10

Reduction

The philosophy is to approach the rational field $\mathbb{Q}$ through the local fields $\mathbb{Q}_p$ and, similarly, to approach the $\mathbb{Q}_p$ through the finite fields $\mathbb{F}_p$ by reduction modulo p. We do no more than is required for the applications.

The mod p map $\mathbb{Z}_p \to \mathbb{F}_p$ is denoted by a bar $a \to \overline{a}$. This is extended to the corresponding 2-dimensional projective planes V, $\overline{V}$ as follows. Let (a_1, a_2, a_3) be projective co-ordinates of a point $\mathbf{a}$ of V. By multiplying a_1, a_2, a_3 by the same element of $\mathbb{Q}_p$, we have without loss of generality

$$\max\{|a_1|, |a_2|, |a_3|\} = 1,$$

where $|\ | = |\ |_p$. Then $(\overline{a_1}, \overline{a_2}, \overline{a_3})$ are the co-ordinates of a well-defined point $\overline{\mathbf{a}}$ of $\overline{V}$.

In a similar way, we define the reduction $\overline{\mathbf{l}}$ of a line

$$\mathbf{l}: \quad l_1X_1 + l_2X_2 + l_3X_3 = 0.$$

If the point $\mathbf{a}$ lies on the line $\mathbf{l}$, then clearly $\overline{\mathbf{a}}$ lies on $\overline{\mathbf{l}}$.

We need only the least sophisticated of the many ways of reducing a cubic curve

$$\mathcal{C}: \quad F(\mathbf{X}) = 0$$

defined over $\mathbb{Q}_p$. Here

$$F(\mathbf{X}) = \sum_{i \le j \le k} f_{ijk} X_i X_j X_k \in \mathbb{Q}_p[\mathbf{X}]$$

where the $f_{ijk} \in \mathbb{Q}_p$ are not all 0 and without loss of generality

$$\max_{i,j,k} |f_{ijk}| = 1.$$

Then

$$\overline{F}(\mathbf{X}) = \sum_{i \le j \le k} \overline{f}_{ijk} X_i X_j X_k \in \mathbb{F}_p[\mathbf{X}]$$

is not the zero polynomial, and defines the reduced curve

$$\overline{\mathcal{C}}: \ \overline{F}(\mathbf{X}) = 0$$

over $\mathbb{F}_p$. It may, of course, be reducible[8].

If a point $\mathbf{a}$ lies on $\mathcal{C}$, then clearly $\overline{\mathbf{a}}$ lies on $\overline{\mathcal{C}}$. There is a weak converse

Lemma 1. *Let $\overline{\mathbf{b}}$ be a nonsingular point of $\overline{\mathcal{C}}$. Then there is an $\mathbf{a}$ on $\mathcal{C}$ such that $\overline{\mathbf{a}} = \overline{\mathbf{b}}$.*

Note. The notation $\overline{\mathbf{b}}$ is intended to denote a point defined over $\mathbb{F}_p$ not necessarily derived from a $\mathbf{b}$. We say that $\overline{\mathbf{b}}$ *lifts* to $\mathbf{a}$. It is easy to see by examples that a singular point on $\overline{\mathcal{C}}$ may or may not lift to a point of $\mathcal{C}$ (cf. Exercises).

We construct $\mathbf{a}$ by successive approximation à la Newton. The generic term for such constructions in p-adic analysis is Hensel's Lemma.

Lemma 2. *Let $G(T) \in \mathbb{Z}_p[T]$ and let $t_0 \in \mathbb{Z}_p$ be such that*

$$|G(t_0)| < 1, \qquad |G'(t_0)| = 1,$$

where G' is the formal derivative of G. Then there is a $t \in \mathbb{Z}_p$ such that

$$G(t) = 0 \qquad |t - t_0| \le G(t_0).$$

Assuming the truth of Hensel's Lemma for the moment, we complete the proof of the Lemma. Since $\overline{\mathbf{b}}$ is nonsingular on $\overline{\mathcal{C}}$, we may suppose that

$$\frac{\partial \overline{F}}{\partial X_1}(\overline{\mathbf{b}}) \neq 0.$$

Pick any $b_j \in \mathbb{Z}_p$ such that $\overline{\mathbf{b}} = (\overline{b}_1, \dots, \overline{b}_n)$. Then the conditions of Hensel's Lemma apply to

$$G(T) = F(T, b_2, \dots, b_n), \qquad t_0 = b_1.$$

Put $\mathbf{a} = (t, b_2, \dots, b_n)$, where t is provided by Hensel. Clearly $F(\mathbf{a}) = 0$, $\overline{\mathbf{a}} = \overline{\mathbf{b}}$, so $\mathbf{a}$ does what is required.

It remains to prove the Hensel's Lemma. Let U be an indeterminate.

[8] In the sense that $\overline{F}(\mathbf{X})$ factorizes. There is an unfortunate clash of meanings between "reduced" (mod p) and "reducible".

Then

$$G(T+U) = G(T) + UG_1(T) + U^2G_2(T) + \dots$$

where $G_j \in \mathbb{Z}_p[T]$ and $G_1 = G'$. Now define

$$u = -G(t_0)/G'(t_0),$$

so

$$G(t_0+u) = u^2G_2(t_0) + u^3G_3(t_0) + \dots .$$

Hence

$$|G(t_1)| \le |G(t_0)|^2,$$

where

$$t_1 = t_0 + u.$$

Clearly

$$|G'(t_1)| = |G'(t_0)| = 1.$$

We may therefore iterate the process and get a fundamental sequence t_j $(t \ge 0)$. The limit t clearly does what is required.

We shall also need information about the behaviour of the intersection of a line and a cubic curve under reduction. From what we have already proved, if $\mathbf{l}$ meets $\mathcal{C}$ in $\mathbf{a}$, then $\overline{\mathbf{l}}$ meets $\overline{\mathcal{C}}$ in $\overline{\mathbf{a}}$. But suppose that $\mathbf{l}$ meets $\mathcal{C}$ in $\mathbf{a}$, $\mathbf{b}$ with $\mathbf{a} \ne \mathbf{b}$: if $\overline{\mathbf{a}} = \overline{\mathbf{b}}$, can we be sure that it has multiplicity ≥ 2 in the intersection?

The following lemma confirms expectations.

Lemma 3. *Suppose that the line $\mathbf{l}$ meets the cubic curve $\mathcal{C}$ in $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$, multiple points of intersection being given with their multiplicities. Then either*

(I) *the entire line $\overline{\mathbf{l}}$ is in $\overline{\mathcal{C}}$ or*

(II) *$\overline{\mathbf{l}}$ meets $\overline{\mathcal{C}}$ in $\overline{\mathbf{a}}$, $\overline{\mathbf{b}}$, $\overline{\mathbf{c}}$, multiple points occuring with the correct multiplicities.*

Proof. We have without loss of generality

$$l_3 = 1 = \max(|l_1|, |l_2|, |l_3|).$$

Consider

$$\begin{aligned} G(X_1, X_2) &= F(X_1, X_2, -l_1X_1 - l_2X_2) \\ &= \mathbb{Z}_p[X_1, X_2]. \end{aligned}$$

Its reduction is

$$\overline{G}(X_1, X_2) = \overline{F}(X_1, X_2 - \overline{l}_1X_1 - \overline{l}_2X_2).$$

If $\overline{G}(X_1, X_2) = 0$, we have case (I) of the Lemma, so we may suppose that

$$\overline{G}(X_1, X_2) \ne 0.$$

We normalize the coefficients of $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ so that

$$\max(|a_1|, |a_2|, |a_3|) = 1.$$

Since $\mathbf{la} = 0$, it follows that

$$(\overline{a}_1, \overline{a}_2) \ne (0, 0)$$

etc.

By hypothesis, there is some $\lambda \in \mathbb{Q}_p$ such that

$$\begin{aligned} G(X_1, X_2) &= \lambda(a_2X_1 - a_1X_2)(b_2X_1 - b_1X_2)(c_2X_1 - c_1X_2) \\ &= \lambda H(X_1, X_2). \end{aligned}$$

Now

$$\begin{aligned} \overline{H}(X_1, X_2) &= (\overline{a}_2X_1 - \overline{a}_1X_2)(\overline{b}_2X_1 - \overline{b}_1X_2)(\overline{c}_2X_1 - \overline{c}_1X_2) \\ &\ne 0. \end{aligned}$$

Hence $\overline{G}$, $\overline{H}$ differ only by a scalar multiple, which is what we needed to prove.

§10. Exercises

1. (i) Let $\mathcal{C}$ be the curve $Y^2 = X^3 + p$ over $\mathbb{Q}_p$. Show that the point $(0, 0)$ on the mod p curve does not lift to a point of $\mathcal{C}$.

(ii) Find an example of an elliptic curve $\mathcal{C}$ over $\mathbb{Q}_p$ such that the mod p curve has a cusp which is the reduction of a point on $\mathcal{C}$.

2. Find examples of curves $\mathcal{C}$ over $\mathbb{Q}_p$ such that the mod p curve has a double point with distinct tangents which (i) lifts, (ii) does not lift, to $\mathcal{C}$.

11

The p-adic case

Let

$$\mathcal{C}: \quad Y^2 = X^3 + AX + B$$

be an elliptic curve defined over $\mathbb{Q}_p$, so

$$4A^3 + 27B^2 \neq 0$$

and, without loss of generality,

$$A, B \in \mathbb{Z}_p.$$

In this section we study the group $\mathfrak{G}$ of points on $\mathcal{C}$ defined over $\mathbb{Q}_p$.

Our tool will be the theory of reduction developed in the preceeding section. For this, we write $\mathcal{C}$ homogeneously

$$\mathcal{C}: \quad Y^2Z = X^3 + AXZ^2 + BZ^3.$$

The reduced curve

$$\overline{\mathcal{C}}: \quad Y^2Z = X^3 + \overline{A}XZ^2 + \overline{B}Z^3$$

over $\mathbb{F}_p$ may be singular but (with an eye to Lemma 3 of §10) we note that $\overline{\mathcal{C}}$ does not contain a line.

Let $\overline{\mathfrak{G}}$ denote the set of points on $\overline{\mathcal{C}}$ defined over $\mathbb{F}_p$ and let $\overline{\mathfrak{G}}^{(0)} \subset \overline{\mathfrak{G}}$ be the non-singular points. Write $\mathfrak{G}^{(0)} \subset \mathfrak{G}$ for the set of points which reduce mod p to $\overline{\mathfrak{G}}^{(0)}$. The map

$$\mathfrak{G}^{(0)} \to \overline{\mathfrak{G}}^{(0)}$$

is surjective by Lemma 1 of §10.

How does the group structure behave? Let $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathfrak{G}$ with

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

This holds if and only if $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ are the intersection of $\mathcal{C}$ with a line $\mathbf{l}$. Then the reductions $\overline{\mathbf{a}}$, $\overline{\mathbf{b}}$, $\overline{\mathbf{c}}$ are the intersections of $\overline{\mathcal{C}}$ with $\overline{\mathbf{l}}$. On $\overline{\mathcal{C}}$ we have defined a group law only for the non-singular points. If $\overline{\mathbf{a}}$, $\overline{\mathbf{b}}$, $\overline{\mathbf{c}} \in \overline{\mathfrak{G}}^{(0)}$, then

$$\overline{\mathbf{a}} + \overline{\mathbf{b}} + \overline{\mathbf{c}} = \overline{\mathbf{o}}.$$

To sum up so far, we have a subgroup $\mathfrak{G}^{(0)}$ of $\mathfrak{G}$ such that there is a group homomorphism $\mathfrak{G}^{(0)} \to \overline{\mathfrak{G}}^{(0)}$ onto $\overline{\mathfrak{G}}^{(0)}$. The kernel of this homomorphism is the set of points which map into $\overline{\mathbf{o}}$, that is, in inhomogeneous co-ordinates, $\mathbf{o}$ itself together with the $(x, y) \in \mathfrak{G}$ with $x \notin \mathbb{Z}_p$, $y \notin \mathbb{Z}_p$. This is called the *kernel of the reduction.*

Next, we look at the structure of the kernel of reduction. If $(x, y) \in \mathfrak{G}$, $x, y \notin \mathbb{Z}_p$, then clearly $|y|^2 = |x|^3$ and so

$$|x| = p^{2n}, \qquad |y| = p^{3n}$$

for some $n \geq 1$. We call n the *level* of (x, y). For (x, y) not in the kernel of reduction the level is 0, by definition. The level of $\mathbf{o}$ is ∞.

Now for integer $N \geq 1$ make the transformation

$$X_N = p^{2N}X, \qquad Y_N = p^{3N}Y, \qquad Z_N = Z,$$

so the equation of $\mathcal{C}$ becomes

$$\mathcal{C}_N: \quad Y_N^2 Z_N = X_N^3 + p^{4N}AX_N Z_N^2 + p^{6N}BZ_N^3.$$

We may use the new co-ordinates for a reduction mod p: the reduced curve is

$$\overline{\mathcal{C}}_N: \quad Y_N^2 Z_N = X_N^3.$$

We can now transfer what was done earlier to the new situation. A point (x, y) maps into the singular point $(0, 0)$ of $\overline{\mathcal{C}}_N$ if its level is $< N$. It is in the kernel of reduction for $\mathcal{C}_N$ if its level is $> N$. Finally, the group of the non-singular points on the $\overline{\mathcal{C}}_N$ defined over $\mathbb{F}_p$ is the additive group of $\mathbb{F}_p$. They are in the image of $\mathfrak{G}$, as before.

For $N \geq 1$ define $\mathfrak{G}^{(N)}$ to be the set of points of $\mathfrak{G}$ of level $\geq N$. We have proved

Lemma 1. *The $\mathfrak{G}^{(N)}$ are groups and*

$$\mathfrak{G} \supset \mathfrak{G}^{(0)} \supset \mathfrak{G}^{(1)} \supset \cdots \supset \mathfrak{G}^{(N)} \supset \cdots.$$

The quotient graphs of $\mathfrak{G}^{(N)}/\mathfrak{G}^{(N+1)}$ for $N \geq 1$ are cyclic of order p. The quotient $\mathfrak{G}^{(0)}/\mathfrak{G}^{(1)}$ is isomorphic to the group of nonsingular points on $\overline{\mathcal{C}}$. Further,

$$\bigcap_N \mathfrak{G}^{(N)} = \{\mathbf{o}\}.$$

The sequence of groups is called the *p-adic filtration.*

Corollary. *Let* $\mathbf{x} = (x, y) \in \mathfrak{G}$ *be of finite order prime to* p. *Then* x, $y \in \mathbb{Z}_p$.

Proof. Otherwise $\mathbf{x}$ is of some level $n \geq 1$. Then $\mathbf{x} \in \mathfrak{G}^{(n)}$, $\mathbf{x} \notin \mathfrak{G}^{(n+1)}$ and so maps into a non-zero element of $\mathfrak{G}^{(n)}/\mathfrak{G}^{(n+1)}$. But this is of order p.

Our next aim is to free the statement in the Corollary from the requirement that the order is prime to p.

The homomorphism of $\mathfrak{G}^{(N)}/\mathfrak{G}^{(N+1)}$ to the additive group mod p is given by

$$(x, y) \to p^{-N} x/y \mod p.$$

For $\mathbf{x} \in \mathfrak{G}^{(1)}$ we introduce $u(\mathbf{x})$ defined by

$$u(\mathbf{x}) = x/y \qquad (\mathbf{x} = (x, y)),$$
$$u(\mathbf{o}) = 0.$$

Note that $|u(\mathbf{x})| = p^{-n}$, where n is the level of $\mathbf{x}$.

Lemma 2. *Let* $\mathbf{x}_1$, $\mathbf{x}_2 \in \mathfrak{G}^{(1)}$. *Then*

$$|u(\mathbf{x}_1 + \mathbf{x}_2) - u(\mathbf{x}_1) - u(\mathbf{x}_2)| \leq \max\{|u(\mathbf{x}_1)|^5,\ |(\mathbf{x}_2)|^5\}.$$

Proof. We may suppose that none of $\mathbf{x}_1$, $\mathbf{x}_2$, $\mathbf{x}_1 + \mathbf{x}_2$ is $\mathbf{o}$. Without loss of generality

$$|u(\mathbf{x}_1)| \geq |u(\mathbf{x}_2)|.$$

Define N to be the level of $\mathbf{x}_1$. We use the co-ordinates X_N, Y_N and the curve $\mathcal{C}_N$ introduced above.

Since neither $\mathbf{x}_1$, nor $\mathbf{x}_2$ maps into the singularity $(0, 0)$ of $\overline{\mathcal{C}}_N$, the line joining them has the shape

$$Z_N = lX_N + mY_N,$$

where

$$|l| \leq 1, \qquad |m| \leq 1.$$

This meets $\mathcal{C}$ where

$$\begin{aligned} 0 = &- Y_N^2(lX_N + mY_N) + X_N^3 \\ &+ p^{4N} A X_N (lX_N + mY_N)^2 \\ &+ p^{6N} B (lX_N + mY_N)^3 \\ = &c_3 X_N^3 + c_2 X_N^2 Y_N + c_1 X_N Y_N^2 + c_0 Y_N^3 \end{aligned} \qquad (*)$$

(say). Here

$$c_3 = 1 + p^{4N} A l^2 + p^{6N} B l^3$$
$$c_2 = 2p^{4N} lmA + 3p^{6N} l^2 mB,$$

so

$$|c_3| = 1, \qquad |c_2| \leq p^{-4N}.$$

The roots X_N/Y_N of $(*)$ are $-p^{-N}u(\mathbf{x}_1 + \mathbf{x}_2)$, $p^{-N}u(\mathbf{x}_1)$ and $p^{-N}u(\mathbf{x}_2)$. Since the sum of the roots is $-c_2/c_3$, the result follows.

Corollary 1.

$$|u(s\mathbf{x})| = |s|\ |u(\mathbf{x})|$$

for all $\mathbf{x} \in \mathfrak{G}^{(1)}$ *and all* $s \in \mathbb{Z}$.

Proof. By induction, for $s > 0$ we have

$$|u(s\mathbf{x}) - su(\mathbf{x})| \leq |u(\mathbf{x})|^5.$$

This proves the result for $p \nmid s$ and for $s = p$. Now use induction on the power of p in s.

Corollary 2. $\mathfrak{G}^{(1)}$ *is torsion-free.*

Corollary 3. *Suppose that* $p \neq 2$, $|4A^3 + 27B^2| = 1$. *Then the torsion subgroup of* $\mathfrak{G}$ *is isomorphic to a subgroup of* $\overline{\mathfrak{G}}$.

Proof. For $\mathfrak{G} = \mathfrak{G}^{(0)}$; and so

$$\overline{\mathfrak{G}} = \mathfrak{G}/\mathfrak{G}^{(1)},$$

where $\mathfrak{G}^{(1)}$ is torsion free.

Note for the Cognoscenti. This all generalizes to algebraic extensions of $\mathbb{Q}_p$. The proof that torsion points of order prime to p have integral co-ordinates continues to hold, but that for points of p-power order may break down if there is ramification.

There is a power-series in $u = u(\mathbf{x})$ which gives a parametrization of the group $\mathfrak{G}^{(N)}$ for large enough N. This was originally shown by transferring the formulae from the complex variable case. A modern approach is by formal groups and formal logarithms, see, for example, Silverman's book.

12

Global torsion

Let

$$\mathcal{C}: \quad Y^2 = X^3 + AX + B$$

be an elliptic curve over $\mathbb{Q}$, so

$$4A^3 + 27B^2 \neq 0$$

and without loss of generality

$$A, B \in \mathbb{Z}.$$

Theorem 1. *The group of rational points on $\mathcal{C}$ of finite order is finite. If $(x, y) \neq \mathbf{o}$ is of finite order, then*

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

and

$$y = 0 \qquad or \qquad y^2 \mid (4A^3 + 27B^2).$$

Proof. Let $\mathfrak{G}$ be the group of points on $\mathcal{C}$ defined over $\mathbb{Q}$ and let $\mathfrak{G}_p$ be the group for $\mathbb{Q}_p$, where p runs through the primes.

Let $(x, y) \neq \mathbf{o}$ be torsion. Since $\mathfrak{G} \subset \mathfrak{G}_p$ we have

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

for all p, and so

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

Now let p be any prime with $p \neq 2$, $p \nmid (4A^3 + 27B^2)$. Then by the last Corollary of §11, the torsion group of $\mathfrak{G}$ is isomorphic to a subgroup of the group of points over $\mathbb{F}_p = \mathbb{Z} \bmod p$. Hence the torsion group is finite. By looking at different p, one can in general restrict the order of the torsion group severely. But the following argument makes it easy to find the torsion points themselves.

If $2(x, y) = \mathbf{o}$, then $y = 0$. Otherwise, $2(x, y) = (x_2, y_2)$ (say) is also torsion, so $x_2,\ y_2 \in \mathbb{Z}$.

Now taking the tangent at (x, y), we have (cf. Formulary)

$$x_2 + 2x = \left(\frac{3x^2 + A}{2y}\right)^2 = \frac{(3x^2 + A)^2}{4(x^3 + Ax + B)}.$$

and so $y^2 = x^3 + Ax + B$ divides $(3x^2 + A)^2$.

But now,

$$(3X^2 + 4A)(3X^2 + A)^2 \equiv 4A^3 + 27B^2 \pmod{X^3 + AX + B} \qquad (*)$$

in $\mathbb{Z}[X, A, B]$, as in readily verified. Hence

$$y^2 \mid (4A^3 + 27B^2),$$

as required. [For more on identity (*), see §16].

Note. There are stronger statements about the torsion of $\mathcal{C}$ when $AB = 0$, see Exercises. Mazur has determined all possible forms of the torsion group. It is one of

$$\mathbb{Z}/n\mathbb{Z} \qquad 1 \leq n \leq 10 \qquad \text{or} \qquad n = 12$$

or

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \qquad 1 \leq n \leq 4;$$

all of which occur.

§12. Exercises

1. Find the torsion groups over $\mathbb{Q}$ of the following elliptic curves:

(i) $Y^2 = X^3 + 1$
(ii) $Y^2 = X^3 - 43X + 166$
(iii) $Y^2 = X^3 - 219X + 1654$
(iv) $Y^2 = X(X - 1)(X + 2)$
(v) $Y^2 = X(X + 1)(X + 4)$
(vi) $X^3 + Y^3 + Z^3 - 15XYZ = 0$
(vii) $Y^2 = X(X + 81)(X + 256)$
(viii) $X_1^2X_2 - X_1X_2^2 - X_1X_3^2 + X_2^2X_3 = 0$

[*Note*: not a random sample!]

2. Fill in the details of the sketched proof of the following theorem [9] [or find a better one!].

Theorem. *Let $A \in \mathbb{Z}$ be 4-th power free. Then all the torsion points on*

$$\mathcal{C} : Y^2 = X(X^2 + A)$$

are given by (I), (II), (III) *below:*

(I) $(0,0)$ *of order* 2.
(II) *If* $A = 4$, *the points* $(2, \pm 4, 1)$ *of order* 4.
(III) *If* $A = -C^2$, $C \in \mathbb{Z}$, *the points* $(\pm C, 0)$ *of order* 2.

Sketch proof.

(i) If $(x, y) = 2(a, b)$, then

$$x = (a^2 - A)^2/4b^2.$$

(ii) The points of order 2 are as stated.
(iii) $(0,0) = 2(a,b)$ for some (a,b) precisely when $A = 4$. The $(\pm C, 0)$ are never of form $2(a,b)$. From now on, let (a,b) be a point of *odd* order.
(iv) $a = \square$
(v) If $d = \gcd(a, A)$ then $a = da_1$, $A = dA_1$ $b = dvb_1$ where $b_1^2 = a_1(da_1^2 + A_1)$.
(vi) There exists f, g, h such that $\gcd(f,g) = 1$ and $a_1 = \pm f^2$, $da_1^2 + A_1 = \pm g^2$, $b_1 = fg$, $d = \pm h^2$
(vii) $a^2 - A = 2h^4 f^4 \mp h^2 g^2$, $b = h^2 fg$.
(viii) $a^2 - A \equiv 0 \pmod{2b}$.
(ix) Hence $f = 1$, $g \equiv 0$ (2), $h \equiv 0$ (2). [*Hint.* First show that $f \mid g$].
(x) Hence $2^4 \mid A$.
(xi) Contradiction!

3. Fill in the sketched proof of the following theorem[10] [or find a better].

Theorem. *Let $B \in \mathbb{Z}$ be 6-th power free and let*

$$\mathcal{C} : \quad Y^2 = X^3 + B.$$

All the torsion points are given by the following.

(I) *If* $B = C^2$, *the points* $(0, \pm C)$ *of order* 3.
(II) *If* $B = D^3$, *the points* $(-D, 0)$ *of order* 2.

[9] cf. T.Nagell. Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre. *Skrifter utg. av det norske videnskak.-akad i Oslo, Mat.-naturv. kl.* **1935**, No 1, 1-25.

[10] The result is due to R.Fueter: Ueber kubische diophantische Gleichungen. *Comm. Math. Helv.* **2** (1930), 68-89; but the argument suggested is based loosely on L.J.Mordell. The infinity of rational solutions of $y^2 = x^3 + k$. *J. London Math. Soc.* **41** (1966), 523-525.

(III) *If* $B = 1$, *the points* $(2, \pm 3)$ *of order* 6.
(IV) *If* $B = -432 = -2^4.3^3$, *the points* $(12, \pm 36)$ *of order* 3.

Sketch proof.

(i) If $(x, y) = 2(a, b)$, $b \neq 0$ then

$$x = (w - 2)a, \qquad w = 9x^3/4y^2.$$

(ii) the elements of 2-power order are as stated.
(iii) Elements $(0, b)$ are of order 3.

From now on, let (a, b) be of odd order with $a \neq 0$. The strategy is to show that $w \in \mathbb{Z}$. The cases with $w = 1$, 2, 3 are then easily dealt with. Otherwise, $|x|_\infty > |a|_\infty$ and so on repeated duplication $|x|_\infty \to \infty$ a contradiction. We sketch a proof that $w \in \mathbb{Z}$.

(iv) If $p \mid B$, $p \nmid a$ then $p \nmid x$.
(v) If $p \mid B$, $p \nmid x$ then $p \nmid a$ [*Hint.* Consider repeated duplication.]
(vi) If $3^l \mid\mid b$, $3^m \mid\mid a$ then $l = 0$, 1 or $l = 2$, $m \geq 1$. [*Hint.* If $l = 3$ deduce that either $3 \nmid x$ or $3^6 \mid B$]
(vii) Hence $w \in \mathbb{Z}_3$.
(viii) $w \in \mathbb{Z}_2$.
(ix) $w \in \mathbb{Z}_q$ for $q | B$, $q \neq 2, 3$.
(x) Hence $w \in \mathbb{Z}$.

4. Show that

$$X^3 + Y^3 + dZ^3 = 0$$

is birationally equivalent to

$$Y^2 = X^3 - 2^4.3^3.d^2$$

If $d > 0$, $d \in \mathbb{Z}$ is cube free, deduce from the preceding exercise that the only cases of torsion are

$$d = 1, \ (1, 0, -1) \text{ and } (0, 1, -1) \text{ of order 3.}$$
$$d = 1, \ (1, 1, -1) \text{ of order 2.}$$

Compare with results of §6 on exceptional points.

5. Let $s \in \mathbb{Q}$. Show that if there is one $k \in \mathbb{Q}$ such that

$$X^3 + sX + k = 0$$

has 3 rational roots, then there are infinitely many.
[*Hint.* Let u be a rational root. Find the condition, in terms of s, u, k: that the two remaining roots are rational.]

6. Let $k \in \mathbb{Q}$, $k \neq 0$. Show that if there are two $s \in \mathbb{Q}$ such that

$$X^3 + sX + k = 0$$

has 3 rational roots, then there are infinitely many.