

Elliptic Curves. HT 2009/10.

This document (from the next sentence onwards) gives a close approximation of what is actually written on the board; in places, it abbreviates some optional material and proofs (the students can see these extra details in the online notes).

Prof D.R. Heath-Brown. Elliptic Curves. rhb@maths.ox.ac.uk

www.maths.ox.ac.uk → Current Students → Undergraduate Students

→ Lecture Notes and Problem Sheets → C9.1b Elliptic Curves.

Already on the webpage:

Preliminary Reading (including Sheet 0 for your own use; not for handing in).

All lecture notes.

All Problem Sheets for HT and a revision sheet for TT.

Please look through the Preliminary Reading (Section 0). I'll make free use of definitions and results from Section 0 (referred to as, e.g., Defn 0.18).

First intercollegiate class (on Sheet 1) will be in 2nd Week.

Useful extra reading:

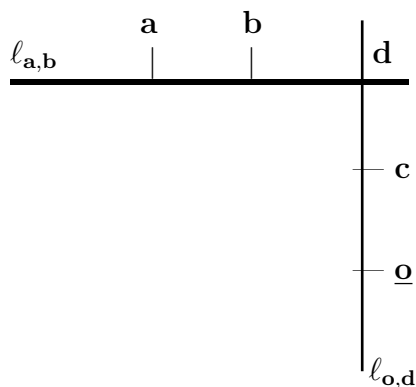
J.W.S. Cassels. Lectures on Elliptic Curves. LMS-ST 24. Cambridge University Press, Cambridge, 1991.

J.H. Silverman. The Arithmetic of Elliptic Curves. GTM 106. Springer-Verlag, 1986.

SECTION 1. THE GROUP LAW ON AN ELLIPTIC CURVE

Definition 1.1. An elliptic curve over a field K is (up to birational equivalence) a nonsingular projective cubic curve, defined over K , with a K -rational point.

Definition 1.2. Let $\mathcal{C} : F(X, Y, Z) = 0$ be an elliptic curve $/K$ [the notation $/K$ means ‘defined over K ’; that is, all of the coefficients of $\mathcal{C}$ are in the field K]. So, $\mathcal{C}$ is a nonsingular projective cubic curve, with a K -rational point, which we shall denote $\underline{o}$. For any two points $\mathbf{a}, \mathbf{b}$ on $\mathcal{C}$, let $\ell_{\mathbf{a}, \mathbf{b}}$ denote the line which meets $\mathcal{C}$ at $\mathbf{a}, \mathbf{b}$ [if $\mathbf{a}, \mathbf{b}$ are distinct then $\ell_{\mathbf{a}, \mathbf{b}}$ is the unique line through $\mathbf{a}, \mathbf{b}$; if $\mathbf{a} = \mathbf{b}$ then $\ell_{\mathbf{a}, \mathbf{b}}$ is the line tangent to $\mathcal{C}$ at $\mathbf{a} = \mathbf{b}$].



Let $\ell_{\mathbf{a}, \mathbf{b}}$ denote the line which meets $\mathcal{C}$ at $\mathbf{a}, \mathbf{b}$.

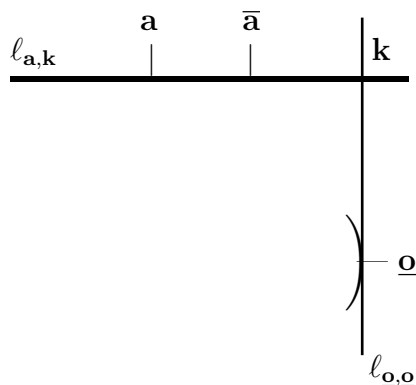
Then $\ell_{\mathbf{a}, \mathbf{b}}$ and $\mathcal{C}$ have 3 points of intersection (Bézout).

Let $\mathbf{d}$ be the third point of intersection between $\mathcal{C}$ and $\ell_{\mathbf{a}, \mathbf{b}}$.

Now, let $\ell_{\underline{o}, \mathbf{d}}$ denote the line which meets $\mathcal{C}$ at $\underline{o}$ and $\mathbf{d}$.

Let $\mathbf{c}$ be the third point of intersection between $\mathcal{C}$ and $\ell_{\underline{o}, \mathbf{d}}$.

Define $\mathbf{a} + \mathbf{b} = \mathbf{c}$.



Let $\ell_{\underline{o}, \underline{o}}$ be the line tangent to $\mathcal{C}$ at $\underline{o}$.

Let $\mathbf{k}$ be the third point of intersection between $\mathcal{C}$ and $\ell_{\underline{o}, \underline{o}}$.

Now, let $\ell_{\mathbf{a}, \mathbf{k}}$ be the line which meets $\mathcal{C}$ at $\mathbf{a}$ and $\mathbf{k}$.

Let $\bar{\mathbf{a}}$ be the third point of intersection between $\mathcal{C}$ and $\ell_{\mathbf{a}, \mathbf{k}}$.

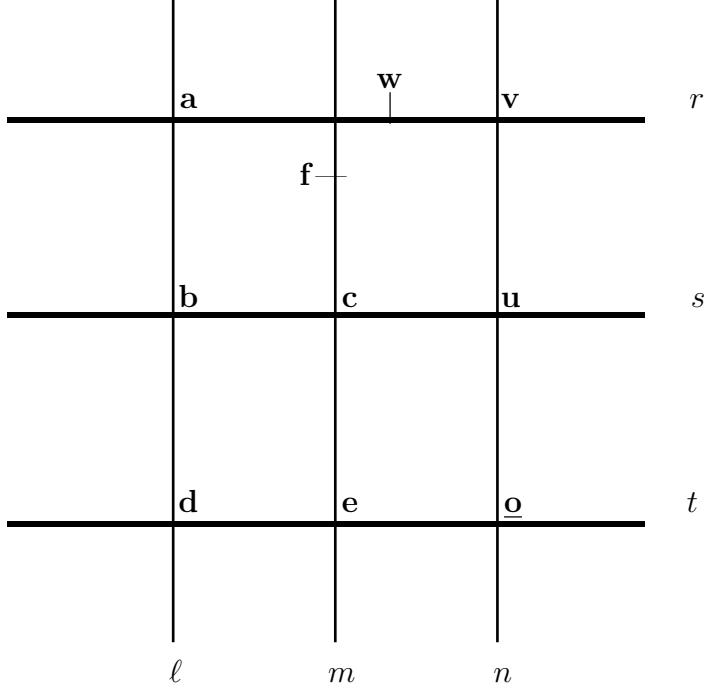
Define $-\mathbf{a}$ to be $\bar{\mathbf{a}}$.

Lemma 1.3. Let $P_1, \dots, P_8$ be such that no 4 points lie on a line and no 7 points lie on a conic. Then there exists a unique point P_9 which is a 9th point of intersection of any two cubics passing through $P_1, \dots, P_8$.

Optional Proof See 0.137.

Theorem 1.4. Let $\mathcal{C}$ be an elliptic curve $/K$, with K -rational point $\underline{o}$. Then $\mathbf{a} + \mathbf{b}$, as in Definition 1.2, gives a commutative group law on the points on $\mathcal{C}$, with identity $\underline{o}$. The inverse of $\mathbf{a}$ is given by the point $-\mathbf{a}$, constructed in in Definition 1.2. Further, the K -rational points $\mathcal{C}(K)$ form a subgroup, called the Mordell-Weil group.

Proof It is easy to show commutativity, the fact that $\underline{o}$ is the identity, and the fact that $-\mathbf{a}$ is the inverse of $\mathbf{a}$. To prove associativity, consider the following diagram.



Here, r, s, t, ℓ, m, n are lines. On each line, the labelled points are the points of intersection between $\mathcal{C}$ and that line. From Defn 1.2:

$$\mathbf{a} + \mathbf{b} = \mathbf{e},$$

and so:

$$(\mathbf{a} + \mathbf{b}) + \mathbf{c} = \text{3rd point of intersection on } \ell_{\underline{o}, \mathbf{f}}.$$

Similarly:

$$\mathbf{b} + \mathbf{c} = \mathbf{v},$$

$$\mathbf{a} + (\mathbf{b} + \mathbf{c}) = \text{3rd point of intersection on } \ell_{\underline{o}, \mathbf{w}}.$$

To show $(\mathbf{a} + \mathbf{b}) + \mathbf{c} = \mathbf{a} + (\mathbf{b} + \mathbf{c})$, it is sufficient to show that $\mathbf{f} = \mathbf{w}$. Let $F_1 = \ell mn$ and $F_2 = rst$, both of which are cubic curves.

$\mathcal{C}$ and F_1 have 8 common points: $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}, \mathbf{u}, \mathbf{v}, \underline{o}$.

$\mathcal{C}$ and F_2 also have these 8 common points: $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}, \mathbf{u}, \mathbf{v}, \underline{o}$.

From Lemma 1.3, the 9th point of intersection of $\mathcal{C}$ and F_1 must be the same as the 9th point of intersection of $\mathcal{C}$ and F_2 ; that is, $\mathbf{f} = \mathbf{w}$, as required.

Hence, $+$ is a commutative group law.

It remains to show that $\mathcal{C}(K)$ is a subgroup. We are given that $\underline{o} \in \mathcal{C}(K)$. Let $\mathbf{a}, \mathbf{b} \in \mathcal{C}(K)$. Since $\underline{o}, \mathbf{a}, \mathbf{b} \in \mathcal{C}(K)$ and $\mathcal{C}/K$, it follows that $\ell_{\mathbf{a}, \mathbf{b}}/K$ and their third point of intersection $\mathbf{d}$ is also in $\mathcal{C}(K)$; similarly, the third point of intersection of $\ell_{\underline{o}, \mathbf{d}}$ and $\mathcal{C}$ is in $\mathcal{C}(K)$, that is: $\mathbf{a} + \mathbf{b} \in \mathcal{C}(K)$. Similarly, $-\mathbf{a} \in \mathcal{C}(K)$. Hence $\mathcal{C}(K)$ is a subgroup, as required. $\square$

Comment 1.5. When two nonsingular cubics $\mathcal{C}_1, \mathcal{C}_2$ are birationally equivalent over K (under $\phi : \mathcal{C}_1 \rightarrow \mathcal{C}_2$), it can be shown that $\mathbf{a}, \mathbf{b}, \mathbf{c}$ on $\mathcal{C}_1$ are collinear iff $\phi(\mathbf{a}), \phi(\mathbf{b}), \phi(\mathbf{c})$ on $\mathcal{C}_2$ are collinear, and ϕ is an isomorphism between $\mathcal{C}_1(K)$ and $\mathcal{C}_2(K)$.

Comment 1.6. If we say ‘let $\mathcal{C} : y^2 = x^3 + 3$ be an elliptic curve’, this is always a shorthand notation for the corresponding projective curve $ZY^2 = X^3 + 3Z^3$.

Theorem 1.7. Let K be a field satisfying $\text{char}(K) \neq 2, 3$ [recall – this means that $1 + 1 \neq 0$ and $1 + 1 + 1 \neq 0$]. Then any elliptic curve over K is birationally equivalent over K to a curve of the form $y^2 = x^3 + Ax + B$.

When $K = \mathbb{Q}$, we can birationally transform any $y^2 = \text{cubic in } x$ to a curve of the form $y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}$, using only maps of the form $(x, y) \mapsto (ax + b, cy)$.

Comment 1.8. Let K be a field satisfying $\text{char}(K) \neq 2, 3$, and let $g(x)$ be a quartic polynomial over K with nonzero discriminant. It can be shown that any curve $\mathcal{D} : y^2 = g(x)$, with a K -rational point, is an elliptic curve, and is birationally equivalent over K to a curve of the form $y^2 = x^3 + Ax + B$ [see p.35 of Cassels].

Comment 1.9. We shall typically take our elliptic curves to have the form

$$\mathcal{E} : y^2 = x^3 + Ax + B, \text{ where } A, B \in K,$$

shorthand for the projective curve $ZY^2 = X^3 + AXZ^2 + BZ^3$. Sometimes it will be convenient to include the x^2 term. Since $\mathcal{E}$ is nonsingular, we must have $\Delta = 4A^3 + 27B^2 \neq 0$, as was shown in Example 0.110. The notation $\Delta = 4A^3 + 27B^2$ is standard.

We shall always choose $\mathbf{o} = (0, 1, 0)$, the point at infinity, as the identity, unless otherwise stated. For an elliptic curve $\mathcal{E}$ written in the form $y^2 = \text{cubic in } x$, the points are $\mathbf{o}$ (the point at infinity) and the affine points (x, y) , and the group law has a simpler description:

Let $\mathbf{d} = (x_3, y_3)$ the 3rd point of intersection of $\mathcal{E}$ and $\ell_{\mathbf{a}, \mathbf{b}}$.

Then $\mathbf{a} + \mathbf{b} = (x_3, -y_3)$, the reflection of $\mathbf{d}$ in the x -axis.

Also: $-(x, y) = (x, -y)$.

We illustrate the group law with the following computation (see also 0.143).

Example 1.10. Let $\mathcal{E} : y^2 = x^3 + 1$. Let us compute $\mathbf{a} + \mathbf{b}$, where $\mathbf{a} = (x_1, y_1) = (-1, 0)$ and $\mathbf{b} = (x_2, y_2) = (0, 1)$.

The line through $\mathbf{a}, \mathbf{b}$ is $\ell_{\mathbf{a}, \mathbf{b}} : y = x + 1$. Substituting this into $\mathcal{E}$, we see that the x -coordinate of any point of intersection satisfies: $(x + 1)^2 = x^3 + 1$, and so:

$$x^3 - x^2 - 2x = 0. \quad (*)$$

We are looking for (x_3, y_3) , the 3rd point of intersection of $\mathcal{E}$ and $\ell_{\mathbf{a}, \mathbf{b}}$. We first find x_3 ; note that x_1, x_2, x_3 must be the roots of $(*)$.

Method A (for finding x_3). $x^3 - x^2 - 2x = (x - x_1)(x - x_2)(x - x_3)$; equating coefficients of x^2 gives: $x_1 + x_2 + x_3 = -(\text{coefficient of } x^2 \text{ in } (*)) = -(-1) = 1$,

so that $(-1) + 0 + x_3 = 1$, giving $x_3 = 2$.

Method B (for finding x_3). Factorise $(*)$ to give: $x(x+1)(x-2)$, whose roots are: $0, -1, 2$. Two of these are the already known $x_1 = -1, x_2 = 0$, and so x_3 must be the remaining root: $x_3 = 2$.

Having found x_3 (by either method), we use $\ell_{\mathbf{a}, \mathbf{b}}$ to compute $y_3 = x_3 + 1 = 3$. In summary: $\mathcal{E}$ and $\ell_{\mathbf{a}, \mathbf{b}}$ intersect at: $(-1, 0), (0, 1), (2, 3)$, and so $(-1, 0) + (0, 1) + (2, 3) = \underline{\mathbf{o}}$.

Finally, $(-1, 0) + (0, 1) = -(2, 3) = (2, -3)$, using the rule that $-(x, y) = (x, -y)$.

One can also obtain an explicit general formula for the group law.

Lemma 1.11. *Let $\mathcal{E} : y^2 = x^3 + Ax + B$, where $A, B \in K$, with (as usual) $\underline{\mathbf{o}}$ = the point at infinity. Let $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$.*

Case 1. *When $x_1 \neq x_2$ then:*

$$x_3 = \frac{x_1x_2^2 + x_1^2x_2 + A(x_1 + x_2) + 2B - 2y_1y_2}{(x_1 - x_2)^2}, \quad y_3 = -\ell x_3 - m,$$

$$\text{where: } \ell = \frac{y_1 - y_2}{x_1 - x_2}, \quad m = \frac{x_1y_2 - x_2y_1}{x_1 - x_2}.$$

Case 2. *When $(x_1, y_1) = (x_2, y_2)$ then $(x_3, y_3) = (x_1, y_1) + (x_1, y_1)$ [which can be written as $2(x_1, y_1)$], and:*

$$x_3 = \frac{x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2}{4y_1^2} = \frac{x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2}{4(x_1^3 + Ax_1 + B)}, \quad y_3 = -\ell x_3 - m,$$

$$\text{where: } \ell = \frac{3x_1^2 + A}{2y_1}, \quad m = \frac{-x_1^3 + Ax_1 + 2B}{2y_1}.$$

Optional Proof See 0.144.

Comment 1.12. When $\Delta = 4A^3 + 27B^2 \neq 0$, all 3 roots of $x^3 + Ax + B$ are distinct, guaranteeing that $y^2 = x^3 + Ax + B$ has no singularities and is an elliptic curve.

When $\Delta = 0$, $y^2 = (x - \alpha)^2(x - \beta)$. and the set of nonsingular points on $\mathcal{E}$, denoted $\mathcal{E}_{ns}$, forms a group [see pp.39–41 of Cassels].

Definition 1.13. Let $\mathcal{E}$ be an elliptic curve and let P be a point on $\mathcal{E}$. For any positive integer m , let mP denote $P + \dots + P$ [m times]. We say that P is an m -torsion point if $mP = \underline{\mathbf{o}}$. The m -torsion group of $\mathcal{E}$, denoted $\mathcal{E}[m]$, is the set of all m -torsion points. We also say that P has *order* m (or that P is a *point of order* m) if m is the smallest positive integer for which $mP = \underline{\mathbf{o}}$. When such m exists, P is a *torsion point* (P has *finite order*). If no such m exists, then P is a non-torsion point (P has *infinite order*). The group of all K -rational torsion points on $\mathcal{E}$ is denoted $\mathcal{E}_{\text{tors}}(K)$ [or sometimes $\mathcal{E}(K)_{\text{tors}}$].

Examples 1.14.

(a) Let $\mathcal{E} : y^2 = x^3 - x$, and let $P = (1, 0)$ so that $-P = (1, -0) = (1, 0) = P$, so that $2P = P + P = P - P = \underline{0}$. But $1 \cdot P = P \neq \underline{0}$, and so 2 is the smallest $m > 0$ such that $mP = \underline{0}$. P has order 2 and $P \in \mathcal{E}_{\text{tors}}(\mathbb{Q})$.

(b) Let $\mathcal{E} : y^2 = x^3 + 1$, and let $P = (0, 1)$. First compute $P + P$. The tangent line $\ell_{P,P}$ to $\mathcal{E}$ at P is $y = 1$. Substituting $y = 1$ into $y^2 = x^3 + 1$ gives $x^3 = 0$, with roots $0, 0, 0$. So, $\mathcal{E}$ meets $\ell_{P,P}$ at $(0, 1)$ with multiplicity 3, and $(0, 1) + (0, 1) + (0, 1) = \underline{0}$. Hence: $(0, 1) + (0, 1) = -(0, 1) = (0, -1)$. In summary:

$1 \cdot (0, 1) = (0, 1), \quad 2 \cdot (0, 1) = (0, -1), \quad 3 \cdot (0, 1) = \underline{0}.$
 $(0, 1)$ has order 3 and $(0, 1) \in \mathcal{E}_{\text{tors}}(\mathbb{Q})$.

When $K = \mathbb{F}_p$, a finite field with p elements, there are of course only finitely many members of $\mathcal{E}(\mathbb{F}_p)$.

Theorem 1.15. (*Hasse*). *Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_p$. Let $N_p = \#\mathcal{E}(\mathbb{F}_p)$ where, as usual, $\mathcal{E}(\mathbb{F}_p)$ should be taken to including $\underline{0}$ [so that N_p is the number of affine points (x, y) on $\mathcal{E}$ with $x, y \in \mathbb{F}_p$, plus 1, to include the point at infinity $\underline{0}$]. Then:*

$$|N_p - (p + 1)| \leq 2\sqrt{p}, \text{ that is, } N_p \in [(p + 1) - 2\sqrt{p}, (p + 1) + 2\sqrt{p}].$$

Similarly, any curve $y^2 = Q(x)$, where $Q(x) = f_4x^4 + \dots + f_0$ has nonzero discriminant, has at least $p - 1 - 2\sqrt{p}$ affine points.

Proof See p.118 of Cassels or p.131 of Silverman. □

Example 1.16. Let $\mathcal{E} : y^2 = x^3 + 4x + 1$, defined over $\mathbb{F}_{13}$. Then:

$$\#\mathcal{E}(\mathbb{F}_{13}) \geq 13 + 1 - 2\sqrt{13} > 6, \text{ so that } \#\mathcal{E}(\mathbb{F}_{13}) \geq 7.$$

$$\text{Similarly, } \#\mathcal{E}(\mathbb{F}_{13}) < 22, \text{ so that } \#\mathcal{E}(\mathbb{F}_{13}) \leq 21.$$

Note that at most 4 of the points on $\mathcal{E}(\mathbb{F}_{13})$ can be $\underline{0}$ and points of the form $(x, 0)$, so there must exist at least 3 affine points $(x, y) \in \mathcal{E}(\mathbb{F}_{13})$ with $y \neq 0$.

SECTION 2. THE p -ADIC NUMBERS $\mathbb{Q}_p$

For $\mathbb{Q}$, let $|\cdot|_\infty$ denote the standard absolute value [e.g. $|-5|_\infty = |5|_\infty = 5$]. Consider the sequence: $x_1 = 1.4, x_2 = 1.41, x_3 = 1.414, \dots$, where x_n is the largest decimal to n decimal places satisfying $x_n^2 < 2$. Then $|x_m - x_n|_\infty \rightarrow 0$ as $m, n \rightarrow \infty$, so that the sequence is Cauchy in $\mathbb{Q}, |\cdot|_\infty$. The sequence x_n cannot be convergent, since if $x_n \rightarrow \alpha$ then clearly $\alpha^2 = 2$ and no such α exists in $\mathbb{Q}$.

We say that $\mathbb{Q}, |\cdot|_\infty$ is *incomplete* (since not every Cauchy sequence is convergent) and the real numbers $\mathbb{R}$ give the *completion* of $\mathbb{Q}, |\cdot|_\infty$. The absolute value $|\cdot|_\infty$ is a special case of the following.

Definition 2.1. Let K be a field. A *valuation* on K is a function $|\cdot| : K \rightarrow \mathbb{R}$ satisfying:

- (1) $|x| \geq 0$ for all $x \in K$, with equality if and only if $x = 0$.
- (2) $|xy| = |x| \cdot |y|$ for all $x, y \in K$.
- (3) $|x + y| \leq |x| + |y|$ for all $x, y \in K$ [the *triangle inequality*].

If a valuation also satisfies the stronger property:

- (3)' $|x + y| \leq \max(|x|, |y|)$, for all $x, y \in K$,

then we say that it is a *non-Archimedean valuation*; otherwise it is an *Archimedean valuation*.

For example, $\mathbb{Q}, |\cdot|_\infty$ (or $\mathbb{R}, |\cdot|_\infty$) is a valuation. It is Archimedean since, for example, $|1 + 1|_\infty \not\leq \max(|1|_\infty, |1|_\infty)$.

Definition 2.2. Fix a prime p . Let $x = \frac{m}{n} \in \mathbb{Q}$. Write $\frac{m}{n} = p^r \frac{a}{b}$, where $p \nmid a, p \nmid b$. Then the *p -adic valuation* (or *p -adic absolute value* or *p -adic size*) is defined to be:

$$|x|_p = \left| \frac{m}{n} \right|_p = p^{-r} \text{ [so, } x \text{ is 'smaller' the higher the power of } p \text{ dividing } x].$$

We also define $|0|_p = 0$. For any $x, y \in \mathbb{Q}$, the *p -adic distance* between x and y is defined to be: $d_p(x, y) = |x - y|_p$. (Note that d_p is a metric)

Example 2.3. In $\mathbb{Q}, |\cdot|_3$, we have: $|\frac{4}{3}|_3 = |3^{-1} \frac{4}{1}|_3 = (3^{-(-1)}) = 3$, $|9|_3 = |3^2 \frac{1}{1}|_3 = 3^{-2} = \frac{1}{9}$, and $|\frac{7}{1}|_3 = |3^0 \frac{7}{1}|_3 = 3^{-0} = 1$.

Also, $d_3(-5, 3) = |-5 - 3|_3 = |-8|_3 = 1$, $d_3(-5, 19) = |-5 - 19|_3 = |-24|_3 = 3^{-1}$ and $d_3(\frac{1}{2}, \frac{1}{5}) = |\frac{3}{10}|_3 = 3^{-1}$.

For integers $m, n, m \not\equiv n \pmod{3} \iff d_3(m, n) = 1, m \equiv n \pmod{3} \iff d_3(m, n) \leq \frac{1}{3}$, $m \equiv n \pmod{3^2} \iff d_3(m, n) \leq \frac{1}{3^2}$, and so on.

Lemma 2.4. The function $|\cdot|_p$ of Definition 2.2 is a non-Archimedean valuation on $\mathbb{Q}$.

Proof (1), (2), (3)' are trivially true when x or $y = 0$. Let $x, y \in \mathbb{Q}, x, y \neq 0$, and write $x = p^r \frac{a}{b}, y = p^s \frac{c}{d}$, where $p \nmid a, b, c, d$.

$$(1) |x|_p = p^{-r} > 0.$$

$$(2) |xy|_p = |p^r \frac{a}{b} p^s \frac{c}{d}|_p = |p^{r+s} \frac{ac}{bd}|_p = p^{-(r+s)} \text{ [since } p \nmid ac, bd] = p^{-r} p^{-s} = |x|_p |y|_p.$$

(3)' Wlog $r \leq s$, giving: $|x + y|_p = |p^r \frac{a}{b} + p^s \frac{c}{d}|_p = |p^r (\frac{a}{b} + p^{s-r} \frac{c}{d})|_p = |p^r \frac{ad + p^{s-r}bc}{bd}|_p$
 $= |p^r \frac{p^k \ell}{bd}|_p$ for some $k \geq 0$ and $\ell \in \mathbb{Z}$ with $p \nmid \ell$ [since $ad + p^{s-r}bc \in \mathbb{Z}$]
 $= p^{-(r+k)} \leq p^{-r} = |x|_p = \max(|x|_p, |y|_p)$. $\square$

Comment 2.5. By induction, $|a_1 + \dots + a_n|_p \leq \max(|a_1|_p, \dots, |a_n|_p)$. It is also easy to show that $|x|_p \neq |y|_p \implies |x + y|_p = \max(|x|_p, |y|_p)$. Furthermore, if $|a_k| > |a_i|_p$ for all i , $1 \leq i \leq n, i \neq k$, then $|a_1 + \dots + a_n|_p = \max(|a_1|_p, \dots, |a_n|_p)$.

Definition 2.6. Let $K, | \cdot |$ be a field with valuation. For $a_n, \ell \in K$, we say that the sequence a_n converges to ℓ [denoted $a_n \rightarrow \ell$] in $K, | \cdot |$ when $|a_n - \ell| \rightarrow 0$ in $\mathbb{R}, | \cdot |_\infty$ as $n \rightarrow \infty$. That is: for any $\epsilon > 0$ there exists $N \in \mathbb{N}$ such that, $|a_n - \ell| < \epsilon$ for all $n > N$. Given a sequence $a_n \in K$, if there exists $\ell \in K$ such that $a_n \rightarrow \ell$ in $K, | \cdot |$ then we say that a_n converges in $K, | \cdot |$, or that it is convergent in $K, | \cdot |$. It is *Cauchy* if $|a_m - a_n| \rightarrow 0$ in $\mathbb{R}, | \cdot |_\infty$ as $m, n \rightarrow \infty$. That is: for any $\epsilon > 0$ there exists $N \in \mathbb{N}$ such that, $|a_m - a_n| < \epsilon$ for all $m, n > N$.

We say that $K, | \cdot |$ is *complete* if every Cauchy sequence is convergent.

Examples 2.7.

(a) Let $a_n = 6^n$. Then $|a_n - 0|_3 = |6^n|_3 = 3^{-n} \rightarrow 0$ as $n \rightarrow \infty$. So $a_n \rightarrow 0$ in $\mathbb{Q}, | \cdot |_3$.

(b) Let $a_1 = 1, a_2 = 11, a_3 = 111, \dots$ so that $9a_n = 999\dots 9$ [n times] and $9a_n + 1 = 10^n$. Then $|9a_n - (-1)|_5 = |10^n|_5 = 5^{-n} \rightarrow 0$, giving $9a_n \rightarrow -1$ in $\mathbb{Q}, | \cdot |_5$. It follows that $a_n \rightarrow -\frac{1}{9}$ in $\mathbb{Q}, | \cdot |_5$.

(c) Let $x_0 = a_0 = 3$. Then $a_0^2 = 9 \equiv 2 \pmod{7}$, and $|x_0^2 - 2|_7 = |a_0^2 - 2|_7 = |7|_7 = 7^{-1} < 1$. We want to find $a_1 \in \{0, \dots, 6\}$ such that $(a_0 + a_1 7)^2 \equiv 2 \pmod{7^2}$.

$$\text{This is satisfied} \iff a_0^2 + 2a_0 a_1 7 + a_1^2 7^2 \equiv 2 \pmod{7^2}$$

$$\iff 6a_1 7 \equiv 2 - 9 = -7 \pmod{7^2} \iff 6a_1 \equiv -1 \pmod{7} \iff a_1 \equiv 1 \pmod{7},$$

so we can take $a_1 = 1$. Let $x_1 = a_0 + a_1 7 = 3 + 1 \times 7 = 10$. Then $x_1^2 = 100 \equiv 2 \pmod{7^2}$ and $|x_1^2 - 2|_7 = 7^{-2}$.

Similarly $x_2 = a_0 + a_1 7 + a_2 7^2 = 3 + 1 \times 7 + 2 \times 7^2 = 108$ satisfies $x_2^2 \equiv 2 \pmod{7^3}$ and $|x_2^2 - 2|_7 \leq 7^{-3}$.

We can inductively find $x_n = a_0 + a_1 7 + \dots + a_n 7^n$ such that $x_n^2 \equiv 2 \pmod{7^{n+1}}$, that is, $|x_n^2 - 2|_7 \leq 7^{-(n+1)}$. Hence $x_n^2 \rightarrow 2$ in $\mathbb{Q}, | \cdot |_7$.

Intuitively, $(3 + 1 \cdot 7 + 2 \cdot 7^2 + \dots)^2 = 2$ in $| \cdot |_7$. The sequence x_n is easily seen to be Cauchy in $\mathbb{Q}, | \cdot |_7$. The sequence is not convergent since if $x_n \rightarrow \alpha$ in $\mathbb{Q}, | \cdot |_7$ then $\alpha^2 = 2$, which is impossible for $\alpha \in \mathbb{Q}$.

(d) Again, let $a_0 = 3$, but now define $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)} = a_n - \frac{a_n^2 - 2}{2a_n}$, for $n \geq 0$, where $f(x) = x^2 - 2$ [the Newton-Raphson formula]. Then:

$$a_0 = 3, a_1 = \frac{11}{6}, a_2 = \frac{193}{132}, \dots$$

Again (as in (c)), $|a_n^2 - 2|_7 \leq 7^{-(n+1)}$ so that $a_n^2 \rightarrow 2$ in $\mathbb{Q}_7$, again forcing a_n to be Cauchy but not convergent.

The last two examples show that $\mathbb{Q}$ is incomplete with respect to the valuation $|\cdot|_7$, and indeed $\mathbb{Q}$ is incomplete with respect to any $|\cdot|_p$. We now define an extension of $\mathbb{Q}$ which performs the same role with respect to $|\cdot|_p$ that $\mathbb{R}$ performs with respect to $|\cdot|_\infty$.

Definition 2.8. The set of *p-adic numbers* $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the valuation $|\cdot|_p$, and is the smallest field containing $\mathbb{Q}$ which is complete with respect to $|\cdot|_p$. For any $\alpha, \beta \in \mathbb{Q}_p$, we say that $\alpha \equiv \beta \pmod{p^n} \iff |\alpha - \beta|_p \leq p^{-n}$ [α is congruent to β modulo p^n]. A member of $\mathbb{Q}_p$ (a *p-adic number*) x can be written in following form (the *p-adic expansion* of x):

$$x = \sum_{n=N}^{\infty} a_n p^n, \text{ where } N \in \mathbb{Z}, a_N \neq 0 \text{ and each } a_n \in \{0, \dots, p-1\},$$

in which case $|x|_p = p^{-N}$, and the a_n are the *digits* of x . We normally use the shorthand notation $a_N \dots a_0, a_1 a_2 \dots$ to represent the above sum. Note that $x \in \mathbb{Q}$ exactly when the digits are eventually periodic.

Examples 2.9. (a) $w = 4 \cdot 5^{-2} + 1 \cdot 5^{-1} + 4 \cdot 5^0 + 1 \cdot 5^1 + 4 \cdot 5^2 + \dots \in \mathbb{Q}_5$ and $|w|_5 = 5^2$. This can be denoted $414, \overline{14}$.

(b) $\alpha = 3 \cdot 7^0 + 1 \cdot 7^1 + 2 \cdot 7^2 + \dots \in \mathbb{Q}_7$ from Example 2.7(c) satisfies $\alpha^2 = 2$.

(c) In $\mathbb{Q}_5$: $27 = 2 + 5^2 = 2 \cdot 5^0 + 0 \cdot 5^1 + 2 \cdot 5^2 = 2, 01$ [the 5-adic expansion of 27].

(d) Let us find the 5-adic expansion of $-1/4$. We have $|-1/4|_5 = 1$ so that the 5-adic expansion of $-1/4$ must be of the form $\alpha = a_0 + a_1 5 + a_2 5^2 + \dots$, each $a_i \in \{0, 1, 2, 3, 4\}$ and $a_0 \neq 0$. This satisfies $-1 = 4(a_0 + a_1 5 + a_2 5^2 + \dots)$ which gives $-1 \equiv 4a_0 \pmod{5}$ and so $a_0 = 1$. Then $-1 = 4(1 + a_1 5 + a_2 5^2 + \dots)$ gives $-5 \equiv 4a_1 5 \pmod{5^2}$, giving $-1 \equiv 4a_1 \pmod{5}$, and so $a_1 = 1$. Similarly, we find that $a_2 = 1, a_3 = 1, \dots$ and we suspect that $-1/4 = 1, \overline{1}$.

Let $\alpha = 1, \overline{1}$. Then $\alpha - 1 = 0, \overline{1} = 5\alpha$, so that $4\alpha = -1$, giving $\alpha = -1/4$, proving that we have the correct 5-adic expansion.

Comment 2.10. The field $\mathbb{Q}$ is often referred to as a *global field* and its completions with respect to valuations, namely $\mathbb{R}$ and $\mathbb{Q}_p$, for any prime p , are its *local fields* (or *localisations*). An equation defined over $\mathbb{Q}$ which has points in $\mathbb{R}$ and every $\mathbb{Q}_p$, but not in $\mathbb{Q}$, is said to *violate the Hasse Principle*.

Definition 2.11. Let K be a field with a non-Archimedean valuation $|\cdot|$. We say that $x \in K$ is an *integer* (with respect to the valuation) when $|x| \leq 1$, and $R = \{x \in K : |x| \leq 1\}$ is the *ring of integers* (or *valuation ring*) of K . The set $\mathcal{M} = \{x \in K : |x| < 1\}$ is the *maximal ideal*, and $k = R/\mathcal{M}$ is the *residue field* [also called the *field of digits*]. The *valuation group*

is the set $G_K = \{|x| : x \in K^*\}$ under multiplication. We say that the valuation is *discrete* if there exists $\delta > 0$ such that $1 - \delta < |x| < 1 + \delta \implies |x| = 1$. When the valuation is discrete, there exists an element $\mathfrak{p} \in \mathcal{M}$ such that $\mathcal{M} = \mathfrak{p}R$; we say that such an element is a *prime element* for the valuation.

The ring of integers for $\mathbb{Q}_p$ is often denoted $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$. The valuation group $G_{\mathbb{Q}_p} = \{p^r : r \in \mathbb{Z}\} = \{\dots, p^{-2}, p^{-1}, p^0, p^1, p^2, \dots\}$, so that $\mathbb{Q}_p$ is discrete, and we can take p as a prime element (or indeed any element with valuation p^{-1}). The maximal ideal is $\mathcal{M} = p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq p^{-1}\}$ and the residue field $\mathbb{Z}_p/p\mathbb{Z}_p$ is isomorphic to $\mathbb{F}_p$, the finite field with p elements.

Theorem 2.12. *Let K be a field, complete with respect to a non-Archimedean valuation $|\cdot|$, and let x_n be a sequence in K . Then: $x_n \rightarrow 0$ in $K \iff \sum x_n$ is convergent in K .*

Proof Let $S_N = \sum_{n=1}^N x_n$.

$\Rightarrow$: Assume that $x_n \rightarrow 0$ in K . Then:

$$|S_N - S_M| = |x_{M+1} + \dots + x_N| \leq \max(|x_{M+1}|, \dots, |x_N|) \rightarrow 0 \text{ as } M, N \rightarrow \infty.$$

S_N is Cauchy and so convergent (since K is complete), giving that $\sum x_n$ is convergent.

$\Leftarrow$: Assume that $\sum x_n$ is convergent, that is, $S_N \rightarrow \ell$ for some $\ell \in K$. Then:

$$|x_n - 0| = |x_n| = |S_n - S_{n-1}| = |S_n - \ell + \ell - S_{n-1}| \leq |S_n - \ell| + |S_{n-1} - \ell| \rightarrow 0 \text{ as } n \rightarrow \infty,$$

so that $x_n \rightarrow 0$ in K , $|\cdot|$. $\square$

For example, $\sum n!$ converges in any $\mathbb{Q}_p$, since $|n!|_p \rightarrow 0$ [it is unknown whether $\sum n! \in \mathbb{Q}$].

The above result applies to $\mathbb{Q}_p$ (since it is non-Archimedean), but not to $\mathbb{R}$ (where, for example, $x_n = \frac{1}{n}$ is a standard counterexample).

Comment 2.13. It is easy to see that, the rules for finite sums in Comment 2.5 and apply to infinite series, namely, when $\sum a_n$ converges, $|\sum a_n| \leq \max |a_n|$. Furthermore, if there exists a_k such that $|a_k| > |a_i|$ for all $i \neq k$, then $|\sum a_n| = |a_k|$; in particular, it is then impossible for $\sum a_n = 0$.

Theorem 2.14. (*Hensel's Lemma*). *Let K be a field, complete with respect to a non-Archimedean valuation $|\cdot|$, with valuation ring $R = \{x \in K : |x| \leq 1\}$.*

Let $f(x) \in R[x]$ and let $a_0 \in R$ satisfy: $|f(a_0)| < |f'(a_0)|^2$. ()*

Then there exists a unique $a \in R$ such that $f(a) = 0$ and $|a - a_0| \leq |f(a_0)|/|f'(a_0)|$.

Proof Define $f_j(x)$ by: $f(x+y) = f_0(x) + f_1(x)y + f_2(x)y^2 + \dots$,

so that $f_0(x) = f(x)$, $f_1(x) = f'(x)$. Define $b_0 = -f(a_0)/f'(a_0)$. By (*), $|b_0| < 1$.

Define $a_1 = a_0 + b_0 = a_0 - f(a_0)/f'(a_0)$. Then:

$$\begin{aligned} |f'(a_1) - f'(a_0)| &= |f'(a_0 + b_0) - f'(a_0)| = |(\text{poly in } a_0)b_0 + (\text{poly in } a_0)b_0^2 + \dots| \\ &\leq |b_0| < |f'(a_0)| \quad (\text{by } (*)), \end{aligned}$$

so that $|f'(a_1)| = |f'(a_0)|$.

$$\begin{aligned} \text{Also, } |f(a_1)| &= |f(a_0 + b_0)| = |f_0(a_0) + f_1(a_0)b_0 + f_2(a_0)b_0^2 + \dots| \\ &= |f_2(a_0)b_0^2 + \dots| \quad [\text{since } f_0(a_0) + f_1(a_0)b_0 = 0] \\ &\leq \max_{j \geq 2} |f_j(a_0)| |b_0|^j \leq |b_0|^2 = \frac{|f(a_0)|^2}{|f'(a_0)|^2} = \rho |f(a_0)| < |f(a_0)|, \text{ where } \rho = \frac{|f(a_0)|}{|f'(a_0)|^2} < 1. \end{aligned}$$

Summarising: $|f'(a_1)| = |f'(a_0)|$ and $|f(a_1)| \leq \rho |f(a_0)| < |f(a_0)|$, where $\rho = \frac{|f(a_0)|}{|f'(a_0)|^2} < 1$.
For all n , given $a_n \in R$, define $b_n = -f(a_n)/f'(a_n)$ and $a_{n+1} = a_n + b_n = a_n - f(a_n)/f'(a_n)$.
Assume, as induction hypothesis, that:

$$|f'(a_n)| = \dots = |f'(a_1)| = |f'(a_0)| \text{ and } |f(a_n)| \leq \rho |f(a_{n-1})| \leq \dots \leq \rho^n |f(a_0)|. \quad (1)$$

Then, as above: $|f'(a_{n+1})| = \dots = |f'(a_1)| = |f'(a_0)|$.

Then $|f(a_{n+1})| \leq |b_n|^2$ [justified as for the case $n = 0$ above]

$$\begin{aligned} &= \frac{|f(a_n)|^2}{|f'(a_n)|^2} = \frac{|f(a_n)|^2}{|f'(a_0)|^2} \quad [\text{by (1), the induction hypothesis}] \\ &\leq \frac{|f(a_0)|}{|f'(a_0)|^2} |f(a_n)| \quad [\text{since } |f(a_n)| \leq |f(a_0)| \text{ by (1), the induction hypothesis}] \\ &= \rho |f(a_n)| \leq \rho^{n+1} |f(a_0)| \quad [\text{by (1), the induction hypothesis}]. \end{aligned}$$

By induction, $\forall n$, $|f'(a_n)| = |f'(a_0)|$ and $|f(a_n)| \leq \rho^n |f(a_0)|$ which $\rightarrow 0$ as $n \rightarrow \infty$. (2)

Now, $|b_n| = |f(a_n)|/|f'(a_n)| = |f(a_n)|/|f'(a_0)| \rightarrow 0$, so by Theorem 2.12,

$a_n = a_0 + b_0 + b_1 + \dots + b_n$ converges to a , say.

By continuity of polynomials, $f(a) = \lim f(a_n) = 0$ [by (2)]. Furthermore:

$$|a - a_0| = |\sum b_n| \leq \max |b_n| = \max \frac{|f(a_n)|}{|f'(a_n)|} = \max \frac{|f(a_n)|}{|f'(a_0)|} = \frac{|f(a_0)|}{|f'(a_0)|} \quad [\text{by (2)}], \text{ as required.}$$

For uniqueness, imagine $\hat{a} \neq a$ also satisfied $f(\hat{a}) = 0$ and $|\hat{a} - a_0| \leq |f(a_0)|/|f'(a_0)|$. Let $\hat{b} = \hat{a} - a \neq 0$.

$$\text{Then } 0 = f(\hat{a}) - f(a) = f(a + \hat{b}) - f(a) = \hat{b}f_1(a) + \hat{b}^2f_2(a) + \dots \quad (3)$$

But $|\hat{b}| = |\hat{a} - a_0 + a_0 - a| \leq \max(|\hat{a} - a_0|, |a - a_0|) \leq |f(a_0)|/|f'(a_0)|$

$$< |f'(a_0)| \quad [\text{by (*)}] = |f_1(a_0)| = |f_1(a)| \quad [\text{by (1) and continuity of } |f'(x)|].$$

This gives $|\hat{b}^j f_j(a)| \leq |\hat{b}^j| \leq |\hat{b}^2| < |\hat{b}f_1(a)|$ for $j \geq 2$, so that the leading term of the sum in (3) has valuation strictly greater than the valuations of the other terms, which is inconsistent with the sum being 0. Hence a is unique. □

Example 2.15. Let $f(x) = x^3 - 7$ and $a_0 = 3$. Then $|f(a_0)|_5 = |3^3 - 7|_5 = 5^{-1}$ and $|f'(a_0)|_5 = |3 \cdot 3^2|_5 = 1$. So $|f(a_0)|_5 < |f'(a_0)|_5^2$ and by Hensel's Lemma there exists $a \in \mathbb{Z}_5$ such that $f(a) = 0$, that is: $a^3 = 7$.

Corollary 2.16. Let $\alpha \in \mathbb{Q}_p$ with $|\alpha|_p = 1$. When $p \neq 2$, α is a square in $\mathbb{Q}_p$ iff it is a square modulo p . When $p = 2$, α is a square in $\mathbb{Q}_p$ iff $\alpha \equiv 1 \pmod{8}$.

Example 2.17. $23 \in (\mathbb{Q}_7^*)^2$ since $|23|_7 = 1$ and $23 \equiv 2 \equiv 3^2 \pmod{7}$. However, $24 \notin (\mathbb{Q}_7^*)^2$ since $|24|_7 = 1$ and $24 \equiv 3 \pmod{7}$, which is not a quadratic residue mod 7.

SECTION 3. THE REDUCTION MAP ON AN ELLIPTIC CURVE

Throughout this section, K denotes a complete non-Archimedean field, with valuation ring $R = \{x : |x| \leq 1\}$, maximal ideal $\mathcal{M} = \{x : |x| < 1\}$ and residue field $k = R/\mathcal{M}$.

Definition 3.1. Then natural mod $\mathcal{M}$ map $R \rightarrow k = R/\mathcal{M} : r \mapsto r + \mathcal{M}$, is a surjection and is denoted $a \mapsto \tilde{a}$ (or sometimes $\bar{a}$). For example in $\mathbb{Z}_5$, if $a = 3 + 2 \cdot 5^1 + \dots$ then $\tilde{a} = 3$; also $\widetilde{17/3} = 2/3 = 2 \cdot 2 = 4$.

Let $a = (a_0, \dots, a_n) \in \mathbb{P}^n(K)$. We define the reduction map to $\mathbb{P}^n(k)$ as follows.

Step 1. There exists i_0 such that $|a_{i_0}| \geq |a_i|$ for $i = 0, \dots, n$. We replace each a_i by a_i/a_{i_0} (which leaves a unchanged) so that now the largest valuation is 1 (*normalised* form).

Step 2. Define $\tilde{a} = (\tilde{a}_0, \dots, \tilde{a}_n)$ [easy to check that this is well defined].

In affine space, if $a = (a_1, \dots, a_n)$ then $\tilde{a} = (\tilde{a}_1, \dots, \tilde{a}_n)$, provided that all $|a_i| \leq 1$.

When $K = \mathbb{Q}_p$, this is just the ‘mod p ’ map, where the coordinates are reduced modulo p .

Example 3.2. In $\mathbb{P}^2(\mathbb{Q}_5)$, let $a = (1/5, 2/15, 2)$. Dividing through by $a_0 = 1/5$ gives $a = (1, 2/3, 10)$ so that $\tilde{a} = (\tilde{1}, \widetilde{2/3}, \widetilde{10}) = (1, 4, 0) \in \mathbb{P}^2(\mathbb{F}_5)$. For $b = (2/3, 25)$ in affine space $A^2(\mathbb{Q}_5)$ [an affine point with no denominators of 5], then $\tilde{b} = (4, 0) \in A^2(\mathbb{F}_5)$.

For the point $P = (1/4, 7/8) \in \mathcal{E}(\mathbb{Q}) \subset \mathcal{E}(\mathbb{Q}_2)$ on the elliptic curve $\mathcal{E} : y^2 = x^3 - x + 1$, we should first write P in projective form: $(1/4, 7/8, 1) = (2/7, 1, 8/7)$ [after dividing through by $7/8$], which reduces modulo 2 to $(0, 1, 0)$, the point at infinity on $\tilde{\mathcal{E}}(\mathbb{F}_2)$. Clearly any $(x, y) \in \mathcal{E}(\mathbb{Q}_p)$ will reduce mod p to the point at infinity iff $|x|_p > 1$ and $|y|_p > 1$.

Definition 3.3. Let $\mathcal{C} : F(X, Y, Z) = 0$ be a projective curve, defined over K . Let $\{f_i\}$ be the set of all coefficients of $\mathcal{C}$. The curve is unchanged if we multiply all the f_i by a nonzero constant, so after dividing through by f_{i_0} such that $|f_{i_0}| \geq |f_i|$ for all i , we can say that $\max(|f_i|) = 1$ [normalised form]. The reduction of $\mathcal{C}$ mod $\mathcal{M}$ is $\tilde{\mathcal{C}} : \tilde{F}(X, Y, Z) = 0$, defined over $k = R/\mathcal{M}$, where every coefficient has been reduced mod $\mathcal{M}$. When $K = \mathbb{Q}_p$, this is again just a matter of reducing the coefficients mod p .

Clearly, a lies on $\mathcal{C} \implies \tilde{a}$ lies on $\tilde{\mathcal{C}}$, when we say that a reduces to $\tilde{a}$.

Definition 3.4. Let $b \in \tilde{\mathcal{C}}(k)$. If there exists $a \in \mathcal{C}(K)$ such that $\tilde{a} = b$, we say that b *lifts* to $\mathcal{C}$ [or that b *lifts* to a point on $\mathcal{C}$].

Example 3.5. Let $\mathcal{E} : ZY^2 = X^3 + pZ^3$, defined over $\mathbb{Q}_p$, and $\tilde{\mathcal{E}} : ZY^2 = X^3$, defined over $\mathbb{F}_p$. $(0, 0, 1) \in \tilde{\mathcal{E}}(\mathbb{F}_p)$ does not lift to a point in $\mathcal{E}(\mathbb{Q}_p)$ (you’ll show this on a Problem Sheet). If we had represented the above curves with the affine shorthand: $\mathcal{E} : y^2 = x^3 + p$ and $\tilde{\mathcal{E}} : y^2 = x^3$, then the above would be expressed by saying that $(0, 0) \in \tilde{\mathcal{E}}(\mathbb{F}_p)$ does not lift.

On the other hand, the following result shows that we can guarantee lifting a nonsingular point on $\tilde{\mathcal{E}}$.

Theorem 3.6. *Let $\mathcal{C}$ be defined over K , written so that the coefficients lie in R . Let $\tilde{\mathcal{C}}$, defined over k , be the reduction of $\mathcal{C}$ modulo $\mathcal{M}$. Let $b \in \tilde{\mathcal{C}}(k)$ be a nonsingular point. Then b lifts to $\mathcal{C}$; that is, there exists $a \in \mathcal{C}(K)$ such that $\tilde{a} = b$.*

Proof Write $\mathcal{C} : F(X_0, X_1, X_2) = 0$ (normalised), so that $\tilde{\mathcal{C}} : \tilde{F}(X_0, X_1, X_2) = 0$. Let $b = (b_0, b_1, b_2) \in \tilde{\mathcal{C}}(k)$ be a nonsingular point. Then at least one of the $\frac{\partial \tilde{F}}{\partial X_i}(b) \neq 0$; wlog say that $\frac{\partial \tilde{F}}{\partial X_0}(b) \neq 0$. Let $\alpha_0, \alpha_1, \alpha_2 \in R$, $\alpha = (\alpha_0, \alpha_1, \alpha_2)$, be such that each $\tilde{\alpha}_i = b_i$ under the natural surjection from R to $k = R/\mathcal{M}$.

Let $f(t) = F(t, \alpha_1, \alpha_2)$. Then $\widetilde{f(\alpha_0)} = \tilde{F}(b) = 0$ so that $|f(\alpha_0)| < 1$. Furthermore, $\widetilde{f'(\alpha_0)} = \frac{\partial \tilde{F}}{\partial X_0}(\tilde{\alpha}) = \frac{\partial \tilde{F}}{\partial X_0}(b) \neq 0$, so that $|f'(\alpha_0)| = 1$. By Hensel's Lemma, there exists $a_0 \in R$ such that $f(a_0) = 0$ and $|a_0 - \alpha_0| < 1$, so that $a = (a_0, \alpha_1, \alpha_2)$ is a point on $\mathcal{C}$ and $\tilde{a} = \tilde{\alpha} = b$, as required. $\square$

Theorem 3.7. *Let $\mathcal{C} : F(X_0, X_1, X_2) = 0$ be a cubic curve defined over K , written so that coefficients of F have maximum valuation 1. Suppose the line $\mathcal{L} : L(X_0, X_1, X_2) = 0$ meets $\mathcal{C}$ at a, b, c . Then either:*

(1) $\tilde{\mathcal{L}} \subset \tilde{\mathcal{C}}$, that is, $\tilde{F}(X_0, X_1, X_2) = \tilde{L}\tilde{M}$, for some M .

or:

(2) $\tilde{\mathcal{L}}$ meets $\tilde{\mathcal{C}}$ precisely at $\tilde{a}, \tilde{b}, \tilde{c}$.

Proof Let $L : \ell_0 X_0 + \ell_1 X_1 + \ell_2 X_2$, written so that $\max(|\ell_0|, |\ell_1|, |\ell_2|) = 1$, wlog $|\ell_0| = 1$; after dividing through by ℓ_0 (and relabelling $\ell_1/\ell_0, \ell_2/\ell_0$ as ℓ_1, ℓ_2), we can take $\mathcal{L} : X_0 = -\ell_1 X_1 - \ell_2 X_2$, where $\ell_1, \ell_2 \in R$. Consider $\tilde{F}(-\tilde{\ell}_1 X_1 - \tilde{\ell}_2 X_2, X_1, X_2)$. If this is 0 then $\tilde{L}$ is a factor of $\tilde{F}$ giving case (1), otherwise (2) clearly follows. $\square$

When $\mathcal{E} : y^2 = x^3 + Ax + B$ ($A, B \in R$), the reduction $\tilde{\mathcal{E}}$ will still be of the form $y^2 = x^3 + \dots$. This cannot contain a line, since any $(y + rx + \dots)(y - x^2/r + \dots)$ would have an x^2y term and so would not give y^2 -cubic in x . Since the group law is constructed by finding intersections between the curve and lines, and since only option (2) applies, the construction of the group law respects the reduction map, giving the following result.

Corollary 3.8. *Let $\mathcal{E} : y^2 = x^3 + Ax + B$ be an elliptic curve, with $A, B \in R$, with reduction $\tilde{\mathcal{E}}$. Let $\tilde{\mathcal{E}}_{ns}(k)$ denote the group of nonsingular points in $\tilde{\mathcal{E}}(k)$, and define: $\mathcal{E}_0(K) = \{P \in \mathcal{E}(K) : \tilde{P} \in \tilde{\mathcal{E}}_{ns}(k)\}$. Then the reduction map $P \mapsto \tilde{P}$ is a homomorphism from $\mathcal{E}_0(K)$ to $\tilde{\mathcal{E}}_{ns}(k)$.*

Definition 3.9. Let $\mathcal{E}_0(K)$ and $\tilde{\mathcal{E}}_{ns}(k)$ be as in Corollary 3.8. The kernel of reduction, denoted $\mathcal{E}_1(K)$, is the kernel of the reduction map from $\mathcal{E}_0(K)$ to $\tilde{\mathcal{E}}_{ns}(k)$. That is:

$$\mathcal{E}_1(K) = \{P \in \mathcal{E}(K) : \tilde{P} = \underline{\mathbf{0}}\}.$$

We can summarise what we know so far by the following exact sequence:

$$0 \longrightarrow \mathcal{E}_1(K) \xrightarrow{i} \mathcal{E}_0(K) \xrightarrow{\sim} \tilde{\mathcal{E}}_{ns}(k) \longrightarrow 0,$$

where i is the inclusion map.

We now wish to look more closely at how we can describe the group law inside $\mathcal{E}_1(K)$, the kernel of reduction, for an elliptic curve:

$$\mathcal{E} : y^2 = x^3 + Ax + B, \quad \text{where } A, B \in R.$$

We adopt the usual convention that the identity is $\mathbf{o}$, the point at infinity so that $\mathcal{E}_1(K) = \{(x, y) \in \mathcal{E}(K) : |x| > 1, |y| > 1\}$. The members of $\mathcal{E}_1(K)$ are in a neighbourhood of $\mathbf{o}$, and it is natural to try to describe the group law as a power series. We therefore perform the following birational transformation:

$$z = -x/y, \quad w = -1/y, \quad \text{with inverse } x = z/w, \quad y = -1/w.$$

This transforms $\mathcal{E}$ to:

$$\frac{1}{w^2} = \frac{z^3}{w^3} + A\frac{z}{w} + B,$$

giving the equation

$$\mathcal{E}' : w = f(z, w) = z^3 + Aw^2z + Bw^3.$$

Note that the point at infinity $\mathbf{o}$ on $\mathcal{E}$ maps to the point $(0, 0)$ on $\mathcal{E}'$, which we take as our group identity on $\mathcal{E}'$. The condition $|x| > 1, |y| > 1$ corresponds to $|z| < 1, |w| < 1$, so that the kernel of reduction for $\mathcal{E}'$ is:

$$\mathcal{E}'_1(K) = \{(z, w) \in \mathcal{E}'(K) : |z| < 1, |w| < 1\}.$$

We now recursively substitute $w = f(z, w)$ into itself. For the first step:

$$\begin{aligned} w = f(z, w) &= f(z, f(z, w)) = z^3 + A(z^3 + Aw^2z + Bw^3)^2z + B(z^3 + Aw^2z + Bw^3)^3 \\ &= z^3 + Az^7 + \dots \end{aligned}$$

Inductively define $f_n(z, w)$ by: $f_1(z, w) = f(z, w)$ and $f_{n+1}(z, w) = f_n(z, f(z, w))$. Define

$$w(z) = \lim_{n \rightarrow \infty} f_n(z, 0) \in \mathbb{Z}[A, B][[z]].$$

The following is then easy to show.

Lemma 3.10. *The power series $w(z) = z^3(1 + \dots) \in \mathbb{Z}[A, B][[z]]$ defined above is the unique power series satisfying $w(z) = f(z, w(z))$.*

This means that $(z, w(z))$ satisfies $\mathcal{E}'$. Any (z, w) in the kernel of reduction must satisfy $w = w(z)$, and so is uniquely determined by z , which is called a *local parameter*.

Comment 3.11. We can recover x, y on $\mathcal{E}$ as formal Laurent series:

$$x(z) = \frac{z}{w(z)} = \frac{z}{z^3(1 + \dots)} = \frac{1}{z^2} + \dots$$

$$y(z) = -\frac{1}{w(z)} = -\frac{1}{z^3(1 + \dots)} = -\frac{1}{z^3} + \dots$$

which gives a formal solution to $\mathcal{E}$.

Let us now perform the addition $(z_1, w_1) + (z_2, w_2)$. As usual, we first write the line $w = \lambda z + \mu$ through the points, given by $\lambda = (w_1 - w_2)/(z_1 - z_2)$ and $\mu = (z_1 w_2 - z_2 w_1)/(z_1 - z_2)$. As long as we are in the kernel of reduction, $w_1 = w(z_1)$ and $w_2 = w(z_2)$, and so:

$$\lambda = \lambda(z_1, z_2) = \frac{w(z_1) - w(z_2)}{z_1 - z_2} = \frac{z_1^3(1 + \dots) - z_2^3(1 + \dots)}{z_1 - z_2} \in \mathbb{Z}[A, B][[z_1, z_2]],$$

with all terms being of degree ≥ 2 , and:

$$\mu = \mu(z_1, z_2) = \frac{z_1 w(z_2) - z_2 w(z_1)}{z_1 - z_2} \in \mathbb{Z}[A, B][[z_1, z_2]].$$

Substituting $w = \lambda z + \mu$ into $\mathcal{E}'$ gives $\lambda z + \mu = z^3 + A(\lambda z + \mu)^2 z + B(\lambda z + \mu)^3$, and so:

$$(1 + A\lambda^2 + B\lambda^3)z^3 + (2A\lambda\mu + 3B\lambda^2\mu)z^2 + \dots = 0.$$

Let $(z_3, w(z_3))$ be the third point of intersection of $\mathcal{E}'$ and the line $w = \lambda z + \mu$, so that z_1, z_2, z_3 are the roots of the above cubic, giving that $z_1 + z_2 + z_3 = -(\text{coeff of } z^2)/(\text{coeff of } z^3)$, so:

$$z_3 = -z_1 - z_2 - \frac{2A\lambda\mu + 3B\lambda^2\mu}{1 + A\lambda^2 + B\lambda^3} \in \mathbb{Z}[A, B][[z_1, z_2]],$$

since the denominator is of the form $1 + \phi(z_1, z_2)$, where $\phi(z_1, z_2)$ has no constant term [and so is an invertible power series, with $1/(1 + \phi(z_1, z_2)) = 1 - \phi(z_1, z_2) + \phi(z_1, z_2)^2 + \dots$].

The sum $(z_1, w_1) + (z_2, w_2) + (z_3, w_3) = \text{the identity}$, and so $(z_1, w_1) + (z_2, w_2) = -(z_3, w_3)$. Negation $(x, y) \mapsto (x, -y)$ induces $(z, w) \mapsto (-z, -w)$ [since $z = -x/y, w = -1/y$], so that the z -coordinate of $(z_1, w_1) + (z_2, w_2)$ is given by $F_{\mathcal{E}}(z_1, z_2)$, where:

$$F_{\mathcal{E}}(z_1, z_2) = z_1 + z_2 + (\text{terms of degree } \geq 2) \in \mathbb{Z}[A, B][[z_1, z_2]].$$

We summarise this as follows.

Lemma 3.12. *Any point (x, y) on $\mathcal{E}$ [$\leftrightarrow (z, w)$ on $\mathcal{E}'$] in the kernel of reduction [namely: $|x| > 1, |y| > 1 \leftrightarrow |z| < 1, |w| < 1$] is uniquely determined by z , with $w = w(z) \in \mathbb{Z}[A, B][[z]]$. The group law is completely described by the above $F_{\mathcal{E}}(z_1, z_2) \in \mathbb{Z}[A, B][[z_1, z_2]]$, which converges to the z -coordinate of the sum of $(z_1, w(z_1))$ and $(z_2, w(z_2))$.*

We have already observed that $F_{\mathcal{E}}(z_1, z_2) = z_1 + z_2 + \text{terms of higher degree}$. The associativity and commutativity properties of the group law on $\mathcal{E}$ also induce the properties:

$$F_{\mathcal{E}}(X, F_{\mathcal{E}}(Y, Z)) = F_{\mathcal{E}}(F_{\mathcal{E}}(X, Y), Z), \quad F_{\mathcal{E}}(X, Y) = F_{\mathcal{E}}(Y, X).$$

SECTION 4. FORMAL GROUPS

Let R be any ring (by *ring* I shall always mean a commutative ring with 1).

Definition 4.1. A (one-parameter, commutative) *formal group* defined over R is a power series $F(X, Y) \in R[[X, Y]]$ satisfying:

- (1) $F(X, Y) = X + Y + \text{terms of degree } \geq 2$.
- (2) $F(X, F(Y, Z)) = F(F(X, Y), Z)$.
- (3) $F(X, Y) = F(Y, X)$.

Example 4.2. The following are all formal groups.

The formal group $F_{\mathcal{E}}(X, Y)$ of an elliptic curve defined over R , as described in Section 3.

The formal additive group $F(X, Y) = \hat{G}_a(X, Y) = X + Y$.

The formal multiplicative group $F(X, Y) = \hat{G}_m(X, Y) = X + Y + XY$.

Note: the last of these is just XY , but translated one unit to the left: $(1 + X)(1 + Y) - 1$ so that the identity is changed from 1 to 0.

Lemma 4.3. Let $F(X, Y)$ be a formal group over a ring R , and let TR_T denote $R[[T]]$.

- (1) There is a unique power series $i(T) \in TR_T$ such that $F(T, i(T)) = 0$.
- (2) $F(X, 0) = X$ and $F(0, Y) = Y$.

Proof (1) Let $Z_1 = -T \in TR_T$; then the terms of $F(T, Z_1)$ all have degree ≥ 2 . Suppose we have $Z_n \in TR_T$ such that $F(T, Z_n) = a_{n+1}T^{n+1} + \dots$ has terms all of degree $\geq n + 1$. Define $Z_{n+1} = Z_n - a_{n+1}T^{n+1}$; then:

$$\begin{aligned} F(T, Z_{n+1}) &= F(T, Z_n - a_{n+1}T^{n+1}) = T + (Z_n - a_{n+1}T^{n+1}) + \dots \\ &= F(T, Z_n) - a_{n+1}T^{n+1} + (\text{terms of degree } \geq n + 2) \\ &= a_{n+1}T^{n+1} - a_{n+1}T^{n+1} + (\text{terms of degree } \geq n + 2), \end{aligned}$$

which has terms all of degree $\geq n + 2$. This inductively defines a power series $i(T)$, whose first n terms agree with Z_n for all n , such that $F(T, i(T)) = 0$. Furthermore, each choice of term of Z_n was forced, so that $i(T)$ is unique.

(2) By a similar argument to (1), there exists a unique $j(T) \in TR_T$ such that $F(j(T), i(T)) = 0$. By (1) we can take $j(T) = T$. By associativity $F(F(0, T), i(T)) = F(0, F(T, i(T))) = F(0, 0) = 0$, so that we can also take $j(T) = F(0, T)$. Since $j(T)$ is unique, it follows that $F(0, T) = T$. Similarly for $F(T, 0) = T$. $\square$

Definition 4.4. Let F, G define formal groups over R . A power series $f(T) \in TR_T$ is a *homomorphism* from F to G if it satisfies $f(F(X, Y)) = G(f(X), f(Y))$. When there also exists an inverse $g(T) \in TR_T$ [that is: $f(g(T)) = g(f(T)) = T$] then $f(T)$ is an *isomorphism*.

Example 4.5. If $\text{char}(R) = 0$ and $\frac{1}{n} \in R$ for all n , then $f(T) = T - T^2/2 + T^3/3 - \dots$ is a homomorphism from $\hat{G}_m$ to $\hat{G}_a$.

Definition 4.6. Let F define a formal group over R . Define the *multiplication by m map* $[m](T) \in R_T$, for $m \in \mathbb{Z}$, inductively by: $[0](T) = 0$, $[m+1](T) = F([m](T), T)$ and $[m-1](T) = F([m](T), i(T))$. This is clearly a homomorphism from F to F , and is of the form: $[m](T) = mT + \text{terms of degree } \geq 2$.

Lemma 4.7. Let $a \in R^*$ [that is: $a \in R$ and $a^{-1} \in R$], and let $f(T) \in TR_T$ be of the form $f(T) = aT + \dots$. Then there exists a unique $g(T) \in TR_T$ such that $f(g(T)) = T$. Furthermore, g satisfies $g(f(T)) = T$.

Proof Let $g(T) = b_1T + b_2T^2 + \dots$. Take $b_1 = a^{-1}$ and (similarly to the proof of Lemma 4.3) inductively define unique $b_2, b_3, \dots$ such that $f(g(T)) = T$ [and $g(f(T)) = T$]. $\square$

Lemma 4.8. The homomorphism $[m] : F \rightarrow F$ of Definition 4.6 is an isomorphism whenever $m \in R^*$.

Proof Since $[m](T) = mT + \text{terms of degree } \geq 2$, we have from the previous lemma that the homomorphism $[m]$ has an inverse, and so is an isomorphism. $\square$

{ *Aside:* Define $\log(T) = \int v(T)$ [with $\log(1) = 0$], where $v(T) = \frac{1}{T}dT$. Then [T variable, S constant] $v(TS) = \frac{1}{TS}d(TS) = v(T)$, so $\log(TS) = \log(T) + f(S)$. Setting $T = 1$ gives $f(S) = \log(S)$.

Define $F(X, Y) = \widehat{G}_m(X, Y) = (1+X)(1+Y) - 1 = X+Y+XY$. Then $\omega(T) = \frac{1}{1+T}dT = (1-T+T^2-\dots)dT$ satisfies $\omega \circ F(T, S) = \omega(T)$ [and $\int \omega(T)$ is a homomorphism from $\widehat{G}_m$ to $\widehat{G}_a$]. }

Definition 4.9. We can represent a differential form on R_T as an expression of the form $\sum_{i=1}^m P_i(T)dQ_i(T)$, where each $P_i(T), Q_i(T) \in R_T$, and these satisfy the natural rules:

$$d(P(T)) = P'(T)dT, \text{ where } P'(T) = \sum_{n=1}^{\infty} a_n n T^{n-1}, \text{ for any } P(T) = \sum_{n=0}^{\infty} a_n T^n,$$

$$d(P(T) + Q(T)) = dP(T) + dQ(T), \quad d(P(T)Q(T)) = P(T)dQ(T) + Q(T)dP(T).$$

An *invariant differential* on a formal group F , defined over R , is a differential form:

$$\omega(T) = P(T)dT \in R_T dT, \text{ satisfying } \omega \circ F(T, S) = \omega(T).$$

Note that $\omega \circ F(T, S)$ is the same as $P(F(T, S))d(F(T, S)) = P(F(T, S))F_X(T, S)dT$, where $F_X(X, Y)$ denotes the partial derivative of $F(X, Y)$ with respect to X . So, the above condition on ω is equivalent to:

$$\omega(T) = P(T)dT \in R_T dT, \text{ satisfying } P(F(T, S))F_X(T, S) = P(T).$$

An invariant differential $\omega(T) = P(T)dT$ is said to be *normalised* if $P(0) = 1$.

Example 4.10. On $\widehat{G}_a$, the formal group defined by $F(X, Y) = X + Y$, we can take $\omega(T) = dT$ as a normalised invariant differential. On $\widehat{G}_m$, the multiplicative formal group defined by $F(X, Y) = X + Y + XY$, we can take $\omega(T) = (1+T)^{-1}dT = (1-T+T^2-\dots)dT$.

Theorem 4.11. *Let F be a formal group over R . There exists a unique normalised invariant differential given by $\omega(T) = F_X(0, T)^{-1}dT \in R_T dT$. Every invariant differential is of the form $a\omega$ for some $a \in R$.*

Proof Let $P(T) = F_X(0, T)^{-1}$. Note that $F_X(0, T) = 1 + \dots$ is invertible, so that $P(T)$ is indeed a member of R_T . Furthermore, $P(0) = 1$, so that it is normalised.

We need to show that ω is an invariant differential. Recall from Definition 4.9 that this is equivalent to: $P(F(T, S))F_X(T, S) = P(T)$ so, in our case, it is sufficient to show:

$$F_X(0, F(T, S))^{-1}F_X(T, S) = F_X(0, T)^{-1},$$

which is true iff:

$$F_X(0, F(T, S)) = F_X(T, S)F_X(0, T).$$

But this last statement is immediate from differentiating $F(U, F(T, S)) = F(F(U, T), S)$ [associativity] with respect to U to get: $F_X(U, F(T, S)) = F_X(F(U, T), S)F_X(U, T)$ and setting $U = 0$. Hence ω is an invariant differential.

Suppose that $\hat{\omega}(T) = Q(T)dT \in R_T dT$ is also an invariant differential, so that $Q(T)$ satisfies $Q(F(T, S))F_X(T, S) = Q(T)$. Substituting $T = 0$ gives $Q(S)F_X(0, S) = Q(0)$, so that $Q(S) = Q(0)F_X(0, S)^{-1}$. It follows that $\hat{\omega} = a\omega$, where $a = Q(0)$. $\square$

Corollary 4.12. *Let f be a homomorphism over R from the formal group F to the formal group G . Let ω_F, ω_G be the normalised invariant differentials on F, G , respectively. Then $\omega_G \circ f = f'(0) \omega_F$.*

Proof First, note that $\omega_G \circ f(F(T, S)) = \omega_G(G(f(T), f(S))) = \omega_G \circ f(T)$, so that $\omega_G \circ f$ is an invariant differential on F . From the previous result, it follows that $\omega_G \circ f = a \omega_F$, for some $a \in R$. Since ω_F, ω_G are normalised, $(1 + \dots)df(T) = a(1 + \dots)dT$, and so $(1 + \dots)f'(T)dT = a(1 + \dots)dT$; equating constant terms gives $a = f'(0)$, as required. $\square$

Corollary 4.13. *Let F be a formal group over R and let, as usual, $[m](T) \in R_T$ denote the multiplication by m map on F , as in Definition 4.6. Let p be prime. Then there exist $f, g \in R_T$ [$f(T) = T + \dots$], such that $[p](T) = pf(T) + g(T^p)$.*

Proof Let ω be the normalised invariant differential on F . Since $[p](T) = pT + \dots$, it satisfies $[p]'(0) = p$. Applying the previous result to $[p]$, a homomorphism from F to itself, gives: $\omega \circ [p] = [p]'(0)\omega = p\omega$, and so

$$p\omega(T) = \omega \circ [p](T) = (1 + \dots)d([p](T)) = (1 + \dots)[p]'(T)dT.$$

Hence $[p]'(T) \in pR_T$. Each term $a_n T^n$ in $[p](T)$ must then satisfy $p|na_n$ in R , and so $p|n$ in $\mathbb{Z}$ or $p|a_n$ in R , as required. $\square$

Definition 4.14. Let $\omega(T) = P(T)dT = (1+c_1T+c_2T^2+\dots)dT$ be the normalised invariant differential for the formal group F over R . When our ring R is a field of characteristic 0, we can define the formal logarithm by: $\log_F(T) = \int \omega(T) = \int P(T)dT = T + \frac{c_1}{2}T^2 + \frac{c_2}{3}T^3 + \dots$ and the *formal exponential function* $\exp_F(T)$ as the unique member of R_T satisfying $\log_F(\exp_F(T)) = \exp_F(\log_F(T)) = T$, which exists by Lemma 4.7.

Theorem 4.15. *Let R be a field of characteristic 0; then $\log_F$ [as in the previous definition] is an isomorphism from F to $\widehat{G}_a$, the additive group $X + Y$.*

Proof Differentiating $\log_F(F(T, S)) - \log_F(T)$ with respect to T gives:

$P(F(T, S))F_X(T, S) - P(T)$ [and this = 0, since $\omega(T) = P(T)dT$ is an invariant differential], and so $\log_F(F(T, S)) - \log_F(T)$ is a power series purely in S , which we denote $f(S)$; that is: $\log_F(F(T, S)) = \log_F(T) + f(S)$. Putting $T = 0$ forces $f(S) = \log_F(S)$. Hence $\log_F$ is a homomorphism; the inverse is $\exp_F$, and so $\log_F$ is an isomorphism. $\square$

Comment 4.16. Note that our proof of the existence of the invariant differential required no appeal to the commutativity axiom $F(X, Y) = F(Y, X)$. If our formal group F is defined over any integral domain R of characteristic 0 (such as $\mathbb{Z}$ or any $\mathbb{Z}_p$), we can define $\log_F, \exp_F$ over K , the field of fractions of R , and see that $F(X, Y) = \exp_F(\log_F(X) + \log_F(Y))$, which forces F to be commutative.

Definition 4.17. Let K be field, complete with respect to a discrete non-Archimedean valuation, $R = \{x \in K : |x| \leq 1\}$ be the valuation ring, $\mathcal{M} = \{x \in K : |x| < 1\}$ be the maximal ideal, and assume that $k = R/\mathcal{M}$ [the residue field] is of characteristic p [for example, $K = \mathbb{Q}_p$, $R = \mathbb{Z}_p$, $\mathcal{M} = p\mathbb{Z}_p$, $k = \mathbb{F}_p$]. Let F be a formal group defined over R . The *group on $\mathcal{M}$ associated to $F(X, Y)$* , denoted $F(\mathcal{M})$, is the set $\mathcal{M}$ together with the group operation: $x \oplus y = F(x, y)$ [which converges for any $x, y \in \mathcal{M}$]. The identity element is 0, and the inverse of x is given by $i(x)$ of Lemma 4.3. Similarly, for any $n \geq 1$, define $F(\mathcal{M}^n)$ to be the set $\mathcal{M}^n$ with the same group operation.

Lemma 4.18. *Let $F, K, R, \mathcal{M}, k$ [with $\text{char}(k) = p$] be as in Definition 4.17.*

- (a) *The identity map: $F(\mathcal{M}^n)/F(\mathcal{M}^{n+1}), \oplus \rightarrow \mathcal{M}^n/\mathcal{M}^{n+1}, +$ is an isomorphism.*
- (b) *Every torsion element of $F(\mathcal{M})$ has order a power of p .*

Proof

- (a) For any $x, y \in \mathcal{M}^n$, $x \oplus y = x + y + \dots \equiv x + y \pmod{\mathcal{M}^{2n}}$, and so is $\equiv x + y \pmod{\mathcal{M}^{n+1}}$.
- (b) It is sufficient to show there does not exist a point of finite order m for any $m > 1$ with $p \nmid m$ [since any w of order mp^n gives $p^n w$ of order m]. But, since $\text{char}(k) = p$, and $p \nmid m$,

we have $|m| = 1$ and so $m \in R^*$. By Lemma 4.8, $[m]$ is an isomorphism from $\mathcal{M}$ to $\mathcal{M}$, which must then have trivial kernel: $[m]z = 0 \implies z = 0$, as required. $\square$

Theorem 4.19. *Let $F, K, R, \mathcal{M}, k$ [with $\text{char}(k) = p$] be as in Defn 4.17. Suppose that $z \in F(\mathcal{M})$ has exact order p^n , for some $n \geq 1$, so that $[p^n](z) = 0$, but $[p^{n-1}](z) \neq 0$. Then:*

$$|z| \geq |p|^{\frac{1}{p^n - p^{n-1}}}.$$

Proof If $\text{char}(R) \neq 0$ then $|p| = 0$, so assume that $\text{char}(R) = 0$. We have from Corollary 4.13 that $[p](T) = pf(T) + g(T^p)$ for some $f(T) = T + \dots \in R_T$ and $g(T) \in R_T$. We shall proceed by induction on n .

Suppose $z \neq 0$, $z \in \mathcal{M}$ and $[p](z) = 0$. Then $0 = pf(z) + g(z^p) = p(z + \dots) + g(z^p)$. We cannot have $|pz| > |z^p|$, since then the term pz would have valuation strictly greater than the valuations all other terms. Hence $|pz| \leq |z^p| = |z|^p$, and so $|p| \leq |z|^{p-1}$, giving $|z| \geq |p|^{\frac{1}{p-1}}$, proving the result for $n = 1$.

Now, assume the result is true for n , and let $z \in F(\mathcal{M})$ have order p^{n+1} . Then $[p](z)$ has order n , and by the induction hypothesis, $|[p](z)| \geq |p|^{\frac{1}{p^n - p^{n-1}}}$. Hence:

$$|p|^{\frac{1}{p^n - p^{n-1}}} \leq |[p](z)| = |pf(z) + g(z^p)| \leq \max(|pz|, |z^p|).$$

But $|z| < 1, |p| < 1$, so that $|p|^{\frac{1}{p^n - p^{n-1}}} \geq |p| > |pz|$, giving $|p|^{\frac{1}{p^n - p^{n-1}}} \leq |z^p|$, and so $|z| \geq |p|^{\frac{1}{p^{n+1} - p^n}}$, as required. $\square$

This has immediate consequences for elliptic curves.

Corollary 4.20. *Let $\mathcal{E} : y^2 = x^3 + Ax + B$, be an elliptic curve, where $A, B \in \mathbb{Z}_p$. The kernel $\mathcal{E}_1(\mathbb{Q}_p)$ of the reduction map $\sim : \mathcal{E}_0(\mathbb{Q}_p) \rightarrow \tilde{\mathcal{E}}_{ns}(\mathbb{F}_p)$ has no torsion (apart from $\mathbf{o}$). Any $(x, y) \in \mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ satisfies $|x|_p \leq 1, |y|_p \leq 1$. When $\tilde{\mathcal{E}}$ is non-singular, $\mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ is isomorphic to a subgroup of $\tilde{\mathcal{E}}(\mathbb{F}_p)$.*

Proof Let $\mathbf{o} \neq (x, y) \in \mathcal{E}(\mathbb{Q}_p)$ be in the kernel of reduction, that is, $|x|_p, |y|_p > 1$. Then, from the equation for $\mathcal{E}$, $|y|_p = |x|_p^{3/2}$ and $|z| = |-x/y|_p = |x|_p^{-1/2} < 1, |w| = |-1/y|_p < 1$. If (x, y) were torsion, then z would be a torsion point in $F_{\mathcal{E}}(\mathcal{M}) = F_{\mathcal{E}}(p\mathbb{Z}_p)$. By Lemma 4.18(b) it must be of order p^n , and so by Theorem 4.19 must satisfy $1 > |z|_p \geq |p|^{\frac{1}{p^n - p^{n-1}}}$. Note that, since $|p|_p = p^{-1}$, any p^n apart from 2^1 [so that $p^n - p^{n-1} > 1$] would force $1 > |z|_p > p^{-1}$, contradicting the fact that $|z|_p$ is p^r for some integer r . The only remaining possibility is that (x, y) is of order 2; but then $y = 0$ and x is a root of $x^3 + Ax + B$; this is incompatible with $|x|_p > 1$ [which makes x^3 have strictly larger valuation than Ax and B]. We conclude that x, y cannot be torsion, and that there is no torsion (apart from $\mathbf{o}$) in the kernel of reduction.

When $\tilde{\mathcal{E}}$ is non-singular, $\mathcal{E}_0(\mathbb{Q}_p) = \mathcal{E}(\mathbb{Q}_p)$ and $\tilde{\mathcal{E}}_{ns}(\mathbb{F}_p) = \tilde{\mathcal{E}}(\mathbb{F}_p)$ and the reduction map $\sim : \mathcal{E}(\mathbb{Q}_p) \rightarrow \tilde{\mathcal{E}}(\mathbb{F}_p)$ contains no nontrivial torsion, and so is injective when restricted to $\mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$; hence $\mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ is isomorphic to a subgroup of $\tilde{\mathcal{E}}(\mathbb{F}_p)$. $\square$

SECTION 5. GLOBAL TORSION

{ *Aside: We now turn to elliptic curves defined over $\mathbb{Q}$, initially concentrating on the group $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ of points of finite order. Any elliptic curve $\mathcal{E} : y^2 = x^3 + Ax + B$, defined over $\mathbb{Q}$ can be transformed with a map of the form $(x, y) \mapsto (k^2x, k^3y)$ so that $A, B \in \mathbb{Z}$. }*

Lemma 5.1. *Let $\mathcal{E} : y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$, be an elliptic curve [so that $\Delta = 4A^3 + 27B^2 \neq 0$]. Let p be a prime satisfying: $p \neq 2$ and $p \nmid \Delta$ (such a prime is said to be of good reduction, since $\tilde{\mathcal{E}} \bmod p$ is still an elliptic curve over $\mathbb{F}_p$). Then $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\tilde{\mathcal{E}}(\mathbb{F}_p)$, and so $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid \#\tilde{\mathcal{E}}(\mathbb{F}_p)$.*

Proof Since $\mathbb{Q} \subset \mathbb{Q}_p$, for any p , $\mathcal{E}(\mathbb{Q}) \leq \mathcal{E}(\mathbb{Q}_p)$ and $\mathcal{E}_{\text{tors}}(\mathbb{Q}) \leq \mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$. Since $p \nmid \Delta$ we have $\tilde{\Delta} \neq 0$ in $\mathbb{F}_p$; since $\text{char}(\mathbb{F}_p) \neq 2$, this is enough to guarantee that $\tilde{\mathcal{E}}$ is non-singular, and so $\tilde{\mathcal{E}}_{\text{ns}}(\mathbb{F}_p) = \tilde{\mathcal{E}}(\mathbb{F}_p)$. By the last result of the previous section (Corollary 4.20), $\mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ is isomorphic to a subgroup of $\tilde{\mathcal{E}}(\mathbb{F}_p)$, as must also be $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ [since $\mathcal{E}_{\text{tors}}(\mathbb{Q}) \leq \mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$]. Lagrange's Theorem then tells us that $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid \#\tilde{\mathcal{E}}(\mathbb{F}_p)$. $\square$

Note that, in particular, the above result tells us that $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is always finite. In practice, we can use reductions modulo finite fields to try to determine $\mathcal{E}_{\text{tors}}(\mathbb{Q})$.

Example 5.2. Let $\mathcal{E} : y^2 = x^3 + 3$, defined over $\mathbb{Q}$. Then $\Delta = 4A^3 + 27B^2 = 4 \cdot 0^3 + 27 \cdot 3^2 = 3^5$. We can choose any prime $p \neq 2, p \nmid \Delta$, that is, $p \neq 2, 3$.

$p = 5$. $\tilde{\mathcal{E}} : y^2 = x^3 + 3$, defined over $\mathbb{F}_5$. Then $\tilde{\mathcal{E}}(\mathbb{F}_5)$ consists of: $\underline{0}, (1, \pm 2), (2, \pm 1), (3, 0)$, giving 6 points. So $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid \#\tilde{\mathcal{E}}(\mathbb{F}_5)$, that is: $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid 6$.

$p = 7$. $\tilde{\mathcal{E}} : y^2 = x^3 + 3$, defined over $\mathbb{F}_7$. Then $\tilde{\mathcal{E}}(\mathbb{F}_7)$ consists of:

$\underline{0}, (1, \pm 2), (2, \pm 2), (3, \pm 3), (4, \pm 2), (5, \pm 3), (6, \pm 3)$, giving 13 points. So $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid 13$.

The only possibility is: $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) = 1$, and so $\mathcal{E}_{\text{tors}}(\mathbb{Q}) = \{\underline{0}\}$. Note that $(1, 2) \in \mathcal{E}(\mathbb{Q})$, but we know that $(1, 2)$ is not of finite order, so that $(1, 2), 2(1, 2), 3(1, 2), \dots$ are all distinct, and can conclude that $\mathcal{E}(\mathbb{Q})$ is infinite.

Note that, if we are given (for example) $\mathcal{F} : y^2 = x^3 + \frac{3}{5^6}$, we can apply $(x, y) \mapsto (5^2x, 5^3y)$ [with inverse $(x, y) \mapsto (\frac{x}{5^2}, \frac{y}{5^3})$] to transform $\mathcal{F}$ to $\mathcal{E}$ and so deduce that $\mathcal{F}_{\text{tors}}(\mathbb{Q}) = \{\underline{0}\}$ also.

Lemma 5.3. *Let $(x_1, y_1) \neq \underline{0}$ be a $\mathbb{Q}$ -rational torsion point on $\mathcal{E} : y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Z}$. Then $x_1, y_1 \in \mathbb{Z}$.*

Proof For any prime p , we have $A, B \in \mathbb{Z} \subset \mathbb{Z}_p$. Furthermore, $(x_1, y_1) \in \mathcal{E}_{\text{tors}}(\mathbb{Q}) \subset \mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$. By the last result of the previous section (Corollary 4.20) we know that $|x_1|_p \leq 1, |y_1|_p \leq 1$. In summary: $x_1, y_1 \in \mathbb{Q}$ and $x_1, y_1 \in \mathbb{Z}_p$ for all primes p .

Imagine that $x_1 \notin \mathbb{Z}$, that is, $x_1 = \frac{m}{n}$, where $m, n \in \mathbb{Z}$, $\gcd(m, n) = 1$, $n \neq \pm 1$. Then some prime p must divide n (and not divide m), giving $|x_1|_p = |\frac{m}{n}|_p = p^r$ (for some $r > 0$), which is > 1 . This contradicts $x \in \mathbb{Z}_p$, and so we conclude that $x_1 \in \mathbb{Z}$. Similarly $y_1 \in \mathbb{Z}$. $\square$

For example, this tells us immediately that the point $(\frac{1}{4}, \frac{7}{8})$ is of infinite order on the elliptic curve $\mathcal{E} : y^2 = x^3 - x + 1$.

Theorem 5.4. (Nagell-Lutz). Let $\underline{o} \neq (x_1, y_1) \in \mathcal{E}_{\text{tors}}(\mathbb{Q})$, where $\mathcal{E} : y^2 = x^3 + Ax + B$, and $A, B \in \mathbb{Z}$. Then $x_1, y_1 \in \mathbb{Z}$ and either $y_1 = 0$ or $y_1^2 \mid \Delta$, where $\Delta = 4A^3 + 27B^2$.

Proof From the last lemma, $x_1, y_1 \in \mathbb{Z}$. If $y_1 = 0$ then the result is satisfied; otherwise, (x_1, y_1) is not 2-torsion and we can consider $(x_2, y_2) = 2(x_1, y_1)$, with $(x_2, y_2) \neq \underline{o}$, and so $x_2, y_2 \in \mathbb{Q}$. But (x_2, y_2) is also a torsion point, so $x_2, y_2 \in \mathbb{Z}$. The line tangent to $\mathcal{E}$ at (x_1, y_1) has slope $\lambda = (3x_1^2 + A)/(2y_1)$; as usual, substituting $y = \lambda x + \mu$ into $\mathcal{E}$ gives $(\lambda x + \mu)^2 = x^3 + Ax + B$ and so $x^3 - \lambda^2 x^2 + \dots = 0$, giving $x_1 + x_1 + x_2 = -(\text{coeff of } x^2)/(\text{coeff of } x^3) = \lambda^2$, that is:

$$x_2 = \left(\frac{3x_1^2 + A}{2y_1} \right)^2 - 2x_1 \in \mathbb{Z}.$$

Now, we know $x_1, x_2 \in \mathbb{Z}$ and so $\left(\frac{3x_1^2 + A}{2y_1} \right)^2 \in \mathbb{Z}$. It follows that $4y_1^2 \mid (3x_1^2 + A)^2$ and so $y_1^2 \mid (3x_1^2 + A)^2$. Also, $y_1^2 = x_1^3 + Ax_1 + B$ and so trivially $y_1^2 \mid (x_1^3 + Ax_1 + B)$. Applying Euclid's Algorithm to $(3x_1^2 + A)^2$ and $x_1^3 + Ax_1 + B$ gives the identity

$$\phi_1(x)\psi_1(x) + \phi_2(x)\psi_2(x) = 4A^3 + 27B^2,$$

where $\phi_1(x) = 3x^2 + 4A$, $\psi_1(x) = (3x^2 + A)^2$, $\phi_2(x) = -27(x^3 + Ax + B)$, $\psi_2(x) = x^3 + Ax + B$. Since $y_1^2 \mid \psi_1(x_1)$ and $y_1^2 \mid \psi_2(x_1)$ we must have $y_1^2 \mid (\phi_1(x_1)\psi_1(x_1) + \phi_2(x_1)\psi_2(x_1)) = \Delta$, as required. $\square$

Example 5.5. Let $\mathcal{E} : y^2 = x^3 + 3x + 1$. Then $\Delta = 4 \cdot 3^3 + 27 \cdot 1^2 = 135 = 5 \cdot 3^3$. If $(x, y) \in \mathcal{E}_{\text{tors}}(\mathbb{Q})$, $(x, y) \neq \underline{o}$, then $x, y \in \mathbb{Z}$ and either $y = 0$ or $y^2 \mid 5 \cdot 3^3$, giving only $y = 0, \pm 1, \pm 3$ as possibilities.

Case $y = \pm 1$. From $\mathcal{E}$, $(\pm 1)^2 = x^3 + 3x + 1$ and so $x(x^2 + 3) = 0$. The only solution in $\mathbb{Z}$ is $x = 0$, giving $(0, \pm 1)$ as the only possibilities.

Case $y = \pm 3$. In this case, $x \in \mathbb{Z}$ satisfies $(\pm 3)^2 = x^3 + 3x + 1$ and so $x^3 + 3x - 8 = 0$. Let $f(x) = x^3 + 3x - 8$. Any integer root x of $f(x)$ must satisfy $x \mid (\text{constant term}) = (-8)$, giving $x = \pm 1, \pm 2, \pm 4, \pm 8$ as the only possibilities. When we substitute these, we find that $f(1), f(-1), \dots, f(-8)$ are all nonzero, so there are no points on $\mathcal{E}$ with $x \in \mathbb{Z}$ and $y = \pm 3$.

Case $y = 0$. In this case, $x \in \mathbb{Z}$ satisfies $0 = x^3 + 3x + 1$, and we only need to check $x = \pm 1$. neither of which are roots of $x^3 + 3x + 1$. So, there are no points on $\mathcal{E}$ with $x \in \mathbb{Z}$ and $y = 0$.

In summary, $\underline{o}, (0, 1), (0, -1)$ are the only possible torsion points. Is $(0, 1) \in \mathcal{E}_{\text{tors}}(\mathbb{Q})$? If it were then so would be $2(0, 1)$. But $2(0, 1) = (0, 1) + (0, 1) = (\frac{9}{4}, -\frac{35}{8})$; the coordinates are not in $\mathbb{Z}$ and so this is not a torsion point. Hence $(0, 1)$ must have infinite order. The same must be true for $(0, -1)$, since it is the inverse of $(0, 1)$. Conclusion: $\mathcal{E}_{\text{tors}}(\mathbb{Q}) = \{\underline{o}\}$.

Comment 5.6. For $\mathcal{E} : y^2 = x^3 + ax^2 + bx + c$, where $a, b, c \in \mathbb{Z}$, take

$$\Delta = \text{Disc}(x^3 + ax^2 + bx + c) = 4a^3c + 27c^2 + 4b^3 - a^2b^2 - 18abc.$$

For any prime $p \nmid 2\Delta$, $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\tilde{\mathcal{E}}(\mathbb{F}_p)$, so $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid \#\tilde{\mathcal{E}}(\mathbb{F}_p)$. Any $(x, y) \in \mathcal{E}_{\text{tors}}(\mathbb{Q})$ $[(x, y) \neq \underline{o}]$ satisfies $x, y \in \mathbb{Z}$, with $y = 0$ or $y^2 \mid \Delta$.

SECTION 6. A 2-ISOGENY ON AN ELLIPTIC CURVE

[In the following, we shall use upper case letters $X, Y, \dots$ for variables, and lower case letters $x, y, \dots$ for a point (x, y) .]

Suppose that $\mathcal{E}$ is an elliptic curve over $\mathbb{Q}$, together with a $\mathbb{Q}$ -rational point of order 2: $(x_0, 0)$. After a birational transformation $(x, y) \mapsto (x + x_0, y)$ [inverse $(x, y) \mapsto (x - x_0, y)$] we can assume that $(0, 0) \in \mathcal{E}(\mathbb{Q})$, so that $Y^2 = \text{cubic in } X$, with no constant term. As usual, after mappings of the form $(x, y) \mapsto (k^2x, k^3y)$, we can assume that the coefficients are in $\mathbb{Z}$. So, our elliptic curve can be taken to have the form

$$\mathcal{C} : Y^2 = X(X^2 + aX + b), \quad a, b \in \mathbb{Z}, \quad b(a^2 - 4b) \neq 0,$$

the last condition ensuring that the curve is non-singular. The point $(0, 0)$ is of order 2 on $\mathcal{C}$.

Let $P = (x, y)$ be a point on $\mathcal{C}$, and let $P_1 = (x, y) + (0, 0) = (x_1, y_1)$. Define $T_{(0,0)}$ by:

$$T_{(0,0)} : \mathcal{C} \rightarrow \mathcal{C} : (x, y) \mapsto (x, y) + (0, 0) = (x_1, y_1).$$

That is, $P \mapsto P + (0, 0)$. What are x_1, y_1 in terms of x, y ?

When $(x, y) = (0, 0)$, then $T_{(0,0)} : (0, 0) \mapsto \mathbf{0}$, since $(0, 0)$ is of order 2. When $x \neq 0$, we first find the line through $(0, 0)$ and (x, y) , which is: $Y = \frac{y}{x}X$. Substituting this into $\mathcal{C}$ gives:

$$\begin{aligned} \left(\frac{y}{x}\right)^2 X^2 &= X(X^2 + aX + b) \\ y^2 X^2 &= x^2 X^3 + ax^2 X^2 + bx^2 X \\ x(x^2 + ax + b)X^2 &= x^2 X^3 + ax^2 X^2 + bx^2 X \quad [\text{since } (x, y) \text{ is on } \mathcal{C}] \\ 0 &= xX^3 - (x^2 + b)X^2 + bxX, \quad [\text{since } x \neq 0] \end{aligned}$$

and so $X(X - x)(xX - b) = 0$. The roots of this cubic are: $X = 0, X = x, X = b/x$. The line $Y = \frac{y}{x}X$ and $\mathcal{C}$ intersect at:

$$(0, 0), (x, y) \text{ and } \left(\frac{b}{x}, \frac{by}{x^2}\right) \quad [\text{since } X = \frac{b}{x} \text{ gives } Y = \frac{y}{x}bx = \frac{by}{x^2}]$$

and so $(x, y) + (0, 0) = \left(\frac{b}{x}, -\frac{by}{x^2}\right) = (x_1, y_1)$, where $x_1 = \frac{b}{x}$, $y_1 = -\frac{by}{x^2}$.

We want to construct a 2-to-1 map ϕ from $\mathcal{C}$ to another curve $\mathcal{D}$ such that $\phi(P + (0, 0)) = \phi(P)$ for any P . We want expressions in x, y , call them $\lambda = \lambda(x, y)$, $\mu = \mu(x, y)$, such that $P = (x, y)$ and $P + (0, 0) = (x_1, y_1)$ map to the same (λ, μ) . Natural attempts are: $x + x_1 = x + \frac{b}{x}$ and $y + y_1 = y - \frac{by}{x^2}$. It turns out to be more convenient to choose $x + x_1 + a$ instead of $x + x_1$.

$$\text{Define: } \lambda = x + x_1 + a = x + \frac{b}{x} + a = \frac{x(x^2 + ax + b)}{x^2} = \frac{y^2}{x^2} = \left(\frac{y}{x}\right)^2.$$

$$\text{Define: } \mu = y + y_1 = y - \frac{by}{x^2}.$$

Both λ, μ are invariant under $T_{(0,0)}$. We have a map from $\mathcal{C}$, given by $(x, y) \mapsto (\lambda, \mu) = \left(\left(\frac{y}{x}\right)^2, y - \frac{by}{x^2}\right)$, which we shall call ϕ . We want to find the new curve $\mathcal{D}$ which this map is to, that is, we want the equation satisfied by λ and μ . Try:

$$\begin{aligned}\mu^2 &= \left(y - \frac{by}{x^2}\right)^2 = \left(\frac{y}{x}\left(x - \frac{b}{x}\right)\right)^2 = \left(\frac{y}{x}\right)^2 \left(x - \frac{b}{x}\right)^2 = \lambda \left(x^2 - 2b + \frac{b^2}{x^2}\right) \\ &= \lambda \left(x^2 + 2b + \frac{b^2}{x^2} - 4b\right) = \lambda \left(\left(x + \frac{b}{x}\right)^2 - 4b\right) = \lambda \left((\lambda - a)^2 - 4b\right) = \lambda(\lambda^2 - 2a\lambda + a^2 - 4b).\end{aligned}$$

So (λ, μ) is a point on the curve $\mathcal{D} : V^2 = U(U^2 + a_1U + b_1)$, where $a_1 = -2a$ and $b_1 = a^2 - 4b$. Our map ϕ is a rational map and it is easy to check that it is a homomorphism, with kernel $\{\underline{0}, (0, 0)\}$; such a map ϕ is a 2-isogeny on $\mathcal{C}$.

We can apply the same process to $\mathcal{D}$, taking $(u, v) \mapsto \left(\left(\frac{v}{u}\right)^2, v - \frac{b_1v}{u^2}\right)$ from $\mathcal{D}$ to the curve $Y^2 = X(X^2 - 2a_1X + a_1^2 - 4b_1)$, which is the same as $Y^2 = X(X^2 + 4aX + 16b)$ [since $-2(-2a) = 4a$ and $a_1^2 - 4b_1 = (-2a)^2 - 4(a^2 - 4b) = 16b$], that is:

$$\frac{Y^2}{64} = \frac{X}{4} \left(\frac{X^2}{16} + \frac{4aX}{16} + \frac{16b}{16} \right) = \frac{X}{4} \left(\frac{X^2}{16} + \frac{aX}{4} + b \right),$$

and so $\left(\frac{Y}{8}\right)^2 = \frac{X}{4} \left(\left(\frac{X}{4}\right)^2 + a\left(\frac{X}{4}\right) + b \right)$. So, the map $\hat{\phi} : (u, v) \mapsto \left(\frac{1}{4}\left(\frac{v}{u}\right)^2, \frac{1}{8}\left(v - \frac{b_1v}{u^2}\right)\right)$ is a map from $\mathcal{D}$ back to $\mathcal{C}$ (the *dual isogeny*). The properties are the same as for ϕ , namely: $\hat{\phi}$ is a homomorphism with kernel $\{\underline{0}, (0, 0)\}$.

Note also that, if we let $\alpha_1 = \frac{-a + \sqrt{a^2 - 4b}}{2}$, $\alpha_2 = \frac{-a - \sqrt{a^2 - 4b}}{2}$ denote the roots of $X^2 + aX + b$, then $\phi((\alpha_1, 0)) = \phi((\alpha_2, 0)) = (0, 0)$, and so the kernel of $\hat{\phi} \circ \phi$ consists precisely of the 2-torsion of $\mathcal{C}$, namely: $\{\underline{0}, (0, 0), (\alpha_1, 0), (\alpha_2, 0)\}$. Indeed, it is easy to show that $\hat{\phi} \circ \phi$ is the multiplication by 2 map on $\mathcal{C}$. We summarise as follows.

Lemma 6.1. *Let $\mathcal{C} : Y^2 = X(X^2 + aX + b)$, where $a, b \in \mathbb{Z}, b \neq 0, a^2 - 4b \neq 0$, and let $\mathcal{D} : V^2 = U(U^2 + a_1U + b_1)$, where $a_1 = -2a$ and $b_1 = a^2 - 4b$.*

$$\text{Define } \phi : \mathcal{C} \longrightarrow \mathcal{D} \text{ by } \phi(x, y) = \left(\left(\frac{y}{x}\right)^2, y - \frac{by}{x^2}\right).$$

$$\text{Define } \hat{\phi} : \mathcal{D} \longrightarrow \mathcal{C} \text{ by } \hat{\phi}(u, v) = \left(\frac{1}{4}\left(\frac{v}{u}\right)^2, \frac{1}{8}\left(v - \frac{b_1v}{u^2}\right)\right).$$

Then the 2-isogenies $\phi, \hat{\phi}$ are 2-to-1 homomorphisms, each with kernel $\{\underline{0}, (0, 0)\}$. Since $\phi, \hat{\phi}$ are defined over $\mathbb{Q}$, we also have $\phi : \mathcal{C}(\mathbb{Q}) \rightarrow \mathcal{D}(\mathbb{Q})$ and $\hat{\phi} : \mathcal{D}(\mathbb{Q}) \rightarrow \mathcal{C}(\mathbb{Q})$. The compositions $\hat{\phi} \circ \phi$ and $\phi \circ \hat{\phi}$ are the multiplication by 2 maps [2] on $\mathcal{C}$ and $\mathcal{D}$, respectively.

We shall concentrate for the moment on $\phi : \mathcal{C} \rightarrow \mathcal{D}$. Note that we can formally invert $(u, v) = \phi(x, y) = \left(\left(\frac{y}{x}\right)^2, y - \frac{by}{x^2}\right)$, as follows. Since $u = \left(\frac{y}{x}\right)^2$, we have $\frac{y}{x} = \pm u^{1/2}$. For the

moment, say $\frac{y}{x} = u^{1/2}$. We also have

$$\begin{aligned} u^{-1/2}v &= \frac{x}{y} \left(y - \frac{by}{x^2} \right) = x - \frac{b}{x}, \\ u &= \left(\frac{y}{x} \right)^2 = \frac{y^2}{x^2} = \frac{x(x^2 + ax + b)}{x^2} = x + a + \frac{b}{x}, \end{aligned}$$

and so: $u^{-1/2}v + u = 2x + a$. Solving for x, y then gives the following preimages.

Lemma 6.2. *Let $\mathcal{C}, \mathcal{D}, \phi$ be as in Lemma 6.1, and let (u, v) be a point on $\mathcal{D}$ with $u \neq 0$. Let*

$$\begin{aligned} x_1 &= (u + u^{-1/2}v - a)/2, & y_1 &= u^{1/2}x_1 = u^{1/2}(u + u^{-1/2}v - a)/2, \\ x_2 &= (u - u^{-1/2}v - a)/2, & y_2 &= -u^{1/2}x_1 = -u^{1/2}(u - u^{-1/2}v - a)/2. \end{aligned}$$

Then $\phi(x_1, y_1) = \phi(x_2, y_2) = (u, v)$.

We shall shortly make use of these to define helpful maps on $\mathcal{C}(\mathbb{Q})$ and $\mathcal{D}(\mathbb{Q})$. First, we recall the notation $\mathbb{Q}^*$ and $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ [see also Example 0.30(b)]. As usual, let $\mathbb{Q}^*$ denote the group of nonzero members of $\mathbb{Q}$ under multiplication, so that $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ is $\mathbb{Q}^*$ modulo squares. For example, $\frac{12}{49} = 3$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ since $\frac{12}{49} = 3\frac{4}{49} = 3\left(\frac{2}{7}\right)^2 = 3$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. Note that any member of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ can be written uniquely as a square free integer (that is, as an integer not divisible by any square except 1).

{ *Aside: Our main aim here is to show the Weak Mordell-Weil Theorem, that $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is finite, which we shall achieve by showing that $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ and $\mathcal{C}(\mathbb{Q})/\hat{\phi}(\mathcal{D}(\mathbb{Q}))$ are finite, and then using the fact that $\hat{\phi} \circ \phi = [2]$. }*

From now on, we denote $\mathcal{C}(\mathbb{Q})$ by $\mathcal{G}$ and $\mathcal{D}(\mathbb{Q})$ by $\mathcal{H}$ [both groups under addition $+$ given by the group law on elliptic curves, with identity $\mathbf{0}$].

Lemma 6.3. *Let $(u, v) \in \mathcal{H}$. Then:*

$$(u, v) \in \phi(\mathcal{G}) \iff u \in (\mathbb{Q}^*)^2 \text{ or } [u = 0 \text{ and } a^2 - 4b \in (\mathbb{Q}^*)^2].$$

Proof

Case 1 $u \neq 0$. From the expressions in Lemma 6.2 for $(x_1, y_1), (x_2, y_2)$ such that $\phi(x_1, y_1) = \phi(x_2, y_2) = (u, v)$, which are in terms of $u, v, u^{1/2}$, we see that:

$$(u, v) \in \phi(\mathcal{G}) \iff u^{1/2} \in \mathbb{Q} \iff u \in (\mathbb{Q}^*)^2.$$

Case 2 $u = 0$. The expressions in Lemma 6.2 do not apply here, since they include $u^{-1/2}$. But we know that $\phi(\alpha_1, 0) = \phi(\alpha_2, 0) = (0, 0)$, where $\alpha_1 = \frac{-a+\sqrt{a^2-4b}}{2}$, $\alpha_2 = \frac{-a-\sqrt{a^2-4b}}{2}$ denote the roots of $X^2 + aX + b$. Hence:

$$(0, 0) \in \phi(\mathcal{G}) \iff \alpha_1 \text{ or } \alpha_2 \in \mathbb{Q} \iff a^2 - 4b \in (\mathbb{Q}^*)^2, \text{ as required.} \quad \square$$

This suggests the following map on $\mathcal{H}$.

Definition 6.4. Define the map $q : \mathcal{H} \rightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$ by:

$$q(u, v) = \begin{cases} u & \text{when } u \neq 0 \\ b_1 = a^2 - 4b & \text{when } u = 0. \end{cases}$$

Also define $q(\mathbf{o}) = 1$.

Note that we can equivalently define $q(u, v)$ to be d such that the preimages of (u, v) under ϕ are defined over $\mathbb{Q}(\sqrt{d})$.

Lemma 6.5. *The map $q : \mathcal{H} \rightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$ of Definition 6.4 is a homomorphism with kernel $\phi(\mathcal{G})$ (so that the induced map $q : \mathcal{H}/\phi(\mathcal{G}) \rightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$ is an injective homomorphism).*

Proof We only show that $q(P+Q) = q(P)q(Q)$ in the typical case when none of $P, Q, P+Q$ are $(0, 0)$ or $\mathbf{o}$. Let $(u_1, v_1), (u_2, v_2), (u_3, v_3)$ be 3 points on $\mathcal{H} = \mathcal{D}(\mathbb{Q})$ which sum to $\mathbf{o}$, [so that $(u_1, v_1) + (u_2, v_2) = (u_3, -v_3)$]. Then these are the 3 points of intersection between $\mathcal{D}$ and some line defined over $\mathbb{Q}$: $V = \ell U + m$, say. Substituting $V = \ell U + m$ into $\mathcal{D}$ gives: $U(U^2 + a_1U + b_1) - (\ell U + m)^2$, whose 3 roots must be u_1, u_2, u_3 . That is: $U(U^2 + a_1U + b_1) - (\ell U + m)^2 = (U - u_1)(U - u_2)(U - u_3)$. Equating constant terms gives: $u_1u_2u_3 = m^2 = 1$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, and so $u_1u_2 = 1/u_3 = u_3$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. Therefore, by the definition of q we have: $q((u_1, v_1))q((u_2, v_2)) = q((u_3, -v_3)) = q((u_1, v_1) + (u_2, v_2))$, so that q is a homomorphism.

The fact that $\ker q = \phi(\mathcal{G})$ is an immediate consequence of Lemma 6.3. $\square$

Lemma 6.6. *The map $q : \mathcal{H} \rightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$ of Definition 6.4 has finite image. Indeed, if $r \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ is written as a square free integer, then $r \in \text{im } q \implies r|b_1$. Under q , $\mathcal{H}/\phi(\mathcal{G})$ is isomorphic to the subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ consisting of all square free integers $r|b_1$ such that*

$$W_r : r\ell^4 + a_1\ell^2m^2 + (b_1/r)m^4 = n^2, \quad \text{for some } \ell, m, n \in \mathbb{Z}, \text{ not all 0, with } \gcd(\ell, m) = 1.$$

When this is satisfied, there is a point $(u, v) \in \mathcal{H}$ such that $q(u, v) = r$, satisfying $u = r(\frac{\ell}{m})^2$.

Proof Let $r \in \mathbb{Q}^*/(\mathbb{Q}^*)^2, r \in \text{im } q, r \in \mathbb{Z}, r$ square free. We want to prove that $r|b_1$. Suppose $r = q(u, v)$, where $(u, v) \in \mathcal{D}(\mathbb{Q})$, which must exist since $r \in \text{im } q$. Then: $r = q(u, v) = u = u^2 + a_1u + b_1$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ [since $u(u^2 + a_1u + b_1) = v^2$]. So, $r, u, u^2 + a_1u + b_1$ are all the same modulo squares, which means we can write:

$$u^2 + a_1u + b_1 = rs^2, \quad u = rt^2, \quad \text{for some } s, t \in \mathbb{Q}.$$

Hence: $(rt^2)^2 + a_1(rt^2) + b_1 = rs^2$. Let $t = \ell/m$, where $\ell, m \in \mathbb{Z}$ and $\gcd(\ell, m) = 1$. Then: $r^2\ell^4/m^4 + a_1r\ell^2/m^2 + b_1 = rs^2$, and so: $r^2\ell^4 + a_1r\ell^2m^2 + b_1m^4 = r(m^2s)^2$. Now, $a_1, b_1, r, \ell, m \in \mathbb{Z}$, so the LHS of this last equation is in $\mathbb{Z}$, and so the RHS is also in $\mathbb{Z}$; that is: $r(m^2s)^2 \in \mathbb{Z}$. Since r is square free, we must therefore have $m^2s \in \mathbb{Z}$. Define: $n = m^2s \in \mathbb{Z}$. Then our equation becomes:

$$r^2\ell^4 + a_1r\ell^2m^2 + b_1m^4 = rn^2, \quad \text{for some } \ell, m, n \in \mathbb{Z}, \gcd(\ell, m) = 1, \quad (*)$$

(from which we have W_r in the statement of the lemma, after dividing both side by r).

We want to show that $r|b_1$, and we know that r is square free. It is sufficient to show, for any prime p , that $p|r \Rightarrow p|b_1$.

Imagine $p|r$ and $p \nmid b_1$, for some prime p . Then $p|r^2\ell^4, a_1r\ell^2m^2, rn^2$ and so by $(*)$, $p|b_1m^4$, which in turn gives: $p|m$ [since $p \nmid b_1$]. Hence, since now $p|r$ and $p|m$, we have: $p^2|r^2\ell^4, a_1r\ell^2m^2, b_1m^4$, and so by $(*)$, $p^2|rn^2$, which in turn gives: $p|n$ [since r is square free]. Hence, since now $p|r, m, n$, we have: $p^3|a_1r\ell^2m^2, b_1m^4, rn^2$, and so by $(*)$, $p^3|r^2\ell^4$, which in turn gives: $p|\ell$ [since r is square free]. This is a contradiction, since $p|\ell$ and $p|m$ but $\gcd(\ell, m) = 1$.

The above assumption that $p|r$ and $p \nmid b_1$ let to a contradiction, and so it is impossible for any prime p to satisfy $p|r$ and $p \nmid b_1$. This is the same as saying that $p|r \Rightarrow p|b_1$ for any prime p . Since r is square free, we conclude that $r|b_1$, as required $\square$

Comment 6.7. If we similarly define $\hat{q} : \mathcal{G} \rightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$ by:

$$\hat{q}(x, y) = \begin{cases} x & \text{when } x \neq 0 \\ b = a_1^2 - 4b_1 & \text{when } x = 0, \end{cases}$$

and $\hat{q}(\underline{\mathbf{o}}) = 1$, then, by the same argument, $\hat{q}$ has finite image. If $r \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ is written as a square free integer, then $r \in \text{im } \hat{q} \implies r|b$. Under $\hat{q}$, $\mathcal{G}/\hat{\phi}(\mathcal{H})$ is isomorphic to the subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ consisting of all square free integers $r|b$ such that

$$\widehat{W}_r : r\ell^4 + a\ell^2m^2 + (b/r)m^4 = n^2, \quad \text{for some } \ell, m, n \in \mathbb{Z}, \text{ not all 0, with } \gcd(\ell, m) = 1.$$

When $\widehat{W}_r$ is satisfied, there is a point $(x, y) \in \mathcal{G}$ such that $q(x, y) = r$, satisfying $x = r\left(\frac{\ell}{m}\right)^2$.

Theorem 6.8. *Both $\mathcal{G}/\hat{\phi}(\mathcal{H})$ and $\mathcal{H}/\phi(\mathcal{G})$ are finite.*

(immediate from 6.5, 6.6, 6.7).

Corollary 6.9. *(The Weak Mordell-Weil Theorem, for an elliptic curve $\mathcal{C}$ which has a rational point of order 2). $\mathcal{G}/2\mathcal{G} = \mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$ is finite.*

Proof We know from Theorem 6.8 that $\mathcal{G}/\hat{\phi}(\mathcal{H})$ and $\mathcal{H}/\phi(\mathcal{G})$ are finite, so let $\mathcal{G}/\hat{\phi}(\mathcal{H}) = \{g_1, \dots, g_k\}$ and $\mathcal{H}/\phi(\mathcal{G}) = \{h_1, \dots, h_\ell\}$. Let $g \in \mathcal{G}$. We can write g as:

$$\begin{aligned} g &= g_i + \hat{\phi}(h), \text{ for some } g_i \in \{g_1, \dots, g_k\}, h \in \mathcal{H} \\ &= g_i + \hat{\phi}(h_j + \phi(g')), \text{ for some } h_j \in \{h_1, \dots, h_\ell\}, g' \in \mathcal{G} \\ &= g_i + \hat{\phi}(h_j) + \hat{\phi}(\phi(g')) \quad [\text{since } \hat{\phi} \text{ is a homomorphism}] \\ &= g_i + \hat{\phi}(h_j) + 2g' \quad [\text{since } \hat{\phi} \circ \phi = [2]] \\ &= g_i + \hat{\phi}(h_j) \quad \text{in } \mathcal{G}/2\mathcal{G}. \end{aligned}$$

Hence $\mathcal{G}/2\mathcal{G}$ is a subset of $\{g_i + \hat{\phi}(h_j) : 1 \leq i \leq k, 1 \leq j \leq \ell\}$, which is finite, and so $\mathcal{G}/2\mathcal{G}$ is finite. $\square$

Theorem 6.10. (*The Weak Mordell-Weil Theorem*). *Let $\mathcal{E}$ be any elliptic curve over $\mathbb{Q}$. Then $\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q})$ is finite.*

(See Chapter VIII of Silverman)

Comment 6.11. A *Boolean* group is defined to be a group such that $g * g$ is the identity, for any element g . A finite Boolean group, generated by the independent elements $g_1, \dots, g_n$, has 2^n elements. Given any Abelian group G , the quotient group $G/2G$ is always Boolean. When $G/2G$ is finite, $\#G/2G$ is always a power of 2 and is isomorphic to $C_2 \times \dots \times C_2$.

Suppose we are give an elliptic curve of the form $\mathcal{C} : Y^2 = X(X^2 + aX + b)$, and we derive the associated objects already described, namely $\mathcal{D} : V^2 = U(U^2 + a_1U + b_1)$, where $a_1 = -2a, b_1 = a^2 - 4b$, with $\mathcal{G} = \mathcal{C}(\mathbb{Q}), \mathcal{H} = \mathcal{D}(\mathbb{Q}), \phi : \mathcal{G} \rightarrow \mathcal{H}, \hat{\phi} : \mathcal{H} \rightarrow \mathcal{G}, q : \mathcal{H}/\phi(\mathcal{G}) \rightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2, \hat{q} : \mathcal{G}/\hat{\phi}(\mathcal{H}) \rightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Then the above results and their proofs give a method for trying to compute $\mathcal{G}/2\mathcal{G}$.

Step 1. Try to find $\mathcal{H}/\phi(\mathcal{G})$ by finding all square free integers $r|b_1$ satisfying W_r .

Step 2. Try to find $\mathcal{G}/\hat{\phi}(\mathcal{H})$ by finding all square free integers $r|b$ satisfying $\widehat{W}_r$.

Step 3. Combine $\mathcal{G}/\hat{\phi}(\mathcal{H})$ and $\hat{\phi}(\mathcal{H}/\phi(\mathcal{G}))$ to generate $\mathcal{G}/2\mathcal{G}$.

Example 6.12. Let $\mathcal{C} : Y^2 = X(X^2 - X + 6)$. Then $\mathcal{G}/2\mathcal{G} = \mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q}) \cong C_2 \times C_2$.

Proof Here, $a = -1, b = 6$ and so $a_1 = -2a = 2, b_1 = a^2 - 4b = -23$, giving $\mathcal{D} : V^2 = U(U^2 + 2U - 23)$. The isogeny $\phi : \mathcal{C} \rightarrow \mathcal{D}$ is given by $\phi(x, y) = \left(\left(\frac{y}{x}\right)^2, y - \frac{by}{x^2}\right) = \left(\left(\frac{y}{x}\right)^2, y - \frac{6y}{x^2}\right)$.

The isogeny $\hat{\phi} : \mathcal{D} \rightarrow \mathcal{C}$ is given by $\hat{\phi}(u, v) = \left(\frac{1}{4}\left(\frac{v}{u}\right)^2, \frac{1}{8}\left(v - \frac{b_1v}{u^2}\right)\right) = \left(\frac{1}{4}\left(\frac{v}{u}\right)^2, \frac{1}{8}\left(v + \frac{23v}{u^2}\right)\right)$.

Step 1. Find $\mathcal{H}/\phi(\mathcal{G})$. We need to consider $r|b_1 = -23, r \in \mathbb{Z}, r$ square free, that is, $r = \pm 1, \pm 23$, and $q(\underline{\mathbf{o}}) = 1, q(0, 0) = b_1 = -23$, so that: $\{1, -23\} \leq \text{im } q \leq \{\pm 1, \pm 23\}$. Note that $-1 \in \text{im } q \iff 23 \in \text{im } q$, and so it is only necessary to check one member of the coset $\{-1, 23\}$.

Choose $r = -1$. Then equation $W_r, r\ell^4 + a_1\ell^2m^2 + (b_1/r)m^4 = n^2$ becomes:

$$W_{-1} : -\ell^4 + 2\ell^2m^2 + 23m^4 = n^2, \quad \text{for some } \ell, m, n \in \mathbb{Z}, \text{ not all 0, with } \gcd(\ell, m) = 1.$$

On completing the square, we obtain:

$$-(\ell^2 - m^2)^2 + 24m^4 = n^2. \quad (1)$$

This gives $-(\ell^2 - m^2)^2 \equiv n^2 \pmod{3}$.

Imagine $3 \nmid (\ell^2 - m^2)$; then $\ell^2 - m^2$ would have an inverse $\alpha \pmod{3}$, and so $-1 \equiv (\alpha n)^2 \pmod{3}$, contradicting the fact that -1 is not a quadratic residue mod 3.

Hence, by reductio, $3|(\ell^2 - m^2)$ and so $3|n$ [since $3|n^2$], giving that $3^2|(\ell^2 - m^2)^2$ and $3^2|n^2$, so that, from (1), $3^2|24m^4$, and so $3|m^4$ [since $3^1||24$], giving $3|m$. But combining $3|m$ with $3|\ell^2 - m^2$ gives $3|\ell^2$, so that $3|\ell$. We have shown that $3|\ell$ and $3|m$, contradicting $\gcd(\ell, m) = 1$. Hence there are no solutions to W_{-1} , giving that $-1 \notin \text{im } q$ [indeed, we have shown that there are no solutions $(\ell, m, n) \neq (0, 0, 0)$ in $\mathbb{Q}_3$].

This gives $\text{im } q = \{1, -23\}$ and $\mathcal{H}/\phi(\mathcal{G}) = \{\underline{\mathbf{o}}, (0, 0)\} = \langle (0, 0) \rangle \cong C_2$.

Step 2. Find $\mathcal{G}/\hat{\phi}(\mathcal{H})$. We need to consider $r|b = 6, r \in \mathbb{Z}$, r square free, that is, $r = \pm 1, \pm 2, \pm 3, \pm 6$. Also, $\hat{q}(\underline{\mathbf{o}}) = 1$, $\hat{q}(2, 4) = 2$, $\hat{q}(3, -6) = 3$, $\hat{q}(0, 0) = b = 6$, so that $\{1, 2, 3, 6\} \leq \text{im } \hat{q} \leq \{\pm 1, \pm 2, \pm 3, \pm 6\}$. Note that $-1 \in \text{im } \hat{q} \iff -2 \in \text{im } \hat{q} \iff -3 \in \text{im } \hat{q} \iff -6 \in \text{im } \hat{q}$, and so it is only necessary to check one member of the coset $\{-1, -2, -3, -6\}$.

Choose $r = -1$. Then $\widehat{W}_{-1}, r\ell^4 + a\ell^2m^2 + (b/r)m^4 = n^2$ becomes:

$$\widehat{W}_{-1} : -\ell^4 - \ell^2m^2 - 6m^4 = n^2, \quad \text{for some } \ell, m, n \in \mathbb{Z}, \text{ not all 0, with } \gcd(\ell, m) = 1.$$

For any $\ell, m, n \in \mathbb{Z}$, $\ell^4, \ell^2m^2, 6m^4 \geq 0$, so $-\ell^4 - \ell^2m^2 - 6m^4 \leq 0$, and

$$\text{LHS} = -\ell^4 - \ell^2m^2 - 6m^4 = 0 \iff \ell^4 = \ell^2m^2 = 6m^4 = 0 \iff \ell = m = 0.$$

Also, $\text{RHS} = n^2 \geq 0$ and $n^2 = 0 \iff n = 0$. Both sides are equal $\iff$ both sides are 0 $\iff \ell = m = n = 0$, but we require ℓ, m, n to be not all 0. Hence there are no solutions to $\widehat{W}_{-1}$, giving that $-1 \notin \text{im } \hat{q}$ [indeed, we have shown that there are no solutions $(\ell, m, n) \neq (0, 0, 0)$ in $\mathbb{R}$].

We conclude that $\text{im } \hat{q} = \{1, 2, 3, 6\}$ and $\mathcal{G}/\hat{\phi}(\mathcal{H}) = \{\underline{\mathbf{o}}, (0, 0), (2, 4), (3, -6)\} = \langle (0, 0), (2, 4) \rangle$.

Step 3. Find $\mathcal{G}/2\mathcal{G}$. This is generated by $\mathcal{G}/\hat{\phi}(\mathcal{H}) = \{\underline{\mathbf{o}}, (0, 0), (2, 4), (3, -6)\} = \langle (0, 0), (2, 4) \rangle$, together with $\hat{\phi}(\mathcal{H}/\phi(\mathcal{G})) = \{\hat{\phi}(\underline{\mathbf{o}}), \hat{\phi}(0, 0)\} = \{\underline{\mathbf{o}}\}$, which gives nothing new that wasn't already in $\mathcal{G}/\hat{\phi}(\mathcal{H})$. Therefore, $\mathcal{G}/2\mathcal{G} = \{\underline{\mathbf{o}}, (0, 0), (2, 4), (3, -6)\} = \langle (0, 0), (2, 4) \rangle \cong C_2 \times C_2$, as required. Note that $(0, 0), (2, 4)$ are independent in $\mathcal{G}/\hat{\phi}(\mathcal{H})$ and so are independent in $\mathcal{G}/2\mathcal{G}$ [since $2\mathcal{G} = \hat{\phi}(\phi(\mathcal{G})) \leq \hat{\phi}(\mathcal{H})$]. $\square$

Comment 6.13. The equations

$$W_r : r\ell^4 + a_1\ell^2m^2 + (b_1/r)m^4 = n^2,$$

$$\widehat{W}_r : r\ell^4 + a\ell^2m^2 + (b/r)m^4 = n^2,$$

[which can also be expressed as: $rX^4 + a_1X^2 + b_1/r = Y^2$ and $rX^4 + aX^2 + b/r = Y^2$, for $X, Y \in \mathbb{Q}$] are called *homogeneous spaces*. Consider $\mathcal{C} : Y^2 = X^3 + 17X$, so that $\mathcal{D} : Y^2 = X^3 - 68X$. For the $r = 2$ case of Step 1 (finding $\mathcal{H}/\phi(\mathcal{G})$), we have $W_2 : 2\ell^4 - 34m^4 = n^2$. Setting $n = 2k$ gives: $\ell^4 - 17m^4 = 2k^2$ (Problem Sheet 4). Here $2 \notin \text{im } q$, even though there exist solutions in $\mathbb{R}$ and every $\mathbb{Q}_p$.

SECTION 7. THE MORDELL-WEIL THEOREM

When $\mathcal{E}$ is an elliptic curve over $\mathbb{Q}$, we've seen that $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ and $\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q})$ are finite. But $\mathcal{E}(\mathbb{Q})$ may sometimes be infinite [if $P \in \mathcal{E}(\mathbb{Q})$ and $P \notin \mathcal{E}_{\text{tors}}(\mathbb{Q})$ then P is of infinite order and so $\mathcal{E}(\mathbb{Q})$ is infinite]. We shall show that $\mathcal{E}(\mathbb{Q})$ [whether finite or infinite] is always finitely generated. That is, we aim to show that, for any elliptic curve $\mathcal{E}$, there exists finite number of elements $P_1, \dots, P_k \in \mathcal{E}(\mathbb{Q})$ such that every $P \in \mathcal{E}(\mathbb{Q})$ can be written as:

$$P = m_1 P_1 + \dots + m_k P_k, \quad m_1, \dots, m_k \in \mathbb{Z}.$$

Definition 7.1. Let A be an Abelian group with group operation $+$.

We say that $h : A \rightarrow \mathbb{R}$ is a *height function* if it satisfies:

- (1) For any $Q \in A$, there exists $C_1 = C_1(Q)$ such that $h(P + Q) \leq 2h(P) + C_1$ for all $P \in A$.
- (2) There exists C_2 , independent of P , such that $h(2P) \geq 4h(P) - C_2$ for all $P \in A$.
- (3) For any C_3 , the set $\{P \in A : h(P) \leq C_3\}$ is finite.

Theorem 7.2. *Let A be an Abelian group which has a height function h , and suppose that $A/2A$ is finite. Then A is finitely generated.*

Proof We are given that $A/2A$ is finite, so let $A/2A = S = \{Q_1, \dots, Q_r\} \subset A$. Let P be any element of A . Then $P = Q_{i_1}$ in $A/2A$ for some $Q_{i_1} \in S$ and so we can write: $P = 2P_1 + Q_{i_1}$, for some $P_1 \in A$. Inductively, continue to write: $P_1 = 2P_2 + Q_{i_2}, P_2 = 2P_3 + Q_{i_3}, \dots$, where each $P_j \in A$ and each $Q_{i_j} \in S$. Now:

$$h(P_j) \leq \frac{1}{4}(h(2P_j) + C_2) \text{ [by (2)]} = \frac{1}{4}(h(P_{j-1} - Q_{i_j}) + C_2) \leq \frac{1}{4}(2h(P_{j-1}) + C'_1 + C_2) \text{ [by (1)]},$$

where:

$$C'_1 = \max\{C_1(-Q) : Q \in S\}. \text{ So, if } h(P_{j-1}) > (C'_1 + C_2)/2 \text{ then:}$$

$$h(P_j) < \frac{1}{4}(2h(P_{j-1}) + 2h(P_{j-1})) = h(P_{j-1}).$$

Imagine that $h(P) > (C'_1 + C_2)/2$ and $h(P_j) > (C'_1 + C_2)/2$ for all j . Then the sequence $h(P), h(P_1), h(P_2), \dots$ would be strictly decreasing, giving infinitely many distinct members of A with height $\leq h(P)$, which would contradict (3).

This contradiction shows that there must exist an n such that $h(P_n) \leq (C'_1 + C_2)/2$. So, we can write: $P = 2P_1 + Q_{i_1} = 2(2P_2 + Q_{i_2}) + Q_{i_1} = \dots$, and after n steps P will be written as a linear combination of P_n and members of S . Let $T = \{Q \in A : h(Q) \leq (C'_1 + C_2)/2\}$. We have shown (since $P_n \in T$) that any $P \in A$ is a linear combination of members of $S \cup T$. Furthermore, T is finite, by (3). In conclusion: A is generated by the finite set $S \cup T$, and so is finitely generated. $\square$

A height function on $\mathcal{E}(\mathbb{Q})$ can be obtained as follows.

Lemma 7.3. *Let $\mathcal{E}$ be an elliptic curve, defined over $\mathbb{Q}$. Define $h_x : \mathcal{E}(\mathbb{Q}) \rightarrow \mathbb{R}$ by:*

$$h_x((x, y)) = \log \max(|a|, |b|), \quad \text{where } x = \frac{a}{b}, \quad a, b \in \mathbb{Z}, \quad \gcd(a, b) = 1,$$

and define $h_x(\underline{0}) = 0$. Then h_x is a height function on $\mathcal{E}(\mathbb{Q})$. Indeed, there exists a constant C , independent of P, Q , such that $|h_x(P + Q) + h_x(P - Q) - 2h_x(P) - 2h_x(Q)| \leq C$, for all $P, Q \in \mathcal{E}(\mathbb{Q})$, from which properties (1),(2) can be deduced [property (3) is trivially true].

For the proof (optional) see, for example, p.201 of Silverman.

Theorem 7.4. *(The Mordell-Weil Theorem). Let $\mathcal{E}$ be any elliptic curve over $\mathbb{Q}$. Then $\mathcal{E}(\mathbb{Q})$ is finitely generated.*

Proof This follows immediately from Theorem 6.10, Theorem 7.2 and Lemma 7.3. □

Comment 7.5. This means that we know what $\mathcal{E}(\mathbb{Q})$ looks like:

$$\mathcal{E}(\mathbb{Q}) \cong \mathcal{E}_{\text{tors}}(\mathbb{Q}) \times \mathbb{Z}^r, \quad \text{for some } r \geq 0, r \in \mathbb{Z}.$$

The number r is called the *rank* of $\mathcal{E}(\mathbb{Q})$ (or just the rank of $\mathcal{E}$). Clearly:

$$\mathcal{E}(\mathbb{Q}) \text{ has finitely many points} \iff \text{rank}(\mathcal{E}(\mathbb{Q})) = 0.$$

To solve $\mathcal{E}(\mathbb{Q})$, we want to know: $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ and r (the rank). Note that:

$$\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q}) \cong \mathcal{E}_{\text{tors}}(\mathbb{Q})/2\mathcal{E}_{\text{tors}}(\mathbb{Q}) \times \left(\mathbb{Z}/2\mathbb{Z}\right)^r,$$

so that:

$$\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q}) \cong \mathcal{E}(\mathbb{Q})[2] \times C_2^r,$$

where $\mathcal{E}(\mathbb{Q})[2]$ denotes the 2-torsion subgroup of $\mathcal{E}(\mathbb{Q})$ (see Comment 0.40).

Example 7.6. Let $\mathcal{C} : Y^2 = X(X^2 - X + 6)$. In Example 6.12, we found that $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q}) \cong C_2 \times C_2$. Also, $\mathcal{C}(\mathbb{C})[2] = \{\underline{0}\} \cup \{\text{points of order 2}\} = \{\underline{0}, (0, 0), (\frac{1+\sqrt{-23}}{2}, 0), (\frac{1-\sqrt{-23}}{2}, 0)\}$, so that $\mathcal{C}(\mathbb{Q})[2] = \{\underline{0}, (0, 0)\} \cong C_2$. Since $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q}) \cong \mathcal{C}(\mathbb{Q})[2] \times C_2^r$, we deduce that $C_2 \times C_2 \cong C_2 \times C_2^r$ and so the rank $r = 1$ [$\mathcal{C}(\mathbb{Q})$ is infinite, but is generated by $\mathcal{C}_{\text{tors}}(\mathbb{Q})$ and one element of infinite order].

SECTION 8. CRYPTOGRAPHY

Public keys allow message to be encoded (not decoded). Suppose A wants to send the integer X to B safely; we assume that everything transmitted can be intercepted.

Step 1. B (in private) takes 2 large prime numbers p, q (usually about 250 digits) and multiplies them together to give $N = pq$, chooses an exponent d , and publicises N, d to the world.

Step 2. A (in private) computes $Y \equiv X^d \pmod{N}$ and sends the message Y to B.

Step 3. B privately computes $\phi(N) = \phi(p)\phi(q) = (p-1)(q-1)$ and also computes (by Euclid's Algorithm) e such that $de \equiv 1 \pmod{\phi(N)}$. Note that:

$$Y^e \equiv (X^d)^e \equiv X^{de} = X^{1+k\phi(N)} \text{ [for some } k \in \mathbb{Z}] \equiv X(X^{\phi(N)})^k \equiv X,$$

since $X^{\phi(N)} \equiv 1 \pmod{N}$ by Euler's Theorem, provided that X, N are coprime. Assuming $X < N$, this decodes the message.

Note that computing $X^d \pmod{N}$ [and $Y^e \pmod{N}$] is fast even when d is large, by writing d in base 2 as $d = 2^{k_1} + \dots + 2^{k_m}$ ($k_1 < \dots < k_m$). One then obtains $X^{2^0} \equiv X$, $X^{2^1} \equiv (X^{2^0})^2$, $X^{2^2} \equiv (X^{2^1})^2, \dots, X^{2^{k_m}}$, by k_m squaring operations, after which:

$$X^d \equiv X^{2^{k_1}} X^{2^{k_2}} \dots X^{2^{k_m}} \pmod{N},$$

which takes roughly $\log d$ operations.

Anyone wishing to crack the code must be able to compute $\phi(N)$, which requires finding p, q from $N = pq$. A naive (and very slow) approach is trial division: checking for each $c = 2, \dots, [\sqrt{N}]$ whether $c|N$.

Much better is Pollard's $p-1$ method. One chooses base a and exponent $k =$ product of powers of small primes. Compute $a^k \pmod{N}$ [as usual, after first writing k in binary], and then $\gcd(a^k - 1, N)$ using Euclid's Algorithm. If there exists prime $p|N$ such that $p-1|k$ [$k = (p-1)s$, say] then:

$$a^k \equiv (a^{p-1})^s \equiv 1^s \equiv 1 \pmod{p} \text{ [by Fermat],}$$

provided that $p \nmid a$. This gives $p|(a^k - 1)$ and so $p|\gcd(a^k - 1, N)$. Unless we have bad luck, $\gcd(a^k - 1, N) \neq N$, and so $\gcd(a^k - 1, N)$ will be a proper factor of N [$\neq 1, \neq N$].

Example 8.1. A four-letter word $L_1L_2L_3L_4$ has been divided into two pairs: L_1L_2 and L_3L_4 . Each of these pairs has been converted into an integer (of at most 4 digits) via the standard map: $A \mapsto 01, B \mapsto 02, \dots, Z \mapsto 26$. These integers have been encoded by taking each to the power of $d = 6587$, modulo $N = 10123$. The encoded message reads:

$$4268, 5744.$$

We shall factorise N by applying Pollard's " $p-1$ " method, using base 2 and exponent 52, and then use the factorisation of N to decode the message. Write 52 as a sum of powers

of 2: $52 = 4 + 16 + 32$. First compute (modulo $N = 10123$): $2^1 \equiv 2$, $2^2 \equiv (2^1)^2 \equiv 4$, $2^4 \equiv (2^2)^2 \equiv 16$, $2^8 \equiv (2^4)^2 \equiv 256$, $2^{16} \equiv (2^8)^2 \equiv 4798$, $2^{32} \equiv (2^{16})^2 \equiv 4798^2 \equiv 1102$ (where each of these was obtained by squaring the previous one, and reducing modulo N). Since $52 = 4 + 16 + 32$, we have: $2^{52} \equiv 2^4 2^{16} 2^{32} \equiv 16 \cdot 4798 \cdot 1102 \equiv 5907 \cdot 1102 \equiv 425$ modulo N , so that $2^{52} - 1 \equiv 424$ modulo N .

Now, compute $\gcd(424, N)$ by Euclid's Algorithm:

$$10123 = 23 \cdot 424 + 371; 424 = 1 \cdot 371 + 53; 371 = 7 \cdot 53 + 0.$$

So, 53 is a factor of N . Compute $10123/53 = 191$, giving the factorisation $N = 10123 = 53 \cdot 191$.

Since $N = 53 \cdot 191$, we have $\phi(N) = 52 \cdot 190 = 9880$. Compute the $\gcd$ of $\phi(N) = 9880$ and $d = 6587$ we see from Euclid's Algorithm (see the online notes for the calculation) that $\gcd(9880, 6587) = 1$ and $3 \cdot 6587 \equiv 1 \pmod{9880}$, that is, 3 is the inverse of 6587 modulo $\phi(N) = 9880$.

The decoding operation is therefore $Y \mapsto Y^3 \pmod{N}$. Computing $4268^3 = 4268^2 \cdot 4268 \equiv 4547 \cdot 4268 \equiv 805 \pmod{N = 10123}$. Also: $5744^3 = 5744^2 \cdot 5744 \equiv 2679 \cdot 5744 \equiv 1216 \pmod{N = 10123}$. The decoded message is therefore: 0805, 1216; that is: HELP.

The Elliptic Curve Method (ECM) for attempting to factor an integer N is as follows. Choose an elliptic curve $\mathcal{E} \pmod{N}$, some point P on $\mathcal{E}$, and some choice of k (normally a product of powers of small primes). Attempt to compute $kP \pmod{N}$ and hope that, in performing one of the additions $kP = k_1P + k_2P$, a denominator will have $\gcd$ with N that is a nontrivial factor of N ($\neq 1$ and $\neq N$).

Example 8.2. Let $N = 10123$, as in Example 8.1. We shall factorise N by applying the Elliptic Curve Method, using the curve $\mathcal{E} : Y^2 = X^3 + 5X - 5$ and $4P$, where $P = (1, 1)$.

The line tangent to $\mathcal{E}$ at $P = (1, 1)$ has slope y' given by $2yy' = 3x^2 + 5$, with $x = 1, y = 1$; that is, the slope is $8/2 = 4$. This tangent line also goes through $(1, 1)$ and so has equation: $Y = 4X - 3$. The x -coordinate of $2P$ is therefore $4^2 - (1 + 1) = 14$, and the y -coordinate is: $-(4 \cdot 14 - 3) = -53 \equiv 10070$, so that $Q = 2P = (14, 10070) \pmod{N = 10123}$. We now wish to double the point $Q = 2P$, and so again the first step is to find the line tangent to $\mathcal{E}$ at Q . This has slope y' given by $2 \cdot 10070 \cdot y' = 3 \cdot 14^2 + 5$, and so we need to compute $(3 \cdot 14^2 + 5)/(2 \cdot 10070) \pmod{N = 10123}$, for which the first step is to find the inverse of $2 \cdot 10070 \equiv 10017 \pmod{N = 10123}$. Using Euclid's Algorithm:

$$10123 = 1 \cdot 10017 + 106; 10017 = 94 \cdot 106 + 53; 106 = 2 \cdot 53 + 0.$$

So, we cannot find the inverse of 10017 (modulo $N = 10123$), and this step has given us our factor 53 of N . As in the previous example, compute $10123/53 = 191$, giving the factorisation $N = 10123 = 53 \cdot 191$.