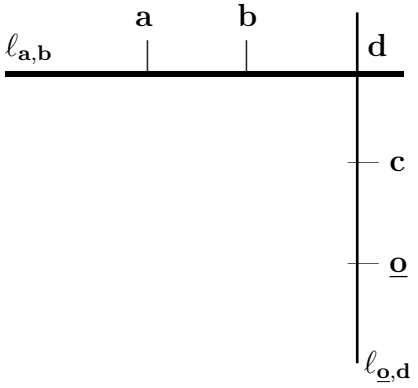
Elliptic Curves. HT 2008/09. E.V. Flynn. flynn@maths.ox.ac.uk

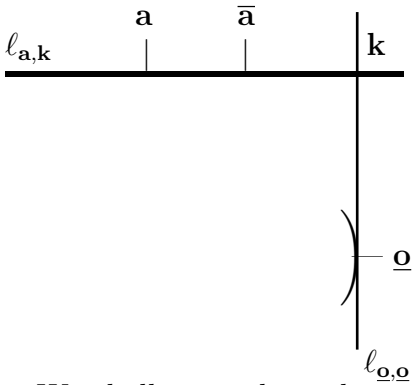
Section 1. The Group Law on an Elliptic Curve

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 $\underline{\mathbf{o}}$. 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 $\ell_{\underline{\mathbf{o}},\mathbf{d}}$ denote the line which meets $\mathcal{C}$ at $\underline{\mathbf{o}}$ and $\mathbf{d}$.
Let $\mathbf{c}$ be the third point of intersection between $\mathcal{C}$ and $\ell_{\underline{\mathbf{o}},\mathbf{d}}$.
Define $\mathbf{a} + \mathbf{b} = \mathbf{c}$.



Let $\ell_{\underline{\mathbf{o}},\underline{\mathbf{o}}}$ be the line tangent to $\mathcal{C}$ at $\underline{\mathbf{o}}$.
Let $\mathbf{k}$ be the third point of intersection between $\mathcal{C}$ and $\ell_{\underline{\mathbf{o}},\underline{\mathbf{o}}}$.
Now, let $\ell_{\mathbf{a},\mathbf{k}}$ be the line which meets $\mathcal{C}$ at $\mathbf{a}$ and $\mathbf{k}$.
Let $\overline{\mathbf{a}}$ be the third point of intersection between $\mathcal{C}$ and $\ell_{\mathbf{a},\mathbf{k}}$.
Define $-\mathbf{a}$ to be $\overline{\mathbf{a}}$.

We shall soon show that $\mathbf{a} + \mathbf{b}$ is a commutative group law on the points on $\mathcal{C}$, with identity $\underline{\mathbf{o}}$ and the inverse of $\mathbf{a}$ given by $-\mathbf{a}$. First we need the following technical lemma.

Lemma 1.3. *Let $P_1, \ldots, P_8$ 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 $P_1, \ldots, P_8$.*

Optional Proof See 0.137.
(1)

Theorem 1.4. *Let $\mathcal{C}$ be an elliptic curve $/K$, with K-rational point $\underline{\mathbf{o}}$. Then $\mathbf{a} + \mathbf{b}$, as in Definition 1.2, gives a commutative group law on the points on $\mathcal{C}$, with identity $\underline{\mathbf{o}}$. 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

Aside: It is apparent that, in the above proof, we have dealt with the 'typical' case, where none of our points are repeated (for the proof of associativity), and none are at infinity (for the proof that $\mathcal{C}(K)$ is a subgroup, since the points were written in affine form). It is straightforward to check these special cases; we shall not bother to do so here.

Comment 1.5. When two nonsingular cubics $\mathcal{C}_1, \mathcal{C}_2$ are birationally equivalent over K (under $\phi : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$), 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. By an elliptic curve, we shall always mean a projective curve, but often write the equation in affine form. Note that, whichever way it is written, we are always referring to the projective curve. For example, if we say 'let $\mathcal{C} : y^2 = x^3 + 3$ be an elliptic curve', it should be understood that this is a shorthand notation for the corresponding projective curve $ZY^2 = X^3 + 3Z^3$.

Theorem 1.7. *Let K be a field satisfying 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 $y^2 =$ 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 $\mathrm{char}(K) \neq 2, 3$, 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

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

which should be regarded as 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.

It is conventional to choose $\underline{\mathbf{o}} = (0, 1, 0)$, the point at infinity, as the identity [we shall always take $\underline{\mathbf{o}} = (0, 1, 0)$ unless otherwise stated]. Note that the line $Z = 0$ meets $\mathcal{E}$ at $\underline{\mathbf{o}}$ three times (such a point is called an *inflexion*). Given a point $\mathbf{a} = (X, Y, Z)$, if we take the line through $\mathbf{a}$ and $\underline{\mathbf{o}} = (0, 1, 0)$ then the third point of intersection is $(X, -Y, Z)$, which must then be $-\mathbf{a}$. In affine form: $\quad -(x, y) = (x, -y)$.

This gives an easy rule for finding the inverse of a point, under the group law, namely: the inverse of $\mathbf{a}$ is its reflection in the x-axis.

So, for an elliptic curve $\mathcal{E}$ written in the form $y^2 =$ cubic in x, the points are $\underline{\mathbf{o}}$ (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.

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:

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

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). Since the roots of $(*)$ are x_1, x_2, x_3, it follows that $x^3 - x^2 - 2x = (x - x_1)(x - x_2)(x - x_3)$; equating coefficients of x^2 gives that:

$$x_1 + x_2 + x_3 = -(\text{coefficient of } x^2 \text{ in } (*)) = -(-1) = 1,$$

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 the equation of $\ell_{\mathbf{a},\mathbf{b}}$ 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, this gives: $(-1, 0) + (0, 1) = -(2, 3) = (2, -3)$, using the rule that negation is given by reflection in the x-axis.

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:*

$$x_3 = \frac{x_1 x_2^2 + x_1^2 x_2 + A(x_1 + x_2) + 2B - 2y_1 y_2}{(x_1 - x_2)^2}, \quad y_3 = -\ell x_3 - m,$$

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

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:*

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

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

Optional Proof See 0.144.

The above formulas give an alternative method for computing the group law, although in practice it often turns out to be easier to compute the group law from first principles, as in Example 1.10.

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 $\Delta = 0$, then this is no longer an elliptic curve and at least two roots of the cubic are repeated: $y^2 = (x - \alpha)^2(x - \beta)$. It is still the case that the set of nonsingular points on $\mathcal{E}$, denoted $\mathcal{E}_{ns}$, forms a group [see pp.39–41 of Cassels]. When $\beta \neq \alpha$ the singularity at $(\alpha, 0)$ is a node. When $\beta = \alpha$ the singularity is a cusp. In either case, the curve can be written: $\left(\frac{y}{x-\alpha}\right)^2 = x - \beta$, and so is birationally equivalent to the conic $w^2 = x - \beta$.

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 $P + \ldots + P$ [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 $2P = P + P = P - P = \underline{\mathbf{o}}$. But $1 \cdot P = P \neq \underline{\mathbf{o}}$, and so 2 is the smallest $m > 0$ such that $mP = \underline{\mathbf{o}}$. 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 $P + P$. Using $2yy' = 3x^2$ at $(0, 1)$ gives $2 \cdot 1 \cdot y' = 3 \cdot 0^2$ and so the tangent line $\ell_{P,P}$ to $\mathcal{E}$ at P has slope 0 and equation of form $y = 0 \cdot x + m$. But the line goes through $(0, 1)$ and so $m = 1$ and the tangent line 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 $(0, 1) + (0, 1) + (0, 1) = \underline{\mathbf{o}}$. Hence: $(0, 1) + (0, 1) = -(0, 1) = (0, -1)$. In summary:

$1 \cdot (0, 1) = (0, 1), \quad 2 \cdot (0, 1) = (0, -1), \quad 3 \cdot (0, 1) = \underline{\mathbf{o}}.$

$(0,1)$ 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 $\mathcal{E}(\mathbb{F}_p)$.

Aside: Each of the p possible x-coordinates $0, \ldots, p-1$ has about a 50% chance of making x^3+Ax+B a square modulo p. When x^3+Ax+B is not a square, there are no corresponding y-coordinates. When $x^3 + Ax + B$ is a square, there are at most two corresponding y-coordinates. So, one might expect 'on average' about p affine points, that is, about $p+1$ points, including the point at infinity.

The following result gives a bound within which the number of points must lie.

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 $\underline{\mathbf{o}}$ [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 $\underline{\mathbf{o}}$]. Then:*

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

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

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

Section 2. The p-adic Numbers $\mathbb{Q}_p$

For $\mathbb{Q}$, let $|\ |_\infty$ denote the standard absolute value [e.g. $|-5|_\infty = |5|_\infty = 5$]. Consider the sequence: $x_1 = 1.4, x_2 = 1.41, x_3 = 1.414, \ldots$, where x_n is the largest decimal to n decimal places satisfying $x_n^2 < 2$. Then $|x_m - x_n|_\infty \to 0$ as $m, n \to \infty$, so that the sequence is Cauchy in $\mathbb{Q}, |\ |_\infty$. The sequence x_n cannot be convergent, since if $x_n \to \alpha$ then clearly $\alpha^2 = 2$ and no such α exists in $\mathbb{Q}$. We say that $\mathbb{Q}, |\ |_\infty$ is *incomplete* (since not every Cauchy sequence is convergent) and the real numbers $\mathbb{R}$ give the *completion* of $\mathbb{Q}, |\ |_\infty$. The absolute value $|\ |_\infty$ is a special case of the following.

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

(1) $|x| \geqslant 0$ 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) $|x + y| \leqslant |x| + |y|$ for all $x, y \in K$ [the *triangle inequality*].

If a valuation also satisfies the stronger property:

(3)′ $|x + y| \leqslant \max(|x|, |y|)$, for all $x, y \in K$,

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

For example, $\mathbb{Q}, |\ |_\infty$ (or $\mathbb{R}, |\ |_\infty$) is a valuation. It is Archimedean since, for example, $|1 + 1|_\infty \not\leqslant \max(|1|_\infty, |1|_\infty)$. We shall now introduce another valuation on $\mathbb{Q}$, which gives a different notion of size and distance.

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 $p \not| \ a, p \not| \ b$. Then the *p-adic valuation* (or *p-adic absolute value* or *p-adic size*) is defined to be:

$|x|_p = |\frac{m}{n}|_p = p^{-r}$ [so, x is 'smaller' the higher the power of p 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 $\mathbb{Q}, |\ |_3$, 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 $|7|_3 = |3^0\frac{7}{1}|_3 = 3^{-0} = 1$.

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, $m \not\equiv n \pmod 3 \iff d_3(m, n) = 1$, $m \equiv n \pmod 3 \iff d_3(m, n) \leqslant \frac{1}{3}$, $m \equiv n \pmod{3^2} \iff d_3(m, n) \leqslant \frac{1}{3^2}$, and so on. The integers m, n are 3-adically closer when they are congruent modulo a higher power of 3.

(2)

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

Proof

Comment 2.5. By induction, $|a_1 + \ldots + a_n|_p \leqslant \max(|a_1|_p, \ldots, |a_n|_p)$. 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, $1 \leqslant i \leqslant n, i \neq k$, then $|a_1 + \ldots + a_n|_p = \max(|a_1|_p, \ldots, |a_n|_p)$.

Definition 2.6. Let $K, |\ |$ be a field with valuation. For $a_n, \ell \in K$, we say that the sequence a_n *converges* to ℓ [denoted $a_n \to \ell$] in $K, |\ |$ when $|a_n - \ell| \to 0$ in $\mathbb{R}, |\ |_\infty$ as $n \to \infty$. 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 $a_n \to \ell$ in $K, |\ |$ then we say that a_n *converges* in $K, |\ |$, or that it is *convergent* in $K, |\ |$. It is *Cauchy* if $|a_m - a_n| \to 0$ in $\mathbb{R}, |\ |_\infty$ as $m, n \to \infty$. 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 $K, |\ |$ is *complete* if every Cauchy sequence is convergent.

Examples 2.7.

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

(b) Let $a_1 = 1,\ a_2 = 11,\ a_3 = 111, \ldots$ so that $9a_n = 999\ldots9$ [n times] and $9a_n + 1 = 10^n$. Then $|9a_n - (-1)|_5 = |10^n|_5 = 5^{-n} \to 0$, giving $9a_n \to -1$ in $\mathbb{Q}, |\ |_5$. It follows that $a_n \to -\frac{1}{9}$ in $\mathbb{Q}, |\ |_5$.

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

This is satisfied $\iff a_0^2 + 2a_0a_1 7 + a_1^2 7^2 \equiv 2 \ (\text{mod } 7^2)$

$\iff 6a_1 7 \equiv 2 - 9 = -7 \ (\text{mod } 7^2) \iff 6a_1 \equiv -1 \ (\text{mod } 7) \iff a_1 \equiv 1 \ (\text{mod } 7)$,

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

Aside: note how the solvability of the last congruence is affected by $|2a_0|_7 = |f'(a_0)|_7$, where $f(x) = x^2 - 2$.

When we similarly solve for $a_2 \in \{0, \ldots, 6\}$ such that $(a_0 + a_1 7 + a_2 7^2)^2 \equiv 2 \ (\text{mod } 7^3)$ we find that $a_2 = 2$, giving $x_2 = a_0 + a_1 7 + a_2 7^2 = 3 + 7 + 98 = 108$. Check: $x_2^2 \equiv 2 \ (\text{mod } 7^3)$ and $|x_2^2 - 2|_7 \leqslant 7^{-3}$.

We can inductively find $x_n = a_0 + a_1 7 + \ldots + a_n 7^n$ such that $x_n^2 \equiv 2 \ (\text{mod } 7^{n+1})$, that is, $|x_n^2 - 2|_7 \leqslant 7^{-(n+1)}$. Hence $x_n^2 \to 2$ in $\mathbb{Q}, |\ |_7$.

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

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

$a_0 = 3,\ a_1 = 3 - \frac{3^2-2}{2\cdot 3} = \frac{11}{6},\ a_2 = \frac{11}{6} - \frac{(\frac{11}{6})^2-2}{2\frac{11}{6}} = \frac{193}{132}$, and so on.

Check that: $|a_0^2 - 2|_7 = |3^2 - 2|_7 \leqslant 7^{-1}$, $|a_1^2 - 2|_7 = |(\frac{11}{6})^2 - 2|_7 = |\frac{49}{36}|_7 \leqslant 7^{-2}$, and that a_n satisfies the same properties as x_n of Example (c), namely: $|a_n^2 - 2|_7 \leqslant 7^{-(n+1)}$ so that $a_n^2 \to 2$ 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 $|\ |_7$, and indeed $\mathbb{Q}$ is incomplete with respect to any $|\ |_p$. We now define an extension of $\mathbb{Q}$ which performs the same role with respect to $|\ |_p$ that $\mathbb{R}$ performs with respect to $|\ |_\infty$.

Definition 2.8. The set of *p-adic numbers* $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the valuation $|\ |_p$, and is the smallest field containing $\mathbb{Q}$ which is complete with respect to $|\ |_p$. For any $\alpha, \beta \in \mathbb{Q}_p$, we say that $\alpha \equiv \beta \pmod{p^n} \iff |\alpha - \beta|_p \leqslant p^{-n}$ ['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):

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

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

Examples 2.9.

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

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

On the other hand, there is no $\beta \in \mathbb{Q}_7$ such that $\beta^2 = 3$ since any such β would satisfy $|\beta|_7^2 = |\beta^2|_7 = |3|_7 = 1$ and so would have 7-adic expansion $\beta = b_0 + b_1 7 + b_2 7^2 + \ldots$ and would satisfy $(b_0 + b_1 7 + b_2 7^2 + \ldots)^2 = 3$. This would give: $b_0^2 \equiv 3 \pmod 7$, which is impossible, since 3 is not a quadratic residue mod 7 [none of $0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2$ are $\equiv 3 \pmod 7$].

(c) In $\mathbb{Q}_5$: $27 = 2 + 5^2 = 2 \cdot 5^0 + 0 \cdot 5^1 + 1 \cdot 5^2 = 2, 01$ [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 $\alpha = a_0 + a_1 5 + a_2 5^2 + \ldots$, each $a_i \in \{0, 1, 2, 3, 4\}$ and $a_0 \neq 0$. This satisfies $-1 = 4(a_0 + a_1 5 + a_2 5^2 + \ldots)$ which gives $-1 \equiv 4a_0 \pmod 5$ and so $a_0 = 1$. Then $-1 = 4(1 + a_1 5 + a_2 5^2 + \ldots)$ 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 $a_2 = 1, a_3 = 1, \ldots$ 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 $|\ |$. We say that $x \in K$ is an *integer* (with respect to the valuation) when $|x| \leqslant 1$, and $R = \{x \in K : |x| \leqslant 1\}$ 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 $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leqslant 1\}$. The valuation group $G_{\mathbb{Q}_p} = \{p^r : r \in \mathbb{Z}\} = \{\ldots, p^{-2}, p^{-1}, p^0, p^1, p^2, \ldots\}$, 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 $\mathcal{M} = p\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leqslant p^{-1}\}$ and the residue field $\mathbb{Z}_p/p\mathbb{Z}_p$ is isomorphic to $\mathbb{F}_p$, the finite field with p elements.

The following result show how, in some respects, analysis is simpler for non-Archimedean valuations.

(3)

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

Proof

For example, $\sum n!$ converges in any $\mathbb{Q}_p$, since $|n!|_p \to 0$ [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, $|\sum a_n| \leqslant \max|a_n|$. 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 $\sum a_n = 0$.

Aside: Recall Example 2.7(d), where $x_0 = 3$, and $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$, where $f(x) = x^2 - 2$, defined a sequence, which is Cauchy (but not convergent) in $\mathbb{Q}, |\ |_7$, and which is convergent in $\mathbb{Q}_7$ to a root of $f(x)$. The following describes when an initial approximation a_0 gives a solution to $f(x)$.

(4)

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

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

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

Proof

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: $a^3 = 7$.

(5)

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 $\alpha \equiv 1 \ (mod\ 8)$.*

Proof

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

The corollary does not apply to decide the status of 14, but in fact we can see that $14 \notin \left(\mathbb{Q}_7^*\right)^2$, since if $14 = \gamma^2$ for some $\gamma \in \mathbb{Q}_7$ then $|\gamma|_7^2 = |\gamma^2|_7 = |14|_7 = 7^{-1}$, contradicting the fact that $|\gamma|_7 = 7^r$ for some $r \in \mathbb{Z}$.

Section 3. The Reduction Map on an Elliptic Curve

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

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

Let $a = (a_0, \ldots, a_n) \in \mathbb{P}^n(K)$. We define the reduction map to $\mathbb{P}^n(k)$ as follows.
Step 1. There exists i_0 such that $|a_{i_0}| \geqslant |a_i|$ for $i = 0, \ldots, n$. 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 $\tilde{a} = (\tilde{a}_0, \ldots, \tilde{a}_n)$ [easy to check that this is well defined].

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

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 $\widetilde{\mathcal{E}}(\mathbb{F}_2)$. 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 $|f_{i_0}| \geqslant |f_i|$ for all i, we can say that $\max(|f_i|) = 1$ [normalised form]. The reduction of $\mathcal{C}$ mod $\mathcal{M}$ is $\widetilde{\mathcal{C}} : \widetilde{F}(X, Y, Z) = 0$, 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 $\widetilde{\mathcal{C}}$, when we say that a reduces to $\tilde{a}$.

Definition 3.4. Let $b \in \widetilde{\mathcal{C}}(k)$. 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 $\widetilde{\mathcal{E}} : ZY^2 = X^3$, defined over $\mathbb{F}_p$. Consider $(0,0,1) \in \widetilde{\mathcal{E}}(\mathbb{F}_p)$. Does it lift to a point in $\mathcal{E}(\mathbb{Q}_p)$? Imagine $(X,Y,Z) \in \mathcal{E}(\mathbb{Q}_p)$ reduces mod p to $(0,0,1) \in \widetilde{\mathcal{E}}(\mathbb{F}_p)$. Then $p|X, p|Y, p \not| Z$, that is, $|X|_p < 1, |Y|_p < 1, |Z|_p = 1$. But all p-adic values are of the form: $\ldots, p^{-2}, p^{-1}, p^0, p^1, \ldots$ so that $|X|_p \leqslant p^{-1}, |Y|_p \leqslant p^{-1}$, and $|X^3|_p \leqslant p^{-3}$. Furthermore, $|pZ^3|_p = |p|_p |Z|_p^3 = p^{-1}$.

Since $|X^3|_p \neq |pZ^3|_p$ we must have $|X^3 + pZ^3|_p = \max\big(|X^3|_p, |pZ^3|_p\big) = p^{-1}$. But then $|Y^2|_p = |ZY^2|_p = |X^3 + pZ^3|_p = p^{-1}$, a contradiction. We conclude that $(0,0,1) \in \widetilde{\mathcal{E}}(\mathbb{F}_p)$ does not lift to a point in $\mathcal{E}(\mathbb{Q}_p)$. *In fact: need not do proof; just refer to Problem Sheet 5.*

If we had represented the above curves with the affine shorthand: $\mathcal{E} : y^2 = x^3 + p$ and $\widetilde{\mathcal{E}} : y^2 = x^3$, then the above would be expressed by saying that $(0,0) \in \widetilde{\mathcal{E}}(\mathbb{F}_p)$ does not lift.

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

(6)

Theorem 3.6. *Let $\mathcal{C}$ be defined over K, written so that the coefficients lie in R. Let $\widetilde{\mathcal{C}}$, defined over k, be the reduction of $\mathcal{C}$ modulo $\mathcal{M}$. Let $b \in \widetilde{\mathcal{C}}(k)$ 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

We wish to see under what circumstances the reduction map is a homomorphism on an elliptic curve.

(7)

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

or:

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

Proof

When we have an elliptic curve written, not as a general cubic, but birationally transformed to the form $\mathcal{E} : y^2 = x^3 + Ax + B$ $(A, B \in R)$ [which, as usual, is shorthand for the projective curve $ZY^2 = X^3 + AXZ^2 + BZ^3$], the reduction $\widetilde{\mathcal{E}}$ will still be of the form $y^2 = x^3 + \ldots$. This cannot contain a line, since any $(y + rx + \ldots)(y - x^2/r + \ldots)$ would have an x^2y term and so would not give $y^2 -$ cubic in x. For such a curve, only option (2) can apply in the previous theorem. Even though $\mathcal{E}$ is an elliptic curve (and therefore nonsingular), the reduction $\widetilde{\mathcal{E}}$ might be singular [for example, when $p|\Delta \in \mathbb{Z}$ so that $\widetilde{\Delta} = 0$ in $\mathbb{F}_p$], but even in that case we still have the group $\widetilde{\mathcal{E}}_{ns}(k)$ of nonsingular points [see Comment 1.12]. 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 $\widetilde{\mathcal{E}}$. Let $\widetilde{\mathcal{E}}_{ns}(k)$ denote the group of nonsingular points in $\widetilde{\mathcal{E}}(k)$, and let $\mathcal{E}_0(K)$ denote the set of points in $\mathcal{E}(K)$ which reduce to members of $\widetilde{\mathcal{E}}_{ns}(k)$, that is, define: $\mathcal{E}_0(K) = \{P \in \mathcal{E}(K) : \widetilde{P} \in \widetilde{\mathcal{E}}_{ns}(k)\}$. Then the reduction map $P \mapsto \widetilde{P}$ is a homomorphism from $\mathcal{E}_0(K)$ to $\widetilde{\mathcal{E}}_{ns}(k)$.*

Definition 3.9. Let $\mathcal{E}_0(K)$ and $\widetilde{\mathcal{E}}_{ns}(k)$ 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 $\widetilde{\mathcal{E}}_{ns}(k)$. That is:

$$\mathcal{E}_1(K) = \{P \in \mathcal{E}(K) : \widetilde{P} = \underline{\mathbf{o}}\},$$

where, as usual, $\underline{\mathbf{o}}$ is the identity element, usually taken to be the point at infinity, in which case

$$\mathcal{E}_1(K) = \{P = (x, y) \in \mathcal{E}(K) : |x| > 1,\ |y| > 1\},$$

since these are the points that map to the point at infinity under the reduction map.

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

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

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 $\underline{\mathbf{o}}$, the point at infinity so that, as already observed, $\mathcal{E}_1(K) = \{(x, y) \in \mathcal{E}(K) : |x| > 1,\ |y| > 1\}$. The members of $\mathcal{E}_1(K)$ are in a neighbourhood of $\underline{\mathbf{o}}$, and it is natural to try to describe the group law as a power series. This will be more transparent if we write our equation in a form where the points in the neighbourhood have coordinates with small, rather than large, valuation. We therefore perform the following birational transformation:

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

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 $\underline{\mathbf{o}}$ 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:

$$w = f(z,w) = f(z, f(z,w)) = z^3 + A(z^3 + Aw^2z + Bw^3)^2z + B(z^3 + Aw^2z + Bw^3)^3$$

$$= z^3 + Az^7 + \dots$$

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

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

The following is then easy to show.

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

Proof

This means that $\big(z, w(z)\big)$ satisfies $\mathcal{E}'$. Since we are working in a non-Archimedean field K, we can appeal to the fact (see Theorem 2.12) that a series converges iff its terms converge to 0. When we are in the kernel of reduction $|z| < 1, |w| < 1$, this applies to the above series $w(z)$ [since $A, B \in R$ and so $|A|, |B| \leqslant 1$]. 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:

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

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

Proof

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:

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

with all terms being of degree $\geqslant 2$, 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:

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

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 $1/(1 + \phi(z_1, z_2)) = 1 - \phi(z_1, z_2) + \phi(z_1, z_2)^2 + \ldots$].

The sum $(z_1, w_1) + (z_2, w_2) + (z_3, w_3) =$ 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:

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

We summarise this as follows.

(8)

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 $(z_2, w(z_2))$.*

Proof

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

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

Of course, the power series $F_{\mathcal{E}}(z_1, z_2) \in \mathbb{Z}[A, B][[z_1, z_2]]$ can be derived for any $\mathcal{E}$ defined over any ring, regardless of convergence considerations. In the next section, we shall consider power series $F(X, Y)$ which satisfy the above properties, and then apply the results to the special case of $F_{\mathcal{E}}(X, Y)$.

Section 4. Formal Groups

Let R be any ring (by *ring* I shall alway 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) $F(X,Y) = X + Y +$ terms of degree $\geqslant 2$.

(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.

Aside: A formal group does not necessarily induce an actual nontrivial commutative group, since there is no guarantee that the power series will converge for any nonzero X, Y; indeed, our arbitrary ring R may not even come together with any structure (such as a valuation or metric) that provides a definition of convergence. It is merely a power series satisfying properties analogous to associativity and commutativity. The definition appears to be missing properties analogous to the existence of an identity element and inverses. In fact, the following result shows these can be deduced from the given axioms.

(9)

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

(1) There is a unique power series $i(T) \in TR_T$ such that $F\big(T, i(T)\big) = 0$.

(2) $F(X,0) = X$ and $F(0,Y) = Y$.

Proof

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 $f\big(F(X,Y)\big) = G\big(f(X), f(Y)\big)$. 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 $\mathrm{char}(R) = 0$ and $\frac{1}{n} \in R$ for all n, then $f(T) = T - T^2/2 + T^3/3 - \ldots$ is a homomorphism from $\widehat{G}_m$ to $\widehat{G}_a$.

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: $[m](T) = mT +$ terms of degree $\geqslant 2$.

(10)

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

Aside: When R is an integral domain, this type of argument can also be interpreted as an application of an adapted version of Hensel's Lemma, applied to the ring R_T, with valuation $|f(T)| = \rho^n$, where ρ is a fixed real number satisfying $0 < \rho < 1$ and n is the degree of the smallest nonzero degree term [for example, $|2T^3 + 5T^4 + \ldots| = \rho^3$]. Here T takes on a similar role for R_T to that performed by p for $\mathbb{Z}_p$.

(11)

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

Proof

Aside: You might have wondered in school about the connection between the two properties of log, that it is the integral of $1/x$*, and that* $\log(ab) = \log(a) + \log(b)$ *[a homomorphism from multiplication to addition]. One way of seeing the connection is to define* $\log(T) = \int v(T)$ *[with* $\log(1) = 0$*], where* $v(T) = \frac{1}{T}dT$*, and note that [regarding* T *as a variable and* S *as a constant]* $v(TS) = \frac{1}{TS}d(TS) = v(T)$*, that is,* v *remains invariant under replacing* T *by* TS*. Therefore* $\log(TS) = \log(T) + f(S)$*, where* $f(S)$ *is a constant; setting* $T = 1$ *gives* $f(S) = \log(S)$*. If we were to adjust the multiplicative group, translating by* -1*, so that the identity is* 0*:* $F(X, Y) = (1+X)(1+Y)-1 = X+Y+XY$*, then* $\omega(T) = \frac{1}{1+T}dT = (1-T+T^2-\ldots)dT$ *would have the property that* $\omega \circ F(T, S) = \omega(T)$ *[and* $\int \omega(T)$ *would give a homomorphism from* $\widehat{G}_m$ *to* $\widehat{G}_a$*]. It is natural to ask whether* ω *is unique (up to constants), and how we would construct* ω *for a general choice of* $F(X, Y)$*.*

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

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

$$\mathrm{d}\big(P(T) + Q(T)\big) = \mathrm{d}P(T) + \mathrm{d}Q(T), \quad \mathrm{d}\big(P(T)Q(T)\big) = P(T)\mathrm{d}Q(T) + Q(T)\mathrm{d}P(T).$$

[Formally, the space of (formal) *differential forms* on R_T is the R_T-module spanned by the symbols $\{\mathrm{d}f : f \in R_T\}$ modulo the submodule spanned by $\{f'\mathrm{d}T - \mathrm{d}f : f \in R_T\}$.]

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

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

Note that $\omega \circ F(T, S)$ is the same as $P(F(T, S))\mathrm{d}(F(T, S)) = P(F(T, S))F_X(T, S)\mathrm{d}T$, 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:

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

An invariant differential $\omega(T) = P(T)\mathrm{d}T$ 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 $\omega(T) = \mathrm{d}T$ as a normalised invariant differential. On $\widehat{G}_m$, the multiplicative formal group defined by $F(X, Y) = X+Y+XY$, we can take $\omega(T) = (1+T)^{-1}\mathrm{d}T = (1-T+T^2-\ldots)\mathrm{d}T$.

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

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

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 $f, g \in R_T$ $[f(T) = T + \ldots]$, such that $[p](T) = pf(T) + g(T^p)$.*

Proof

Definition 4.14. Let $\omega(T) = P(T)\mathrm{d}T = (1+c_1T+c_2T^2+\ldots)\mathrm{d}T$ be the normalised invariant differential for the formal group F over R. For the special case when our ring R is a field of characteristic 0, we can define the formal logarithm by: $\log_F(T) = \int \omega(T) = \int P(T)\mathrm{d}T = T + \frac{c_1}{2}T^2 + \frac{c_2}{3}T^3 + \ldots$ 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.

(15)

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

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 $F(X,Y) = \exp_F\big(\log_F(X) + \log_F(Y)\big)$, which forces F to be commutative. So, at least when F is defined over an integral domain of characteristic 0, we have the somewhat surprising fact that the commutativity axiom is redundant; it can be deduced from: $F(X,Y) = X + Y +$ terms of degree $\geqslant 2$ and associativity. It is possible to construct non-commutative formal groups, but only when defined over unusual rings.

Definition 4.17. Let K be field, complete with respect to a discrete non-Archimedean valuation, $R = \{x \in K : |x| \leqslant 1\}$ be the valuation ring, $\mathcal{M} = \{x \in K : |x| < 1\}$ be the maximal ideal, and assume that $k = R/M$ [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 $n \geqslant 1$, 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 $char(k) = p$] be as in Definition 4.17.*
(a) The identity map: $F(\mathcal{M}^n)/F(\mathcal{M}^{n+1}), \oplus \to \mathcal{M}^n/\mathcal{M}^{n+1}, +$ is an isomorphism.
(b) Every torsion element of $F(\mathcal{M})$ has order a power of p.

Proof

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

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

Proof

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 $\sim : \mathcal{E}_0(\mathbb{Q}_p) \to \widetilde{\mathcal{E}}_{ns}(\mathbb{F}_p)$ has no torsion (apart from $\underline{\mathbf{o}}$). Any $(x, y) \in \mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ satisfies $|x|_p \leqslant 1, |y|_p \leqslant 1$. When $\widetilde{\mathcal{E}}$ is non-singular, $\mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}(\mathbb{F}_p)$.*

Proof

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 $A, B \in \mathbb{Z}$. The following result is a consequence over $\mathbb{Q}$ of the p-adic results of the last section.

(19)

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 $p \not| \Delta$ (such a prime is said to be of good reduction, since $\widetilde{\mathcal{E}}$ mod p is still an elliptic curve over $\mathbb{F}_p$). Then $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}(\mathbb{F}_p)$, and so $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid \#\widetilde{\mathcal{E}}(\mathbb{F}_p)$.*

Proof

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 $p \neq 2, p \not| \Delta$, that is, $p \neq 2, 3$.
$p = 5$. $\widetilde{\mathcal{E}} : y^2 = x^3 + 3$, defined over $\mathbb{F}_5$. Then $\widetilde{\mathcal{E}}(\mathbb{F}_5)$ consists of: $\underline{\mathbf{o}}, (1, \pm 2), (2, \pm 1), (3, 0)$, giving 6 points. So $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid \#\widetilde{\mathcal{E}}(\mathbb{F}_5)$, that is: $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid 6$.
$p = 7$. $\widetilde{\mathcal{E}} : y^2 = x^3 + 3$, defined over $\mathbb{F}_7$. Then $\widetilde{\mathcal{E}}(\mathbb{F}_7)$ consists of:
$\underline{\mathbf{o}}, (1, \pm 2), (2, \pm 2), (3, \pm 3), (4, \pm 2), (5, \pm 3), (6, \pm 3)$, 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 $\mathcal{E}_{\text{tors}}(\mathbb{Q}) = \{\underline{\mathbf{o}}\}$. Note that $(1, 2) \in \mathcal{E}(\mathbb{Q})$, but we know that $(1, 2)$ is not of finite order, so that $(1, 2), 2(1, 2), 3(1, 2), \ldots$ 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 $\mathcal{F}_{\text{tors}}(\mathbb{Q}) = \{\underline{\mathbf{o}}\}$ also.

Aside: Another consequence of the p-adic results of the last section is the integrality of the coordinates of any torsion point.

Lemma 5.3. *Let $(x_1, y_1) \neq \underline{\mathbf{o}}$ 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 example, this tells us immediately that the point $(\frac{1}{4}, \frac{7}{8})$ is of infinite order on the elliptic curve $\mathcal{E} : y^2 = x^3 - x + 1$,

Aside: Reduction to finite fields usually works well enough in practice, but there is the potential problem that it might leave us with $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ undetermined. For example, suppose that, after trying several primes, we repeatedly find that $3 \mid \#\widetilde{\mathcal{E}}(\mathbb{F}_p)$, but a search has not found a point of order 3. In that case, the group $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ would be unresolved. It would be nice to have a finite search area within which the members of $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ must lie. This is provided by the following result.

Theorem 5.4. *(Nagell-Lutz). Let* $\underline{\mathbf{o}} \neq (x_1, y_1) \in \mathcal{E}_{\text{tors}}(\mathbb{Q})$*, 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

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 $(x, y) \in \mathcal{E}_{\text{tors}}(\mathbb{Q})$, $(x, y) \neq \underline{\mathbf{o}}$, 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 $x|(\text{constant term}) = (-8)$, giving $x = \pm 1, \pm 2, \pm 4, \pm 8$ as the only possibilities. When we substitute these, we find that $f(1), f(-1), \ldots, f(-8)$ 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, $\underline{\mathbf{o}}, (0, 1), (0, -1)$ 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: $\mathcal{E}_{\text{tors}}(\mathbb{Q}) = \{\underline{\mathbf{o}}\}$.

The previous method of reductions modulo finite fields is usually quicker in practice, but the Nagell-Lutz method is an effective procedure.

Comment 5.6. It was merely to ease the algebra in previous sections that we used only the form $y^2 = x^3 + Ax + B$, and all of the previous arguments apply equally well to any elliptic curve $\mathcal{E} : y^2 = x^3 + ax^2 + bx + c$, where $a, b, c \in \mathbb{Z}$, with Δ now taken to be the discriminant of $x^3 + ax^2 + bx + c$, which has the formula:

$$\Delta = 4a^3c + 27c^2 + 4b^3 - a^2b^2 - 18abc.$$

So, it remains true that, for any prime $p \not| \, 2\Delta$, $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\widetilde{\mathcal{E}}(\mathbb{F}_p)$, that $\#\mathcal{E}_{\text{tors}}(\mathbb{Q}) \mid \#\widetilde{\mathcal{E}}(\mathbb{F}_p)$, and that any $(x, y) \in \mathcal{E}_{\text{tors}}(\mathbb{Q})$ $[(x, y) \neq \underline{\mathbf{o}}]$ 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 $X, Y, \ldots$ for variables, and lower case letters $x, y, \ldots$ 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 $Y^2 =$ cubic in X, with no constant term. As usual, after mappings of the form $(x, y) \mapsto (k^2 x, k^3 y)$, we can assume that the coefficients are in $\mathbb{Z}$. So, our elliptic curve can be taken to have the form

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

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:

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

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

When $(x, y) = (0, 0)$, then $T_{(0,0)} : (0, 0) \mapsto \underline{\mathbf{o}}$, 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:

$$\left(\frac{y}{x}\right)^2 X^2 = X(X^2 + aX + b)$$

$$y^2 X^2 = x^2 X^3 + a x^2 X^2 + b x^2 X$$

$$x(x^2 + ax + b)X^2 = x^2 X^3 + a x^2 X^2 + b x^2 X \text{ [since } (x, y) \text{ is on } \mathcal{C}]$$

$$0 = xX^3 - (x^2 + b)X^2 + bxX, \text{ [since } x \neq 0]$$

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:

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

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 $\phi\big(P+(0,0)\big)=\phi(P)$ for any P. We want expressions in x,y, call them $\lambda(x,y),\ \mu(x,y)$, 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 $x+x_1$.

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

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

Both λ,μ are invariant under $T_{(0,0)}$. We have a map from $\mathcal{C}$, given by $(x,y)\mapsto(\lambda,\mu)=\left(\big(\frac{y}{x}\big)^2,y-\frac{by}{x^2}\right)$, 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:

$$\mu^2=\Big(y-\frac{by}{x^2}\Big)^2=\Big(\frac{y}{x}\big(x-\frac{b}{x}\big)\Big)^2=\Big(\frac{y}{x}\Big)^2\Big(x-\frac{b}{x}\Big)^2=\lambda\Big(x^2-2b+\frac{b^2}{x^2}\big)$$

$$=\lambda\Big(x^2+2b+\frac{b^2}{x^2}-4b\Big)=\lambda\Big(\big(x+\frac{b}{x}\big)^2-4b\Big)=\lambda\Big((\lambda-a)^2-4b\Big)=\lambda(\lambda^2-2a\lambda+a^2-4b).$$

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 (but not a birational transformation, since it is 2-to-1). It is easy to check that it is a homomorphism, with kernel $\{\underline{\mathbf{o}},(0,0)\}$; such a map ϕ is a 2-*isogeny* on $\mathcal{C}$.

We can apply the same process to $\mathcal{D}$, taking $(u,v)\mapsto\left(\big(\frac{v}{u}\big)^2,v-\frac{b_1v}{u^2}\right)$ 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:

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

and so $\left(\frac{Y}{8}\right)^2=\frac{X}{4}\Big(\big(\frac{X}{4}\big)^2+a\big(\frac{X}{4}\big)+b\Big)$. So, the map $\hat{\phi}:(u,v)\mapsto\left(\frac{1}{4}\big(\frac{v}{u}\big)^2,\frac{1}{8}\big(v-\frac{b_1v}{u^2}\big)\right)$ 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 $\{\underline{\mathbf{o}},(0,0)\}$.

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 $\phi\big((\alpha_1,0)\big) = \phi\big((\alpha_2,0)\big) = (0,0)$, and so the kernel of $\hat{\phi}\circ\phi$ consists precisely of the 2-torsion of $\mathcal{C}$, namely: $\{\underline{\mathbf{o}},(0,0),(\alpha_1,0),(\alpha_2,0)\}$. 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* $b_1 = a^2 - 4b$.

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

$$\textit{Define}\ \ \hat{\phi} : \mathcal{D} \longrightarrow \mathcal{C}\ \ \textit{by}\ \ \hat{\phi}(u, v) = \Big(\frac{1}{4}\Big(\frac{v}{u}\Big)^2, \frac{1}{8}\Big(v - \frac{b_1 v}{u^2}\Big)\Big).$$

Then the 2*-isogenies* $\phi, \hat{\phi}$ *are* 2*-to-*1 *homomorphisms, each with kernel* $\{\underline{\mathbf{o}}, (0, 0)\}$. *Since* $\phi, \hat{\phi}$ *are defined over* $\mathbb{Q}$, *we also have* $\phi : \mathcal{C}(\mathbb{Q}) \to \mathcal{D}(\mathbb{Q})$ *and* $\hat{\phi} : \mathcal{D}(\mathbb{Q}) \to \mathcal{C}(\mathbb{Q})$. *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.*

Proof

We shall concentrate for the moment on $\phi : \mathcal{C} \to \mathcal{D}$. 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

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

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

(23)

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*

$$x_1 = \big(u + u^{-1/2}v - a\big)/2, \quad y_1 = u^{1/2}x_1 = u^{1/2}\big(u + u^{-1/2}v - a\big)/2,$$

$$x_2 = \big(u - u^{-1/2}v - a\big)/2, \quad y_2 = -u^{1/2}x_1 = -u^{1/2}\big(u - u^{-1/2}v - a\big)/2.$$

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

Proof

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 $\underline{\mathbf{o}}$].

(24)

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

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

Definition 6.4. Define the map $q : \mathcal{H} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ 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 $q(\underline{\mathbf{o}}) = 1$.

(25)

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

Proof

Lemma 6.6. *The map $q : \mathcal{H} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ of Definition 6.4 has finite image. Indeed, if $r \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$ is written as a square free integer, then $r \in im\ q \implies r|b_1$. 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*

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

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

Proof

Comment 6.7. If we similarly define $\hat{q} : \mathcal{G} \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ 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 $x = r\big(\frac{\ell}{m}\big)^2$.

Proof

(28)

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

Proof

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

Theorem 6.10.

The proof of the more general version is in a similar spirit, but requires some algebraic number theory, working in the number field $\mathbb{Q}(\alpha)$, where α is a root of $F(X)$.

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 $g_1, \ldots, g_n$, 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 $C_2 \times \ldots \times C_2$.

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 $\mathcal{G} = \mathcal{C}(\mathbb{Q}), \mathcal{H} = \mathcal{D}(\mathbb{Q})$, $\phi : \mathcal{G} \to \mathcal{H}$, $\hat{\phi} : \mathcal{H} \to \mathcal{G}$, $q : \mathcal{H}/\phi(\mathcal{G}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$, $\hat{q} : \mathcal{G}/\hat{\phi}(\mathcal{H}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$. 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 $\hat{\phi}\big(\mathcal{H}/\phi(\mathcal{G})\big)$ 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 $\phi : \mathcal{C} \to \mathcal{D}$ is given by $\phi(x, y) = \Big(\big(\frac{y}{x}\big)^2, y - \frac{by}{x^2}\Big) = \Big(\big(\frac{y}{x}\big)^2, y - \frac{6y}{x^2}\Big)$. The isogeny $\hat{\phi} : \mathcal{D} \longrightarrow \mathcal{C}$ is given by $\hat{\phi}(u, v) = \Big(\frac{1}{4}\big(\frac{v}{u}\big)^2, \frac{1}{8}\big(v - \frac{b_1 v}{u^2}\big)\Big) = \Big(\frac{1}{4}\big(\frac{v}{u}\big)^2, \frac{1}{8}\big(v + \frac{23v}{u^2}\big)\Big)$.

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: $\{1, -23\} \leqslant \text{im } q \leqslant \{\pm 1, \pm 23\}$.

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:

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

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

Imagine $3 \not| \ (\ell^2 - m^2)$; then $\ell^2 - m^2$ would have an inverse α mod 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, $r = \pm1, \pm2, \pm3, \pm6$. 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 $\{1, 2, 3, 6\} \leqslant \text{im } \hat{q} \leqslant \{\pm1, \pm2, \pm3, \pm6\}$. 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 $\ell, m, n \in \mathbb{Z}$, $\ell^4, \ell^2m^2, 6m^4 \geqslant 0$, so $-\ell^4 - \ell^2m^2 - 6m^4 \leqslant 0$, 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, RHS $= n^2 \geqslant 0$ 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 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 $\hat{\phi}\big(\mathcal{H}/\phi(\mathcal{G})\big) = \{\hat{\phi}(\underline{\mathbf{o}}), \hat{\phi}(0, 0)\} = \{\underline{\mathbf{o}}\}$, 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 $2\mathcal{G} = \hat{\phi}(\phi(\mathcal{G})) \leq \hat{\phi}(\mathcal{H})$].

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*. Finding $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$, as in the last example, comes down to deciding, for each $r|b_1$, whether W_r has a solution $\ell, m, n \in \mathbb{Z}$, not all 0, with $\gcd(\ell, m) = 1$, and for each $r|b$, whether $\widehat{W}_r$ has such a solution.

In the last example, it turned out that each $W_r, \widehat{W}_r$ either had a solution ℓ, m, n, or we were able to show such a solution was impossible with a modulo-power-of-p argument (a p-adic argument) or that it was impossible in $\mathbb{R}$. That is, each $W_r, \widehat{W}_r$ either had a point or it was impossible in $\mathbb{R}$ or some $\mathbb{Q}_p$.

This doesn't always happen. It is possible in some examples for W_r or $\widehat{W_r}$ to have solutions in $\mathbb{R}$ and every $\mathbb{Q}_p$, but not in $\mathbb{Q}$ [that is, for there to be a violation of the Hasse Principle]. For example, consider $\mathcal{C} : Y^2 = X^3 + 17X$. Here, $a = 0, b = 17$, so that $a_1 = 0, b_1 = -68$, giving $\mathcal{D} : Y^2 = X^3 - 68X$. When computing $\mathcal{H}/\phi(\mathcal{G})$, we consider $r|b_1 = -68$ and so $r = \pm 1, \pm 2, \pm 17, \pm 34$. For the case $r = 2$, the homogeneous space $r\ell^4 + a_1\ell^2 m^2 + (b_1/r)m^4 = n^2$ becomes $2\ell^4 - 34m^4 = n^2$. Note that the equation forces n to be even; setting $n = 2k$ and dividing both sides by 2 gives the slightly simpler form: $\ell^4 - 17m^4 = 2k^2$. As shown on Problem Sheet 4, this has no solutions $k, \ell, m \in \mathbb{Z}$ (not all 0, $\gcd(\ell, m) = 1$) [as shown on Problem Sheet 4], and so $2 \notin \text{im } q$, even though there exist solutions in $\mathbb{R}$ and every $\mathbb{Q}_p$ [and so proving $2 \notin \text{im } q$ requires an argument different to those in the last example]. Instances of such W_r (or $\widehat{W_r}$) correspond to members of a structure known as the *Shafarevich-Tate group*.

Comment 6.14. There is another approach to the Weak Mordell-Weil Theorem, using Galois cohomology. Recall that the slick definition of $q : \mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q})) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ is that $q(Q) = d$, where $\mathbb{Q}(\sqrt{d})$ is the field over which P, P' are defined, where $\phi(P) = \phi(P') = Q$. Since $\ker q = \{\underline{\mathbf{o}}, (0,0)\}$, we must have $P' = P + (0,0)$. Furthermore, if $\sigma_1 : a + b\sqrt{d} \mapsto a + b\sqrt{d}$, $\sigma_2 : a + b\sqrt{d} \mapsto a - b\sqrt{d}$ is the Galois group of the extension $\mathbb{Q}(\sqrt{d}) : \mathbb{Q}$, then $P' = \sigma_2(P)$. So, we have a 1-1 correspondence between $\{k_1 = \underline{\mathbf{o}}, k_2 = (0,0)\}$, given by $k_1 \leftrightarrow \sigma_1$ and $k_2 \leftrightarrow \sigma_2$, with the property that, for any member of $\{P, P'\}$, the effect of adding k_i is the same as applying σ_i. We then have a map which takes a member of $\mathcal{D}(\mathbb{Q})/\phi(\mathcal{C}(\mathbb{Q}))$ to a $1-1$ correspondence between $\{\underline{\mathbf{o}}, (0,0)\}$ and the Galois group of a quadratic number field. As we have seen, there are two main elements required to prove the Weak Mordell-Weil Theorem: showing that q is a homomorphism and that im q is finite. For showing that q is a homomorphism, suppose that $q(Q_1) = d_1$ and $q(Q_2) = d_2$. Then, by definition, P_1, P_1' [such

that $\phi(P_1) = \phi(P_1') = Q_1$] and defined over $\mathbb{Q}(\sqrt{d_1})$, and P_2, P_2' [such that $\phi(P_2) = \phi(P_2') = Q_2$] and defined over $\mathbb{Q}(\sqrt{d_2})$. Now, since ϕ is a homomorphism, $\phi(P_1 + P_2) = Q_1 + Q_2$ and $P_1 + P_2$ is defined over $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$. But $\sqrt{d_1} \mapsto -\sqrt{d_1}$, $\sqrt{d_2} \mapsto -\sqrt{d_2}$ has the same effect as adding $(0, 0)$ to each of P_1, P_2 and so leaves $P_1 + P_2$ unchanged, so that $P_1 + P_2$ is defined over $\mathbb{Q}(\sqrt{d_1 d_2})$; similarly for the other preimage of $Q_1 + Q_2$ under ϕ. Hence $q(Q_1 + Q_2) = d_1 d_2 = q(Q_1)q(Q_2)$, giving that q is a homomorphism [without needing to work explicitly with the group law]. For the finiteness of im q, let $q(Q) = d$, a square free integer, and imagine that a prime p of good reduction is a factor of d. By the definition of q, there are P, P', defined over $\mathbb{Q}(\sqrt{d})$ such that $\phi(P) = \phi(P') = Q$. But, on reduction modulo $\sqrt{p}$, conjugation $\sqrt{d} \mapsto -\sqrt{d}$ has no effect modulo $\sqrt{p}$, contradicting the fact that $P' = P + (0, 0)$ is distinct from P. Hence d has only primes dividing the discriminant as factors, and so has only finitely many possibilities.

This approach is cleaner, and does not require getting our hands dirty with explicit group law manipulations. On the other hand, it is often worth a more from-first-principles proof (as given previously), as it provides us with an explicit method for trying to compute $\mathcal{C}(\mathbb{Q})/2\mathcal{C}(\mathbb{Q})$.

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 $P_1, \ldots, P_k \in \mathcal{E}(\mathbb{Q})$ such that every $P \in \mathcal{E}(\mathbb{Q})$ can be written as:

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

This will be achieved via height functions; we first describe the general properties of a height function on a general Abelian group.

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

We say that $h : A \longrightarrow \mathbb{R}$ 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.

(30)

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

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 $h_x : \mathcal{E}(\mathbb{Q}) \to \mathbb{R}$ by:*

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

and define $h_x(\underline{\mathbf{o}}) = 0$. 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.

Aside: The proof uses the explicit group law; for example, $x' = a'/b'$, the x-coordinate of $2P = 2(x,y)$ is given by (quartic in x)/(cubic in x), and so $\max(|a'|,|b'|)$ is 'approximately' $\max(|a|,|b|)^4$, giving that $\log\max(|a'|,|b'|)$ is 'approximately' $4\log\max(|a|,|b|)$, that is $h_x(2P)$ is 'approximately' $4h_x(P)$. It is only necessary to control the amount of cancellation occurring, when writing the x-coordinate of $2P$ in lowest terms.

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

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

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

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

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

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

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

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, $\mathcal{C}(\mathbb{C})[2] = \{\underline{\mathbf{o}}\} \cup \{\text{points of order } 2\} = \{\underline{\mathbf{o}}, (0,0), \big(\frac{1+\sqrt{-23}}{2}, 0\big), \big(\frac{1-\sqrt{-23}}{2}, 0\big)\}$, so that $\mathcal{C}(\mathbb{Q})[2] = \{\underline{\mathbf{o}}, (0,0)\} \cong C_2$. 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 $d = 2^{k_1} + \ldots + 2^{k_m}$ $(k_1 < \ldots < k_m)$. One then obtains $X^{2^0} \equiv X$, $X^{2^1} \equiv (X^{2^0})^2$, $X^{2^2} \equiv (X^{2^1})^2, \ldots, X^{2^{k_m}}$, by k_m squaring operations, after which:

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

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 $c = 2, \ldots, [\sqrt{N}\,]$ 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:

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

provided that $p \not| a$. 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: $A \mapsto 01, B \mapsto 02, \ldots, Z \mapsto 26$. 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 be 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:

$$\left(\begin{smallmatrix}1 & 0 \\ 0 & 1\end{smallmatrix} \mid \begin{smallmatrix}9880 \\ 6587\end{smallmatrix}\right) \to^{R_1 - R_2} \left(\begin{smallmatrix}1 & -1 \\ 0 & 1\end{smallmatrix} \mid \begin{smallmatrix}3293 \\ 6587\end{smallmatrix}\right) \to^{R_2 - 2R_1} \left(\begin{smallmatrix}1 & -1 \\ -2 & 3\end{smallmatrix} \mid \begin{smallmatrix}3293 \\ 1\end{smallmatrix}\right) \to^{R_1 - 3293R_2} \left(\begin{smallmatrix}* & * \\ -2 & 3\end{smallmatrix} \mid \begin{smallmatrix}0 \\ 1\end{smallmatrix}\right),$$

where the $*$ entries need not be computed. This gives us, all in the same computation, that $\gcd(9880, 6587) = 1$, and the bottom row of the last matrix gives $\gcd(9880, 6587)$ as a linear combination of $9880, 6587$, namely: $1 = -2 \cdot 9880 + 3 \cdot 6587$. Hence $3 \cdot 6587 \equiv 1 \pmod{9880}$, that is, 3 is the inverse of 6587 modulo $\phi(N) = 9880$.

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

The exponent k is typically chosen to be a product of powers of the first r primes, for some r. Pollard's $p - 1$ Method is fast when there exists at least one prime $p|N$ such that $p - 1 = \#\mathbb{F}_p^*$ is only divisible by small primes, so that $\text{order}(a)|\#\mathbb{F}_p^*|k$.

When Pollard's $p - 1$ method is slow for some N, we can replace 'powers of an integer base a' with multiples kP of a point P on an elliptic curve $\mathcal{E}$.

We hope that, there exists prime $p|N$ such that $\#\widetilde{\mathcal{E}}(\mathbb{F}_p)|k$, which would guarantee that $kP = \underline{\mathbf{o}}$ (the point at infinity) mod p; that is to say, a denominator divisible by p, in which case, taking the gcd of the denominator and N will reveal the factor p. This will be fast if there exists $p|N$ such that $\#\widetilde{\mathcal{E}}(\mathbb{F}_p)$ is only divisible by small primes. Each new choice of elliptic curve gives a new chance of this happening.

The Elliptic Curve Method (ECM) for attempting to factor an integer N is as follows. Choose an elliptic curve $\mathcal{E}$ mod 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 $Q = 2P = (14, 10070)$ (modulo $N = 10123$). 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 $(3 \cdot 14^2 + 5)/(2 \cdot 10070)$ (modulo $N = 10123$), for which the first step is to find the inverse of $2 \cdot 10070 \equiv 10017$ (modulo $N = 10123$). 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 $N = 10123 = 53 \cdot 191$.

References

[1] J.W.S. Cassels. *Lectures on Elliptic Curves.* LMS–ST **24**. Cambridge University Press, Cambridge, 1991.
[2] J.H. Silverman. *The Arithmetic of Elliptic Curves.* GTM **106**. Springer-Verlag, 1986.