1. (a) [14 marks] i. State the Hasse estimate.

ii. Prove that the equation $y^2 = x^3 + x - 3$ has a solution $(x, y) \in \mathbb{F}_p^2$ for every prime number p.

iii. Determine the structure of the group $\mathcal{E}(\mathbb{F}_5)$ where $\mathcal{E} : y^2 = x^3 + x - 3$.

iv. State Hensel's Lemma.

v. Prove that the equation $y^2 = x^3 + x - 3$ has a solution $(x, y) \in \mathbb{Q}_p^2$ for every prime number p

(b) [11 marks] i. Find the 7-adic expansions of the rational numbers $\frac{1}{6}$ and $\frac{4}{21}$.

ii. For k a non-negative integer and p a prime number, define

$$a(k, p) := \sum_{n=0}^{\infty} n^k p^n \in \mathbb{Q}_p.$$

Prove that $a(k, p) \in \mathbb{Q}$ for all such k and p. Furthermore, show that for any fixed k the set

$$\{a(k, p) : p \text{ a prime}\} \subset \mathbb{Q}$$

is infinite.

Solution:

(a)

(i) [Bookwork: 2 marks]

For an elliptic curve $\mathcal{E} : y^2 = Q(x)$ (Q a cubic) over $\mathbb{F}_p$ (so p must be odd), we have

$$\#\mathcal{E}(\mathbb{F}_p) \in [(p + 1) - 2\sqrt{p}, (p + 1) + 2\sqrt{p}].$$

(ii) [Easy: 3 marks] Since for any prime $p \geqslant 5$ we have $(p + 1) - 2\sqrt{p} > 1$, the Hasse bound gives solutions for $p \geqslant 5$ provided the equation defines an elliptic curve modulo p. The discriminant is $4 \cdot (+1)^3 + 27 \cdot (-3)^2 = 247 = 13 \cdot 19$. So we need only check $p = 2, 3$ and $p = 13, 19$. For $p = 2$ we see $(0, 1)$ is a solution. For $p = 3$ we see $(2, 1)$ is a solution. For $p = 13$ we see for example $(0, 6)$ is a solution, and for $p = 19$ we have $(0, 4)$ a solution. (In fact, since the cubic has a repeated root modulo these primes, this repeated root must be defined over the field, giving a point of the form $(\star, 0)$ in each case: so there is nothing special about the equation at all.)

(iii) [New but easy: 2 marks] One sees the points here are $\{O, (1, 2), (1, 3), (4, 0)\}$ so the group has order 4. Since there is only one two torsion point $(\star, 0)$ it cannot be $C_2 \times C_2$, so must be C_4.

(iv) [Bookwork: 2 marks]

Let K be a field, complete with respect to a non-Archimedean valuation $|\cdot|$, with valuation ring $R = \{x \in K : |x| \leqslant 1\}$.

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

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

(v)

[New: 5 marks] By the Hasse bound for $p \geqslant 11$ the group of points modulo p has order at least 6, and so cannot consider entirely of 2-torsion (there can be at most 3 such points). So for $p \geqslant 11$, with $p \neq 13$ or 19 there must always be a point $(\bar{x}, \bar{y}) \in \mathbb{F}_p^2$ with $\bar{y} \neq 0$. This is also true for $p = 3, 5, 7$; for example the points $(2, 1), (1, 2), (4, 3)$ respectively. Lift $(\bar{x}, \bar{y})$ in the trivial way to $(x, y) \in \mathbb{Z}^2$. Then taking $f(T) = T^2 - (x^3 + x - 3)$ we have $f'(T) = 2T$,

and so the point $T = y$ satisfies Hensel's Lemma, and we find a solution $(x, \hat{y}) \in \mathbb{Z}^2$ with $\hat{y} = y \bmod p$.

When $p = 13$ or 19 we can do just the same, with the points $(0, 1)$ and $(0, 6)$, respectively, found above.

For $p = 2$ we start with the point $(0, 1) \in \mathbb{F}_2^2$, and take $f(T) = T^3 + T - 3 - 1^2 = T^3 + T - 4$. Then $f'(T) = 3T^2 + 1$, so again the hypothesis of Hensel's Lemma is satisfied and we can lift to get a point $(\hat{x}, 1) \in \mathbb{Z}_2^2$ where $\hat{x} = 0 \bmod 2$.

(b)

(i) [New: 3 marks] We see $\frac{1}{6} = -\sum_{n=0}^{\infty} 7^n$, by specialising the identity $\frac{1}{1-x} = \sum_n x^n$.

We have

$$\frac{4}{21} = \frac{8}{42} = -\frac{1}{7}\cdot(1+7)(1+7+7^2+\cdots) = -\frac{1}{7}\cdot(1+2\cdot 7+2\cdot 7^2+\cdots) = -7^{-1}-2\cdot(1+7+7^2+\cdots)$$

(ii)

[New: 5 marks] We have the identity of formal power series

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n.$$

Applying the operator $(x\frac{d}{dx})^k$ to the LHS gives a rational function whose denominator is a power of $1 - x$. So we may evaluate it at $x = p$ to get a rational number. Applying the same operator to the RHS gives the series $\sum_n n^k x^n$. We may also evaluate this at $x = p$ (since it converges p-adically at this point) to get a p-adic number $\sum_{n=0}^{\infty} n^k p^n$. The p-adic number equals the rational number we obtained from the LHS.

[New: 3 marks] For the second part, if the set is finite then by the pigeon-hole principle, there is some prime p such that the equation

$$\left(x\frac{d}{dx}\right)^k \frac{1}{1-x} = a(k, p)$$

has infinitely many solutions x which are primes. Note the LHS is a rational function of degree -1 (seen by considering local expansion) with $(1 - x)^{k+1}$ on the denominator. It follows we can find a non-zero polynomial in x with infinitely many solutions in primes, a contradiction.

2. (a) [8 marks] Let R be a ring (commutative with a multiplicative identity). Define what is meant by a *formal group* over R.

When K is a field, complete with respect to a discrete non-Archimedean valuation, and R is its valuation ring with maximal ideal $\mathcal{M}$, explain how given a formal group over R one may give $\mathcal{M}$ the structure of a group. (In particular, you should explain carefully why inverses exist.)

(b) [7 marks] Let $\mathcal{E} : y^2 = x^3 + Ax + B$ be an elliptic curve, where $A, B \in \mathbb{Z}$, and let p be an odd prime not dividing its discriminant. Show that the order $\#\mathcal{E}(\mathbb{Q})$ of the torsion subgroup of $\mathcal{E}$ divides the order $\#\tilde{\mathcal{E}}(\mathbb{F}_p)$ of the group of points on the reduction $\tilde{\mathcal{E}}$ of the curve modulo p. [*Any results on formal groups proved in lectures may be assumed provided they are clearly stated.*]

(c) [10 marks] Now let B be a positive integer and $\mathcal{E}$ be the elliptic curve $y^2 = x^3 + B$.

i. Prove carefully that the torsion subgroup of $\mathcal{E}$ always has order dividing 6. [*You may assume that given coprime integers a and n, there are infinitely many primes p with* $p \equiv a \bmod n$.]

ii. Explain why 2 divides the order of the torsion subgroup of $\mathcal{E}$ if and only if B is the cube of an integer.

iii. Show that 3 divides the order of the torsion subgroup of $\mathcal{E}$ if and only if B is the square of an integer.

Solution:

(a)

[Bookwork: 2 marks] A *formal group* defined over R is a power series $F(X,Y) \in R[[X,Y]]$ satisfying:

(1) $F(X,Y) = X + Y +$ terms of degree $\geqslant 2$.

(2) $F(X, F(Y,Z)) = F(F(X,Y), Z)$.

(3) $F(X,Y) = F(Y,X)$.

[Bookwork: 6 marks] The *group on* $\mathcal{M}$ *associated to* $F(X,Y)$, denoted $F(\mathcal{M})$, is the set $\mathcal{M}$ together with the group operation: $x \oplus y = F(x,y)$ [which converges for any $x, y \in \mathcal{M}$]. The identity element is 0, and the inverse of x is given by $i(x)$, defined below.

Let $F(X,Y)$ be a formal group over a ring R, and let R_T denote $R[[T]]$. Then there is a unique power series $i(T) \in TR_T$ such that $F\big(T, i(T)\big) = 0$.

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

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

which has terms all of degree $\geqslant n+2$. This inductively defines a power series $i(T)$, whose first n terms agree with Z_n for all n, such that $F\big(T, i(T)\big) = 0$. Furthermore, each choice of term of Z_n was forced, so that $i(T)$ is unique. [Note: some students may further explain why $F(T,0) = 0$, but this is not necessary to obtain full marks.]

(b)

[Bookwork: 7 marks] We use two results on torsion in formal groups:

Fact 1: Every torsion element in $F(\mathcal{M})$ has order a power of p (residue characteristic).

Fact 2: if $z \in F(\mathcal{M})$ has order p^n then $|z| \geqslant |p|^{\frac{1}{p^n - p^{n-1}}}$.

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

Since p does not divide the discriminant, $\tilde{\mathcal{E}}$ is non-singular, $\mathcal{E}_0(\mathbb{Q}_p) = \mathcal{E}(\mathbb{Q}_p)$ and $\tilde{\mathcal{E}}_{ns}(\mathbb{F}_p) = \tilde{\mathcal{E}}(\mathbb{F}_p)$ and the reduction map $\mathcal{E}(\mathbb{Q}_p) \to \tilde{\mathcal{E}}(\mathbb{F}_p)$ contains no nontrivial torsion, and so is injective when restricted to $\mathcal{E}_{\text{tors}}(\mathbb{Q}_p)$; in particular, $\mathcal{E}_{\text{tors}}(\mathbb{Q})$ is isomorphic to a subgroup of $\mathcal{E}(\mathbb{Q})(\mathbb{F}_p)$ and so the order of the first divides that of the second by Lagrange's theorem.

(c)

(i) [Mainly new, though starting idea is on problem sheet.]

[2 marks: problem sheet] For p not dividing B with $p \equiv 2 \bmod 3$ the (non-singular) curve has $p+1$ points modulo p — since then $x \mapsto x^3 + B$ is a bijection modulo p, and so we get $2 \times \frac{p-1}{2} + 1$ affine points and the point at infinity. This this will be true for infinitely many p.

[4 marks: new] Suppose that some prime $\ell \neq 2, 3$ divides $p+1$ for all primes p with $p \equiv 2 \bmod 3$ and p not dividing B. Then $p \equiv -1 \bmod \ell$ for all primes $p \equiv 2 \bmod 3$ and p not dividing B. Hence the congruence $X \equiv 1 \bmod \ell$, $X \equiv 2 \bmod 3$ has no solutions in primes X for p not dividing B. By CRT we can write this as a congruence $X \equiv a \bmod 3\ell$ where $\gcd(3\ell, a) = 1$, contradicting the hint.

If 4 divided all $p+1$ (for p not divding B) there would not be infinitely many primes with $p \equiv 1 \bmod 4$. Likewise, if 9 divided all such $p+1$ there would be no primes (not dividing B) with $p \equiv 2 \bmod 9$.

Hence no prime power except 2 and 3 divides $p+1$ for all p with $p \equiv 2 \bmod 3$. Hence the greatest common divisor of $p+1$ for all p not dividing B with $p \equiv 2 \bmod 3$ divides 6. The global torsion order thus divides 6 (as it divides the gcd of $p+1$ over all odd p with p not dividing $\Delta = 27B^2$, by (b)).

So we need only consider 2 and 3 torsion.

(ii) [1 mark: bookwork] We have two torsion if and only if B is a cube, for 2-torsion points are always of the form $(x, 0)$ so we need to be able to solve $x^3 = -B$, i.e. $(-x)^3 = B$.

(iii) [1 mark: similar to problem sheet] If B is a square, then $(0, \pm\sqrt{B})$ is a three torsion point.

[2 marks: new] Conversely if $P = (x, y)$ has order 3 then $2P = -P = (x, -y)$ where $y \neq 0$ (since otherwise P is 2-torsion). The x-coordinate of $2(x, y)$ is $m^2 - 2x$ where $m = 3x^2/2y$. (Here m is the gradient of the tangent line at P, and putting $y = mx + \star$ into the equation for the curve and looking at the coefficient of x^2 gives the first coordinate of the third point of intersection.) So we get

$$x = \frac{9x^4}{4y^2} - 2x$$

that is $4xy^2 = 3x^4$. So either $x = 0$ (giving us the points $(0, \pm\sqrt{B})$) or $4y^2 = 3x^3$. But $y^2 = x^3 + B$ and so we get $x^3 + 4B = 0$. But then $x^3 = -4B$ and $y^2 = x^3 + B = -3B < 0$, which is impossible.

3. Let p be an odd prime and $\mathcal{E}_p : y^2 = x(x^2 + p^3)$ be an elliptic curve.

(a) [17 marks] When $p \equiv 1 \bmod 8$ prove that the rank of $\mathcal{E}_p$ is at most two, and when $p \not\equiv 1 \bmod 8$ prove that the rank of $\mathcal{E}_p$ is at most one.

(b) [8 marks] Show further that when $p \equiv 3 \bmod 16$ or $p \equiv 7 \bmod 16$ then the rank of $\mathcal{E}_p$ is zero.

[*You may use any results from lectures provided they are clearly stated. It may also help to recall that for an odd prime p we have that 2 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \bmod 8$.*]

Solution:

[This question is new, but similar calculations have been done on problem sheets and past exam papers. The method is in the lecture notes.]

(a) We consider the curves $\mathcal{G} : y^2 = x(x^2 + ax + b)$ and $\mathcal{H} : y^2 = x(x^2 + a_1x + b_1)$. Here $a = 0, b = p^3$ and $a_1 = -2a = 0, b_1 = a^2 - 4b = -4p^3$. For the two descent we first need to consider squarefree $r|b_1$ such that

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

for some $\ell, m, n \in \mathbb{Z}$ not all zero with $\gcd(\ell, m) = 1$.

So we consider $r = \pm 1, \pm 2, \pm p, \pm 2p$. Now $q(O) = 1, q((0, 0)) = -4p^3 \equiv -p$ are in the image of the q map. Thus

$$-1 \in \mathrm{im}(q) \Leftrightarrow p \in \mathrm{im}(q),\ 2 \in \mathrm{im}(q) \Leftrightarrow -2p \in \mathrm{im}(q),\ -2 \in \mathrm{im}(q) \Leftrightarrow 2p \in \mathrm{im}(q).$$

So we need just check whether $-1, 2, -2 \in \mathrm{im}(q)$. [4 marks]

For $r = -1$, we have equation

$$-\ell^4 + 4p^3m^4 = n^2.$$

If $p|\ell$ then $p^3|LHS$ hence $p^3|n^2$ which forces $p^2|n$ and hence $p^4|n$ and thus we find also $p|m$. So we can exclude this. Thus assuming p does not divide ℓ, we find modulo p that $(-1) \equiv (n/\ell^2)^2$. Thus when $p \equiv 3 \bmod 4$ we see that -1 is not in the image (and make no conclusion otherwise). [2 marks]

For $r = 2$, we have equation

$$2\ell^4 - 2p^3m^4 = n^2.$$

If $p|\ell$ then the same argument as before shows also $p|m$. So we can exclude this. Thus assuming p does not divide ℓ, we find modulo p that $2 \equiv (n/\ell^2)^2$. Thus when $p \equiv 3, 5 \bmod 8$ we see that 2 is not in the image (and make no conclusion otherwise). [2 marks]

For -2, we have equation

$$-2\ell^4 + 2p^3m^4 = n^2.$$

If $p|\ell$ then the same argument as before shows also $p|m$. So we can exclude this. Thus assuming p does not divide ℓ, we find modulo p that $-2 \equiv (n/\ell^2)^2$. Thus when $p \equiv 5, 7 \bmod 8$ we see that -2 is not in the image (and make no conclusion otherwise). [2 marks]

Thus under q the group $\mathcal{H}/\phi(\mathcal{G})$ is isomorphic to a subgroup of:

$$\begin{array}{ll} p \equiv 1 \bmod 8 & \langle -1 \cdot (\mathbb{Q}^*)^2, 2 \cdot (\mathbb{Q}*)^2, -2 \cdot (\mathbb{Q}^*)^2, -p \cdot (\mathbb{Q}^*)^2 \rangle \text{ (a rank 3 group)} \\ p \equiv 3 \bmod 8 & \langle -2 \cdot (\mathbb{Q}^*)^2, -p \cdot (\mathbb{Q}^*)^2 \rangle \text{ (rank 2 group)} \\ p \equiv 5 \bmod 8 & \langle -1 \cdot (\mathbb{Q}^*)^2, -p \cdot (\mathbb{Q}^*)^2 \rangle \text{ (rank 2 group)} \\ p \equiv 7 \bmod 8 & \langle 2 \cdot (\mathbb{Q}^*)^2, -p \cdot (\mathbb{Q}^*)^2 \rangle \text{ (rank 2 group).} \end{array}$$

[1 mark]

For the second isogeny, we need to consider squarefree divisors of $b = p^3$, i.e., just $\pm 1, \pm p$. Now $p^3 \equiv p$ (mod squares), so we know $1 = \hat{q}(O), p \equiv \hat{q}((0, 0))$ are in the image and need only consider -1.

For -1 we get

$$-\ell^4 - p^3m^4 = n^2$$

which has no non-trivial solutions (as the LHS is $\leqslant 0$ and the RHS is $\geqslant 0$).

Thus under $\hat{q}$ the group $\mathcal{G}/\hat{\phi}(\mathcal{H})$ is isomorphic to a subgroup of $\langle p \cdot (\mathbb{Q}*)^2 \rangle$ (rank 1). [3 marks]

To find $\mathcal{G}/2\mathcal{G}$ we combine $\hat{\phi}\,(\mathcal{H}/\phi(\mathcal{G}))$ and $\mathcal{G}/\hat{\phi}(\mathcal{H})$. Note that $q((0,0)) = -p$ and $\hat{\phi}(0,0) = O$ with $\hat{q}(O) = 1$. So the "$-p \cdot (\mathbb{Q}^*)^2$" above makes no contribution, and our bound on $\mathcal{G}/2\mathcal{G}$ is one less than the sum of the ranks for the two parts. Since the 2-torsion subgroup of $\mathcal{G}$ is of order 2 (as we never have $x^2 \neq -p^3$), we subtract a further 1 to get the claimed bound on Mordell-Weil group of $\mathcal{G}$. [3 marks]

(b) Here we need to examine the equations

$$2\ell^4 - 2p^3m^4 = \pm n^2$$

modulo 16. Note $n = 2n_1$ must be even and we can rewrite as

$$\ell^4 - p^3m^4 = \pm 2n_1^2.$$

Now if ℓ is even so is m (and vice-versa), so both ℓ and m must be odd. Hence $\ell^4, m^4 = 1 \bmod 16$ so we have

$$1 - p^3 \equiv \pm 2n_1^2 \equiv 2 \cdot \pm 0, \pm 2 \cdot 1, \pm 2 \cdot 4, \pm 2 \cdot 9 \bmod 16.$$

Hence

$$1 - p^3 \equiv 0, \pm 2, \pm 8 \bmod 16.$$

The sign here is whether we are looking at the case 2 or -2. [3 marks]

For $p \equiv 3 \bmod 16$ we need to exclude that -2 is the image. Now $p^3 \equiv 11 \bmod 16$ and so if -2 is in the image one of the following is true:

$$1 - 11 \equiv 0, 2, 8 \bmod 16.$$

But these are all false. [2 marks]

For $p \equiv 7 \bmod 16$ we need to exclude that 2 is the image. Now $p^3 \equiv 7 \bmod 16$ and so if 2 is in the image one of the following is true:

$$1 - 7 \equiv 0, -2, -8 \bmod 16.$$

But these are all false. [2 marks]

In both cases our analysis reduces the rank bound by one, as required.