1. (a) [5 marks] Compute the 61-adic expansions of $-\frac{11}{5}$ and $\frac{11}{5}$.

(b) [8 marks] Find $x \in \mathbb{Q}$ with $|x^3+3x+1|_5 \leqslant 5^{-4}$. Prove there does not exist $x \in \mathbb{Q}_5$ with $x^3+5x+5=0$.

(c) [5 marks] Let S be a set of prime numbers, and $\alpha \in \mathbb{Z}$. When S is finite, show that there exists a sequence $x_n \in \mathbb{Z}$ of *distinct* integers such that

$$x_n \to \alpha \text{ as } n \to \infty$$

with respect to every valuation $|\cdot|_p$ for $p \in S$.

Does the same result hold when S is infinite? Justify your answer.

(d) [7 marks] Find the structure of the group $\mathcal{E}(\mathbb{F}_5)$ where $\mathcal{E} : y^2 = x^3 + x - 1$.

[*You may use any results from lectures provided they are clearly stated.*]

Solution 1. (a) [Similar] We have

$$-\frac{11}{5} = -\frac{11\cdot 12}{5\cdot 12} = \frac{10+2\cdot 61}{1-61}$$
$$= (10+2\cdot 61)(1+61+61^2+61^3+61^4+\cdot)$$
$$= 10\cdot 1 + 12\cdot 61 + 12\cdot 61^2 + 12\cdot 61^3 + \cdots$$

Now

$$-(a_0+a_1p+ap^2+\cdots) = (p-a_0) + ((p-1)-a_1)p + ((p-1)-a_2)p^2 + \cdots$$

since adding negative the LHS to the RHS gives $p+(p-1)p+(p-1)p^2+\cdots = 0$. Thus

$$\frac{11}{5} = 51 + 48\cdot 61 + 48\cdot 61^2 + \cdots$$

(b) [New but similar]
For the first part we use Newton iteration:

$$x' := x - \frac{f(x)}{f'(x)} = x - \frac{x^3+3x+1}{3x^2+3}.$$

We can start with $x_0 = 1$, and then

$$x_1 = 1 - \frac{5}{6} = \frac{1}{6}.$$

Next

$$x_2 = \left(\frac{1}{6}\right) - \frac{\left(\frac{1}{6}\right)^3 + 3\left(\frac{1}{6}\right)+1}{3\left(\frac{1}{6}\right)^2+3}.$$

Now we know from discussions in lectures that in fact Newton iteration has quadratic convergence so $|f(x_2)| \leqslant 5^{-4}$. The above expression for x_2 is accepted as the answer, but it is not hard (especially with mechanical aid) to find explicitly

$$x_2 = -\frac{107}{333}.$$

For the second part, suppose such an x exists and let $|x|_5 = 5^{-n}$ (obviously x is not zero). Then the terms in $x^3 + 5x + 5$ have norms $5^{-3n}, 5^{-n-1}, 5^{-1}$. By the triangle inequality, to get a sum zero we need the largest two of these norms to be the same (for otherwise the norm of the sum is the norm of the largest and so the sum is non-zero). If $n \leqslant 0$ there is a unique largest one, 5^{-3n}, and if $n > 0$ the unique largest one is 5^{-1}.

(c) [New]

Note we don't allow setting $x_n = \alpha$ for all n.

Define $x_n := \alpha + \left(\prod_{p \in S} p\right)^n$.

For the second part the answer is yes. Write $S := \{p_1, p_2, \cdots\}$ and define

$$x_n := \alpha + \left(\prod_{i=1}^{n} p_i\right)^n.$$

(d) [Similar] Let $f(x) = x^3+x-1$. Then for $x = 0, 1, 2, 3, 4$ we find $f(x) = -1, 1, 4, 4, 2 \bmod 5$, by a computation. The first 4 values only are squares, and all non-zero. Thus there are $4 \times 2 = 8$ affine points, and so 9 projective points. Hence the group is $C_3 \times C_3$ or C_9.

To, try to, rule out the former we must try and find an affine point of order $\neq 3$. We take $P = (0, 2)$. The gradient of the tangent at P is $(3x^2 + 1)/(2y)$, evaluated at P, which is $1/4 = 4$. Thus the tangent must be $y = 4x + 2$. Putting this into the equation we get that the x-coordinates of intersects of $\ell_{P,P}$ and $\mathcal{E}$ satisfy $(-x + 2)^2 = x^3 + x + 1$ and so $x^3 - x^2 + \cdots = 0$. So the third point of intersection has x-coordinate $1 - 0 - 0 = 1$ and so must be $(1, 4)$. Hence $2P = (1, -4) \neq -P$. So P must have order 9 and the group is C_9.

2. (a) [10 marks] For $a \in \mathbb{Q}$ let $\mathcal{E}_a$ be the curve $y^2 = x^3 + ax - a$.

i. Find the discriminant $\Delta(a)$ of $x^3 + ax - a$.

ii. Assume now $\Delta(a) \neq 0$. Let $P = (1, 1) \in \mathcal{E}_a(\mathbb{Q})$. Show that

$$2P = \left(\frac{1}{4}(a^2 + 6a + 1), \frac{1}{8}(-a^3 - 9a^2 - 15a + 1)\right).$$

Deduce that P is not of order 4.

iii. For $a \in \mathbb{Q}$ with $\Delta(a) = 0$, identify the singular points on $\mathcal{E}_a$ and say whether each is a cusp or a node.

(b) [5 marks] Compute the torsion subgroup $\mathcal{E}(\mathbb{Q})_{\text{tors}}$ of the curve $\mathcal{E} : y^2 = x^3 - 15x + 22$.

(c) [5 marks] Show that the equation $y^2 = x^3 - 4x^2 + 5x - 2$ has infinitely many solutions $(x, y) \in \mathbb{Z}^2$.

(d) [5 marks] Let R be a commutative ring with a 1, and let F be a formal group over R. For m a non-negative integer define the multiplication by m map $[m](T) \in R[[T]]$ inductively by: $[0](T) = 0, [m+1](T) := F([m](T), T)$. Prove that $[2](T)$ is a homomorphism from F to F.

[*You may use any results from lectures provided they are clearly stated.*]

Solution:

(a) [New but easy: replacing bookwork]

i. [1 mark] We have "$\Delta = 4a^3 + 27b^2$" so $\delta(a) = 4a^3 + 27(-a)^2 = a^2(4a + 27)$.

ii. [3 marks] The tangent at a point (x, y) has gradient $\frac{dy}{dx} = \frac{3x^2+a}{2y}$. So at P we get $\frac{3+a}{2}$. So the tangent is $Y = \frac{3+a}{2}X + c$, and putting in $(1, 1)$ to this we get $c = 1 - \frac{3+a}{2} = -\frac{1+a}{2}$. Putting into the equation for the curve gives

$$\left(\frac{3+a}{2}X + c\right)^2 = X^3 + aX - a$$

and equating coefficients of X^2 we get the x-coordinate of $2P$ is

$$\left(\frac{3+a}{2}\right)^2 - 2 = \frac{1}{4}(a^2 + 6a + 1).$$

The y-coordinate is the negative of

$$\frac{3+a}{2} \times \left(\left(\frac{3+a}{2}\right)^2 - 2\right) - \frac{1+a}{2}$$

$$= \frac{1}{8}(-a^3 - 9a^2 - 15a + 1).$$

Note this calculation is fine when E_a is singular too, as $(1, 1)$ is never a singular point.

[2 marks] Now if P has order 4 then $2P$ has order 2 and so has y-coordinate zero. If $-a^3 - 9a^2 - 15a + 1 = 0$ has rational solution, then it has an integral one. Reducing modulo 5 and taking $a \in \{0, 1, 2, 3, 4\}$ we see there are no solutions modulo 5, hence no integral solutions. (Or better, just observe ± 1 not roots, as roots divide constant.)

iii. [2 marks] For $a = 0$ we have $y^2 = x^3$, upon which $(0, 0)$ is a cusp. For $a = -27/4$ we get

$$x^3 + ax - a = (x + 3)(x - 3/2)^2$$

and the point $(3/2, 0)$ is a node.

(b) [Similar] By inspection we find $P := (-1, 6) \in \mathcal{E}(\mathbb{Q})$. Using the equation $2y\frac{dy}{dx} = 3x^2 - 15$ we find the tangent line at P has gradient $m = -1$, thus is $y = -x + 5$. Substituting this into the equation for the curve and comparing coefficients of x^2 on both sides we have $m^2 = (-1) + (-1) + x_{2P}$ and so $2P = (3, -2)$. The line joining P and $2P$ has gradient $(6 + 2)/(-1 - 3) = -2$ and so we have $(-2)^2 = -1 + 3 + x_{3P}$ and $3P = (2, \star)$ and from the curve equation we see $\star = 0$. Hence $3P$ has order 2 and so $6P = \underline{\mathbf{o}}$. Note since $2P, 3P \neq \underline{\mathbf{o}}$ the order of P is exactly 6.

Reducing modulo 3 we see the discriminant is zero. (Note one can reduce the coefficients modulo p first, before computing "$4a^3 + 27b^2$"). Reducing modulo 5 it is non-zero. The points modulo 5 are $\underline{\mathbf{o}}$ along with $(2, 0), (3, \pm 2), (4, \pm 1)$, thus the torsion group has size at most 6 (from a result in lectures). Thus it is $\langle P \rangle$.

(c) [New] (Of course an elliptic curve cannot have infinitely many integral points, so this curve must be singular!)

We have $x^3 - 4x^2 + 5x - 2 = (x - 1)^2(x - 2)$ and so this cubic curve is singular. In general for $y^2 = (x - a)^2(x - b)$ we have the birational change of variables $z = x - b, w = y/(x - a)$, with inverse $x = z + b, y = (z - a + b)w$, with transforms our curve to $w^2 = z$. The latter has the obvious solutions $w = n \in \mathbb{Z}$ and $z = n^2$, which map to $(n^2 + b, (n^2 - a + b)n)$ on the original curve. Thus in our case we have $(n^2 + 2, (n^2 + 1)n)$ for $n \in \mathbb{Z}$.

(d) [New: I mentioned this briefly in the lectures but it is not in the notes.] One computes $[1](T) = F([0](T), T) = F(0, T) = T$, the last equality being in lectures.

Hence $[2](T) = F([1](T), T) = F(T, T)$. Thus according to the definition of a homomorphism in lectures we must show that $[2](F(X, Y)) = F([2](X), (2)[Y])$, that is

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

We do this using commutativity and associativity. To see the steps it is simplest to first prove $(X + Y) + (X + Y) = (X + X) + (Y + Y)$. One has

$$(X + Y) + (X + Y) = X + (Y + (X + Y)) = X + ((X + Y) + Y)$$

$$= X + (X + (Y + Y)) = (X + X) + (Y + Y).$$

Mimicking this proof one has

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

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

using associativity, commutativity, associativity, associativity.

3. (a) [10 marks] Compute the rank of the curve $y^2 = x(x^2 + 3x + 5)$.

(b) [15 marks] Compute the Mordell-Weil group of the curve $y^2 = x(x^2 + 10x + 8)$.

[*You may use any results from lectures provided they are clearly stated.*]

Solution:

(a) [New, but quite simple and similar to problem sheets: replacing bookwork]

[1 mark] Following notation in the lecture notes, we have $a = 3$, $b = 5$, $a_1 = -2a = -6$, $b_1 = a^2 - 4b = -11$. Thus $\mathcal{D} : v^2 = u(u^2 - 6u - 11)$.

[3 marks] Thus for $\mathcal{H}/\phi(\mathcal{G})$ we need to consider $r \in \{\pm 1, \pm 11\}$, and we have $q(0) = 1$, $q((0, 0)) = b_1 = -11$. For $r = -1$ we see that $(-1, 2) \in \mathcal{H}$ and maps under q to -1, so $-1 \in \mathrm{Im} q$. Hence $\mathcal{H}/\phi(\mathcal{G}) = \langle (0, 0), (-1, 2) \rangle \cong C_2^2$.

[3 marks] For $\mathcal{G}/\hat{\phi}(\mathcal{H})$ we need to consider $r \in \{\pm 1, \pm 5\}$, and $\hat{q}(0) = 1$, $\hat{q}((0, 0)) = b = 5$. For $r = -1$ we have $\hat{W}_{-1} : -\ell^4 + 3\ell^2 m^2 - 5m^4 = n^2$, i.e. $-(\ell^2 - 2m^2)^2 - \ell^2 m^2 - m^4 = n^2$. But we see this has no non-trivial solutions since always $LHS \leqslant 0$ and $RHS \geqslant 0$. So $\mathcal{G}/\hat{\phi}(\mathcal{H}) = \langle (0, 0) \rangle$.

[3 marks] Overall $\mathcal{G}/2\mathcal{G}$ is generated by $(0, 0)$ and $\hat{\phi}((-1, 2)) = (1, 3)$. Note these points are independent in this quotient, as they are independent in $\mathcal{G}/\hat{\phi}(\mathcal{H})$ (the map $\hat{q}$ takes values 5 and 1 on them). Since the two torsion of our curve is C_2 we get rank $2 - 1 = 1$.

(b) [New, but similar to lectures and problem sheets] Following notation in the lecture notes, we have $a = 10$, $b = 8$, $a_1 = -2a = -20$, $b_1 = a^2 - 4b = 68$. Thus $\mathcal{D} : v^2 = u(u^2 - 20u + 68)$.

[3 marks] To compute the torsion since $b(a^2 - 4b) = 8 \cdot 68 \neq 0 \bmod p$ for $p = 3, 5$ we can try finding points for these small primes. For $p = 3$ we get equation $y^2 = x(x^2 + x + 2)$, and we find points $O, (0, 0), (1, \pm 1), (2, \pm 1)$. For $p = 5$ we get $y^2 = x(x^2 + 3)$ and find points

$O, (0,0), (1,\pm 2), (2,\pm 2), (3,\pm 1), (4,\pm 1)$. Thus the torsion order divides $\gcd(6,10) = 2$, and must be 2.

We now apply descent.

[4 marks] Thus for $\mathcal{H}/\phi(\mathcal{G})$ we need to consider $r \in \{\pm 1, \pm 2, \pm 17, \pm 34\}$, and we have $q(0) = 1$, $q((0,0)) = b_1 = 17$. Since $a_1 \leqslant 0$ the equations W_r for r negative have no solutions in $\mathbb{R}$, hence none in $\mathbb{Q}$. Thus it is enough to consider $r = 2$ (or $r = 34$). By inspection $(2,8) \in \mathcal{H}$. (Note $\mathcal{D}$ has rank 2 with non-torsion generators $(17,17)$ and $(2,8)$.) One alternatively spots that

$$W_2 : 2\ell^4 - 20\ell^2 m^2 + 34m^4 = n^2$$

has solution $(\ell, m, n) = (1,1,2)$. (Taking $r = 34$ the points on the curve and homogeneous space are, respectively, $(34, 2^3 \cdot 17)$ and $(1,1,2)$.) Thus

$$\mathcal{H}/\phi(\mathcal{G}) = \langle (0,0), (2,8) \rangle \cong \{1, 2, 17, 34\} \cong C_2 \times C_2.$$

[4 marks] For $\mathcal{G}/\hat{\phi}(\mathcal{H})$ we need to consider $r \in \{\pm 1, \pm 2\}$. We have as usual $\hat{q}(0) = 1$ and $\hat{q}((0,0)) = 8 = 2$. So it is enough to consider $r = -1$. Here

$$W_{-1} : -\ell^4 + 10\ell^2 m^2 - 8m^4 = n^2.$$

This has solution $(1,1,1)$, corresponding to the point $(-1,-1)$ on $\mathcal{C}$. (Note $\mathcal{C}$ has rank 2 and the non-torsion generators are $(-1,-1)$ and $(-2,4)$). So

$$\mathcal{G}/\hat{\phi}(\mathcal{H}) = \langle (0,0), (-1,-1) \rangle \cong \{\pm 1, \pm 2\} \cong C_2 \times C_2.$$

[1 mark] Thus $\mathcal{G}/2\mathcal{G}$ is generated by $(0,0), (-1,-1), \hat{\phi}((0,0))(= O), \hat{\phi}((2,8))$.

Since the 2-torsion in $\mathcal{C}$ is dimension 1, this shows the rank of $\mathcal{C}$ is at most $3 - 1 = 2$. To prove it is exactly 2 we could try and show that $(0,0), (-1,-1), \hat{\phi}((2,8)) = (4,-16)$ are independent in $\mathcal{G}/2\mathcal{G}$. Now we know that $(-1,-1)$ and $(4,-16)$ are points of infinite order, and $\hat{q}((-1,-1)) = -1$, $\hat{q}((4,-16)) = 4 = 1$. Note the latter is expected as $\hat{q}$ is trivial on the image of $\hat{\phi}$. So we cannot use the $\hat{q}$ map to prove that the two infinite order points $(-1,-1)$ and $(4,-16)$ are independent.

[3 marks] However, one can instead consider the two points $(-1,-1)$ and $(2,8)$ of infinite order. We have $\hat{q}((2,8)) = 2$ (which was the same as $\hat{q}((0,0))$ which is why we didn't need this point before). Since $-1 \neq 2$ in $\mathbb{Q}^\star/(\mathbb{Q}^\star)^2$ these two points are in fact independent in $\mathcal{G}/\hat{\phi}(\mathcal{H})$ and hence also in $\mathcal{G}$.