1. (a) [11 marks] State and prove *Hensel's Lemma*.

   (b) [6 marks] Let p be a prime and a an integer.

   (i) Show that if p divides a then $x^p - x + a$ splits into linear factors over $\mathbb{Z}_p$, and otherwise $x^p - x + a$ has no roots in $\mathbb{Z}_p$.

   (ii) Compute an integer x such that $x \equiv 1 \bmod 3$ and $x^3 - x + 3 = 0 \bmod 3^4$.

   (iii) Hence, or otherwise, find integers x and y such that $x^3 - x = 3^y - 3$ and $x > 3$.

   (c) [8 marks] Let p be a prime. Show that $x^2 + 7y^3 + 5z^5 = 0$ has a solution $x, y, z \in \mathbb{Z}_p$ with $(x, y, z) \neq (0, 0, 0)$.
   [*Hint: It may help to observe* $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} > 1$.]

2. (a) [6 marks] Compute the torsion subgroup of the elliptic curve $y^2 = x^3 + 5x^2 + 3x + 7$.

   (b) [6 marks] Let n be an integer with $n > 2$. Show that the equation $y^2 = x^3 + x + (n^2 - 2)$ has infinitely many rational solutions.

   (c) [13 marks] Let R be a field of characteristic zero and let

$$F(X, Y) := \frac{X + Y}{1 + XY} \in R[[X, Y]].$$

   (i) Prove that F defines a formal group over R.

   (ii) Compute explicitly the formal logarithm $\log_F(T)$.

   (iii) Hence find an explicit isomorphism $f(T) \in TR[[T]]$ from F to the formal multiplicative group

$$\widehat{G}_m(X, Y) = X + Y + XY$$

   with $f(T)$ a rational function in T.

3. (a) [14 marks] Let $\mathcal{C} : Y^2 = X(X^2 + aX + b)$, where $a, b \in \mathbb{Z}, b \neq 0, a^2 - 4b \neq 0$, and let $\mathcal{D} : V^2 = U(U^2 + a_1U + b_1)$, where $a_1 = -2a$ and $b_1 = a^2 - 4b$. Let the map q be defined by

$$q : \mathcal{D}(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2, \ \ (u, v) \mapsto u \text{ when } u \neq 0,$$

$$q : (0, 0) \mapsto b_1, \ \ q : \underline{\mathbf{o}} \mapsto 1.$$

   (i) Show that $q(P + Q) = q(P)q(Q)$ in the case when none of $P, Q, P + Q$ are $(0, 0)$ or $\underline{\mathbf{o}}$.

   (ii) Let $P = (u, v) \in \mathcal{D}(\mathbb{Q})$ with $P \neq (0, 0)$. Explicitly compute the sum $P + (0, 0)$, and deduce that $q(P + (0, 0)) = q(P)q((0, 0))$.

   (iii) By considering the remaining cases, prove that q is a homomorphism.

   (b) [11 marks] Compute the rank of the elliptic curve $y^2 = x(x^2 - 3x + 10)$.

Solutions:

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

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 $|a - a_0| \leqslant |f(a_0)|/|f'(a_0)|$. [2 marks]

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

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

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

$|f'(a_1) - f'(a_0)| = |f'(a_0 + b_0) - f'(a_0)| = |(\text{poly in } a_0)b_0 + (\text{poly in } a_0)b_0^2 + \ldots|$

$\qquad \leqslant |b_0| < |f'(a_0)| \quad (\text{by } (*)),$

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

Also, $|f(a_1)| = |f(a_0 + b_0)| = |f_0(a_0) + f_1(a_0)b_0 + f_2(a_0)b_0^2 + \ldots|$

$= |f_2(a_0)b_0^2 + \ldots|$ [since $f_0(a_0) + f_1(a_0)b_0 = 0$]

$\leqslant \max_{j \geqslant 2} |f_j(a_0)||b_0|^j \leqslant |b_0|^2 = \frac{|f(a_0)|^2}{|f'(a_0)|^2} = \rho|f(a_0)| < |f(a_0)|$, where $\rho = \frac{|f(a_0)|}{|f'(a_0)|^2} < 1$.

Summarising: $|f'(a_1)| = |f'(a_0)|$ and $|f(a_1)| \leqslant \rho|f(a_0)| < |f(a_0)|$, where $\rho = \frac{|f(a_0)|}{|f'(a_0)|^2} < 1$. [3 marks]

For all n, given $a_n \in R$, define $b_n = -f(a_n)/f'(a_n)$ and $a_{n+1} = a_n + b_n = a_n - f(a_n)/f'(a_n)$.

Assume, as induction hypothesis, that:

$|f'(a_n)| = \ldots = |f'(a_1)| = |f'(a_0)|$ and $|f(a_n)| \leqslant \rho|f(a_{n-1})| \leqslant \ldots \leqslant \rho^n|f(a_0)|. \qquad (1)$

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

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

$= \frac{|f(a_n)|^2}{|f'(a_n)|^2} = \frac{|f(a_n)|^2}{|f'(a_0)|^2}$ [by (1), the induction hypothesis]

$\leqslant \frac{|f(a_0)|}{|f'(a_0)|^2}|f(a_n)|$ [since $|f(a_n)| \leqslant |f(a_0)|$ by (1), the induction hypothesis]

$= \rho|f(a_n)| \leqslant \rho^{n+1}|f(a_0)|$ [by (1), the induction hypothesis].

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

Now, $|b_n| = |f(a_n)|/|f'(a_n)| = |f(a_n)|/|f'(a_0)| \to 0$, so (by a standard theorem in non-archimedean analysis)

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

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

$|a - a_0| = |\sum b_n| \leqslant \max |b_n| = \max \frac{|f(a_n)|}{|f'(a_n)|} = \max \frac{|f(a_n)|}{|f'(a_0)|} = \frac{|f(a_0)|}{|f'(a_0)|}$ [by (2)], as required. [4 marks]

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

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

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

$< |f'(a_0)|$ [by (*)] $= |f_1(a_0)| = |f_1(a)|$ [by (2) and continuity of $|f'(x)|$].

This gives $|\hat{b}^j f_j(a)| \leqslant |\hat{b}^j| \leqslant |\hat{b}^2| < |\hat{b}f_1(a)|$ (since $|\hat{b}| \neq 0$ & $|\hat{b}| < |f_1(a)|$) for $j \geqslant 2$, so that the leading term of the sum in (3) has valuation strictly greater than the valuations of the other

terms, which is inconsistent with the sum being 0. Hence a is unique. [2 marks]

(b) (i) [2 marks] Let $f(x) = x^p - x + a$. If $p|a$ then $f(x) = x^p - x = \prod_{\alpha=0}^{p-1}(x-\alpha) \bmod p$. Also for any $\alpha \in \mathbb{Z}$, $f'(\alpha) = p\alpha^{p-1} - 1 + a \equiv -1 \neq 0 \bmod p$. So we may apply Hensel's lemma to each $0 \leqslant \alpha \leqslant p-1$ to get a root $\hat{\alpha}$ and factorisation $f(x) = \prod_{\alpha=0}^{p-1}(x-\hat{\alpha})$.

[1 mark] Suppose now $a \bmod p \neq 0$. Then for any $\alpha \in \mathbb{Z}$ we have $f(\alpha) = \alpha^p - \alpha + a \equiv a \neq 0 \bmod p$, so there are no roots modulo p and thus none in $\mathbb{Z}_p$.

(ii) [2 marks] Let $a_0 = 1$ and $f(x) = x^3 - x + 3$, so $f'(x) = 3x^2 - 1$. Then iterating Newton we find

$$a_1 = 1 - \frac{3}{2} = -\frac{1}{2},\ a_2 = -\frac{1}{2} - \frac{-\frac{1}{8} + \frac{1}{2} + 3}{\frac{3}{4} - 1} = 13.$$

We know as the lifting is in fact quadratically convergent this should be a solution. And indeed $13^3 - 13 + 3 = 2187 = 3^7$.

(iii) [1 mark: *this also gives a hint for the calculation in (ii)*] $x = 13$ and $y = 7$.

(c) [*This is new, but a similar idea is used in question 1 of the 2017 paper.*]

Let p be a prime and consider the sets

$$A_2 := \{x^2 : x \in \mathbb{F}_p^\star\},\ A_3 := \{7y^3 : y \in \mathbb{F}_p^\star\},\ A_5 := \{5z^5 : z \in \mathbb{F}_p^\star\}.$$

Assume now $p \neq 5, 7$ (to make sure none of these sets are just $\{0\}$). Since always $x \mapsto x^m$ is at most m to 1 on $\mathbb{F}_p^\star$ these sets have size at least $(p-1)/2$, $(p-1)/3$ and $(p-1)/5$ respectively. As

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} > 1$$

they must overlap. [1 mark]

If $A_2 \cap A_3 \neq \emptyset$ we can find non-zero $x, y \in \mathbb{F}_p$ so that $x^2 = 7y^3 \bmod p$ and then $x^2 + 7(-y)^3 + 5 \cdot 0^5 \equiv 0 \bmod p$. We can now apply Hensel, using for $p \neq 2$ the polynomial $f(X) = X^2 + 7(-y)^3$ with starting value $X = x$, to get a solution $(\hat{x}, -y, 0)$. And using for $p = 2$ the polynomial $f(Y) = 7Y^3 + x^2$ with starting value $Y = -y$, to get a solution $(x, \hat{y}, 0)$. [2 marks]

If $A_2 \cap A_5 \neq 0$ we can find non-zero $x, z \in \mathbb{F}_p$ so that $x^2 = 5z^5 \bmod p$ and then $x^2 + 7 \cdot 0^3 + 5(-z)^5 \equiv 0 \bmod p$. Now apply Hensel, using $f(X) = X^2 + 5(-z)^5$ for $p \neq 2$ and $f(Z) = 5Z^5 + x^2$ for $p = 2$. [2 marks]

If $A_3 \cap A_5 \neq 0$ we can find non-zero $y, z \in \mathbb{F}_p$ so that $7y^3 = 5z^5 \bmod p$ and then $0^2 + 7(-y)^3 + 5z^5 \equiv 0 \bmod p$. Now apply Hensel, using $f(Y) = 7Y^3 + 5(-z)^5$ for $p \neq 3$ and $f(Z) = 5Z^5 + 2(-y)^3$ for $p = 3$. [2 marks]

Finally when $p = 5$ as $x \mapsto x^3$ is a bijection on $\mathbb{F}_p$ we have $A_2 \cap A_3 \neq \emptyset$, and the argument before works. And for $p = 7$, since $x \mapsto x^5$ is a bijection on $\mathbb{F}_p$ we have $A_2 \cap A_5 \neq 0$, and we find a solution as before. [1 mark]

2 (a) [Similar: I think this is a little tricky though, as it is somewhat different from the other computations of this sort they have done.]

Reducing modulo 3 we get the equation $y^2 = x^3 + 2x^2 + 7$. Now the polynomial on the RHS has no solutions in $\mathbb{F}_3$, and thus must be squarefree (any repeated root must be defined over the ground field). So the reduction is smooth, and once checks the points over $\mathbb{F}_3$ are

$$\{\underline{\mathbf{o}}, (0,1), (0,2), (1,1), (1,2)\}.$$

So by the results in lectures the torsion subgroup has order dividing 5. [2 marks]

Now there is the obvious point $P = (1,4)$ on the curve. So all we need to do is check whether this order 5 (rather than infinite order). The tangent at a point (x,y) has gradient

$$\frac{3x^2 + 10x + 3}{2y}.$$

So the tangent at P is $y = 2x + 2$. Putting into the curve we get

$$4x^2 + \cdots = x^3 + 5x^2 + \cdots$$

$$x^3 + x^2 + \cdots = (x - x(2P))(x-1)(x-1).$$

So $x(2P) = -3$, and $2P = (-3, 4)$. Doubling again we see that the tangent at $2P$ has gradient

$$\frac{3 \cdot 9 + 10 \cdot (-3) + 3}{8} = 0.$$

So this tangent is $y = 4$. Putting in we get

$$(x^3 + 5x^2 + 3x + 7) - 16 = (x+3)(x+3)(x - x(4P)).$$

So looking at constants we get $x(4P) = 1$, and so $4P = (1, -4)$. Without further computation one now sees $P + 4P = \underline{\mathbf{o}}$. [4 marks]

(b) [Similar / New: they have seen that a non-rational solution implies positive rank.] This equation defines an elliptic curve exactly when $\Delta_n := 4 + 27(n^2 - 2)^2 \neq 0$. So let us first assume $\Delta_n \neq 0$. [1 mark]

The curve has the obvious point $P = (1, n)$. The strategy is to double it and observe $2P$ is not integral, when $n \neq \pm 2$, so $2P$ has infinite order (by an important result from lectures) giving our infinite set of solutions. [1 mark]

The tangent at a point (x,y) has gradient

$$\frac{3x^2 + 1}{2y}$$

so at P this is $\frac{4}{2n} = \frac{2}{n}$. Hence the tangent line is $y = \frac{2}{n}x + n - \frac{2}{n}$. Thus

$$\left(\frac{2}{n}x + \cdots\right)^2 = x^3 + 0x^2 + \cdots$$

and

$$x^2 - \frac{4}{n^2}x + \cdots = (x-1)(x-1)(x - x(2P)).$$

Thus we find

$$x(2P) = \frac{4}{n^2} - 2.$$

This is not integral provided $n \neq \pm 1, \pm 2$. [3 marks]

On the discriminant, if we suppose $\Delta_n = 0$ then reducing mod 5 we get $-1 + 2(n^2-2)^2 \equiv 0 \bmod 5$ and so $(n^2-2)^2 = \frac{1}{2} \equiv 3 \bmod 5$, which is a contradiction. Or alternatively, note Δ_n is in fact always positive. [1 mark]

(c)

(i) [4 marks: similar] We need to check the axioms. Commutativity is obvious, and also

$$F(X,Y) = X + Y + \cdots$$

since $(1+XY)^{-1} = 1 + (XY) + (XY)^2 + \cdots$. For associativity we have

$$F(X, F(Y,Z)) = \frac{X + \frac{Y+Z}{1+YZ}}{1 + X\left(\frac{Y+Z}{1+YZ}\right)}$$

and

$$F(F(X,Y),Z) = \frac{\frac{X+Y}{1+XY} + Z}{1 + \frac{X+Y}{1+XY}Z}$$

and both are

$$\frac{X+Y+Z+XYZ}{1+YZ+XY+XZ}.$$

(ii) [4 marks: similar]

The canonical differential is $F_X(0,T)^{-1}dT$. One computes

$$F_X(X,Y) = \frac{(1+XY) - (X+Y)Y}{(1+XY)^2} = \frac{1-Y^2}{(1+XY)^2}.$$

Hence $F_X(0,T) = 1 - T^2$. So

$$\omega = \frac{dT}{1-T^2}$$

and the formal logarithm is

$$\int \omega = \int \frac{dT}{(1+T)(1-T)} = \frac{1}{2}\log\left(\frac{1+T}{1-T}\right) \ \left(= \tanh^{-1}(T)\right).$$

(iii) [New] Thus by the lectures

$$\log_F(T) = \frac{1}{2}\log\left(\frac{1+T}{1-T}\right)$$

is an isomorphism from F to the formal additive group $\widehat{G}_a$. [1 mark]

Now $\log(1+T)$ is an isomorphism from $\widehat{G}_m$ to $\widehat{G}_a$, with inverse $\exp(T) - 1$. [1 mark] Thus the composition

$$\exp\left(\frac{1}{2}\log\left(\frac{1+T}{1-T}\right)\right) - 1$$

is an isomorphim. But this is not a rational function in T. [2 marks]

However, recall that multiplication by 2 is an isomorphism from $\widehat{G}_a$ to itself. This allows us to remove the factor $\frac{1}{2}$ and take

$$\exp\left(\log\left(\frac{1+T}{1-T}\right)\right) - 1 = \frac{2T}{1-T}.$$

[2 marks] (And indeed one can check by a computation this is indeed a homomorphism, and the series is certainly functionally invertible.)

3 (a) (i) [Bookwork] [6 marks] Let $(u_1, v_1), (u_2, v_2), (u_3, v_3)$ be 3 points on $\mathcal{H} = \mathcal{D}(\mathbb{Q})$ which sum to $\underline{\mathbf{o}}$, [so that $(u_1, v_1) + (u_2, v_2) = (u_3, -v_3)$]. Then these are the 3 points of intersection between $\mathcal{D}$ and some line defined over $\mathbb{Q}$: $V = \ell U + m$, say. Substituting $V = \ell U + m$ into $\mathcal{D}$ gives: $U(U^2 + a_1U + b_1) - (\ell U + m)^2$, whose 3 roots must be u_1, u_2, u_3. That is: $U(U^2 + a_1U + b_1) - (\ell U + m)^2 = (U - u_1)(U - u_2)(U - u_3)$. Equating constant terms gives: $u_1u_2u_3 = m^2 = 1$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$, and so $u_1u_2 = 1/u_3 = u_3$ in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$. (Note $u_1u_2u_3 \neq 0$, by our assumption.) Therefore, by the definition of q we have: $q\big((u_1, v_1)\big)q\big((u_2, v_2)\big) = q\big((u_3, -v_3)\big) = q\big((u_1, v_1) + (u_2, v_2)\big)$.

(ii) [The first part is in the lectures, but on the curve $\mathcal{C}$. The second part is new.] [5 marks]

When $u \neq 0$, we first find the line through $(0, 0)$ and (u, v), which is: $V = \frac{v}{u}U$. Substituting this into $\mathcal{D}$ gives:

$$\left(\frac{v}{u}\right)^2 U^2 = U(U^2 + a_1U + b_1)$$

$$v^2U^2 = u^2U^3 + a_1u^2U^2 + b_1u^2U$$

$$u(u^2 + a_1u + b_1)U^2 = u^2U^3 + a_1u^2U^2 + b_1u^2U \text{ [since } (u, v) \text{ is on } \mathcal{D}]$$

$$0 = uU^3 - (u^2 + b_1)U^2 + b_1uU, \text{ [since } u \neq 0]$$

and so $U(U - u)(uU - b_1) = 0$. The roots of this cubic are: $U = 0, U = u, U = b_1/u$. The line $V = \frac{v}{u}U$ and $\mathcal{D}$ intersect at:

$$(0, 0), (u, v) \text{ and } \left(\frac{b_1}{u}, \frac{b_1v}{u^2}\right) \text{ [since } U = \tfrac{b_1}{u} \text{ gives } V = \tfrac{v}{u}\tfrac{b_1}{u} = \tfrac{b_1v}{u^2}]$$

and so $(u, v) + (0, 0) = \left(\frac{b_1}{u}, -\frac{b_1v}{u^2}\right)$

Thus $q(P + (0, 0)) = b_1/u \equiv b_1 \cdot u = q((0, 0))q(P)$.

(iii) [3 marks: new, and I think a little tricky.] If P or Q is $\underline{\mathbf{o}}$ the result is immediate. If $P + Q = \underline{\mathbf{o}}$ then we have $Q = -P$ and then always $q(Q) = q(P)$ and so $q(P)q(Q) = q(P)^2 \equiv 1 = q(\underline{\mathbf{o}})$. If $P = Q = (0, 0)$ then $P + Q = \underline{\mathbf{o}}$ and $b_1 \cdot b_1 \equiv 1$. It remains then to consider the case $P + Q = (0, 0)$.

Then $Q = -P + (0, 0)$ so by (ii) we have $q(Q) = q(-P + (0, 0)) = q(-P)q((0, 0))$ which is $q(P)q((0, 0))$. Thus $q(P)q(Q) = q(P)^2q((0, 0)) \equiv q((0, 0)) = q(P + Q)$.

(b) [Similar: this is a standard type of exam question.] Using the notation from lectures we have $a = -3, b = 10, a_1 = 6, b_1 = -31$, and $C : y^2 = x(x^2 - 3x + 10)$, $D : v^2 = u(u^2 + 6u - 31)$. [1 mark]

We first consider $\mathcal{H}/\phi(\mathcal{G})$. Under q this is isomorphic to a subgroup of the squarefree divisors of $b_1 = -31$. So $\mathrm{im}(q) \leqslant \langle -1, -31\rangle$. Taking $r = -1$ we easily spot the point $(-1, 6) \in D(\mathbb{Q})$ with $q((-1, 6)) = -1$. And $q((0, 0)) = -31$. So $\mathrm{im}(q) = \langle -1, 31\rangle \cong C_2^2$. [4 marks]

We next consider $\mathcal{G}/\hat{\phi}(\mathcal{H})$. Under $\hat{q}$ this is isomorphic to a subgroup of the squarefree divisors of $b = 10$. So $\mathrm{im}(\hat{q}) \leqslant \langle -1, 2, 5\rangle$. Again we easily spot points $(2, 4)$ and $(5, 10)$ on $C(\mathbb{Q})$ and so 2 and 5 are in the image. For $r = -1$ the homogeneous space is

$$W_{-1} : -\ell^4 - 3\ell^2m^2 - 10m^4 = n^2.$$

This has no non-trivial solutions in $\mathbb{R}$, since always LHS is $\leqslant 0$ and RHS is $\geqslant 0$, so none in $\mathbb{Z}$. Hence $\mathrm{im}(\hat{q}) \leqslant \langle 2, 5\rangle > \cong C_2$. [5 marks]

So in conclusion using the formula from Sheet 4 Question 3, the rank is $2 + 2 - 2 = 2$. [1 mark]