Solutions to Exercises in Cassels Lectures on Elliptic Curves

Yankı Lekili

Chapter 0

No exercises given.

Chapter 1

No exercises given.

Chapter 2

1) For each sets of p,m,r given, either find an $x \in \mathbb{Z}$ such that

$$|r - x|_p \leq p^{-m}$$

or show that no such x exists.

(i) $p = 257$, $r = 1/2$, $m = 1$;

► $|\frac{1}{2} - x| \leq 257^{-1}$ if and only if $257 \mid 2x - 1$. So, take $x = 258/2 = 129$.

(ii) $p = 3$, $r = 7/8$, $m = 2$;

► $|\frac{7}{8} - x| \leq 3^{-2}$ if and only if $9 \mid 8x - 7$. So, take $x = 2$.

(iii) $p = 3$, $r = 7/8$, $m = 7$;

► $|\frac{7}{8} - x| \leq 3^{-7}$ if and only if $3^7 \mid 8x - 7$. We try to solve $8x = 7(3^i)$ order by order for $i = 2, \ldots, 7$. For $i = 2$, the previous exercise gives 2 is a solution, so let's write $x = 2 + 3^2 a_2 + 3^3 a_3 + 3^4 a_4 + 3^5 a_5 + 3^6 a_6$ for $a_i \in \{0, 1, 2\}$. $8.2 - 7 = 9$ so to solve $8x = 7(27)$ we need a non-zero a_2. We try $a_2 = 1$ and get $8.(2 + 9) - 7 = 81 \equiv 0(81)$, hence we can take $x = 2 + 3^2 + 3^4 a_4 + 3^5 a_5 + 3^6 a_6$. We try $a_4 = 1$, then $8(2 + 9 + 81) - 7 = 729 = 3^6$. Hence, we get $x = 2 + 9 + 81 + 729$. Finally, let us try $a_6 = 1$, we compute $729 + 8.729 = 9.729 = 3^8$. So, take $x = 821$.

(iv) $p = 3$, $r = 5/6$, $m = 9$;

► $|\frac{5}{6} - x| \leq 3^{-9}$ if and only if $3^{10} \mid 6x - 5$ (since $3 \mid 6$). But, this is impossible since $6x - 5 \equiv 2(3)$.

(v) $p = 5$, $r = 1/4$, $m = 4$;

► $|\frac{1}{4} - x| \leq 5^{-4}$ if and only if $5^4 \mid 4x - 1$.

Let's try to solve $4x \equiv 1(5^i)$ for $i = 1, 2, 3, 4$. Write $x = a_0 + 5a_1 + 5^2a_2 + 5^3a_3$ with $a_i \in \{0, 1, 2, 3, 4\}$. We can easily see $a_0 = 4$ solves $4x \equiv 1(5)$. Next, we try $4.(4 + 5a_1) \equiv 1(25)$. This reduces to $20a_1 \equiv 10(25)$, which has a solution $a_1 = 3$. Next, we have $4.(4+5.3+25a_2) \equiv 1(125)$ which reduces to $100a_2 = 50(125)$. So, take $a_2 = 3$. Finally, we have $4.(4+5.3+25.3+125.a_3) \equiv 1(625)$ which is equivalent to $500a_3 = 250(625)$. Hence, $a_3 = 3$. So, take $x = 4 + 5.3 + 25.3 + 125.3 = 469$.

2) Construct further examples along the lines of Exercise 1 until the whole business seems trivial.

► Take $p = 57$, just kidding.

3) For given p, m, r either find an $x \in \mathbb{Z}$ such that

$$|r - x^2|_p \leq p^{-m}$$

or show that no such x exists.

(i) $p = 5$, $r = -1$, $m = 4$;

► $|-1 - x^2|_p \leq 5^{-4}$ if and only if $5^4 | x^2 + 1$. Let's try $x = a_0 + a_15 + a_25^2 + a_35^3$. We need $a_0^2 + 1 \equiv 0(5)$. There are two solutions to this: $a_0 = 2, 3$. We look for solutions of the form $x_0 = 2 + a_15 + a_25^2 + a_35^3$ and $x_1 = 3 + b_15 + b_25^2 + b_35^3$. Next, we need to solve $(2 + a_15)^2 + 1 \equiv 0(25)$ and $(3 + b_15)^2 + 1 \equiv 0(25)$. We get $5 + 20a_1 \equiv 0(25)$ and $10 + 30b_1 \equiv 0(25)$. Thus, $a_1 = 1$ and $b_1 = 3$. Next, we solve $(2 + 1.5 + a_25^2)^2 + 1 \equiv 0(125)$ and $(3 + 3.5 + b_25^2)^2 + 1 \equiv 0(125)$. We get $50 + 100a_2 \equiv 0(125)$ and $75 + 25b_2 \equiv 0(125)$. Thus, $a_2 = 2$ and $b_2 = 2$. Finally, we look for solutions to $(2 + 1.5 + 2.5^2 + a_35^3)^2 + 1 \equiv 0(125)$ and $(3 + 3.5 + 2.5^2 + b_35^3)^2 + 1 \equiv 0(125)$. Expanding these, we find $125 + 500a_3 \equiv 0(625)$ and $250 + 125b_3 \equiv 0(625)$, so $a_3 = 1$ and $b_3 = 3$. Therefore, the solutions are

$$2 + 1.5 + 2.5^2 + 1.5^3, \quad 3 + 3.5 + 2.5^2 + 3.5^3$$

(ii) $p = 5$, $r = 10$, $m = 3$;

► $|10 - x^2|_p \leq 5^{-3}$ if and only if $5^3 \mid x^2 - 10$. This means $5|x^2$ but that implies $25|x^2$. However $25 \nmid 10$, therefore, there is no solution to this with $x \in \mathbb{Z}$.

(iii) $p = 13$, $r = -4$, $m = 3$;

► $|-4 - x^2|_p \leq 13^{-3}$ if and only if $13^3 \mid x^2 + 4$.

We see easily that $3^2 + 4 \equiv 0(13)$ so let's try $x = 3 + a_113 + a_213^2$. Then, we get $(3 + 13a_1)^2 + 4 \equiv 0(13^2)$. Hence, $13 + 78a_1 \equiv 0(169)$, so $a_1 = 2$. Then, we need to solve $(3 + 2.13 + a_2.13^2)^2 + 4 \equiv 0(13^3)$. This gives $5.13^2 + a_258.13^2 \equiv 0(13^3)$, hence $a_2 = 10$. So, take $x = 3 + 2.13 + 10.13^2$. There is another solution if you try $x = 10 + b_113 + b_213^2$. and working this out gives another solution $x = 10 + 10.13 + 2.13^2$.

(iv) $p = 2$, $r = -7$, $m = 6$;

► $|-7-x^2|_p \leq 2^{-6}$ if and only if $2^6 \mid x^2+7$.

We try out $x = 1+2a_1+2^2a_2+2^3a_3+2^4a_4+2^5a_5$ for $a_i \in \{0,1\}$. If we square this, we see that whether $a_5 = 0$ or 1 does not matter, therefore, we can take $a_5 = 0$. Let's consider modulo 32, then by a similar reason whether $a_4 = 0$ or 1 doesn't matter, so let's consider the equation:

$$(1+2a_1+2^2a_2+2^3a_3)^2+7 \equiv 0(32)$$

We see that this is equivalent to $(1+2a_1+4a_2)^2+16a_3+7 \equiv 0(32)$. Let's now reduce to modulo (16), then we get the equation

$$(1+2a_1)^2+8a_2+7 \equiv 0(16)$$

Now, by inspection, we can see that the only solutions are $a_1 = 1, a_2 = 0$ or $a_1 = 0, a_2 = 1$. Getting back to the modulo (32) equation, we get that the only solutions are $a_1 = 1, a_2 = 0, a_3 = 1$ or $a_1 = 0, a_2 = 1, a_3 = 0$. Finally, we want to see if either of these can be extended to the solution of the original problem for some $a_4 \in \{0,1\}$. We try $x = 1+2.1+8.1+16a_4$ and $x = 1+4.1+16a_4$ for $a_4 \in \{0,1\}$. In the first case, we get $x^2+7 \equiv 128+32a_4(64)$ and in the second case we get $x^2+7 = 32+32a_4(64)$ and we see that the latter one gives the solution: $x = 1+4.1+16.1 = 21$.

(v) $p = 7$, $r = -14$, $m = 4$;

► $|-14-x^2|_p \leq 7^{-4}$ if and only if $7^4 \mid x^2+14$.

It follows that $7 \mid x$ but then $7^2 \mid x^2$. Now, we arrive at contradiction, because $7^4 \mid x^2+14$, in particular implies $7^2 \mid x^2+14$ and this together with $7^2 \mid x^2$ implies $7^2 \mid 14$ which is false.

(vi) $p = 7$, $r = 6$, $m = 3$;

► $|6-x^2|_p \leq 7^{-3}$ if and only if $7^3 \mid x^2-6$.

No solution because there is no $x \in \mathbb{Z}$ such that x^2-6 is divisible by 7 as can be easily checked by trying out $x = 0,1,2,3,4,5,6$.

(vii) $p = 7$, $r = 1/2$, $m = 3$;

► $|\frac{1}{2}-x^2|_p \leq 7^{-3}$ if and only if $7^3 \mid 2x^2-1$.

Looking modulo 7, we see we have $x = 2+7a_1+7^2a_2$ or $x = 5+7b_1+7^2b_2$ are possible solution. We then look at modulo 7^2, we get $7^2 \mid 7+7a_1$ and $7^2 \mid 28b_1$, so we take $a_1 = 6$ and $b_1 = 0$. Finally, $7^3 \mid 2(2+7.6+7^2a_2)^2-1$ gives $7^3 \mid 2.7^2+a_2 7^2$, hence $a_2 = 5$. Similarly, $7^3 \mid 2(5+7^2b_2)^2-1$ gives $7^3 \mid 7^2+6b_2 7^2$, thus $b_2 = 1$. We conclude that $2+7.6+7^2.5$ and $5+7^2.1$ are the desired solutions.

4) As in Exercise 2.

► Solution as in Exercise 2.

5) Let $p > 0$ be a prime, $p \equiv 2(3)$. For any integer $a, p \nmid a$, show that there is an $x \in \mathbb{Z}_p$ with $x^3 = a$.

► Consider the group homomorphism $x \to x^3$ from $\mathbb{F}_p^\times$ to itself. Since $3 \nmid p-1$, there are no order 3 elements in $\mathbb{F}_p^\times$. Therefore, this map is injective, hence also surjective. This means that we can find x_1 with $x_1^3 \equiv a(p)$. Next, suppose that we have $x_n^3 \equiv a(p^n)$ and pose $x_{n+1} = x_n + p^n y$ and we seek to solve $x_{n+1}^3 \equiv a(p^{n+1})$. We compute $x_{n+1}^3 = (x_n + p^n y)^3 \equiv x_n^3 + 3p^n x_n^2 y(p^{n+1})$. As by assumption $p^n \mid x_n^3 - a$, if we let y such that $3x_n^2 y = \frac{x_n^3 - a}{p^n}(p)$ (which we can do since $p \nmid 3x_n^2$, as $p \nmid a$ and $p \neq 3$), then $p^{n+1} \mid x_{n+1}^3 - a$ as required.

Chapter 3

6) (i) Let $p > 2$ prime and let $b, c \in \mathbb{Z}$, $p \nmid b$. Show that $bx^2 + c$ takes precisely $\frac{1}{2}(p+1)$ distinct values mod p for $x \in \mathbb{Z}$.

► It suffices to show the special case $b = 1, c = 0$, since $bm + c \equiv bn + c(p)$ implies $m \equiv n(p)$ as $p \nmid b$. Now, $x^2 \equiv y^2(p)$ then $(x-y)(x+y) \equiv 0(p)$, hence $x \equiv y(p)$ or $x \equiv -y(p)$. Therefore, the map $x \to x^2(p)$ is two-to-one except at 0, so the number of elements in the image is $1 + \frac{p-1}{2} = \frac{p+1}{2}$.

(ii) Suppose that, further, $a \in \mathbb{Z}$, $p \nmid a$. Show that there are $x, y \in \mathbb{Z}$ such that $bx^2 + c \equiv ay^2(p)$.

► The sets of elements of the form $bx^2 + c$ and ay^2 both contain $\frac{p+1}{2}$ elements since $\frac{p+1}{2} + \frac{p+1}{2} > p$, these sets have to overlap.

7) Let $a, b, c \in \mathbb{Z}_p$, $|a|_p = |b|_p = |c|_p = 1$ where p is prime, $p > 2$. Show that there are $x, y \in \mathbb{Z}_p$ such that $bx^2 + c = ay^2$.

► From the previous exercise, we know that there is a solution (x_1, y_1) modulo p. Suppose (x_n, y_n) satisfy $bx_n^2 + c \equiv ay_n^2(p^n)$. Let $x_{n+1} = x_n + p^n u$ and $y_{n+1} = y_n + p^n v$. Then, we want to solve $bx_n^2 + 2bx_n p^n u + c \equiv ay_n^2 + 2ay_n p^n v(p^{n+1})$. This boils down to solving $2bx_n u - 2ay_n v \equiv \frac{ay_n^2 - bx_n^2 - c}{p^n}(p)$. This can be solved as long as p does not divide both x_n and y_n and we know that because $|c|_p = 1$.

8) Let $p > 2$ be prime, $a_{ij} \in \mathbb{Z}$ $(1 \leq i, j \leq 3)$, $a_{ji} = a_{ij}$ and let $d = \det(a_{ij})$. Suppose that $p \nmid d$. Show that there are $x_1, x_2, x_3 \in \mathbb{Z}$ not all divisible by p, such that $\sum_{i,j} a_{ij} x_i x_j = 0(p)$.

► Suppose $a_{ij} = a_{ji} \neq 0$, make a $\mathbb{Z}$-linear change of co-ordinates by sending $x_i \to x_i - a_{ij} x_j$ to transform $\sum_{i,j} a_{ij} x_i x_j$ to $f_1 x_1^2 + f_2 x_2^2 + f_3 x_3^2$. The condition on d becomes $p \nmid f_1 f_2 f_3$. Take $x_3 = 1$ (or any integer that is not divisible by p), then the problem reduces to what we solved in Exercise 1 by letting $f_1 = b$, $x_1 = x$, $f_2 = -a$, $x_2 = y$, $f_3 x_3^2 = c$.

9) Let $a, b, c \in \mathbb{Z}$, $2 \nmid abc$. Show that a necessary and sufficient condition that the only solution in $\mathbb{Q}_2$ of $ax^2 + by^2 + cz^2 = 0$ is the trivial one is that $a \equiv b \equiv c(4)$.

► Suppose $(a_1, a_2, a_3) \neq 0$ is a non-trivial solution in $\mathbb{Q}_2$ then we can assume that $\max |a_i|_2 = 1$ by multiplying with an element of $\mathbb{Q}_2$. This means that at least one the a_i is a unit. Now, since $aa_1^2 + ba_2^2 + ca_3^2 = 0$ and $2 \nmid abc$, it follows that precisely two of the a_j are units. Because of the non-archimedean inequality, we must have two of the $|aa_1|^2, |ba_2|^2, |ca_3|^2$ must be equal and the

other one is less than or equal to. Suppose, for instance, that $|a_2| = |a_3| = 1$, and $|a_1| \leq 1$. By examining modulo 2, we see then that $|a_1| < 1$. Now, $2 \mid a_1$, hence it follows that $b + c \equiv 0(4)$ but b, c are odd, hence b is not equivalent to c modulo 4.

Conversely, suppose that $(a, b, c) \neq (1, 1, 3)$ or $(1, 3, 3)$ modulo 4, and we want to construct a solution in $\mathbb{Q}_2$. By multiplying the equation with -1, we can assume that we are in the case where $(a, b, c) = (1, 1, 3)$ modulo 4, or equivalently we are interested in the equation $ax^2+by^2 = (-c)z^2$. Now, multiply both sides with $-(1/c)$ to and redefine a, b to reduce to the case $ax^2 + by^2 = z^2$ where we still have $(a, b) = (1, 1)$ modulo 4. We now appeal to Lemma 4 from Chapter 2, which says that $ax^2 + by^2$ is a square in $\mathbb{Q}_2$ if and only if $ax^2 + by^2 \equiv 1(8)$. We have that a, b are either 1 or 5 modulo 8. So it suffices to find solutions for the four equations: $x^2 + y^2 \equiv 1(8), 5x^2 + y^2 \equiv 1(8), x^2 + 5y^2 \equiv 1(8), 5x^2 + 5y^2 \equiv 1(8)$. It is very easy to solve these congruence equations. For example $(3, 0), (1, 2), (2, 1), (2, 1)$ are solutions in the respective order.

10) For each of the following sets of a, b, c find the set of primes p (including ∞) for which the only solution of $ax^2 + by^2 + cz^2 = 0$ in $\mathbb{Q}_p$ is the trivial one:

(i) (a,b,c) = (1,1,-2)

▶ Since the equation is homogeneous for $p \neq \infty$, we may assume that if there is a non-trivial solution (x, y, z), then $x, y, z \in \mathbb{Z}_p$.

We see that $(1, 1, 1)$ is a solution in $\mathbb{Z}$. Therefore, there are non-trivial solutions for every p (including ∞).

(ii) (a,b,c) = (1,1,-3)

▶ This is the equation $x^2 + y^2 = 3z^2$. It is easy to obtain solutions over $\mathbb{R}$ such as $(\sqrt{3}, 0, 1)$. There are no non-trivial solutions over $\mathbb{Q}_2$ by the previous exercise since $1 \equiv -3(4)$. There are no solutions over $\mathbb{Q}_3$ since the only way $x^2 + y^2$ is divisible by 3 is if both x and y are divisible by 3 but that implies z has to be divisible by 3, and continuing this way we see that $|x|_3 = |y|_3 = |z|_3 = 0$, which implies $x = y = z = 0 \in \mathbb{Q}_3$. There are non-trivial solutions over any other prime by Exercise 2.

(iii) (a,b,c) = (1,1,1)

▶ This is the equation $x^2 + y^2 + z^2 = 0$. There are no non-trivial solutions over $\mathbb{R}$ since the left hand side is strictly positive unless $x = y = z = 0$. There are no non-trivial solutions over $\mathbb{Q}_2$ by the previous exercise. There are non-trivial solutions over any other prime by Exercise 2.

(iv) (a,b,c) = (14,-15,33)

▶ This is the equation $14x^2 + 33z^2 = 15y^2$.

There are non-trivial solutions over $\mathbb{R}$: Take, for example, $(15\sqrt{14}, 0, 14\sqrt{15})$. There are non-trivial solutions over $\mathbb{Q}_2$ by the previous exercise, since 14 is not equivalent to 33 modulo 4. By Exercise 2, there are non-trivial solutions over any prime $p > 11$. It remains to the understand the cases $p = 3, 5, 7, 11$.

We see that $|x|_3 < 1$, hence we can write $x = 3\tilde{x}$ with $\tilde{x} \in \mathbb{Z}_3$. We then get the equivalent equation, $42\tilde{x}^2 + 11z^2 = 5y^2$. Multiplying both sides by 5, we get $5.42\tilde{x}^2 + 55z^2 = (5y)^2$. Now,

we can appeal to Lemma 3 from Chapter 2, which says that a number is a square in $\mathbb{Q}_3$ if and only if it is over $\mathbb{F}_3$. Reducing mo 3, we get $5.42\tilde{x}^2 + 55z^2 = z^2$. Hence, for any value of z, we will get solutions.

$14x^2 + 33z^2 \equiv 4x^2 + 3z^2(5)$. The only way $4x^2 + 3z^2$ is divisible by 5 is if both x and z are divisible by 5 but that implies that y has to be divisible by 5, and continuing this way we see that $|x|_5 = |y|_5 = |z|_5 = 0$, which implies $x = y = z = 0 \in \mathbb{Q}_5$.

$15y^2 - 33z^2 \equiv y^2 + 2z^2(7)$. The only way $y^2 + 2z^2$ is divisible by 7 is if both y and z are divisible by 7 but that implies that x has to be divisible by 7, and continuing this way we see that $|x|_7 = |y|_7 = |z|_7 = 0$, which implies $x = y = z = 0 \in \mathbb{Q}_7$.

If we multiply both sides by 14 we get to the equivalent equation: $(14x)^2 = 14.15y^2 - 14.33z^2$. To see that this has solutions over $\mathbb{Q}_{11}$ we can appeal to Lemma 3 from Chapter 2, which says that a number is a square in $\mathbb{Q}_{11}$ if and only if it is over $\mathbb{F}_{11}$. Reducing mod 11, we get $14.15y^2 - 14.33z^2 = y^2$. Hence, for any non-zero value of y, we will get solutions.

11) Do you observe anything about the parity of the number N of primes (including ∞) for which there is insolubility? If not, construct similar exercises and solve them until the penny drops.

▶ It seems to be always even.

12) (i) Prove your observation in (6) in the special case $a = 1, b = -r, c = -s$, where r, s are distinct primes > 2. [Hint. Quadratic reciprocity]

▶ This is the equation $x^2 = ry^2 + sz^2$. Given r, s are prime numbers, the only primes where we may not have non-trivial solutions are $p = 2, r, s$. By Exercise 4, there are non-trivial solutions in $\mathbb{Q}_2$ if and only if at least one of r and s is 1 mod (4). As for solutions $\mathbb{Q}_r$ we need to see if $x^2 \equiv sz^2(r)$ is solvable or equivalently whether s is a quadratic residue modulo r, and similarly for $\mathbb{Q}_s$ we need to see if $x^2 \equiv ry^2(s)$ is solvable or equivalently whether r is a quadratic residue modulo s. The required evenness is now a direct consequence of quadratic reciprocity law which says: If r or s are congruent to 1 modulo 4, then: $x^2 \equiv r(s)$ is solvable if and only if $x^2 \equiv s(r)$ is solvable, and if r and s are congruent to 3 modulo 4, then: $x^2 \equiv r(s)$ is solvable if and only if $x^2 \equiv s(r)$ is not solvable.

(ii) [Difficult.] Prove your observation for all $a, b, c \in \mathbb{Z}$.

▶ This is equivalent to quadratic reciprocity. A proof is given in Cassel's book "Rational quadratic forms" Lemma 3.4. The proof is similar to the previous problem but there are far more cases.

Chapter 4

13) Let $m \in \mathbb{Z}, m > 1$ and suppose that there is some $f \in \mathbb{Z}$ such that $f^2 + f + 1 \equiv 0(m)$. Show that $m = u^2 + uv + v^2$ for some $u, v \in \mathbb{Z}$.

▶ We consider the open ellipse $x^2 + xy + y^2 < 2m$. Its area is πab where a, b are lengths of semi-major and semi-minor axis, which can be found by setting $x = y$ and $x = -y$. This gives

$a = 2\sqrt{\frac{m}{3}}$ and $b = 2\sqrt{m}$, respectively. Hence, the area is equal to $\frac{4m\pi}{\sqrt{3}}$, which is greater than $4m$.

Now, consider the lattice L in $\mathbb{Z}^2$ given by $y \cong fx\,(m)$. This is clearly an index m subgroup of $\mathbb{Z}^2$. Hence, by Theorem 1, there is a non-zero (u, v) in L and in the open ellipse above. This satisfies $0 < u^2 + uv + v^2 < 2m$ and $u^2 + uv + v^2 \equiv u^2(1 + f + f^2) \equiv 0(m)$. Hence, $u^2 + uv + v^2 = m$, as required.

14) Find a prime $p > 0$ for which there is an $f \in \mathbb{Z}$ such that $1 + 5f^2 \equiv 0(p)$ but p is not of the shape $u^2 + 5v^2 (u, v \in \mathbb{Z})$.

▶ Consider $p = 7$. Then $f = 2$ satisfies $1 + 5f^2 \equiv 0(7)$. But, $7 \neq u^2 + 5v^2$ for any $u, v \in \mathbb{Z}$ as can be verified directly, or by noting that 2 is not a quadratic residue modulo 5.

The point of this exercise is that the approach to this problem as in the previous problem fails. Indeed, the area of the ellipse $x^2 + 5y^2 < 2p$ is $2p\pi/\sqrt{5}$ which is not greater than $4p$.

Chapter 5

15) Let $F(X, Y, Z) = 5X^2 + 3Y^2 + 8Z^2 + 6(YZ + ZX + XY)$. Find rational integers x, y, z not all divisible by 13, such that $F(x, y, z) \equiv 0(13^2)$.

▶ If we apply the linear change of co-ordinates given by $X \to 5X - 3Y$, $Y \to 5Y - 5Z$ and $Z \to 5Z$, we obtain the conic $125X^2 + 30Y^2 + 125Z^2$. Since 5 divides all the coefficients, let us consider the conic $25X^2 + 6Y^2 + 25Z^2$ instead. Finally, we can send $5X, 5Z \to X, Z$ to get to the conic $X^2 + 6Y^2 + Z^2$. All of these changes were invertible over $\mathbb{Q}_{13}$, therefore, solving $X^2 + 6Y^2 + Z^2 \equiv 0(13^2)$ will lead to the solution of the original problem. It is easy to see that $(2, 0, 3)$ gives a solution over $\mathbb{F}_{13}$. Hence, we try $X = 2 + 13x, Y = 13y, Z = 3 + 13z$ with $x, y, z \in \{0, \ldots, 12\}$. We get

$$(2 + 13x)^2 + 6.(13.y)^2 + (3 + 13z)^2 \equiv 0(13^2)$$

This gives $13 + 52x + 78z \equiv 0(13^2)$. Hence, $(x, y, z) = (0, 0, 2)$ is a solution. Hence, we conclude that $(X, Y, Z) = (2, 0, 29)$ is a solution to $X^2 + 6Y^2 + Z^2 \equiv 0(13^2)$. Reverting this back to a solution for the original problem, we get $(68, 28, 141)$ as a solution, which gives $F(68, 28, 141) = 13^2.1640$.

16) Let $F(X, Y, Z) = 7X^2 + 3Y^2 - 2Z^2 + 4YZ + 6ZX + 2XY$. Find rational integers x, y, z not all divisible by 17, such that $F(x, y, z) \equiv 0(17^3)$.

▶ By using Lagrangian reduction method (completing to squares), we can diagonalize F. This gives the following. If we apply the change of coordinates $Y \to X-(4/5)Y$, $Z \to Z+Y+(7/10)X$ we get the form $(83/10)X^2 + 5Y^2 - 2Z^2$. Multiplying by 10, we reduce to finding a solution to

$$83X^2 + 50Y^2 - 20Z^2 \equiv 0(17^3)$$

modulo 17, this reduces to $2X^2 + Y^2 + 3Z^2 \equiv 0(17)$. To which it is easy to find solutions - for example $(2, 3, 0)$ is a solution. Now, to lift this to modulo 17^2, we try $2 + 17x_1, 3 + 17y_1, 17z_1$ and try to solve

$$83(2 + 17x_1)^2 + 50(3 + 17y_1)^2 - 20(17z_1)^2 \equiv 0(17^2)$$

which becomes

$$83(4 + 68x_1) + 50(9 + 102y_1) \equiv 0(17^2)$$

This simplifies to

$$9x_1 + 11y_1 \equiv 5(17)$$

to which $x_1 = 0$, $y_1 = 2$ give a solution. Now, if we calculate with $(2, 3 + 17.2, 0)$, it is easy to verify that we get

$$(17.5 - 2)(4) + (17.3 - 1)(3 + 17.2)^2 \equiv 0(17^3)$$

To return back to the original equation, we multiply by 10 and apply the change of co-ordinates, to get

$$F(20, 354, 384) \equiv 0(17^3)$$

Dividing by 2, we get the simpler solution $(10, 177, 192)$. One can calculate that

$$F(10, 177, 192) = 35.17^3$$

Chapter 6

17) (i) Show that the cubic curve

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

is non-singular provided that $4A^3 + 27B^2 \neq 0$.

▶ Let $F(X, Y, Z) = Y^2Z - X^3 - AXZ^2 - BZ^3$. To find singular points, we compute

$$\frac{\partial F}{\partial X} = -3X^2 - AZ^2 = 0$$

$$\frac{\partial F}{\partial Y} = 2YZ = 0$$

$$\frac{\partial F}{\partial Z} = Y^2 - 2AXZ - 3BZ^2 = 0$$

The second one gives, either $Y = 0$ or $Z = 0$. If $Z = 0$, we conclude from the other equations that $X = Y = 0$, hence this is not a valid point. So, it must be that $Y = 0$ and $Z = 1$ (up to scaling). Then, the first and third equations, we get: $A = -3X^2$ and $3B = -2AX$. Thus, if $X = 0$, then $A = B = 0$ and we have a singular point at $[0 : 0 : 1]$. Otherwise, $-\frac{A}{3} = \frac{9B^2}{4A^2}$, hence $4A^3 + 27B^2 = 0$ (which is also satisfied when $A = B = 0$. Thus, we conclude that if $4A^3 + 27B^2 \neq 0$, the curve is non-singular.

(ii) If $4A^3 + 27B^2 = 0$, find a singularity and decide whether it is a cusp, or a double point with distinct tangents.

▶ If $4A^3 + 27B^2 = 0$, we have two cases 1) $A = B = 0$, then $[0 : 0 : 1]$ is the unique singular point or 2) If $4A^3 + 27B^2 = 0$ but $A \neq 0$, then $[-3B/2A : 0 : 1]$ is the unique singular point.

In case 1), the affine equation is given by $Y^2 = X^3$. This is a cusp singularity, tangent cone at the origin is given by $Y^2 = 0$. In case 2), we apply the transformation $X \to X - (3B/2A)Z$ to send the singularity to $[0 : 0 : 1]$, then the affine equation (using $4A^3 + 27B^2 = 0$) is given by $Y^2 + (9B/2A)X^2 = X^3$. Thus, we get an ordinary node singularity. The tangent cone at the origin is given by $(Y - \sqrt{(9B/2A)}X)(Y + \sqrt{(9B/2A)}X) = 0$.

18) (i) Let $F(\mathbf{x}) = a_1X_1^3 + a_2X_2^3 + a_3X_3^3 + dX_1X_2X_3$, where $a_1a_2a_3 \neq 0$. Show that $F(x) = 0$ is non-singular provided that $27a_1a_2a_3 + d^3 \neq 0$.

► We compute the derivatives

$$\frac{\partial F}{\partial X_1} = 3a_1X_1^2 + dX_2X_3 = 0$$
$$\frac{\partial F}{\partial X_2} = 3a_2X_2^2 + dX_1X_3 = 0$$
$$\frac{\partial F}{\partial X_3} = 3a_3X_3^2 + dX_1X_2 = 0$$

Note if any $X_i = 0$, these equations imply, all the other X_j are also zero. Hence, we can assume $X_i \neq 0$ for any i. Now, taking the second terms to the right hand side and multiplying the three equations yield $27a_1a_2a_3 = -d^3$. So, if $27a_1a_2a_3 + d^3 \neq 0$, the curve is non-singular.

(ii) If $a_1 = a_2 = a_3 = 1, d = -3$, show that any point (x_1, x_2, x_3) with $x_1^3 = x_2^3 = x_3^3 = x_1x_2x_3 = 1$ is a singularity.

► In this case, it is easy to see that $F(\mathbf{x}) = (X_1+X_2+X_3)(X_1+\xi X_2+\xi^2X_3)(X_1+\xi^2X_2+\xi X_3)$ where $\xi^3 = 1$.

(iii) How does the result of (ii) square with the result proved in the text that a cubic curve has at most one singularity?

► The text assumed irreducible (over $\overline{\mathbb{Q}}$), whereas this curve is reducible (assuming ξ belongs to the ground field, otherwise there is a unique singularity anyway.)

19) Let $F(\mathbf{x})$ be as in the previous question and suppose that $F(\mathbf{x}) = 0$ is non-singular.

(i) Let $F(\mathbf{x}) = 0$. Show that the third intersection $\mathbf{t}$ of the tangent at $\mathbf{x}$ is given by

$$t_j = x_j(a_{j+1}x_{j+1}^3 - a_{j+2}x_{j+2}^3) \quad (j = 1, 2, 3)$$

where the suffixes are taken mod 3.

► The tangent line at $\mathbf{x} = (x_1, x_2, x_3)$ is given by

$$T(\mathbf{x}) = (3a_1x_1^2 + dx_2x_3)X_1 + (3a_2x_2^2 + dx_1x_3)X_2 + (3a_3x_3^2 + dx_1x_2)X_3 = 0$$

It suffices to verify that the given $\mathbf{t} = (t_1, t_2, t_3)$ satisfies $F(\mathbf{t}) = 0$ and $T(\mathbf{t}) = 0$. We compute

$$\begin{aligned} F(\mathbf{t}) = {} & a_1x_1^3(a_2x_2^3 - a_3x_3^3)^3 + a_2x_2^3(a_3x_3^3 - a_1x_1^3)^3 + a_3x_3^3(a_1x_1^3 - a_2x_2^3)^3 \\ & + dx_1x_2x_3(a_1x_1^3 - a_2x_2^3)(a_2x_2^3 - a_3x_3^3)(a_3x_3^3 - a_1x_1^3) \end{aligned}$$

Replacing $dx_1x_2x_3$ with $-x_1^3-x_2^3-x_3^3$ in the second line, it is easy to then see that all the terms cancel and we get $F(\mathbf{t})=0$.

Similarly,

$$\begin{aligned}T(\mathbf{t}) &= (3a_1x_1^3+dx_1x_2x_3)(a_2x_2^3-a_3x_3^3)\\ &\quad+(3a_2x_2^3+dx_1x_2x_3)(a_3x_3^3-a_1x_1^3)\\ &\quad+(3a_3x_3^3+dx_1x_2x_3)(a_1x_1^3-a_2x_2^3)\\ &=0\end{aligned}$$

(ii) Let $\mathbf{x},\mathbf{y}$ be distinct points on $F(\mathbf{x})=0$. Show that the third intersection point $\mathbf{z}$ of the line joining them is given by

$$z_j = x_j^2y_{j+1}y_{j+2}-y_j^2x_{j+1}x_{j+2}.$$

[Formulae of Desboves]

▶ The line through $\mathbf{x},\mathbf{y}$ is given by the equation

$$\ell_{\mathbf{x},\mathbf{y}}(\mathbf{z}) = (x_2y_3-x_3y_2)X+(x_3y_1-x_1y_3)Y+(x_1y_2-x_2y_1)Z=0$$

It suffices to show that $\mathbf{F}(\mathbf{z})=0$ and $\ell_{\mathbf{x},\mathbf{y}}(\mathbf{z})=0$. We compute

$$\begin{aligned}F(\mathbf{z}) &= a_1(x_1^2y_2y_3-y_1^2x_2x_3)^3+a_2(x_2^2y_3y_1-y_2^2x_3x_1)^3+a_3(x_3^2y_1y_2-y_3^2x_1x_2)^3\\ &\quad+d(x_1^2y_2y_3-y_1^2x_2x_3)(x_2^2y_3y_1-y_2^2x_3x_1)(x_3^2y_1y_2-y_3^2x_1x_3)\\ &=0\end{aligned}$$

and

$$\begin{aligned}\ell_{\mathbf{x},\mathbf{y}}(\mathbf{z}) &= (x_2y_3-x_3y_2)(x_1^2y_2y_3-y_1^2x_2x_3)\\ &\quad+(x_3y_1-x_1y_3)(x_2^2y_3y_1-y_2^2x_3x_1)\\ &\quad+(x_1y_2-x_2y_1)(x_3^2y_1y_2-y_3^2x_1x_2)\\ &=0\end{aligned}$$

20) Starting with the solution $(2,-1,-1)$ of $X^3+Y^3+7Z^3=0$, find 10 distinct solutions.

▶ Note that the equation is homogeneous, so we should ensure $gcd(X,Y,Z)=1$. We start with $(2,-1,-1)$ and generate other solutions by using Desboves formulae. We apply the formulae from Exercise 3i) to $\mathbf{x}_1=(2,-1,-1)$ to get $(12,15,-9)$ which we then divide by 3 to get $\mathbf{x}_2=(4,5,-3)$. We apply the same formula to get $\mathbf{x}_3=(1256,-1265,183)$. Next, considering secant between $\mathbf{x}_1$ and $\mathbf{x}_3$ gives a new point $\mathbf{x}_4=(-65882,90271,-40049)$ (the secant formula gives 38 times this).

The numbers are getting big, so let's make another observation. If (x,y,z) is a solution so is (y,x,z). Therefore, $\mathbf{x}_5=(-1,2,-1)$ is also a solution. Taking the secant between $\mathbf{x}_1$ and $\mathbf{x}_5$ leads to $\mathbf{x}_6=(1,-1,0)$. In fact, it follows easily from Exercise 3ii) that if (x,y,z) is a solution, the secant line between (x,y,z) and $(1,-1,0)$ intersects the curve at (y,x,z). In any case, we get $\mathbf{x}_7=(5,4,-3)$ and $\mathbf{x}_8=(-1265,1256,183)$ as other new points. Taking a secant line between $\mathbf{x}_1$ and $\mathbf{x}_7$ gives $\mathbf{x}_9=(-73,17,38)$, and our last point $\mathbf{x}_{10}=(17,-73,38)$ is obtained by switching the first two co-ordinates.

Chapter 7

21) Let $\mathbf{o}$, $\mathbf{a}$ be rational points on the nonsingular cubic $\mathcal{C}$. Construct the point $-\mathbf{a}$ with respect to the group law for which $\mathbf{o}$ is the neutral element.

▶ How to do this is already explained in the chapter: Take the tangent line at $\mathbf{o}$ and call the third point that it meets the cubic $\mathbf{k}$. Now take the line through $\mathbf{a}$ and $\mathbf{k}$. The claim is that third point of intersection of this line with $\mathcal{C}$ is $-\mathbf{a}$. To see this: We take the third point of intersection of the line through $\mathbf{a}$ and $-\mathbf{a}$, which is $\mathbf{k}$. Then we join $\mathbf{k}$ to $\mathbf{o}$ and take the third intersection point. But, since the line through $\mathbf{k}$ and $\mathbf{o}$ is tangent to $\mathcal{C}$ at $\mathbf{o}$. The third point of intersection is $\mathbf{o}$. This proves that $\mathbf{a} + (-\mathbf{a}) = \mathbf{o}$ as required.

22) Let $\mathbf{o}$, $\mathbf{o}_1$ be rational points on the nonsingular cubic $\mathcal{C}$. Show how the group law for which $\mathbf{o}_1$ is the neutral element can be expressed in terms of that for which $\mathbf{o}$ is the neutral element.

▶ Let us write $+_1$ for the group law corresponding to $\mathbf{o}_1$ and $+$ for the group law corresponding to $\mathbf{o}$. We will prove

$$\mathbf{x} +_1 \mathbf{y} = \mathbf{x} + \mathbf{y} - \mathbf{o}_1$$

Indeed, let the third intersection of $\mathbf{x}$ and $\mathbf{y}$ with $\mathcal{C}$ be $\mathbf{z}$. then $\mathbf{x} + \mathbf{y}$ is the third intersection of the line through $\mathbf{o}$ and $\mathbf{z}$ and $\mathbf{x} +_1 \mathbf{y}$ is the third intersection of the line through $\mathbf{o}_1$ and $\mathbf{z}$ with $\mathcal{C}$. It follows that

$$(\mathbf{x} +_1 \mathbf{y}) + \mathbf{o}_1 = \mathbf{x} + \mathbf{y}$$

Which is equivalent to $\mathbf{x} +_1 \mathbf{y} = \mathbf{x} + \mathbf{y} - \mathbf{o}_1$, as claimed.

23) Let $\mathbf{o}, \mathbf{a}$ be rational points on the nonsingular cubic $\mathcal{C}$ and suppose that $3\mathbf{a} = \mathbf{o}$ with respect to the group law based on $\mathbf{o}$. Let $\mathbf{b} = 2\mathbf{a}$. Show that each side of the triangle $\mathbf{o}, \mathbf{a}, \mathbf{b}$ meets the tangent to $\mathcal{C}$ of the opposite vertex at a point of $\mathcal{C}$. Take $\mathbf{o}, \mathbf{a}, \mathbf{b}$ as the triangle of reference and express this condition in terms of the coefficients of the cubic form determining $\mathcal{C}$.

▶ The fact that tangent to $\mathbf{a}$ intersects the line through $\mathbf{o}$ and $\mathbf{b}$ at a point of $\mathcal{C}$ is immediate from $a + a = b$, and similarly the fact that tangent to $\mathbf{b}$ intersects the line through $\mathbf{o}$ and $\mathbf{a}$ at a point of $\mathcal{C}$ is immediate from $b + b = a$. Finally, the fact that tangent through $\mathbf{o}$ intersects the line through $\mathbf{a}$ and $\mathbf{b}$ at a point of $\mathcal{C}$ follows from $a + b = 0$.

Now, let $\mathbf{a} = [1 : 0 : 0]$, $\mathbf{o} = [0 : 1 : 0]$ and $\mathbf{b} = [0 : 0 : 1]$. Consider a general cubic form F that passes through these points. It has an equation of the form:

$$F(X, Y, Z) = cXYZ + a_1XY^2 + a_2YZ^2 + a_3ZX^2 + b_1Z^2X + b_2X^2Y + b_3Y^2Z$$

(There are no terms corresponding to X^3, Y^3, Z^3 by the condition that F passes through $\mathbf{a}, \mathbf{o}, \mathbf{b}$).

Now, we have the lines

$$\ell_{\mathbf{o},\mathbf{b}} = \{X = 0\}$$
$$\ell_{\mathbf{a},\mathbf{b}} = \{Y = 0\}$$
$$\ell_{\mathbf{a},\mathbf{o}} = \{Z = 0\}$$

and the tangent lines

$$t_{\mathbf{a}} = \{b_2Y + a_3Z = 0\}$$
$$t_{\mathbf{o}} = \{a_1X + b_3Z = 0\}$$
$$t_{\mathbf{b}} = \{b_1X + a_2Y = 0\}$$

The intersections of these lines

$$\ell_{\mathbf{o},\mathbf{b}} \cap t_{\mathbf{a}} = \{[0 : a_3 : -b_2]\}$$
$$\ell_{\mathbf{a},\mathbf{b}} \cap t_{\mathbf{o}} = \{[b_3 : 0 : -a_1]\}$$
$$\ell_{\mathbf{a},\mathbf{o}} \cap t_{\mathbf{b}} = \{[a_2 : -b_1 : 0]\}$$

The condition that these lie on $\mathcal{C}$ is equivalent to

$$a_1b_1 = a_2b_2 = a_3b_3$$

24) Let $\mathcal{C}$ be the curve

$$X^3 + Y^3 - XZ^2 - YZ^2 + 7XYZ = 0$$

and let $\mathbf{x} = (x, y, z)$ be a point on $\mathcal{C}$ defined over some $\mathbb{Q}_p$. Show that $y/x \to -1$ as $\mathbf{x} \to (0, 0, 1)$ (with respect to the p-adic topology).

▶ Since the equation is homogeneous, we can assume that $\max\{|x|_p, |y|_p, |z|_p\} = 1$. We want to show that for every $M > 0$, there exists an $N > 0$ such that if $|x|_p, |y|_p, |z - 1|_p < p^{-N}$, then $|\frac{y}{x} + 1|_p < p^{-M}$. In fact, we will see that taking $N = M$ works.

Let us write $x = p^N x', y = p^N y'$ and $z = 1 + p^N z'$ with $|x'|_p, |y'|_p, |z'|_p \leq 1$. Plugging in these to the equation of the curve $\mathcal{C}$, we get

$$p^{3N}x'^3 + p^{3N}y'^3 + 7p^{2N}x'y'(1 + p^N z') = (p^N x' + p^N y')(1 + p^N z')^2$$

Thus, depending on whether $x|y$ or $y|x$, we see that either $p^N x|x+y$ or $p^N y|x+y$. Equivalently, either $|x + y|_p < p^{-N}|x|_p$ or $|x + y|_p < p^{-N}|y|_p$. In either case, we see that $|x + y|_p < |x|_p$ or $|x + y|_p < |y|_p$, which by the non-archimedean property implies that $|x|_p = |y|_p$, hence the two possibilities are the same. Thus, we conclude that $|\frac{y}{x} + 1|_p < p^{-N}$ as required.

25) In this question everything is defined over $\mathbb{Q}_p$ for some p. Let $\mathbf{a}$ be a nonsingular point on the cubic curve

$$F(X, Y, Z) = 0$$

and let $t(\mathbf{X}) = 0$ be the tangent. Let $l(\mathbf{X}) = 0, m(\mathbf{X}) = 0$ be lines through $\mathbf{a}$ distinct from the tangent. Show that there are d, e, f such that

$$dl(\mathbf{X}) + em(\mathbf{X}) + ft(\mathbf{X}) = 0$$

(identically) with $d \neq 0$, $e \neq 0$. Show that

$$m(\mathbf{x})/l(\mathbf{x}) \to -d/e$$

as $\mathbf{x} \to \mathbf{a}$.

▶ Let $t(\mathbf{X}) = a_1X + b_1Y + c_1Z, l(\mathbf{X}) = a_2X + b_2Y + c_2Z$ and $m(\mathbf{X}) = a_3X + b_3Y + c_3Z$. If we form the matrix with rows $(a_1, b_1, c_1), (a_2, b_2, c_2), (a_3, b_3, c_3)$, we see that $\mathbf{a}$ is a non-zero vector in the kernel of this matrix, hence there must be a linear relation between the rows of this matrix, in other words, we have constants, d, e, f such that

$$dl(\mathbf{X}) + em(\mathbf{X}) + ft(\mathbf{X}) = 0$$

Now, it cannot be that d or $e = 0$, since this implies that $t(\mathbf{X})$ coincides with $l(\mathbf{X})$ or $m(\mathbf{X})$ which is ruled out by definition. Thus, to show that $m(\mathbf{x})/l(\mathbf{x}) \to -d/e$ as $\mathbf{x} \to \mathbf{a}$, it suffices to observe that the rational function $g(\mathbf{x}) = t(\mathbf{x})/l(\mathbf{x})$ vanishes at $\mathbf{a}$. Indeed, being a tangent line the restriction of t to $F = 0$ vanishes to order at least two at $\mathbf{a}$ whereas any other line, such as l gives a simple zero.

(NB: This exercise is a generalisation of the previous one.)

Chapter 8

26) Transform the following curves to canonical form:

(i) $X^3 + Y^3 + dZ^3 = 0$

▶ This is covered in Chapter 8 as case (i). The result is

$$\boxed{Y^2Z = X^3 - 2^4.3^3.d^2Z^3}$$

(ii) $X^3 + Y^3 + Z^3 - 3mXYZ = 0$

▶ We compute the derivatives of $F = X^3 + Y^3 + Z^3 - 3mXYZ$.

$$\frac{\partial F}{\partial X} = 3X^2 - 3mYZ$$
$$\frac{\partial F}{\partial Y} = 3Y^2 - 3mXZ$$
$$\frac{\partial F}{\partial Z} = 3Z^2 - 3mXY$$

From this, it is easy to see that the values of m for which $m^3 = 1$ give singular curves, otherwise we get smooth cubics (assuming ground field has characteristic $\neq 3$). We can take $\mathbf{o} = [1 : -1 : 0]$ as a base point. Computing the tangent line at this point we get

$$t(\mathbf{o}) = \{X + Y + mZ = 0\}$$

We can in fact see that $\mathbf{o}$ is an inflexion point by computing $F(1,Y,Z)|_{t(\mathbf{o})} = (1-m^3)Z^3$. Alternatively, it is easy to see that the line $t(\mathbf{o})$ does not intersect the curve $\{F=0\}$ at any other point.

Now, we need to apply a linear transformation of co-ordinates, taking $\mathbf{o}$ to $[0:1:0]$ and the line $X+Y+mZ=0$ to $Z=0$. One such transformation is given by $(X,Y,Z)\to(Y,-mX-Y+Z,X)$, then plugging this into the equation of F, we get

$$Y^3+(-mX-Y+Z)^3+X^3+3mXY(mX+Y-Z)=0$$

This simplifies (setting $Z=1$) to

$$(m^3-1)X^3-3m^2X^2+3mX-1=3Y^2+3mXY-3Y$$

Multiply both sides by the non-zero number $3^3(m^3-1)^2$ and use the substitution $(3(m^3-1)X, 3^2(m^3-1)Y)\to(X,Y)$ to get to the equation.

$$X^3-9m^2X^2+27m(m^3-1)X-27(m^3-1)^2=Y^2+3mXY-9(m^3-1)Y$$

which is an elliptic curve in the Weierstrass form. Now, if ground field has characteristic $\neq 2$, we can further simplify by sending $Y\to Y-\frac{3mX}{2}+\frac{9(m^3-1)}{2}$ to get

$$Y^2=X^3-\frac{27m^2}{4}X^2+27(\frac{m}{2})(m^3-1)X-\frac{27}{4}(m^3-1)^2$$

We can further simplify it by sending $X\to X+\frac{9m^2}{4}$ to get to

$$Y^2=X^3-\frac{27}{2}(\frac{m^4}{8}+m)X+\frac{27}{4}(\frac{m^6}{8}-\frac{5m^3}{2}-1)$$

which by multiplying with 2^6 and rescaling X and Y can finally be simplified to

$$\boxed{Y^2=X^3-27(m^4+8m)X+54(m^6-20m^3-8)}$$

(iii) $Y^2-kT^2=X^2, Y^2+kT^2=Z^2$

▶ We first apply a change of variablex $(X,Y,Z,T)\to(X+T,T,Z+T,Y)$ to rewrite these equations as

$$kY^2+X^2+2XT=0, Z^2-kY^2+2ZT=0$$

Then, as explained in the Chapter, these equations are equivalent to

$$Z(kY^2+X^2)+X(kY^2-Z^2)=0$$

Now, we notice that $[0:0:1]$ is a point on the curve with tangent line $X=0$ which intersects the curve at the third point $[0:1:0]$. We want to bring our curve to a form where we can

apply Nagell's algorithm as explained in the text. If we do the transformation $(X, Y, Z) \to (X, Y - Z, Y)$ and then we obtain the curve

$$X^2Y - XY^2 + (kX + kY)(Y - Z)^2 = 0$$

which is given in affine co-ordinates ($Z = 1$) by

$$F_3(X, Y) + F_2(X, Y) + F_1(X, Y)$$

with $F_3(X, Y) = X^2Y + (k-1)XY^2 + kY^3$, $F_2(X, Y) = -2k(XY + Y^2)$ and $F_1(X, Y) = k(X+Y)$. Note that we arranged it so that $(0, 0)$ and $(0, 1)$ are points on the curve and the y-axis given by $X = 0$ is tangent to the curve at $(0, 1)$, so we can apply precisely the formulae given in the Chapter 8(ii). We thus get that our curve is equivalent to

$$s^2 = G(t)$$

with $s = 2F_3(1, t)x + F_2(1, t)$ and $G(t) = F_2(1, t)^2 - 4F_1(1, t)F_3(1, t)$. Expanding out $G(t)$, we get

$$G(t) = 4k^2(t + t^2)^2 - 4k(t + 1)(t - t^2 + k(t^2 + t^3)) = 4k(t^3 - t)$$

Hence, our curve is equivalent to $s^2 = 4k(t^3 - t)$. Multiplying both sides by k^2 and redefining $y = ks/2$ and $x = kt$, we arrive at the final equation

$$\boxed{y^2 = x^3 - k^2x}$$

NB: This curve is related to the question of whether k is a congruent number.

(iv) $X_1^2X_2 - X_1X_2^2 - X_1X_3^2 + X_2^2X_3 = 0$

▶ We let $X_1 = Y, X_2 = X, X_3 = Z$ and get the equation

$$F = Y^2X - YX^2 - YZ^2 + X^2Z = 0$$

We take $\mathbf{o} = [0 : 1 : 0]$. We compute the derivatives

$$\frac{\partial F}{\partial X} = Y^2 - 2XY + 2XZ$$
$$\frac{\partial F}{\partial Y} = 2XY - X^2 - Z^2$$
$$\frac{\partial F}{\partial Z} = -2YZ + X^2$$

We see that the tangent line $t(\mathbf{o}) = X = 0$, and this intersect the curve defined by F at another point $\mathbf{p} = [0 : 0 : 1]$. We want to work in an affine chart where both these points are visible and p is at the origin. Applying the transformation $(X, Y, Z) \to (X, Y, Z - Y)$ arranges $\mathbf{o} = [0 : 1 : 1]$ and $\mathbf{p} = [0 : 0 : 1]$. Our equation becomes:

$$Y^2X - YX^2 - Y(Z - Y)^2 + X^2(Z - Y) = 0$$

Setting $Z = 1$ and reorganizing according to degree we get

$$F_3(X,Y) + F_2(X,Y) + F_1(X,Y)$$

with $F_3(X,Y) = -Y^3 + Y^2X - 2YX^2$, $F_2(X,Y) = X^2 + 2Y^2$ and $F_1(X,Y) = -Y$. As in Chapter 8(ii), we set $s = 2F_3(1,t)x + F_2(1,t)$ and $G(t) = F_2(1,t)^2 - 4F_1(1,t)F_3(1,t)$. Our curve is now equivalent to $s^2 = G(t)$. Expanding out $G(t)$, we get the equation

$$s^2 = 4t^3 - 4t^2 + 1$$

Now, multiplying by 4^2 and redefining $y = 4s$ and $x = 4t$, we arrive at the equation

$$y^2 = x^3 - 4x^2 + 16$$

Finally, if the ground field has charactersitic $\neq 3$, we can do the substitution $x \to x + 4/3$ to get

$$y^2 = x^3 - \frac{16}{3}x + \frac{16.19}{27}$$

which we can then rescale to

$$\boxed{y^2 = x^3 - 2^4.3^3x + 2^4.3^3.19}$$

This can be recognized as the modular curve $X_1(11)$, see https://www.lmfdb.org/EllipticCurve/Q/11/a/3.

27) [Difficult.] Show that the group law on $X^2 = Y^2 - T^2, Z^2 = Y^2 + T^2$ with $(1,1,1,0)$ as neutral element is given by $\mathbf{x}_3 = \mathbf{x}_1 + \mathbf{x}_2$, where

$$\begin{aligned} x_3 &= x_2t_2y_1z_1 - x_1t_1y_2z_2 \\ y_3 &= y_2t_2z_1x_1 - y_1t_1z_2x_2 \\ z_3 &= z_2t_2x_1y_1 - z_1t_1x_2y_2 \\ t_3 &= t_2^2x_1^2 - t_1^2x_2^2 = t_2^2y_1^2 - t_1^2y_2^2 = t_2^2z_1^2 - t_1^2z_2^2 \end{aligned}$$

Coursework problem.

28) (i) Find all the points defined over the field $\mathbb{F}_5$ of 5 elements on each of

$$\begin{aligned} Y^2Z &= X^3 + XZ^2 \\ Y^2Z &= X^3 + 2XZ^2 \\ Y^2Z &= X^3 + Z^3 \end{aligned}$$

Check in each case that they form a group under the group law, with $(0,1,0)$ as neutral element.

► These are in Weierstrass from, so the only point at infinity is $\mathbf{o} = [0 : 1 : 0]$. Now, we let $Z = 1$ and consider the affine equations:

$$Y^2 = X^3 + X$$
$$Y^2 = X^3 + 2X$$
$$Y^2 = X^3 + 1$$

Recall that the quadratic residues mod 5 are $\{0, 1, 4\}$. Now, we plug in $X = 0, 1, 2, 3, 4$ and see if these give quadratic residues. As a result we get the following solutions:

$$\begin{aligned} Y^2Z = X^3 + XZ^2 &: \{[0:1:0], [0:0:1], [2:0:1], [3:0:1]\} \\ Y^2Z = X^3 + 2XZ^2 &: \{[0:1:0], [0:0:1]\} \\ Y^2Z = X^3 + Z^3 &: \{[0:1:0], [0:1:1], [0:4:1], [2:2:1], [2:3:1], [4:0:1]\} \end{aligned}$$

The associated groups can easily be determined to be $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

To see the first one, note that all the non-identity elements have order 2. We can see this by considering the tangent lines at those points and see that the third point of intersection is at the identity. Namely, $X = 0$ is the tangent line at $[0 : 0 : 1]$, $2X + Z = 0$ is the tangent line at $[2 : 0 : 1]$ and $X + 2Z = 0$ is the tangent line at $[3 : 0 : 1]$.

The second one and the third one have to be the groups $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$ since these are the only abelian groups of order 2 and 6.

(ii) As (i) but with other $\mathbb{F}_p$ and other curves

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

Find an example where the group is not cyclic. Can you find an example where the group requires more than 2 generators?

► This problem is a bit strange, because the first example given in (i) provides an example of a group that is not cyclic (since every non-trivial element has order 2). However, let's study another example (which I ran into while browsing a lecture by Silverman). Consider the curve

$$y^2 = x^3 - 5x + 8$$

over $\mathbb{F}_{37}$, by substituting values of x modulo 37 and checking if $x^3 - 5x + 8$ is a square or not, we find that the following is the complete list of 45 points over $\mathbb{F}_{37}$:

$$\begin{aligned} &(1, \pm 2), (5, \pm 21), (6, \pm 3), (8, \pm 6), (9, \pm 27), (10, \pm 25), \\ &(11, \pm 27), (12, \pm 23), (16, \pm 19), (17, \pm 27), (19, \pm 1), (20, \pm 8), \\ &(21, \pm 5), (22, \pm 1), (26, \pm 8), (28, \pm 8), (30, \pm 25), (31, \pm 9), \\ &(33, \pm 1), (34, \pm 25), (35, \pm 26), (36, \pm 7), \mathbf{o} \end{aligned}$$

One can check that as an abelian group we get a group isomorphic to $\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ generated by $(28, -8)$ and $(9, -27)$.

NB: It is a theorem that working over $\mathbb{F}_p$ the group of points of an elliptic curve is either a finite cyclic group or is a product of two finite cyclic groups (see, for example, Theorem 4.1 in [5]). Therefore, it is impossible to find an example where the group requires more than 2 generators.

29) In the curves considered below, the point at infinity is taken as neutral element for the group law.

(i) Let $Y^2 = (X - \alpha)(X^2 + aX + b)$ be an elliptic curve. Show that the transformation $\mathbf{x} \to \mathbf{x} + (\alpha, 0)$ induces a fractional-linear transformation

$$T : x \to (t_{11}x + t_{12})/(t_{21}x + t_{22})$$

Check that $T^2 : x \to x$.

▶ The addition formula for the curve given is worked out in Silverman's book on page 54. Namely, for a curve in the Weierstrass form $y^2 = x^3 + a_2x^2 + a_4x + a_6$, the result (x_3, y_3) of addition of two distinct points (x_1, y_1) and (x_2, y_2) is given by

$$\begin{aligned} x_3 &= \lambda^2 - a_2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned}$$

where $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$. Plugging into this formula, we get

$$\boxed{T(x) = \frac{\alpha x + b + a\alpha}{x - \alpha}}$$

Now, it is easy to compute

$$T^2(x) = \frac{\alpha \frac{\alpha x + b + a\alpha}{x - \alpha} + b + a\alpha}{\frac{\alpha x + b + a\alpha}{x - \alpha} - \alpha} = x$$

(ii) Consider $Y^2 = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$ and let T_1, T_2, T_3 be as in (i) with $\alpha = \alpha_j$ $(j = 1, 2, 3)$. Show that T_1, T_2, T_3 commute and that

$$T_1T_2T_3 : x \to x$$

▶ We have

$$\begin{aligned} T_1(x) &= \frac{\alpha_1 x + \alpha_2\alpha_3 - \alpha_1(\alpha_2 + \alpha_3)}{x - \alpha_1} \\ T_2(x) &= \frac{\alpha_2 x + \alpha_1\alpha_3 - \alpha_2(\alpha_1 + \alpha_3)}{x - \alpha_2} \\ T_3(x) &= \frac{\alpha_3 x + \alpha_1\alpha_2 - \alpha_3(\alpha_1 + \alpha_2)}{x - \alpha_3} \end{aligned}$$

We compute

$$T_1T_2(x) = \frac{\alpha_3 x - (\alpha_1+\alpha_2)\alpha_3 + \alpha_1\alpha_2}{x-\alpha_3} = T_3(x)$$

From this it follows that $T_1T_2(x) = T_2T_1(x)$ and $T_1T_2T_3(x) = x$.

(iii) Let $\mathcal{T}_j$ be the 2×2 matrix of coefficients $\begin{pmatrix} t_{11} & t_{21} \\ t_{12} & t_{22} \end{pmatrix}$ in (i) with $\alpha = \alpha_j$ $(j = 1, 2, 3)$. Show that

$$\mathcal{T}_1\mathcal{T}_2 + \mathcal{T}_2\mathcal{T}_1 = 0$$

▶ We calculate

$$\begin{aligned}\mathcal{T}_1\mathcal{T}_2 &= \begin{pmatrix} \alpha_1 & 1 \\ \alpha_2\alpha_3 - \alpha_1(\alpha_2+\alpha_3) & -\alpha_1 \end{pmatrix}\begin{pmatrix} \alpha_2 & 1 \\ \alpha_1\alpha_3 - \alpha_2(\alpha_1+\alpha_3) & -\alpha_2 \end{pmatrix} \\ &= \begin{pmatrix} (\alpha_1-\alpha_2)\alpha_3 & \alpha_1-\alpha_2 \\ (\alpha_1-\alpha_2)(\alpha_1\alpha_2 - \alpha_3(\alpha_1+\alpha_2)) & (\alpha_2-\alpha_1)\alpha_3 \end{pmatrix}\end{aligned}$$

Hence, $\mathcal{T}_1\mathcal{T}_2 + \mathcal{T}_2\mathcal{T}_1 = 0$.

(iv) Find the fixed points of T_1 and show that they are interchanged by T_2.

Suppose $T_1(x) = x$, then $x^2 - 2\alpha_1 x - \alpha_2\alpha_3 + \alpha_1(\alpha_2+\alpha_3) = 0$. Therefore, we have

$$x = \alpha_1 \pm \sqrt{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)}$$

Let's now compute the image of this under T_2:

$$T_2(x) = \frac{\pm\alpha_2\sqrt{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)}) + (\alpha_1-\alpha_2)\alpha_3}{(\alpha_1-\alpha_2) \pm \sqrt{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)}}$$

Now, multiplying numerator and denominator with $(\alpha_1-\alpha_2)\mp\sqrt{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)}$, it is easy to see directly the simplifications that lead to $T_2(x) = \alpha_1 \mp \sqrt{(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)}$, as required.

30) Find a necessary and sufficient condition that a line $Y = lX + m$ should be an inflexional tangent to

$$Y^2 = X^3 + AX + B$$

Hence find a general formula for the curves in canonical form having a rational point of order 3.

▶ If the line $Y = lX + m$ intersects the cubic $Y^2 = X^3 + AX + B$ at an inflection point (x, y) that means that (x, y) is the only intersection point between these curves. Let $F(X) = X^3 + AX + B - (lX + m)^2$. Then we must have that $F(X)$ has a unique triple root at x. We can express this as:

$$\begin{aligned} F(x) &= x^3 - l^2x^2 + (A - 2lm)x + B - m^2 = 0 \\ F'(x) &= 3x^2 - 2l^2x + (a - 2lm) = 0 \\ F''(x) &= 6x - 2l^2 = 0 \end{aligned}$$

Thus, assuming base characteristic is not 2 or 3, the last equation gives $x = l^2/3$. The second equation gives $A = l^4/3 + 2lm$ and the first one gives $B = m^2 - l^6/27$. Thus, the general such curve should have the form

$$Y^2 = X^3 + (\frac{l^4}{3} + 2lm)X + m^2 - \frac{l^6}{27}$$

Conversely, plugging in $x = l^2/3$ to the right hand side gives $\frac{l^6}{9} + \frac{2l^3m}{3} + m^2 = (\frac{l^3}{3} + m)^2$. Hence, $(x, y) = (\frac{l^2}{3}, \frac{l^3}{3} + m)$ is an order 3 point on such an elliptic curve.

We note that by doing a coordinate change $X \to X + \frac{l^2}{3}$, the equation becomes

$$Y^2 = (X + \frac{l^2}{3})^3 + (\frac{l^4}{3} + 2lm)(X + \frac{l^2}{3}) + m^2 - \frac{l^6}{27} = X^3 + (lX + \frac{l^3}{3} + m)^2$$

The tangent line then also becomes $Y = lX + \frac{l^3}{3} + m$. Hence, redefining m to be $m + \frac{l^3}{3}$ gives us that the equation of the elliptic curve is

$$\boxed{Y^2 = X^3 + (lX + m)^2}$$

with the inflection point at $(x, y) = (0, m)$ and the tangent line $Y = lX + m$. (Note that we get a non-singular cubic if and only if $m \neq 0$.)

31) Find a necessary and sufficient condition that a line $Y = lX + m$ should be an inflexional tangent to $Y^2 = X(X^2 + aX + b)$. Hence find a general formula for curves in canonical form having a point of order 6.

▶ We argue as in the previous problem. Let $F(X) = X(X^2 + aX + b) - (lX + m)^2$. Then if (x, y) is an inflection point we must have:

$$\begin{aligned} F(x) &= x^3 + (a - l^2)x^2 + (b - 2lm)x - m^2 = 0 \\ F'(x) &= 3x^2 + 2(a - l^2)x + (b - 2lm) = 0 \\ F''(x) &= 6x + 2(a - l^2) = 0 \end{aligned}$$

Hence, over a field of characteristic not equal to 2 or 3, the third equation gives $x = (l^2 - a)/3$. The second equation gives $b = (l^2 - a)^2/3 + 2lm$. The first equation gives $(l^2 - a)^3/27 = m^2$. Thus, we find out that $\frac{l^2-a}{3}$ should be a square. Then, we can pick t such that $\frac{l^2-a}{3} = t^2$ and $m = t^3$. We find out that $a = l^2 - 3t^2$ and $b = t^3(2l + 3t)$. Thus, this leads to the canonical form

$$Y^2 = X(X^2 + (l^2 - 3t^2)X + t^3(2l + 3t))$$

and the tangent line at the inflection point is given by $Y = lX + t^3$.

Plugging in $X = t^2$, we find out that the order 3 points are at $(t^2, \pm t^2(l + t))$. The given order 2 point is at $(0, 0)$ so the order 6 points are given by

$$(0, 0) \pm (t^2, \pm(l + t)t^2) = (t(2l + 3t), \pm(l + t)t(2l + 3t)).$$

32) Let

$$F(X,Y,Z) = X^2Y + XZ^2 + 2Y^3 + Z^3$$

Find a birational transformation defined over $\mathbb{Q}$ taking the curve $F = 0$ into canonical form with the point $(1,0,0)$ going to the point at infinity.

▶ We take $\mathbf{o} = [1:0:0]$. We compute the derivatives

$$\begin{aligned}\frac{\partial F}{\partial X} &= 2XY + Z^2\\ \frac{\partial F}{\partial Y} &= X^2 + 6Y^2\\ \frac{\partial F}{\partial Z} &= 2XZ + 3Z^2\end{aligned}$$

We see that the tangent line $t(\mathbf{o}) = Y = 0$, and this intersect the curve defined by F at another point $\mathbf{p} = [1:0:-1]$. We want to work in an affine chart where both these points are visible and p is at the origin. Applying the transformation $(X,Y,Z) \to (X,Y,Z-X)$ arranges $\mathbf{o} = [1:0:1]$ and $\mathbf{p} = [1:0:0]$. We further apply a permutation $(X,Y,Z) \to (Z,X,Y)$ which brings our equation to

$$Z^2X + Z(Y-Z)^2 + 2X^3 + (Y-Z)^3 = 0$$

with $\mathbf{o} = [0:1:1]$ and $\mathbf{p} = [0:0:1]$ with the tangent line to $\mathbf{o}$ given by $X = 0$. We can now apply the method given in Chapter 8(ii). Setting $Z = 1$ and reorganizing according to degree we get

$$F_3(X,Y) + F_2(X,Y) + F_1(X,Y)$$

with $F_3(X,Y) = 2X^3 + Y^3$, $F_2(X,Y) = -2Y^2$ and $F_1(X,Y) = X + Y$. We set $s = 2F_3(1,t)x + F_2(1,t)$ and $G(t) = F_2(1,t)^2 - 4F_1(1,t)F_3(1,t)$. Our curve is now equivalent to $s^2 = G(t)$. Expanding out $G(t)$, we get the equation

$$s^2 = -4t^3 - 8t - 8$$

Now, multiplying by 4^2 and redefining $y = 4s$ and $x = -4t$, we arrive at the equation

$$y^2 = x^3 + 32x - 128$$

which we can then rescale to

$$\boxed{y^2 = x^3 + 2x - 2}$$

NB: This curve is available in lmfdb as https://www.lmfdb.org/EllipticCurve/Q/2240/b/1.

33) Find a birational transformation defined over $\mathbb{Q}$ taking

$$X_1^2 - 2X_2^2 + X_3^2 = 0, X_2^2 - 2X_3^2 + X_4^2 = 0$$

into canonical form, with $(1,1,1,1)$ going to the point at infinity.

► First, we do the change of co-ordinates $(X_1, X_2, X_3, X_4) \to (X_1 + X_2, X_2, X_3 + X_2, X_4 + X_2)$ which gives the equations

$$X_1^2 + X_3^2 + 2X_2(X_1 + X_3) = 0$$
$$X_4^2 - 2X_3^2 + 2X_2(X_4 - 2X_3) = 0$$

and in the new co-ordinates, we have $\mathbf{o} = (0, 1, 0, 0)$. Now, we can eliminate X_2, relabeling $X_1 = X, X_3 = Y, X_4 = Z$, we get

$$F(X, Y, Z) \coloneqq (X^2 + Y^2)(Z - 2Y) - (X + Y)(Z^2 - 2Y^2) = 0$$

with a rational point given by $Z - 2Y = X + Y = 0$, that is, $\mathbf{o} = (1, -1, -2)$. We compute the derivatives

$$\frac{\partial F}{\partial X} = 2XZ - 4XY - Z^2 + 2Y^2$$
$$\frac{\partial F}{\partial Y} = -2X^2 + 2YZ + 4XY - Z^2$$
$$\frac{\partial F}{\partial Z} = X^2 + Y^2 - 2XZ - 2YZ$$

Thus, we see that the tangent line at $\mathbf{o}$ is $t(\mathbf{o}) = X + 3Y - Z$. We easily compute that $t(\mathbf{o})$ intersects our curve also at $\mathbf{p} = (1, 0, 1)$.

Now, in order to apply the method given in Chapter 8(ii), we want o move $\mathbf{o}$ to $(0, 1, 1)$, and $\mathbf{p}$ to $(0, 0, 1)$ and the tangent line at $\mathbf{o}$ to $X = 0$, we apply the transformation $(X, Y, Z) \to (X + Z, -Y, Z - 3Y)$

Now, in order to move $\mathbf{o}$ to $(0, 1, 0)$ and the tangent line $t(\mathbf{o})$ to $Z = 0$, we apply the transformation $(X, Y, Z) \to (X + Y + Z, -Y, X - 2Y)$. Then the equation becomes

$$((X + Z)^2 + Y^2)(Z - Y) - ((Z - 3Y)^2 - 2Y^2)(X + Z - Y) = 0$$

Setting $Z = 1$ and reorganizing according to the degree we get

$$F_3(X, Y) + F_2(X, Y) + F_1(X, Y)$$

with $F_3(X, Y) = 6Y^3 - 7XY^2 - X^2Y$, $F_2(X, Y) = X^2 + 4XY - 12Y^2$, $F_1(X, Y) = X + 6Y$. We set $s = 2F_3(1, t)x + F_2(1, t)$ and $G(t) = F_2(1, t)^2 - 4F_1(1, t)F_3(1, t)$. Our curve is now equivalent to $s^2 = G(t)$. Expanding out $G(t)$, we get the equation

$$s^2 = 48t^3 + 44t^2 + 12t + 1$$

Multiplying by 36 and redefining $y = 6s$ and $x = 12t$, we get

$$y^2 = x^3 + 11x^2 + 36x + 36$$

We notice that -2 is a root of the right hand side, so Sending $x \to x - 2$ simplifies the equation to

$$\boxed{y^2 = x(x + 1)(x + 4)}$$

By a further change of variables by sending $x \to x - (5/3)$ and multiplying both sides with 3^6 and rescaling, one can get to the form

$$y^2 = x^3 - 351x + 1890$$

This curve is a model for $X_0(24)$, see https://www.lmfdb.org/EllipticCurve/Q/24/a/4

Chapter 9

No exercises given.

Chapter 10

34) (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 $\mathcal{C}$.

▶ The mod p reduction of $\mathcal{C}$ is $Y^2 = X^3$ and this curve is singular at $(0,0)$. Suppose $(a,b) \in \mathbb{Z}_p^2$ is a point reducing to $(0,0)$, then $p|a$, hence $p^3|a^3$, so $p|a^3+p$ but $p^2 \nmid a^3+p$, hence a^3+p cannot be a square in $\mathbb{Z}_p$.

(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 $\mathcal{C}$.

▶ $y^2 = x^3 + px, \mathbf{p} = (0,0)$ or $y^2 = x^3 + p^2, \mathbf{p} = (0,p)$.

35) 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 $\mathcal{C}$.

▶ (i) $y^2 = x^3 + x^2 + p^2$ and $\mathbf{p} = (0,p)$, or $y^2 = x^3 + x^2 + px$ and $\mathbf{p} = (0,0)$.

(ii) $y^2 = x^3 + x^2 + p$ reduces to $y^2 = x^3 + x^2$ with a node at $(0,0)$, and if (a,b) reduces to $(0,0)$, then $p|a$ so $p|a^3 + a^2 + p$ but $p^2 \nmid a^3 + a^2 + p$, hence $a^3 + a^2 + p$ cannot be a square in $\mathbb{Z}_p$.

Chapter 11

No exercises given.

Chapter 12

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

(i) $Y^2 = X^3 + 1$

▶ $4a^3 + 27b^2$ is 27. So, the only possible y-coordinates for torsion elements are $\{0, \pm 1, \pm 3\}$. We obtain the following rational points for these:

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

together with $\mathbf{o}$ (the point at infinity) we get 6 elements. To actually verify that all of these points are torsion points, we start with $P = (2, 3)$ and compute

$$2P = (0, 1), 3P = (-1, 0), 4P = (0, -1), 5P = (2, -3), 6P = \mathbf{o}$$

Hence, $(2, 3)$ generates the torsion subgroup and the final answer is $\boxed{\mathbb{Z}/6\mathbb{Z}}$.

This curve appears in lmfdb, see https://www.lmfdb.org/EllipticCurve/Q/36/a/4.

(ii) $Y^2 = X^3 - 43X + 166$

▶ $4a^3 + 27b^2$ is $425984 = 2^{15} \cdot 13$. Since $3 \nmid D$, we have the reduction homomorphism $E(\mathbb{Q})_{tors} \to E(\mathbb{F}_3)$ is an injection. It is easy to see that

$$E(\mathbb{F}_3) = \{\mathbf{o}, (0, 1), (0, 2), (1, 1), (1, 2), (2, 1), (2, 2)\}$$

Hence $E(\mathbb{Q})_{tors}$ must have an order dividing 7. Thus, we have to see whether it $E(\mathbb{Q})_{tors}$ is trivial or not. So, it suffices to find a non-trivial torsion element.

Since the squares of the y-coordinates of the torsion points must divide D, the y-coordinates must be in the set

$$\{0, \pm 1, \pm 2, \pm 4, \pm 8, \pm 16, \pm 32, \pm 64, \pm 128\}$$

By trying the small values, we arrive at a point $P = (3, 8)$. Now, we use the doubling formula to compute

$$2P = (-5, -16), 4P = (11, 32), 8P = (3, 8)$$

which shows that P is an order 7 element. Hence, the final answer is $\boxed{\mathbb{Z}/7\mathbb{Z}}$.

This curve appears in lmfdb, see https://www.lmfdb.org/EllipticCurve/Q/26/b/2

(iii) $Y^2 = X^3 - 219X + 1654$

▶ The $4a^3+27b^2$ is $31850496 = 2^{17} \cdot 3^5$. Thus, the mod 5 reduction is injective. We compute

$$E(\mathbb{F}_5) = \{\mathbf{o}, (0, 2), (0, 3), (1, 1), (1, 4), (2, 2), (2, 3), (3, 2), (3, 3)\}$$

and find that it has order 9. Therefore, $E(\mathbb{Q})_{tors}$ can be either trivial, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/9\mathbb{Z}$.

To show that it is the latter, it suffices to find a torsion point that is not of order 3. For an odd order torsion point (x, y), we have $y | 2^8 3^2$. By trying small values, we find $P = (11, \pm 24)$ and we compute

$$2P = (-13, 48), 4P = (35, -192), 8P = (11, -24) = -P$$

Hence, P has order 9. Therefore, the final answer is $\boxed{\mathbb{Z}/9\mathbb{Z}}$.

This curve appears in lmfdb, see https://www.lmfdb.org/EllipticCurve/Q/54/b/2

(iv) $Y^2 = X(X - 1)(X + 2)$

▶ By changing $X \to X - \frac{1}{3}$ and rescaling, we arrive at the Weierstrass equation $Y^2 = X^3 - 189X + 540$. $4a^3 + 27b^2$ is $-2^2 3^{14}$.

Thus, the mod 5 reduction is injective. We compute

$$E(\mathbb{F}_5) = \{\mathbf{o}, (0,0), (2,0), (3,0)\}$$

Thus, the order of $E(\mathbb{Q})_{tors}$ can be at most 4. On the other hand, we have four 2-torsion points: $\{\mathbf{o}, (0,0), (1,0), (-2,0)\}$. Hence, the final answer is $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}$.

This curve appears in lmfdb, see https://www.lmfdb.org/EllipticCurve/Q/96/b/3

(v) $Y^2 = X(X+1)(X+4)$

▶ We have shown before that this elliptic curve has simplified Weierstrass form given by $Y^2 = X^3 - 351X + 1890$. $4a^3 + 27b^2 = -2^4 3^{14}$

Reducing mod 5, we get the curve $Y^2 = X^3 - X$ and an injective homomorphism $E(\mathbb{Q})_{tors} \to E(\mathbb{F}_5)$. We compute

$$E(\mathbb{F}_5) = \{\mathbf{o}, (0,0), (1,0), (2,1), (2,4), (3,2), (3,3), (4,0)\}$$

which is an abelian group of order 8. Hence, elements of $E(\mathbb{Q})_{tors}$ can have orders $1, 2, 4$ or 8. It is easy to see that the original equation has order 2 elements $(0,0), (-1,0), (-4,0)$ and in the simplified Weierstrass form these give the elements of order 2

$$(15,0), (6,0), (-21,0)$$

Therefore, $E(\mathbb{Q})_{tors}$ has order 4 or 8 and has exactly 3 elements of order 2. Therefore, the answer could be either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. To see that that it is the latter, we also consider the point[1] $(2,6)$ which gives an integer solution to the original equation, and becomes $P = (33, 162)$ for the simplified Weierstrass equation. We use the doubling formula to compute that $P + P = (15, 0)$. Hence, P gives an order 4 point. Therefore, the final answer is $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}}$.

This curve is a model for $X_0(24)$, see https://www.lmfdb.org/EllipticCurve/Q/24/a/4

(vi) $X^3 + Y^3 + Z^3 - 15XYZ = 0$

▶ We have shown before that this elliptic curve has Weierstrass form $Y^2 = X^3 - 27(5^4 + 8.5)X + 54(5^6 - 20.5^3 - 8) = X^3 - 17955X + 708318$. The discriminant is $(-16)(4a^3 + 27b^2) = 2^{18}3^9 31^3$.

Therefore, $E(\mathbb{Q})_{tors}$ injects into both $E(\mathbb{F}_5)$ and $E(\mathbb{F}_7)$. Reducing mod 5, we get $Y^2 = X^3 + 3$ and reducing mod 7, we get $Y^2 = X^3 + 2$, and we compute

$$E(\mathbb{F}_5) = \{\mathbf{o}, (1,2), (1,3), (2,1), (2,4), (3,0)\}$$

[1] In general, if $Y^2 = X(X+r^2)(X+s^2)$, then order 2 points are $(0,0), (-r^2,0), (-s^2,0)$ and order 4 points are given by $(rs, \pm rs(r+s)), (-rs, \pm rs(r-s))$. Doubling formula shows that the square of the order 4 points are the order 2 point $(0,0)$.

and

$$E(\mathbb{F}_7) = \{\mathbf{o}, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}$$

In particular, we see that the order of $E(\mathbb{F}_5)$ is 6, and the order of $E(\mathbb{F}_7)$ is 9. This implies that the order of $E(\mathbb{Q})_{tors}$ can be 1 or 3. To see that it is 3, it suffices to exhibit a point of order 3.

One way to see this is to check that the points $[1:-1;0], [0:1:-1]$ and $[-1:0:1]$ are all inflection points of the original equation. Indeed, in a previous problem, we have shown that $[1:-1:0]$ is an inflection point for any curve defined by $F(X,Y,Z) = X^3 + Y^3 + Z^3 - 3mXYZ$, $m^3 \neq 1$. By symmetry, it follows that $[0:1:-1]$ and $[-1:0:1]$ are also inflection points. In terms of the simplified Weierstrass equation, these correspond to the solutions $\mathbf{o}, (147, 1116), (147, -1116)$.

Therefore, we conclude that $E(\mathbb{Q})_{tors}$ is isomorphic to $\boxed{\mathbb{Z}/3\mathbb{Z}}$.

This curve is available in lmfdb as https://www.lmfdb.org/EllipticCurve/Q/1674/c/2

(vii) $Y^2 = X(X+81)(X+256)$

▶ The simplified Weierstrass form is $Y^2 = X^3 - 1386747X + 368636886$ where the transformation is given by $(X,Y) \to (9X + 1011, 27Y)$. $4a^3 + 27b^2 = -6998115764183040000 = -2^{16} \cdot 3^{20} \cdot 5^4 \cdot 7^2$.

Thus, we have to examine $E(\mathbb{F}_{11})$, as $p = 11$ is the smallest primes for which $E(\mathbb{Q})_{tors} \to E(\mathbb{F}_p)$ maps injectively. Reducing mod 11, we get the curve $Y^2 = X^3 + X + 2$ and we can compute

$$E(\mathbb{F}_{11}) = \{\mathbf{o}, (1, \pm 2), (2, \pm 1), (4, \pm 2), (5, 0), (6, \pm 2), (7, 0), (8, \pm 4), (9, \pm 5), (10, 0)\}$$

In particular, we see that the order of $E(\mathbb{F}_{11})$ is 16. On the other hand, from the original form of the equation we can see that there are three 2-torsion points are given by $(0,0), (-81,0), (-256,0)$. These correspond to $(1011,0), (282,0), (-1293,0)$ in the simplified Weierstrass form. Since the original equation is of the form $Y^2 = X(X+r^2)(X+s^2)$ for $r = 9$ and $s = 16$ we find the following integral solution

$$(rs, \pm rs(r+s)), (-rs, \pm rs(r-s))$$

which give order 4 points (one can easily check by doubling formula that the square of these points is $(0,0)$). Therefore, $E(\mathbb{Q})_{tors}$ can be either $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. To see that it is the latter, we need to find an order 8 point. One way is to brute force search by trying (x,y) such that $y^2 | D$. This eventually will give the point $P = (24, 840)$ which satisfies the original equation and such that $P + P = (rs, rs(r+s)) = (144, 3600)$. Thus, we get that the final answer is $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}}$.

NB: This curve is available in lmfdb as https://www.lmfdb.org/EllipticCurve/Q/210/e/6

A more satisfactory answer is the following theorem:

Theorem. *Let a, b, c be a Pythagorean triple, i.e. $a^2 + b^2 = c^2$. Consider the elliptic curve*

$$Y^2 = X(X + a^4)(X + b^4)$$

This curve has torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

We can list the 2-torsion points as

$$(0, 0), (-a^4, 0), (-b^4, 0)$$

the 4-torsion points as

$$(a^2b^2, \pm a^2b^2(a^2 + b^2)), (-a^2b^2, \pm a^2b^2(a^2 - b^2))$$

and finally the 8-torsion points as

$$\begin{aligned}
&(ab(a + c)(b + c), \pm abc(a + b)(a + c)(b + c)),\\
&(ab(a - c)(b - c), \pm abc(a + b)(a - c)(b - c)),\\
&(ab(a + c)(b - c), \pm abc(a - b)(a + c)(b - c)),\\
&(ab(a - c)(b + c), \pm abc(a - b)(a - c)(b + c))
\end{aligned}$$

Note that the discriminant is $\Delta = 16a^8b^8c^4(a - b)^2(a + b)^2$ and it is easy to check that $y^2|\Delta$ for all torsion points (x, y) given above.

I verified that these given points are on the curve given by direct calculation and checked with the degree doubling formula that for any (x, y) listed as an 8-torsion point, we have

$$\frac{(x^2 - a^4b^4)^2}{4y^2} = a^2b^2$$

This proves the theorem, but there is a more conceptual proof. Elliptic curves over $\mathbb{Q}$ with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ give rise to a genus 0 modular curve whose rational parametrization is well known, e.g. there is the famous table 3 in this paper: https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/plms/s3-33.2.193

We reproduce Kubert's parametrization which is given in Tate's normal form as

$$y^2 + (1 - c)xy - by = x^3 - bx^2$$

where $b = (2t - 1)(t - 1)$ and $c = (2t - 1)(t - 1)/t$ and t is of the form $t = \alpha(8\alpha + 2)/8\alpha^2 - 1$ with $\alpha \in \mathbb{Q}$.

Now, getting rid of the xy and y terms, we find that this curve is birationally equivalent to

$$y^2 = x^3 + x^2((2t - 1)^4 - 8t^2(t - 1)^2) + x2^4t^4(t - 1)^4$$

Letting $\alpha = u/v$, one can eventually show that this is equivalent to

$$y^2 = x^3 + Ax^2 + Bx$$

where

$$A = 2^8u^4(2u+v)^4 + v^4(4u+v)^4$$
$$B = 2^8u^4v^4(2u+v)^4(4u+v)^4$$

Finally letting $m = u$ and $n = (2u+v)/2$, we get

$$y^2 = x^3 + 2^8((m^2-n^2)^4 + (2mn)^4)x^2 + 2^{16}((2mn)^4(m^2-n^2)^4)x$$

and after rescaling x and y by powers of 2, this returns our original curve with $(m^2-n^2, 2mn, m^2+n^2)$ parametrizing the Pythagorean triples.

(viii) $X_1^2X_2 - X_1X_2^2 - X_1X_3^2 + X_2^2X_3 = 0$

▶ We have seen in a previous exercise that this curve is equivalent to $Y^2 = X^3 - 2^43^3X + 2^43^319 = X^3 - 432X + 8208$. If we chase through the calculation given there we find that the transformation is given by the following formula:

$$X = 36\frac{X_1}{X_2} - 12, Y = 108 - \frac{216X_1X_3}{X_2^2}$$

We calculate $4a^3 + 27b^2$ to be $1496537856 = 2^8 \cdot 3^{12} \cdot 11$. Thus, the mod 5 reduction is injective. We compute

$$E(\mathbb{F}_5) = \{\mathbf{o}, (3,2), (3,3), (4,2), (4,3)\}$$

Hence, the order of $E(\mathbb{Q})_{tors}$ can be either 1 or 5. Now, it is easy to note that the following are some rational points on the original curve given in terms of X_1, X_2, X_3,

$$(1,0,0), (0,1,0), (0,0,1), (1,1,0), (1,1,1)$$

Under the transformation described above, these give the five points

$$\mathbf{o}, (-12, 108), (-12, -108), (24, 108), (24, -108)$$

It can be checked by direct calculation that these comprise the 5-torsion points (a simple way is to start with, say $P = (-12, 108)$ and see via the doubling formula that $6P = P$). Hence, the final answer is $\boxed{\mathbb{Z}/5\mathbb{Z}}$.

This is a model for the modular curve $X_1(11)$, see https://www.lmfdb.org/EllipticCurve/Q/11/a/3. This curve is known as "the first elliptic curve in nature" and has another equivalent equation given by $Y^2 + Y = X^3 - X^2$. The above points correspond to

$$\mathbf{o}, (0,-1), (0,0), (1,-1), (1,0)$$

in these co-ordinates.

37) Fill in the details of the sketched proof of the following theorem [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.*

► Note that if A was not 4-th power free, we could make it 6-power free, because $Y^2 = X^3 + AX$ and $Y^2 = X^3 + Au^4X$ for $u \in \mathbb{Q}^*$ are isomorphic.

(i) The doubling formula gives that if $(x, y) = 2(a, b)$ for $b \neq 0$, then

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

(ii) The points of order 2 are of the form $(x, 0)$, so we see that $(0, 0)$ is a 2-torsion point and there are other 2-torsion points only if $A = -C^2$, in which case $(\pm C, 0)$ are 2-torsion points.

(iii) Now, if $(0, 0) = 2(a, b)$, then $a^2 = A$ by the doubling formula, but we also have $b^2 = a(a^2+A)$ since $(a, b) \in \mathcal{C}$. It follows that $b^2 = 2a^3$. Then $a = 2u$ for u odd (otherwise $2^4|A$). But, now u^3 must be a square, so u must be square, but again since A is 4^{th} power free, this forces that $u = 1$, and $a = 2$, and $A = 4$. Now, if $A = 4$, indeed $(2, \pm 4)$ are in $\mathcal{C}$ and $2(2, \pm 4) = (0, 0)$, hence these give the order 4 points. We also note that it is impossible for $(\pm C, 0) = 2(a, b)$, because the doubling formula implies that $\pm C$ is a square, but then $A = -C^2$ is a 4^{th} power.

(iv) Next, suppose that there exists a point (a, b) of odd order, say $2m+1$. Let $m(a, b) = (a_m, b_m)$, then $2(a_m, b_m) = -(a, b) = (a, -b)$, hence $a = (a_m^2 - A)^2/4b_m^2$ from which we see that a is a square number.

(v) Let $d = \gcd(a, A)$, then $a = da_1$, $A = dA_1$ with $\gcd(a_1, A_1) = 1$. Since $b^2 = a(a^2 + A)$, we conclude that $b = db_1$ with $b_1^2 = a_1(da_1^2 + A_1)$.

(vi) Now, note that $gcd(a_1, da_1^2 + A_1) = 1$, hence both a_1 and $da_1^2 + A_1$ are squares (a_1 is positive because a is a square and d is positive). Let us put $a_1 = f^2$ and $da_1^2 + A_1 = g^2$ with $\gcd(f, g) = 1$ and we can choose the signs of f and g so that $b_1 = fg$. Note also that since $a = da_1$ is a square, and a_1 is a square, it follows that $d = h^2$ for some h.

(vii) Next, we note that $a^2 - A = d^2a_1^2 - dA_1 = 2d^2a_1^2 - dg^2 = 2h^4f^4 - h^2g^2$, and $b = db_1 = h^2fg$.

(viii) On the other hand, since $2(a, b)$ has integer x-coordinate, it follows from doubling formula that $2b|a^2 - A$.

(ix) But, $a^2 - A = 2h^4f^4 - h^2g^2$, $b = h^2fg$, so $h^2f|a^2 - A$ implies $h^2f|h^2g^2$, hence $f|g^2$. But $\gcd(f, g) = 1$, hence $f = 1$. Also $2h^2|a^2 - A$ implies $2h^2|h^2g^2$, hence $2|g$. Now, $2g|a^2 - A$ implies, $2g|2h^4$, hence $g|h^4$ and in particular $2|h$.

(x) Now, $b_1 = g$, hence $2|b_1$, so $4|b_1^2 = d + A_1 = h^2 + A_1$. But $2|h$, hence $4|A_1$, and so $16|h^2 A_1 = A$, which contradicts to the fact that A was assumed to be 4^{th} power free.

38) Fill in the sketched proof of the following theorem [or find a better]

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

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

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.

(III) If $B = 1$, the points $(2, \pm 3)$ of order 6.

(IV) If $B = -432 = -2^4 3^2$, the points $(12, \pm 36)$ of order 3.

▶ Note that if B was not 6-th power free, we could make it 6-power free, because $Y^2 = X^3 + B$ and $Y^2 = X^3 + Bu^6$ for $u \in \mathbb{Q}^*$ are isomorphic.

(i) Suppose that $(x, y) = 2(a, b)$ and $b \neq 0$. The doubling formula gives

$$x = \frac{a(a^3 - 8B)}{4b^2}$$

But $B = b^2 - a^3$, hence $x = \frac{a(9a^3 - 8b^2)}{4b^2} = a(w - 2)$ for $w = 9a^3/4b^2$.

(ii) The order 2-elements are of the form $(x, 0)$ solving $X^3 + B = 0$. This admits a rational solution if and only if $B = D^3$ for some non-zero integer, and in that case $X^3 + D^3 = (X + D)(X^2 - XD + D^2)$ and we see that $X^2 - XD + D^2 = (X - (D/2))^2 + (3/4)D^2$ does not have rational solutions, hence $(-D, 0)$ is the unique point of order 2 as stated in (II).

(iii) If (a, b) has order 3, then $a(w - 2) = a$, hence either $a = 0$ or $w = 2$. If $a = 0$, then we get the order 3 elements stated in (I) where $C = b$.

Suppose now that $a \neq 0$, and (a, b) is an element of odd order. We claim that $w \in \mathbb{Z}$.

(iv) If $p \mid B$ and $p \nmid a$, then from $4b^2 x = a^3 - 8aB$, we see that $p \nmid x$.

(v) Conversely, suppose $p \mid B$ and $p \nmid x$, we claim that $p \nmid a$. Since (a, b) is an element of odd order, we get that $(a, b) = (2 \cdot 2 \cdots 2 \cdot 2)(x, y))$. Now, the previous argument applied recursively gives $p \mid B$ and $p \nmid x$ implies $p \nmid a$.

(vi) Since x is an integer, we have $aw = 9a^4/4b^2$ is an integer. If $3^2 \nmid b$, then clearly $w \in \mathbb{Z}_3$. So suppose $3^2 | b$ but $3^3 \nmid b$, then since $aw \in \mathbb{Z}$, we have $3|a$. Then, it follows that $w = 9a^3/4b^2 \in \mathbb{Z}_3$. Finally, suppose $3^3 | b$, then since $aw \in \mathbb{Z}$, $3|a$ but if $3^2 \nmid a$, then it follows that $3 \nmid x$, which contradicts part (v) since $3|B = b^2 - a^3$ and $3|a$. Therefore, it follows that $3^2|a$, and we get that $3^6 | B = b^2 - a^3$, which is a contradiction. Hence, $w \in \mathbb{Z}_3$.

(vii) Since $aw \in \mathbb{Z}$, $2|a$, which gives $w \in \mathbb{Z}_2$ if $2 \nmid b$. Now suppose $2|b$ but $2^2 \nmid b$, then if $2^2 \nmid a$, we get a contradiction to part (v), since $2|B = b^2 - a^3$ and $2|a$ but $2 \nmid x$. Therefore, $2^2 \mid a$, which implies $w \in \mathbb{Z}_2$. Finally, suppose, $2^2|b$, then since $aw \in \mathbb{Z}$, we have $2^2|a$. Now, if $2^3 \nmid b$, then we get $w = 9a^3/4b^2 \in \mathbb{Z}_2$. Otheriwse, if $2^3|b$, then we get $2^6|B$, which is a contradiction. Hence, $w \in \mathbb{Z}_2$.

(viii) Suppose $p|B$ and $p \neq 2, 3$. If $p|b$, then since $9a^4/4b^2 \in \mathbb{Z}$, we must have that $p|a$. If $p^2 \nmid b$, then $w = 9a^3/4b^2 \in \mathbb{Z}_p$ so suppose $p^2 \mid b$. Then, we must have $p^2|a$, as otherwise, we have $p|a$, $p|b$, hence $p|B$ but $p \nmid x$ contradicting part (v). Now, if $p^3 \nmid b$, then $w \in \mathbb{Z}_p$. Otherwise, $p^6|B$, which is a contradiction. So, $w \in \mathbb{Z}_p$ for all $p|B$.

(ix) Since (a, b) is an odd torsion point, by Nagell-Lutz, we have $b^2|27B^2$. Hence, any prime $p|b$ must divide $3B$. Since we showed that $w = 9a^3/4b^2 \in \mathbb{Z}_p$ for all $p|B$, $p = 2$ and $p = 3$, it follows that $w \in \mathbb{Z}_p$ for all primes, hence $w \in \mathbb{Z}$.

(x) Suppose $w = 2$, then $x = 0$. Then, we must be have the situation given in (I). Hence $y = \pm C$, and $B = C^2$. On the other hand, $w = 2$ implies $9a^3 = 8b^2$, hence $a = 2k^2$ and $b = 3k^3$ for some integer k. But, $B = b^2 - a^3$ is 6^{th} power free, so $k = \pm 1$. The $a = 2$, $b = \pm 3$. It follows, that $B = 1$. Then, we conclude that we are in the situation given in (III) with $(2, \pm 3)$ of order 6 and $(0, \pm 1) = 2(2 \pm 3)$ of order 3. It is easy to see that these are all the torsion points (for example, $27B^2 = 27$, hence the y-coordinates of any odd order torsion element has to be ± 1 or e± 3.)

(xi) Suppose $w \neq 1, 2, 3$. Then $|w - 2|_\infty > 1$, hence $|x|_\infty > |a|_\infty$. But since (a, b) is assumed to be an odd torsion element, we must have $(2 \cdot 2 \cdots 2 \cdots 2)(x, y) = (a, b)$ after doubling enough times. Each time we double we the x-coordinate gets multiplied by a non-zero integer (if it was zero at some point, we recover the case (III)), but this is a contradiction, since $|x|_\infty$ can never be made smaller, hence can never become $|a|_\infty$.

(xi) Finally, let's consider the cases $w = 1$ and $w = 3$.

If $w = 1$, then $9a^3 = 4b^2$, which implies $b = 12k^3$ and $a = 4k^2$ but $B = b^2 - a^3$ is 6^{th} power free, hence $k = \pm 1$. So, $a = 4$ and $b = \pm 12$, and $B = 80 = 2^4 \cdot 5$. Moreover, $(x, y) = (-4, \pm 4)$. Doubling again, we get $2(x, y) = (44, -292)$. Thus, we see that the point (x, y) does not have $w = 1, 2$ or 3, hence $(-4, \pm 4)$ cannot be torsion. Thus, we arrive at a contradiction. (Alternatively, we can double again, and we get $(58124/5329, -14438588/389017)$. These are not integer, hence we see that $(4, 12)$ could not have been torsion.)

If $w = 3$, then $9a^3 = 12b^2$, which implies $b = \pm 36$ and $a = 12$. Hence $B = 36^2 - 12^3 = -432 = 2^4 3^2$. Then, we get that $(12, \pm 36)$ are elements of order 3, and we recover the case in (IV).

39) 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

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

► In a previous problem, we have already seen that $X^3 + Y^3 + dZ^3 = 0$ has the Weierstrass normal form $\tilde{Z}\tilde{Y}^2 = \tilde{X}^3 - 2^4 3^3 d^2 \tilde{Z}^3$. (In fact, this is covered in Chapter 8 of the book.) The transformation is given by $(\tilde{X}, \tilde{Y}, \tilde{Z}) = (-12dZ, 36d(X - Y), X + Y)$.

Now, from the previous problem we see that the only way this curve can have torsion is if $B = -2^4 3^3 d^2$ is equal to C^2, D^3 or -432 for integers C, D. It follows that the first case cannot occur, and the second and third cases if $d = 2$ and $d = 1$, respectively.

If $d = 2$, $B = (-12)^3$, hence it has an order 2 element given by $(12, 0)$ and if $d = 1$, $B = -432$ and it has order 3 elements given by $(12, \pm 36)$. We then see that under the above transformation, these points correspond to the stated points.

40) 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.]

► Suppose u is a rational root, then we can write

$$X^3 + sX + k = (X - u)(X^2 + uX + u^2 + s)$$

Thus, to have 3 roots, we must have that $u^2 - 4(u^2 + s) = -3u^2 - 4s$ has a rational square root v. Conversely, suppose v is a rational number such that $v^2 = -3u^2 - 4s$, then we see that $X^3 + sx + k = (X - u)(X + (u + v)/2)(X + (u - v)/2)$ where s and k are determined by the formula $s = (-3u^2 - v^2)/4$ and $k = u(v^2 - u^2)/4 = -u(u^2 + s)$.

In other words, the cubic polynomial $X^3 + sX + k$ has 3 rational roots if and only if the conic

$$3U^2 + V^2 + 4s = 0$$

has a rational solutions (u, v). Now, if there exists such a rational solution determined by a particular value of k, then we deduce that the conic $3U^2 + V^2 + 4s = 0$ is birational to a line, hence it must have infinitely many rational points. This, in turn, gives infinitely many k.

41) 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.

► We argue similarly to the problem before. If u is a rational root, we can write

$$X^3 + sX + k = (X - u)(X^2 + uX - (k/u))$$

Now, to have 3 roots, we must have $u^2 + 4(k/u)$ has a rational square root v. In other words, we are looking for rational solutions of the cubic curve

$$U^3 + 4k = UV^2$$

Conversely, a solution (u, v) determines $k = (uv^2 - u^3)/4$, $s = (-3u^2 - v^2)/4 = -u^2 - (k/u)$.

The hypothesis of the problem gives us rational points $(u_1, \pm v_1)$, $(u_2, \pm v_2)$ on this curve such that $3u_1^2 + v_1^2 \neq 3u_2^2 + v_2^2$ (corresponding to two different s values). Note that $u_i \neq 0$ since $k \neq 0$. We can homogenise this equation to $U^3 + 4kW^3 = UV^2$ with rational points $(u_1, \pm v_1, 1)$ and $(u_2, \pm v_2, 1)$ then de-homogenize by setting $U = 1$, to get to the curve $1 + 4kW^3 = V^2$ with rational points $(1/u_1, \pm v_1/u_1), (1/u_2, \pm v_2/u_2)$. Multiplying by 4^2k^2 and rescaling, we arrive at the curve

$$V^2 = W^3 + 16k^2$$

with rational points $(4k/u_1, \pm 4kv_1/u_1)$, $(4k/u_2, \pm 4kv_2/u_2)$.

We want to show that this curve has non-zero rank which would give us infinitely many solutions (u, v) to the original equation $U^3 + 4k = UV^2$. It suffices to show that at least one of our rational points is not a torsion element.

Now, referring to a previous problem, we have an equation of the form $Y^2 = X^3 + B$ with $B = 16k^2$. In this case, we have $B = C^2$, hence there are two points of order 3 of the form $(0, \pm C)$ but our rational points have the first co-ordinate non-zero, hence cannot be these. If $k \neq (1/4)m^3$ for some rational number m then these are all the torsion points, hence each of our given rational points are non-torsion (hence there are infinitely many rational points).

If $k = (1/4)m^3$, then we have the curve $V^2 = W^3 + m^6$. (In particular, this curve is equivalent to $V^2 = W^3 + 1$). It has an order 2 point $(-m^2, 0)$ and order 6 points $(2m^2, \pm 3m^3)$, which lead to the solutions

$$(-m, 0), ((1/2)m, \pm(3/2)m)$$

of the original equation $U^3 + 1 = UV^2$. These determine the polynomial

$$X^3 - (3/4)m^2X + (m^3/4) = (X + m)(X - (m/2))(X - (m/2))$$

Thus, all three of these solutions give $s = -3m^2/4$. We conclude that $k = (1/4)m^3$ does not satisfy the hypothesis of the problem. Hence, in this case, there is a unique value of s such that $X^3 + sX + (m^3/4)$ has 3 rational roots, namely $s = -(3/4)m^2$. So this case is ruled out by assumption.

Chapter 13

42) Let $\mathcal{C} : Y^2 = X^3 + AX + B$ be defined over $\mathbb{Q}$. Let $\mathbb{Q}(\sqrt{d})$ be a quadratic extension of $\mathbb{Q}$ and let the non-trivial automorphism be denoted by $(')$. Let $\mathbf{x}$ be a point of $\mathcal{C}$ defined over $\mathbb{Q}(\sqrt{d})$. Show that $\mathbf{x} + \mathbf{x}'$ is defined over $\mathbb{Q}$ and that $\mathbf{x} - \mathbf{x}' = (u, v)$ where u and $v/\sqrt{d}$ are in $\mathbb{Q}$.

Deduce that the group of the points on $\mathcal{C}$ defined over $\mathbb{Q}(\sqrt{d})$ may be determined once the groups over $\mathbb{Q}$ on $\mathcal{C}$ and $dY^2 = X^3 + AX + B$ are known.

▶ Let $\mathbf{x} = (x, y)$ and $\mathbf{x}' = (x', y')$. If $x = x'$ then $x \in \mathbb{Q}$, and so $y' = \pm y$. If $y' = y$, then $\mathbf{x} = \mathbf{x}' \in \mathcal{C}(\mathbb{Q})$, or if $y' = -y$, $\mathbf{x} + \mathbf{x}' = \mathbf{o}$. So, suppose $x \neq x'$, the line through $\mathbf{x}$ and $\mathbf{x}'$ is given by

$$Y = \ell X + m, \quad \ell = \frac{y - y'}{x - x'}, \quad m = \frac{xy' - x'y}{x - x'}$$

Thus, we see that both ℓ and m are fixed by the non-trivial automorphism of $\mathbb{Q}(\sqrt{d})$, hence $\ell, m \in \mathbb{Q}$. Now, since the x-coordinate of $\mathbf{x}+\mathbf{x}'$ is given by $\ell^2 - x - x'$ and since $x + x'$ and ℓ are in $\mathbb{Q}$, it follows that $\ell^2 - x - x' \in \mathbb{Q}$. Finally, the y-coordinate of $\mathbf{x}+\mathbf{x}'$ is given by $-\ell(\ell^2 - x - x') - m$ and so it also is in $\mathbb{Q}$.

Similarly, the line through $\mathbf{x} = (x, y)$ and $-\mathbf{x}' = (x', -y')$ is given by

$$Y = \ell X + m, \quad \ell = \frac{y + y'}{x - x'}, \quad m = \frac{-xy' - x'y}{x - x'}$$

Thus, the non-trivial automorphism of $\mathbb{Q}(\sqrt{d})$, send $(\ell, m) \to (-\ell, -m)$. Hence the x-coordinate of $\mathbf{x} - \mathbf{x}'$ given by $\ell^2 - x - x'$ is in $\mathbb{Q}$. But the y-coordinate given by $-\ell(\ell^2 - x - x') - m$ is sent to minus itself, hence it has to be of the form v such that $v/\sqrt{d} \in \mathbb{Q}$.

Now, let $A = \mathcal{C}(\mathbb{Q}(\sqrt{d}))$ be a finitely generated abelian group and $\sigma : A \to A$ the involution $\mathbf{x} \to \mathbf{x}'$ induced by the non-trivial automorphism of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d}/\mathbb{Q}))$. It is easy to verify using the addition formula that σ respects the group law on A (see, for example, Proposition 6.3 in [4].). In particular, σ preserves A_{tors} and sends the free abelian part of A to itself.

We consider the subgroups $A^{\sigma=1} \coloneqq \{p \in A : \sigma(p) = p\}$ and $A^{\sigma=-1} \coloneqq \{p \in A : \sigma(p) = -p\}$ of A. Thus,$(x, y) \in A^{\sigma=1}$ if and only if $(x, y) \in \mathcal{C}(\mathbb{Q})$, and $(x, y) \in A^{\sigma=-1}$ if and only if $(x, y/\sqrt{d})$ is in $\mathcal{C}_d(\mathbb{Q})$, where $\mathcal{C}_d$ is the quadratic twist of $\mathcal{C}$ defined by the equation $dy^2 = x^3 + AX + B$.

In general, it may not be the case that σ is diagonalizable, i.e. $A \neq A^{\sigma=1} \oplus A^{\sigma=-1}$. There are two things that might go wrong: 1) It may not even be true that $A^{\sigma=1} \cap A^{\sigma=-1} = \{\mathbf{o}\}$ and 2) It may not be true that the group homomorphism $A^{\sigma=1} \times A^{\sigma=-1} \to A$ is surjective.

Luckily, though, only finitely many things can go wrong. If $p \in A^{\sigma=1} \cap A^{\sigma=-1}$, then $p = \sigma(p) = -p$, hence p is a 2-torsion point of $\mathcal{C}(\mathbb{Q})$. That is, $p = (x, 0)$ such that $x \in \mathbb{Q}$ and $x^3 + Ax + B = 0$. Note that, $\mathcal{C}(\mathbb{Q}(\sqrt{d}))$ may have other 2-torsion points. For example, $Y^2 = X^3 - dX$ has 2-torsion points $(\pm\sqrt{d}, 0)$ and $(0, 0)$ and $\sigma(\sqrt{d}, 0) = (-\sqrt{d}, 0)$. Thus, the map $A^{\sigma=1} \times A^{\sigma=-1} \to A$ has a finite kernel given by a subgroup of 2-torsion points of $\mathcal{C}(\mathbb{Q})$. On the other hand, any element in $2A$ is in the image. Indeed, if $\mathbf{q} = 2\mathbf{p}$, then we can write

$$\mathbf{q} = (\mathbf{p} + \sigma(\mathbf{p})) + (\mathbf{p} - \sigma(\mathbf{p}))$$

which shows that $\mathbf{q}$ is in the image of $A^{\sigma=1} \times A^{\sigma=-1} \to A$. Since by the weak Mordell theorem (over $\mathbb{Q}(\sqrt{d})$) we know that $2A$ is finite index in A, this implies that the image of $A^{\sigma=1} \times A^{\sigma=-1}$ is finite index in A. In particular, we conclude that

$$\boxed{\mathrm{rank}\,(\mathcal{C}(\mathbb{Q}(\sqrt{d})) = \mathrm{rank}\,\mathcal{C}(\mathbb{Q}) + \mathrm{rank}\,\mathcal{C}_d(\mathbb{Q})}$$

In fact, we can a bit more precise by using the following result:

Lemma. *Given any automorphism σ of $\mathbb{Z}^r$ with $\sigma^2 = \mathrm{Id}$, one can choose a basis so that*

$$\sigma = L^{\oplus m} \oplus (-\mathrm{Id})^{\oplus n} \oplus \mathrm{Id}^{\oplus o}$$

where $2m + n + o = r$ and $L = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$.

The proof of this lemma is by induction (see [1, Lemma 1]).

Now, on the rank 2 abelian group $\mathbb{Z}^2$ summand where the involution acts by L, we can see that

$$L\begin{pmatrix}2\\1\end{pmatrix} = \begin{pmatrix}2\\1\end{pmatrix} \quad \text{and} \quad L\begin{pmatrix}0\\1\end{pmatrix} = -\begin{pmatrix}0\\1\end{pmatrix}$$

These elements generate and index 2 subgroup of $\mathbb{Z}^2$ which lie in the image of $A^{\sigma=1} \times A^{\sigma=-1}$. Hence, in general, the image of $A^{\sigma=1} \times A^{\sigma=-1}$ is an index $2m$ subgroup of $\mathbb{Z}^r$.

Here is an explicit example. Consider the elliptic curve

$$E : Y^2 = X^3 + X^2 - 1$$

over $\mathbb{Q}(i)$ which is listed in https://www.lmfdb.org/EllipticCurve/2.0.4.1/4232.1/a/1. Its quadratic twist is $E' : Y^2 = X^3 - X^2 + 1$. We have the following :

$$E(\mathbb{Q}(i)) = \mathbb{Z}^2, \quad E(\mathbb{Q}) = \mathbb{Z}, \quad E'(\mathbb{Q}) = \mathbb{Z}$$

Now, one can show that a set of generators of the abelian group $E(\mathbb{Q}(i))$ is given by

$$\mathbf{p} = (-i-1, -1), \quad \mathbf{q} = (0, -i).$$

We have $\sigma(\mathbf{p}) = (i-1, -1) = \mathbf{p} + \mathbf{q}$ and $\sigma(\mathbf{q}) = (0, i) = -\mathbf{q}$. So, σ is represented by the matrix $\begin{pmatrix}1 & 0\\ 1 & -1\end{pmatrix}$. Note that $\sigma(2\mathbf{p} + \mathbf{q}) = 2\mathbf{p} + \mathbf{q}$ and indeed, one can compute that $2\mathbf{p} + \mathbf{q} = (1, 1)$. Thus, we have the identifications

$$E(\mathbb{Q}(i))^{\sigma=1} = E(\mathbb{Q}) = \mathbb{Z} \cdot (2\mathbf{p} + \mathbf{q}), \quad E(\mathbb{Q})^{\sigma=-1} = E'(\mathbb{Q}) = \mathbb{Z} \cdot \mathbf{q}$$

Thus, the image of $E(\mathbb{Q}) \times E'(\mathbb{Q}) \to E(\mathbb{Q}(i))$ is the index 2 subgroup $2\mathbb{Z} \times \mathbb{Z} \subset \mathbb{Z} \times \mathbb{Z}$.

43) This question assumes knowledge of the arithmetic of $\mathbb{Q}(\rho)$ where $\rho^3 = 1$, $\rho \neq 1$.

Fill in the details of the sketched proof of the

Theorem 0.1. *Let $d = q_1 q_2$ where $q_1 > 0$, $q_2 > 0$ are rational primes with $q_1 \equiv 2(9)$, $q_2 \equiv 5(9)$. Then the only rational point on*

$$\mathcal{C} : X_1^3 + X_2^3 + dX_3^3 = 0$$

is $(1, -1, 0)$.

▶ We first recall some basics of the arithmetic in $\mathbb{Z}[\rho]$. We refer to [2, Chapter 9] for details. Recall that $\mathbb{Z}[\rho]$ is an Euclidean domain with a multiplicative norm given by $N(a + b\rho) = a^2 - ab + b^2$, hence it is an unique factorization domain (UFD). The units in this ring are given by norm 1 elements: $\pm 1, \pm\rho, \pm\rho^{-1}$. The element $\lambda = \rho - \rho^{-1}$ is an irreducible element with $N(\lambda) = 3$. The quotient $\mathbb{Z}[\rho]/(\lambda) = \mathbb{F}_3$ is the field of 3 elements. Note that $3 = -\lambda^2$ is not prime in $\mathbb{Z}[\rho]$. We will also use the fact that any rational prime $p \in \mathbb{Z}$ remains a prime in $\mathbb{Z}[\rho]$ if $p \equiv 2(3)$. Finally, we recall the cubic residue chartacter: For π prime in $\mathbb{Z}[\rho]$ with $N(\pi) \neq 3$,

and $\alpha \in \mathbb{Z}[\rho]$, we define $\chi_\pi(\alpha) = \alpha^{\frac{N(\pi)-1}{3}} (\pi)$. For α not divisible π, one has $\chi_\pi(\alpha) \in \{1, \rho, \rho^2\}$ and $\chi_\pi(\alpha) = 1$ if and only if the equation $x^3 = \alpha\,(\pi)$ has a solution.

(i) It is enough to prove that the only points on $\mathcal{C}$ defined over $\mathbb{Q}(\rho)$ is those with $X_3 = 0$. Indeed, we can assume that any such solution has $X_1 = 1$, then X_2 can be -1 or ρ or ρ^{-1}, and the only rational solution among these it $(1, -1, 0)$.

(ii) If (x_1, x_2, x_3) is defined over $\mathbb{Q}(\rho)$ and on the curve, we can assume without loss of generality that they are coprime in pairs in $\mathbb{Z}[\rho]$. Indeed, since $\mathbb{Z}[\rho]$ is a UFD, the usual notion of greatest common divisors work in $\mathbb{Z}[\rho]$. Thus, after clearing the denominators by an overall factor, we can assume that $x_1, x_2, x_3 \in \mathbb{Z}[\rho]$ and $gcd(x_1, x_2, x_3) = 1$. Now, if a prime element $p \in \mathbb{Z}[\rho]$ divides any two of x_1, x_2, x_3, then because $x_1^3 + x_2^3 + dx_3^3 = 0$, and d is cube free, p divides the third one. Thus, we conclude that x_1, x_2, x_3 are pairwise coprime.

(iii) Now $x_1^3 + x_2^3$ factorizes over $\mathbb{Z}[\rho]$, hence we have

$$(x_1 + x_2)(\rho x_1 + \rho^{-1} x_2)(\rho^{-1} x_1 + \rho x_2) = -q_1 q_2 x_3^3$$

We want to show that there are $\alpha_1, \alpha_2, \alpha_3, \xi_1, \xi_2, \xi_3 \in \mathbb{Z}[\rho]$ such that either

$$\begin{aligned} x_1 + x_2 = \alpha_1 \xi_1^3, \qquad & \rho x_1 + \rho^{-1} x_2 = \alpha_2 \xi_2^3 \\ \rho^{-1} x_1 + \rho x_2 = \alpha_3 \xi_3^3, \qquad & \alpha_1 \alpha_2 \alpha_3 = d, \end{aligned}$$

or

$$\begin{aligned} x_1 + x_2 = \lambda \alpha_1 \xi_1^3, \qquad & \rho x_1 + \rho^{-1} x_2 = \lambda \alpha_2 \xi_2^3 \\ \rho^{-1} x_1 + \rho x_2 = \lambda \alpha_3 \xi_3^3, \qquad & \alpha_1 \alpha_2 \alpha_3 = d, \end{aligned}$$

where $\lambda = \rho - \rho^{-1} = \sqrt{-3}$.

By using the unique factorization property, we can write $x_1 + x_2 = \theta_1 \xi_1^3$, $\rho x_1 + \rho^{-1} x_2 = \theta_2 \xi_2^3$ and $\rho^{-1} x_1 + \rho x_2 = \theta_3 \xi_3^3$ with $\theta_1, \theta_2, \theta_3, \xi_1, \xi_2, \xi_3 \in \mathbb{Z}[\rho]$ such that $\theta_1, \theta_2, \theta_3$ are cube free. Now, if θ_1, θ_2 and θ_3 are pairwise coprime, it follows that $\theta_1 \theta_2 \theta_3 = -q_1 q_2$, so we can simply take $\alpha_i = -\theta_i$ and we end up with the first case listed above.

Suppose now that $1 \neq g = gcd(\theta_1, \theta_2)$, so $g | \theta_1$ and $g | \theta_2$. Then $g | x_1 + x_2$ and $g | \rho x_1 + \rho^{-1} x_2$, by considering $\rho(x_1 + x_2) - (\rho x_1 + \rho^{-1} x_2) = \lambda x_2$ we see that $g | \lambda x_2$. But, g is relatively prime to x_2, since $g | x_1 + x_2$ and, x_1 and x_2 are relatively prime. Hence $g = \lambda$ (up to a unit). In particular, we conclude that $\lambda | x_1 + x_2$ and $\lambda | \rho x_1 + \rho^{-1} x_2$. Thus, we have $x_1 = 1(\lambda)$ and $x_2 = -1(\lambda)$ or $x_1 = -1(\lambda)$ and $x_2 = 1(\lambda)$, hence it also follows that $\lambda | \rho^{-1} x_1 + \rho x_2$. Similar argument shows that if $gcd(\theta_1, \theta_3)$ or $gcd(\theta_2, \theta_3)$ are non trivial, they have to be equal to λ, thus we conclude that $\theta_i = -\lambda \alpha_i$ for some $\alpha_i \in \mathbb{Z}[\rho]$ such that α_1, α_2 and α_3 are pairwise coprime. This gives the desired statement.

(iv) $\alpha_1 \xi_1^3 + \alpha_2 \xi_2^3 + \alpha_3 \xi_3^3 = 0$, $\alpha_1 \alpha_2 \alpha_3 = d$.

This is immediate because $1 + \rho + \rho^{-1} = 0$.

(v) Any rational q_1-adic unit is congruent to a cube mod q_1, but ρ is not congruent to a cube. And similar for q_2.

The clearer statement is the following: Let $\pi = q_1$ or q_2, and n be a rational prime (a prime number in $\mathbb{Z}$) such that n is relatively prime to π, then there exists $x \in \mathbb{Z}[\rho]$ such that $x^3 = n\,(\pi)$. This follows from the elementary properties of the cubic residue character and is the statement that $\chi_\pi(n) = 1$ (see Chapter 9, corollary to Proposition 9.3.4 in [2]).

Similarly, we can see that $\chi_\pi(\rho) = \rho^{\frac{N\pi-1}{3}} \in \{\rho^{\frac{q_1^2-1}{3}}, \rho^{\frac{q_2^2-1}{3}}\} = \{\rho, \rho^2\}$, hence ρ is not a cubic residue mod π.

(vi) After multiplying $\alpha_1, \alpha_2, \alpha_3$ all by ρ or ρ^{-1}, if necessary, we may suppose that $\{\alpha_1, \alpha_2, \alpha_3\}$ is a permutation of $\{\pm 1, \pm 1, \pm q_1 q_2\}$ or $\{\pm 1, \pm q_1, \pm q_2\}$.

We have seen in (iii) that α_1, α_2, α_3 are pair-wise coprime and $\alpha_1\alpha_2\alpha_3 = q_1 q_2$. We know that q_1 and q_2 are prime in $\mathbb{Z}[\rho]$ since they are both congruent to 2 modulo 3, we must have that $\alpha_1, \alpha_2, \alpha_3$ is a permutation of $\{u_1, u_2, u_3 q_1 q_2\}$ or $\{u_1, u_2 q_1, u_3 q_2\}$ for u_1, u_2, u_3 units in $\mathbb{Z}[\rho]$ such that $u_1 u_2 u_3 = 1$. Now, if (u_1, u_2, u_3) is $(\pm\rho, \pm\rho, \pm\rho)$ or $(\pm\rho^2, \pm\rho^2, \pm\rho^2)$, then we can multiply the all by ρ or ρ^2 if necessary and arrange $u_1 = u_2 = u_3 = 1$ as required. Otherwise, it must be the case that, up to a permutation (u_1, u_2, u_3) is equal to $(1, \rho, \rho^2)$. Again by multiplying all by ρ or ρ^2 we can actually arrange that $u_1 = 1, u_2 = \rho, u_3 = \rho^2$ or $u_1 = 1, u_2 = \rho^2$ and $u_3 = \rho$. Suppose, for example, we have $\alpha_1 = 1$, $\alpha_2 = \rho q_1$ and $\alpha_2 = \rho^2 q_2$, then we arrive at an equation

$$\xi_1^3 + \rho q_1 \xi_2^3 + \rho^2 q_2 \xi_3^3 = 0$$

Now, examining this equation modulo q_2, we reduce to

$$\xi_1^3 + \rho q_1 \xi_2^3 = 0\,(q_2)$$

But, the previous part shows that q_1 is a cube modulo q_2 (as q_1 and q_2 are relatively prime), hence the last equation implies that ρ is a cube modulo q_2, which contradicts what was proven in the previous part. The other cases can be handled using reduction modulo q_1 or q_2 in a similar way.

(vii) The equation $\xi_1^3 + q_1 \xi_2^3 + q_2 \xi_3^3 = 0$ is impossible mod 9 [and indeed mod λ^3].

Modulo 9, the equation becomes $x_1^3 + 2x_2^3 + 5x_3^3 = 0$. We may suppose that if there is any solution then there is one where $gcd(x_1, x_2, x_3) = 1$. Recall that

$$9 = \rho^4 (1-\rho)^4$$

Hence, the quotient ring $\mathbb{Z}[\rho]/(9) = \mathbb{Z}[\rho]/(1-\rho)^4$ has 81 elements represented by $a + b\rho$ for $a, b \in \{0, 1, \ldots, 8\}$. Now,

$$(a + b\rho)^3 = (a^3 - 3ab^2 + b^3) + (3a^2 b - 3ab^2)\rho$$

We can see that the possible values (modulo 9) for x_1^3 are $\{0,\ 1,\ 8,\ 3+6\rho,\ 6+3\rho\}$, the possible values of $2x_2^3$ are $\{0,\ 2,\ 7,\ 3+6\rho,\ 6+3\rho\}$ and the possible value of $5x_3^3$ are $\{0,\ 4,\ 5,\ 3+$

$6\rho,\quad 6+3\rho\}$. In order for these to add up to zero modulo 9, we must have that $(x_1^3, 2x_2^3, 5x_3^3)$ is a permutation of $(0,0,0), (0, 3+6\rho, 6+3\rho), (3+6\rho, 3+6\rho, 3+6\rho), (6+3\rho, 6+3\rho, 6+3\rho)$ but this implies that $3|x_1^3, x_2^3, x_3^3$ and so $1-\rho|x_1, x_2, x_3$ hence they are not relatively prime. A contradiction.

(viii) If $\{\alpha_1, \alpha_2, \alpha_3\}$ is a permutation of $\{\pm 1, \pm 1, \pm d\}$, then $|\xi_1\xi_2\xi_3|_\infty < |x_1x_2x_3|_\infty$.

By adjusting ξ_i to $-\xi_i$ if necessary, we deduce that $\xi_1^3 + \xi_2^3 + d\xi_3^3 = 0$ so, (ξ_1, ξ_2, ξ_3) satisfies the same equation as (x_1, x_2, x_3) but $x_3 = \pm\xi_1\xi_2\xi_3$ or $x_3 = \pm\lambda\xi_1\xi_2\xi_3$, hence $|x_3|_\infty = |\xi_1\xi_2\xi_3|_\infty$ or $|x_3|_\infty = 3|\xi_1\xi_2\xi_3|_\infty$. We may also assume that $|x_1x_2| > 3$, since $|x_1x_2| \leq 3$ and $x_3 \neq 0$, forces $|x_1^3 + x_2^3|_\infty < d|x_3|_\infty^3$ as $d \geq 10$ as long as $x_3 \neq \pm 1$, and we can easily check that no solutions are obtained also for $x_3 \pm 1$. Thus, we conclude that

$$|x_1x_2x_3|_\infty > |\xi_1\xi_2\xi_3|_\infty$$

and the result follows by descent.

References

[1] L. K. Hua, I. Reiner, Automorphisms of the Unimodular Group

[2] K. Ireland, M. Rosen, A classical introduction to Modern Number theory.

[3] Silverman- The Arithmetic of Elliptic Curves

[4] Silverman-Tate Ratinal points on Elliptic Curves

[5] Washington-Elliptic Curves Number Theory and Cryptography