1. PUT ON WEBLEARN DON'T E-MAIL

(a) [10 marks] i. Compute the 5-adic expansion of $-\frac{3}{8}$.

ii. Find $x \in \mathbb{Q}$ with $|x^2-17|_2 \leqslant 2^{-10}$. Hence, or otherwise, find $x \in \mathbb{Z}$ with $|x^2-17|_2 \leqslant 2^{-10}$.

(b) [9 marks] Let p be a prime number. Consider the projective curve

$$\mathcal{C} : X^3 - X^2Z + 2XYZ - Y^3 = 0$$

over $\mathbb{Q}_p$, with reduction $\tilde{\mathcal{C}}$ over the residue field $\mathbb{F}_p$.

i. Show that there exists a point $P \neq (0,0,1)$ in $\mathcal{C}(\mathbb{Q}_p)$ which lifts the point $(0,0,1) \in \tilde{\mathcal{C}}(\mathbb{F}_p)$.

ii. Adapting your construction, or otherwise, prove that there exists an infinite set of distinct points

$$\{P_\beta \in \mathcal{C}(\mathbb{Q}_p) : \beta \in \mathbb{Z}_p\}$$

with $P_0 = (0,0,1)$ and such that every P_β is a lift of $(0,0,1) \in \tilde{\mathcal{C}}(\mathbb{F}_p)$.

(c) [6 marks] Let P be the point $(2,-1)$ on the elliptic curve $y^2 = x^3 - 2x - 3$. Using the Elliptic Curve Method, factorise 437 by calculating $3P$.

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

Solution 1.

(a) (i) [Similar: 4 marks] The shortest way to do this is write

$$-\frac{3}{8} = -\frac{9}{24} = \frac{4+5}{1-5^2}$$

$$= 4(1+5+5^2+\dots) + 5(1+5+5^2+\cdots) = 4 + 1\cdot 5 + 4\cdot 5^2 + 1\cdot 5^3 + 4\cdot 5^4 + \cdots .$$

I expect students to do it by solving $-3 = 8(a_0 + a_1 5 + \cdots)$ recursively and spotting a pattern.

(ii) [Similar: 4 marks]

One uses Newton iteration, starting with $a_0 := 1$. Then

$$a_1 := 1 - \frac{1^2 - 17}{2} = 9$$

$$a_2 := 9 - \frac{9^2 - 17}{18} = \frac{49}{9}.$$

Now one observes easily $|1^2 - 17| = 2^{-4}$ and $|9^2 - 17|_2 = |64|_2 = 2^{-6}$. We know Newton iteration is quadratic, so expect $a_2 = 49/9$ should work. A not too difficult hand calculation show

$$a_2^2 - 17 = \frac{2401}{81} - 17 = \frac{2401 - 17\cdot 81}{81} = \frac{2401 - 1377}{81} = \frac{1024}{81}$$

so indeed this works.

[New, 2 marks] To get $x \in \mathbb{Z}$ is trickier since the method for lectures for finding integral solutions has linear convergence. However, it is enough to compute 9^{-1} mod 1024. Using Euclid

$$1024 = 113\cdot 9 + 7,\ 9 = 1\cdot 72,\ 7 = 3\cdot 2 + 1$$

so

$$1 = 7 - 3 \cdot 2 = 7 - 3(9 - 7) = 4 \cdot 7 - 3 \cdot 9$$
$$= 4 \cdot (1024 - 113 \cdot 9) - 3 \cdot 9$$
$$= 4 \cdot 1024 - (4 \cdot 113 + 3) \cdot 9$$

So we have the inverse is -455 (or $+569$) giving a solution $-455 \cdot 49 = -22295$ (or $+27881 \equiv 233 \bmod 2^{10}$). (All these calculations are quite easy by hand: I did them that way myself. Of course a solution to the second part solves the first too.)

(b) [Similar / New : They have seen applications of Hensel's lemma to lifting points on curves in the case in which the point over the residue field is smooth. And also used Hensel's lemma to lift repeated roots of polynomials. But they haven't before put both together.]

(i) [6 marks. Note the coefficient 2 is there since otherwise the curve would have the obvious points $(\alpha, \alpha, 1)$ for any α. This 2 also makes the analysis more interesting.]

Setting "$Z = 1$" we work on the affine curve defined by

$$x^3 - x^2 + 2xy - y^3.$$

Observe that $(0, p)$ reduces to $(0, 0)$, which is the affine point on the curve we want to find a new lift for. Consider the polynomial

$$f(t) := t^3 - t^2 + 2pt - p^3.$$

Then $f(0) = -p^3$ and $f'(t) = 3t^2 - 2t + 2p$ so $f'(0) = 2p$. Thus when $p \neq 2$ we have $|f(0)| < |f'(0)|^2$ and Hensel's lemma applies. So we can find $\alpha \in \mathbb{Z}_p$ with $|\alpha - 0| < |f(0)|/|f'(0)| = 1/p^2$, that is $\alpha \equiv 0 \bmod p^2$, and such that $f(\alpha, p) = 0$. Then we have that $P := (\alpha, p, 1)$ is a desired lift.

When $p = 2$ we can start with the point $(0, p^3)$. Then take $f(t) := t^3 - t^2 + 2p^3t - p^9$. So $f(0) = -p^9$ and $f'(t) = 3t^2 - 2t + 2p^2$ so $f'(0) = 2p^3$. So again we have $|f(0)| < |f'(0)|^2$ and we can lift to find a $P = (\alpha, p^3, 1)$. (Of course this works for any p.)

(ii) [3 marks] We can adapt this by starting instead with $(0, p^3\beta)$ for any $\beta \in \mathbb{Z}_p$. Now consider the polynomial

$$f_\beta(t) := t^3 - t^2 + 2p^3\beta t - p^9\beta^3.$$

Then $f_\beta(0) = -p^9\beta^3$ and $f'_\beta(t) = 3t^2 - 2t + 2p^3\beta$ so $f'_\beta(0) = 2p^3\beta$. Thus always $|f(0)| < |f'(0)|^2$ and Hensel's lemma applies. So we can find $\alpha \in \mathbb{Z}_p$ such that $f(\alpha, p) = 0$. Then we have that $P_\beta := (\alpha, p^3\beta, 1)$ is a desired lift.

(c) [Similar: 6 marks]

The tangent through P has gradient

$$\frac{3x^2 - 2x}{2y}|_{(x,y)=(2,-1)} = -5.$$

So the line is $y = -5x + 9$. Thus x-coordinate of $2P$ is $(-5)^2 - 2 \cdot 2 = 21$, and the y-coordinate is $-(-5 \cdot 21 + 9) = 96$. So $2P = (21, 96)$.

To compute $3P = P + 2P$ we first compute the gradient of the line joining them. It is

$$\frac{96 + 1}{21 - 2} = \frac{97}{19}$$

and so the line is $y = \frac{97}{19}x - \frac{213}{19}$. Thus the x-coordinate of $3P$ is

$$\left(\frac{97}{19}\right)^2 - (21+2) = \frac{1106}{361}$$

and y-coordinate is the negative of

$$\frac{97}{19} \cdot \frac{1106}{361} - \frac{213}{19}$$

which is $-30389/6859$.

The factorisation will be revealed doing the computations modulo 437 and when trying to find the inverse of 19 modulo 437 via Euclid's algorithm discovering that $437 = 19 \cdot 23$.

2. (a) [6 marks] Find the structure of the group $\mathcal{E}(\mathbb{F}_7)$ for the elliptic curves
   i. $\mathcal{E} : y^2 = x^3 + 1$
   ii. $\mathcal{E} : y^2 = x^3 + 3x + 1$.

(b) [4 marks] Compute the torsion subgroup $\mathcal{E}(\mathbb{Q})_{\text{tors}}$ of the curve $\mathcal{E} : y^2 = x^3 + 1$.

(c) [6 marks] Prove that the point $(-1, -1) \in \mathcal{E}(\mathbb{Q})$ on the elliptic curve $\mathcal{E} : y^2 = x^3 + x + 3$ has infinite order.

(d) [9 marks] i. Let $F(X, Y) \in R[[X, Y]]$ be a formal group defined over a ring R. Suppose that R is an integral domain and also $F(X, Y) \in R[X, Y]$, that is to say $F(X, Y)$ is a polynomial. Show that

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

for some $c \in R$.

ii. Let R be an arbitrary (commutative) ring. Prove for any $c \in R$ that $F_c(X, Y) := X + Y + cXY \in R[[X, Y]]$ defines a formal group. Compute the invariant differential for this formal group F_c. Show when R is a field that all of these formal groups F_c with $c \neq 0$ are isomorphic.

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

Solution:

2. (a) [6 marks: Similar and easy] A fairly easily calculation shows that the points are

$$\{O, (0, \pm 1), (1, \pm 3), (2, \pm 3), (3, 0), (4, \pm 3), (5, 0), (6, 0)\}$$

and

$$\{O, (0, \pm 1), (2, \pm 1), (3, \pm 3), (4, 0), (5, \pm 1), (6, \pm 2)\}$$

respectively. So both groups have order 12 so are either C_{12} or $C_2 \times C_6$. Now the former group has one point of order 2, and the latter group 3 points. Points of order 2 have the form $(\star, 0)$, and so looking at the sets one sees the answers are $C_2 \times C_6$ and C_{12} respectively. (Note here no point additions are needed to determine the group.)

(b) [4 marks: Similar] We know from (a) i. this group embeds in $C_2 \times C_6$. But $x^3 + 1$ has only one rational root -1, so we do not have three 2-torsion points but rather 1, and so the

group has order at least 2 and dividing 6. There is the obvious point $Q = (0, 1)$. Now (from problems sheets) one suspects Q is a 3-torsion point. Indeed the tangent at Q has gradient $3x^2/2y = 0$ and is $Y = 1$. Putting this in the equation one gets $1^2 = X^3 + 1$ and so $X^3 = 0$, that is, the tangent line intersects the curve with multiplicity 3, and so $Q+Q+Q = 0$. Thus we have a point of order 3 and the group must be C_6.

(c) [6 marks: Similar] Let $P = (-1, -1)$. Note that $(-1)^2 = 1$ and so you cannot use Nagell-Lutz to prove the point has infinite order. So let us try doubling P. One computes the tangent line has gradient

$$\frac{dy}{dx} = \frac{3x^2 + 1}{2y}|_{(x,y)=(-1,-1)} = -2.$$

So it is $y = -2x - 3$. We have

$$x^3 + x + 3 - (-2x - 3)^2 = (x + 1)^2(x - 6).$$

So the point $2P$ has x-coordinate 6 and y coordinate the negative of $-2 \cdot 6 - 3$, so is $(6, 15)$. This is still integral, but now we can apply Nagell-Lutz. The discriminant is $4a^3+27b^2 = 247$ and 15^2 does not divide 247. So $2P$ cannot have finite order, and thus P cannot have finite order.

(d) (i) [5 marks: New and perhaps tricky] First suppose the degree in X of $F(X, Y)$ is $n \geqslant 2$. As $F(F(X, Y), Z) = F(X, F(Y, Z))$ we have that the degree in X of the LHS is n^2 and of the RHS is n. Here we use that R is an integral domain (or more precisely just has no zero divisors) so if the leading term in X in $F(X, Y)$ is $aX^n g(Y)$ with $g(Y)$ monic then that of the LHS is $a^2X^{n^2}g(Y)^{n+1}$ and $a^2 \neq 0$ (and also as $g(Y)$ is monic $g(Y)^{n+1} \neq 0$). Hence $n^2 = n$ so we must have $n \leqslant 1$. Likewise to see the degree in Y is $\leqslant 1$ consider the degree in Z of both sides of $F(F(X, Y), Z) = F(X, F(Y, Z))$. Finally we know $F(X, Y) = X + Y +$ higher order terms , so it must be of the given form.

(ii) [1 mark: New and trivial] The only axiom that really needs checking is that

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

that is

$$(X + Y + cXY) + Z + c(X + Y + cXY)Z = X + (Y + Z + cYZ) + cX(Y + Z + cYZ).$$

And indeed both sides equal

$$X + Y + Z + c(XY + XZ + YZ) + c^2XYZ.$$

[1 mark: New and easy] From the notes the invariant differential is "$F_X(0, T)^{-1}dT$ which is $dT/(1 + cT)$.

[2 marks: New and not hard] Let $c \neq 0$ and define $f(T) := cT \in TR[T]$. Note this power series has a functional inverse T/c since R is a field. One checks

$$f(F_c(X, Y)) = F_1(f(X), f(Y))$$

that is

$$c(X + Y + cXY) = cX + cY + cXcY.$$

So f gives an isomorphism from F_c to F_1, and so all such F_c are isomorphic.

3. (a) [15 marks] Let p be a prime with $p \equiv 1 \bmod 4$. Assume that 2 is not a fourth power modulo p.

i. Prove that the affine curve $2Y^2 = X^4 - p$ has no points in $\mathbb{Q}$.

ii. Show that the rank of the curve $y^2 = x(x^2 + p)$ is at most 1.

(b) [10 marks] Compute the Mordell-Weil group of the curve $y^2 = x(x^2 + 7x - 10)$.

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

Solution:

(a) [The point of (a) is local methods will not always work: when 2 is a quadratic residue mod p there is non-trivial 2-torsion in Sha.]

(i) [Similar 8 marks in total: The case $p = 17$ is on the problem sheets. The proof is very similar, but it will require care to adapt the argument to get full marks.]

Suppose that $(x, y) \in \mathbb{Q}^2$ is a solution. Write $x = t/r$ where $\gcd(r, t) = 1$. Then $2y^2 = (t/r)^4 - p$, that is $2(yr^2)^2 = t^4 - pr^4 \in \mathbb{Z}$. Hence $2(yr^2)^2 \in \mathbb{Z}$. It follows that $yr^2 \in \mathbb{Z}$ (since any denominator when squared cannot be cancelled by the 2).

So let $yr^2 = s \in \mathbb{Z}$. Our equation becomes

$$2s^2 = t^4 - pr^4$$

in integers.

First let's consider the easy case that 2 is not a square mod p. Reducing our equation we get $2s^2 \equiv t^4 \bmod p$. If $p|s$ we get $p|t$ and hence $p^2|(2s^2 - t^4) = -pr^4$, so $p|r$, a contradiction. So p does not divide s and we get $2 \equiv (t^2/s)^2 \bmod p$, a contradiction.

So we can assume now that 2 is a square modulo p. (This is the interesting case where we cannot use a local argument.)

Let ℓ be a prime dividing s. Now we have assumed that if $\ell = 2$, then ℓ is a square modulo p. So let ℓ be odd. We shall prove again that ℓ is a square modulo p.

We get $t^4 \equiv pr^4 \bmod \ell$. Now if $\ell|r$ then also $\ell|t$, a contradiction. So we have $(t/r)^4 \equiv p \bmod \ell$. In particular p is a square modulo ℓ, that is, either $p \equiv 0 \bmod \ell$ or

$$\left(\frac{p}{\ell}\right) = 1.$$

In the former case we have $\ell = p$ and so from our equation we find $p|r$ and $p|t$, a contradiction. So in fact $\ell \neq p$.

In the latter case as $p \equiv 1 \bmod 4$ and since ℓ is odd we deduce by quadratic reciprocity that

$$\left(\frac{\ell}{p}\right) = 1.$$

Since all primes dividing s are (non-zero) squares modulo p, we deduce also that s is a (non-zero) square modulo p. So write $s = \alpha^2 \bmod p$. Then reducing our equation modulo p we get

$$2\alpha^4 \equiv t^4 \bmod p.$$

We have already seen that $\alpha \neq 0 \bmod p$, so finally we get

$$2 \equiv (t/\alpha)^4 \bmod p.$$

This contradicts our assumption on p.

(ii) [Similar 7 marks in total] Using notation in lectures we have $a = 0$, $b = p$ and $a_1 = 0$, $b_1 = -4p$.

[1 mark] For $\mathcal{H}/\phi(\mathcal{G})$ we need to consider $r \in \{\pm 1, \pm 2, \pm p, \pm 2p\}$. We have $q(0) = 1$ and $q((0,0)) = -4p \equiv -p$.

[3 marks] For $r = 2$, suppose we have a solution to $2\ell^4 - 2pm^4 = n^2$, with ℓ, m, n not all zero etc. As n must be even putting $n = 2k$ we get $\ell^4 - pm^4 = 2k^2$. Note we cannot have $m = 0$ (looking at powers of 2 on both sides) so dividing through get

$$2\left(\frac{k}{m^2}\right)^2 = \left(\frac{\ell}{m}\right)^4 - p.$$

This contradicts our result from (a)(i).

[1 mark] For $r = p$ we get $p\ell^4 - 4m^4 = n^2$. If this has a solution there is a point $Q \in \mathcal{H}$ with $q(Q) = p$.

[1 mark] For $\mathcal{G}/\hat{\phi}(\mathcal{H})$ we need to consider $r \in \{\pm 1, \pm p\}$. Since $a = 0$ and $b > 0$ the homogeneous space will have no solutions for $r < 0$. Thus $\mathrm{Im}(\hat{q}) = \{1, p\}$.

[1 mark] Putting these together we get $\mathcal{G}/2\mathcal{G}$ is generated by either $(0,0)$ or, when Q above exists, $(0,0), \hat{\phi}(Q)$. So has rank $\leqslant 2$. Since $x^2 + p$ is irreducible the 2-torsion has rank 1 and we get rank $\leqslant 1$ for the Mordell-Weil group.

(b) [New, but similar to lectures and problem sheets. Having rank 2 is a bit unusual.]

(This question is a bit easier than in 2020 since one doesn't need to do anything with points in $\mathcal{H}$.)

Following notation in the lecture notes, we have $a = 7$, $b = -10$, $a_1 = -2a = -14$, $b_1 = a^2 - 4b = 89$. Thus $\mathcal{D} : v^2 = u(u^2 - 14u + 89)$.

[3 marks] To compute the torsion since $b(a^2 - 4b) = -10 \cdot 89 \neq 0 \bmod p$ for $p = 3, 7$ 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 $O, (0,0), (2, \pm 3), (3, \pm 2), (6, \pm 3)$. Thus the torsion order divides $\gcd(6, 8) = 2$, and must be 2.

We now apply descent.

[2 marks] Thus for $\mathcal{H}/\phi(\mathcal{G})$ we need to consider $r \in \{\pm 1, \pm 89\}$, and we have $q(0) = 1$, $q((0,0)) = b_1 = 89$. Since $a_1 \leqslant 0$ the equations W_r for r negative have no solutions in $\mathbb{R}$, hence none in $\mathbb{Q}$.

[3 marks] For $\mathcal{G}/\hat{\phi}(\mathcal{H})$ we need to consider $r \in \{\pm 1, \pm 2, \pm 5, \pm 10\}$. We have as usual $q(0) = 1$ and $q((0,0)) = b = -10$. By inspection one (eventually) finds the points $(-1, 4)$ and $(2, 4) \in \mathcal{G}$ and $\hat{q}((-1, 4)) = -1$, $\hat{q}((2, 4)) = 2$. So we have $\mathrm{Im}(\hat{q}) = \langle -1, 2, -10 \rangle \cong C_2^3$.

[1 mark] Thus $\mathcal{G}/2\mathcal{G}$ is generated by $(0,0), (-1, -4), (2, 4)\hat{\phi}((0,0))(= O)$ so is isomorphic to C_2^3.

[1 mark] Since $x^2 + 7x - 10$ has no rational roots (its discriminant is 89) the 2-torsion is C_2, so the rank is $3 - 1 = 2$.