bb = b^2 - 2Db & => b = 0 \text{ or } 2D + B = b \\ x: & Bc + Cb = -8Dc & \Longrightarrow B - 9b = -8D. \end{array}$$

If $b = 0$ then $D = B = 0$. Otherwise, substituting for D in the third equation gives

$$B = -5b/3, \qquad D = 4b/3$$

(which also holds if $b = 0$). The final equation then reduces to

$$-5b/3 - 9b = -32b/3,$$

which is an identity.

Multiplying by 3 (to make the coefficients integral),

$$u(x) = 3x^3 - 5bx - 27c, \qquad v(x) = 3x^2 + 4b;$$

yielding

$$u(x)f(x) - v(x)g(x) = -27c^2 - 4b^2 = D,$$

as required $\triangleleft$

Remarks:

1. For any polynomials $f(x), g(x) \in \mathbb{Z}[x]$, the integers $m \in Z$ for which there exist $u(x), v(x) \in \mathbb{Z}[x]$ such that

   $$u(x)f(x) - v(x)g(x) = m$$

   form an ideal in $\mathbb{Z}$. Accordingly there is a least integer, say $S = S(f, g)$, such that m has this property if and only if $S \mid m$.

   We saw in Lemma 1 that the resultant $R(f, g)$ has this property. Accordingly,

   $$S(f, g) \mid R(f, g).$$

   We know of course that $f(x), g(x)$ have a factor in common if and only if $R(f, g) = 0$. Note that it doesn't matter here whether one is speaking of factors in $\mathbb{Q}[x]$ or $\mathbb{Z}[x]$; since $Z[x]$ is a unique factorisation domain it follows easily that if $f(x), g(x) \in \mathbb{Z}[x]$ have a common factor $d(x) \in \mathbb{Q}[x]$ — which we may take to be monic — then $md(x)$ is a common factor in $\mathbb{Z}[x]$, where m is the *lcm* of the denominators of the coefficients of $d(x)$, ie the smallest integer such that $md(x) \in \mathbb{Z}[x]$.

2. Turning to our polynomials $f(x), g(x)$, it is clear that these do not have a factor in common, since

$$g(x) = f'(x)^2 - (2x + a)f(x).$$

So an irreducible common factor of $f(x), g(x)$ would also be a factor of $f'(x)$, in which case $f(x)$ would have a double root, excluded in the definition of an elliptic curve. Thus $R(f, g) \neq 0$.

In fact it is a straightforward if lengthy task to show that

$$R(f, g) = D^2;$$

so Lemma 1 would not have given us the stronger result we are looking for.

3. It is not entirely clear (to me at least) *why* $S(f, g) = D$ rather than D^2.

Nor is it clear to me why $u(x), v(x)$ have the special form above, with the coefficients of x^2 in $u(x)$ and x in $v(x)$ both 0.

The result now follows as before; since $x, y \in \mathbb{Z}$,

$$y^2 \mid f(x), g(x) \Longrightarrow y^2 \mid D.$$

It remains to consider the general case, when $a \neq 0$.
Let

$$f_0(x) = f(x - a/3),\ g_0(x) = g(x - a/3),$$

so that

$$f_0(x) = x^3 + b'x + c'.$$

It follows from the identity

$$(x - a/3)^3 + a(x - a/3)^2 + b(x - a/3) + c = x^3 + b'x + c',$$

that

$$b' = b - a^2/3,\ c' = c - ab/3 + 2a^3/27.$$

From the result we established when $a = 0$,

$$u_0(x)f_0(x) - v_0(x)g_0(x) = -(4b'^3 + 27c'^2) = D,$$

where

$$u_0(x) = 3x^3 - 5b'x - 27c', \qquad v(x) = 3x^2 + 4b'.$$

Substituting $x + a/3$ for x,

$$u_0(x + a/3)f(x) - v_0(x + a/3)g(x) = D.$$

But

$$\begin{aligned}
u_0(x + a/3) &= 3(x + a/3)^3 - 5b'(x + a/3) - 27c' \\
&= 3(x + a/3)^3 - 5(b - a^2/3)(x + a/3) - (27c - 9ab + 2a^3) \\
&= 3x^3 + ax^2 + \frac{1}{3}(a^2 - 15b - 5a^2)x + \frac{1}{9}(a^3 + 5a^3) - (27c - 9ab + 2a^3) \\
&= \frac{1}{3}\left(9x^3 + 3ax^2 + (a^2 - 15b - 5a^2)x + (8a^3 - 54c + 18ab)\right),
\end{aligned}$$

while

$$\begin{aligned}
v_0(x + a/3) &= 3(x + a/3)^2 + 4b' \\
&= 3x^2 + 2ax + a^2/3 + 4b - 4a^2/x \\
&= 3x^2 + 2ax + (4b - a^2).
\end{aligned}$$

Multiplying by 3,

$$u(x)f(x) - v(x)g(x) = 3D,$$

where

$$u(x) = 9x^3+3ax^2+(a^2-15b-5a^2)x+(8a^3-54c+18ab),\ v(x) = 9x^2+6ax+3(4b-a^2).$$

It follows as before that

$$y^2 \mid 3D.$$

Finally, we observe that if $3 \mid a$ then $b', c' \in \mathbb{Z}$, ie we can reduce the equation to the form $y^2 = x^3 + b'x + c$ without introducing fractions, so our previous argument shows that

$$y^2 \mid D.$$

◂

6.5 Examples

In these examples we compute the torsion group F of various elliptic curves $\mathcal{E}(\mathbb{Q})$.

1. We look first at the curve

$$\mathcal{E}(\mathbb{Q}) : y^2 = x^3 + 1.$$

Recall that the discriminant of the polynomial

$$f(x) = x^3 + bx + c$$

is

$$D = -\left(4b^3 + 27c^2\right).$$

Thus in the present case

$$D = -27.$$

It follows from Nagell-Lutz (Theorem 6.2) that

$$y = 0, \pm 1, \pm 3.$$

There is just one point of order 2, ie with $y = 0$, namely $(-1, 0)$.

If $y = \pm 1$ then $x = 0$, giving the two points $(0, \pm 1)$.

If $y = \pm 3$ then $x^3 = 8$, giving the two points $(2, \pm 3)$.

It remains to determine which of these points $(0, \pm 1), (2, \pm 3)$ are of finite order – remembering that the Nagell-Lutz condition $y^2 \mid D$ is *necessary* (if $y \neq 0$) but by no means *sufficient*.

The tangent at $P = (0, 1)$ has slope

$$m = \frac{p'(x)}{2y} = \frac{3x^2}{2y} = 0.$$

Thus the tangent at P is

$$y = 1.$$

This meets $\mathcal{E}$ where

$$x^3 = 0,$$

ie thrice at P. In other words P is a flex, and so of order 3.

Turning to the point $(2, 3)$ we have

$$m = \frac{3x^2}{2y} = 2.$$

and so the tangent at this point is

$$y = 2x - 1,$$

which meets $\mathcal{E}$ again at $(0, -1)$. Thus

$$2(2, 3) = -(0, -1) = (0, 1).$$

We conclude that $(2, 3)$ (and $(2, -3) = -(2, 3)$) are of order 6, and

$$F = \mathbb{Z}/(6).$$

2. Consider the curve
$$\mathcal{E}(\mathbb{Q}) : y^2 = x^3 - 1.$$

   Again, $D = -27$, and there is one point $(1, 0)$ of order 2.

   But now

$$\begin{aligned} y = \pm 1 &\implies x^3 = 2, \\ y = \pm 3 &\implies x^3 = 10, \end{aligned}$$

   neither of which has solutions in $\mathbb{Z}$. We conclude that

$$F = \mathbb{Z}/(2).$$

3. Suppose F is the torsion subgroup of

$$\mathcal{E}(\mathbb{Q}) : y^2 = x^3 + x$$

   We have
$$D = -4,$$

   and so
$$y = 0, \pm 1, \pm 2.$$

   There is just one point of order 2, ie with $y = 0$, namely $(0, 0)$.

   If $y = \pm 1$ then
$$x^3 + x - 1 = 0.$$

   Note that *a rational root* $\alpha \in \mathbb{Q}$ *of a monic polynomial*

$$x^n + a_2 x^{n-1} + \cdots + a_n$$

   with integral coefficients $a_i \in \mathbb{Z}$ *is necessarily integral:* $\alpha \in \mathbb{Z}$. And evidently $\alpha \mid a_n$. Thus in the present case the only possible rational roots of the equation are $x = \pm 1$; and neither of these is in fact a root.

   If $y = \pm 2$ then
$$x^3 + x - 4 = 0.$$

The only possible solutions to this are $x = \pm 1, \pm 2, \pm 4$; and it is readily verified that none of these is in fact a solution.

We conclude that

$$F = \mathbb{Z}/(2).$$

4. Consider the curve

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

This curve is singular, since $f(x) = x^3 - x^2$ has a double root, (and so $D = 0$). Thus it is not an elliptic curve, and so is outside our present study, although we shall say a little about singular cubic curves in the next Chapter.

5. Consider the curve

$$\mathcal{E}(\mathbb{Q}) : y^2 - y = x^3 - x.$$

This has 6 obvious integral points, namely $(0,0), (0,1), (1,0), (1,1), (-1,0), (-1,1)$.

We can bring the curve to standard form by setting $y_1 = y - 1/2$, ie $y = y_1 + 1/2$, to complete the square on the left. The equation becomes

$$y_1^2 = x^3 - x + 1/4.$$

Now we can make the coefficients integral by the transformation

$$y_2 = 2^3 y_1, \ x_2 = 2^2 x,$$

giving

$$y_2^2 = x_2^3 - 2^4 x_2 + 2^6/4,$$

since the coefficient of x has weight 4, while the constant coefficient has weight 6. (In practice it is probably easier to apply this transformation first, and then complete the square; that way our coefficients always remain integral.) Our new equation is

$$y_2^2 = x_2^3 - 16x_2 + 16,$$

with discriminant

$$\begin{aligned} D &= -(4 \cdot 2^{12} + 27 \cdot 2^8) \\ &= -2^8(64 + 27) \\ &= -2^8 91. \end{aligned}$$

By Nagell-Lutz, if $(x_2, y_2) \in F$ then $x_2, y_2 \in \mathbb{Z}$ and

$$y_2 = 0, \pm 1, \pm 2, \pm 4, \pm 8, \pm 16.$$

Note however that if P is not of order 2, ie $y_2 \neq 0$, then

$$y = \frac{y_2 - 4}{8} \in \mathbb{Z}$$

by Theorem 6.2. Only the cases $y_2 = \pm 4$ satisfy this condition. Thus we only have to consider

$$y_2 = 0, \pm 4.$$

If $y_2 = 0$ then

$$x_2^3 - 16x_2 + 16 = 0.$$

But

$$\begin{aligned} 16 \mid x_2^3 &\implies 4 \mid x_2 \\ &\implies 32 \mid x_2^3, 16x_2 \\ &\implies 32 \mid 16, \end{aligned}$$

which is absurd. Thus there are no points of order 2 on $\mathcal{E}$.

Finally, if $y_2 = \pm 4$ then

$$16 = x_2^3 - 16x_2 + 16 \implies x_2^3 - 16x_2 = 0 \implies x_2 = 0, \pm 4.$$

This gives the 6 'obvious' points we mentioned at the beginning.

It remains to determine which of these points are of finite order.

Reverting to the original equation, suppose $P = (0, 0)$. We have

$$(2y - 1)\frac{dy}{dx} = 3x^2 - 1,$$

ie

$$\frac{dy}{dx} = \frac{3x^2 - 1}{2y - 1}.$$

Thus the tangent at P has slope $m = 1$, and so is

$$y = x.$$

This meets the curve again at $(1, 1)$. Hence

$$2(0, 0) = -(1, 1) = (1, 0).$$

The tangent at $(1,0)$ has slope $m = -2$, and so is

$$y = -2x + 2,$$

which meets $\mathcal{E}$ where

$$(-2x+2)^2 - x(-2x+2) = x^3 - x,$$

ie

$$x^3 - 6x^2 + 9x - 4 = 0.$$

We know this has two roots equal to 1. The third root must satisfy

$$2 + x = 6,$$

ie

$$x = 4.$$

At this point

$$y = -2x + 2 = -6.$$

We know that this point $(4, -6)$ is not of finite order, by Nagell-Lutz. It follows that $(1,0)$ is of infinite order. Hence so is $(0,0)$ since $2(0,0) = (1,0)$; and so too are $(1,1) = -(1,0)$ and $(0,1) = -(0,0)$

It remains to consider the points $(-1, 0$ and $(-1,1) = -(-1,0)$. Note that if these are of finite order then they must be of order 3 (since there would be just 3 points in F), ie they would be flexes.

The tangent at $P = (-1,0)$ has slope $m = -2$, and so is

$$y = -2x - 2.$$

This meets $\mathcal{E}$ where

$$(-2x-1)^2 - x(-2x-1) = x^3 - x.$$

We know that this has two roots -1. Hence the third root is given by

$$-2 + x = 6,$$

ie

$$x = 8,$$

as before. At this point

$$y = -2x + 2 = -14.$$

So

$$2(-1, 0) = -(8, -14).$$

Again, we know by Nagell-Lutz that this point is of infinite order, and so therefore is $(-1, 0)$ and $(-1, 1) = -(-1, 0)$.

To verify that $P = (4, -6)$, for example, is not of finite order, we may note that the tangent at this point has slope

$$m = -\frac{47}{11}.$$

But the tangent

$$y = mx + d$$

at P meets the curve again where

$$(mx + d)^2 - x(mx + d) = x^3 - x,$$

ie at a point (x_1, y_1) with

$$2 \cdot 4 + x_1 = m^2 - m.$$

By Nagell-Lutz, $x_1 \in \mathbb{Z}$ (since we have seen that there are no points of order 2), and so $m^2 - m \in \mathbb{Z}$, which is manifestly not the case.

We conclude that the torsion-group of this curve is trivial:

$$F = \{0\}.$$