1. (a) [15 marks]

(i) Let $\mathcal{C}$ be a non-singular projective cubic curve defined over a field K, with a K-rational point $\underline{\mathbf{o}}$. Describe the standard law for adding two points on $\mathcal{C}$, and prove that it is associative.
[*Standard results from geometry may be assumed provided they are clearly stated. For associativity, you may assume points are in a suitably "general position". You do not need to describe the inverse of a point, verify other group axioms, or check that $\mathcal{C}(K)$ is a subgroup.*]

(ii) Now let $\mathcal{C}$ be the non-singular projective curve $X^3 + Y^3 + Z^3 = 0$ over the field $\mathbb{F}_5$ and $\underline{\mathbf{o}} = (1, 2, 1)$. Compute the sum $\mathbf{a} + \mathbf{b}$ where $\mathbf{a} = (2, 1, 1)$ and $\mathbf{b} = (3, 3, 1)$ are points in $\mathcal{C}(\mathbb{F}_5)$.
[*It may simplify your calculations to first list all the points in $\mathcal{C}(\mathbb{F}_5)$.*]

(b) [10 marks] Let $p \neq 3, 5$ be a prime and $f(x, y) = 3x^3 + 4y^3 - 5$.

(i) Show that at least one element of the set $\{3, 5, 15, 45\}$ must be a cube modulo p.
[*It may help to consider the quotient group of $(\mathbb{Z}/p\mathbb{Z})^*$ modulo cubes.*]

(ii) If 3 is a cube modulo p then show that there exists $x \in \mathbb{Q}_p$ with $f(x, 1) = 0$.

(iii) If 5 is a cube modulo p then show that there exists $x \in \mathbb{Q}_p$ with $f(x, -x) = 0$.

(iv) If 15 is a cube modulo p then show that there exists $x \in \mathbb{Q}_p$ with $f(x, \frac{5}{7}) = 0$.

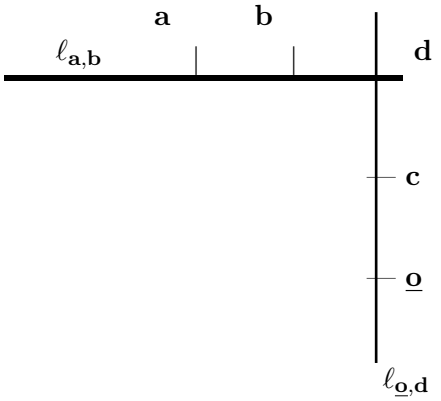
(v) If 45 is a cube modulo p then show that there exists $x \in \mathbb{Q}_p$ with $f(x, 0) = 0$.

[*Hensel's lemma may be used without proof provided it is clearly stated.*]

Solution 1.

(a) (i) [Bookwork: 10 marks] (See page 1-2 of the course notes.)

Let C be a nonsingular projective cubic curve, with a K-rational point, which we shall denote $\underline{\mathbf{o}}$. For any two points $\mathbf{a}, \mathbf{b}$ on C, let $\ell_{\mathbf{a},\mathbf{b}}$ denote the line which meets C at $\mathbf{a}, \mathbf{b}$ [if $\mathbf{a}, \mathbf{b}$ are distinct then $\ell_{\mathbf{a},\mathbf{b}}$ is the unique line through $\mathbf{a}, \mathbf{b}$; if $\mathbf{a} = \mathbf{b}$ then $\ell_{\mathbf{a},\mathbf{b}}$ is the line tangent to C at $\mathbf{a} = \mathbf{b}$].

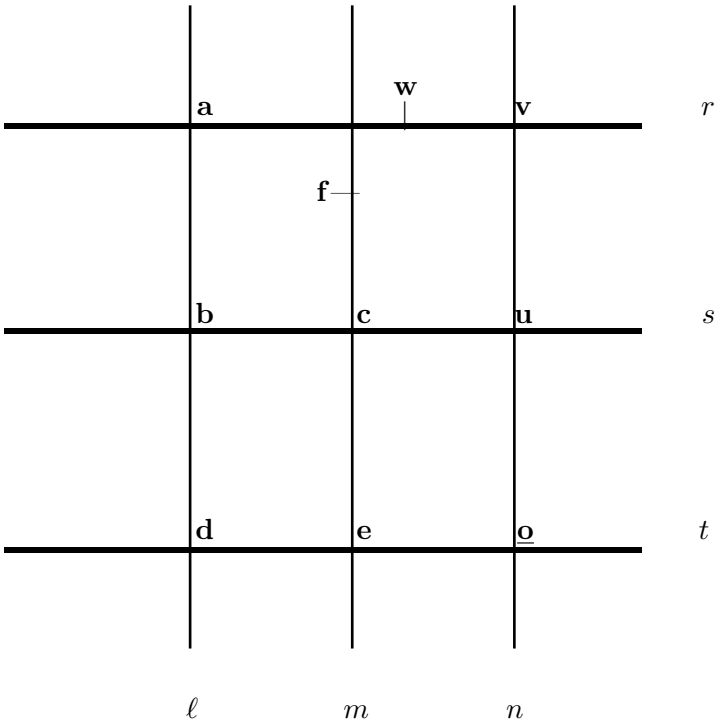


Let $\ell_{\mathbf{a},\mathbf{b}}$ denote the line which meets C at $\mathbf{a}, \mathbf{b}$.
Then $\ell_{\mathbf{a},\mathbf{b}}$ and C have 3 points of intersection (Bézout).
Let $\mathbf{d}$ be the third point of intersection between C and $\ell_{\mathbf{a},\mathbf{b}}$.
Now, let $\ell_{\underline{\mathbf{o}},\mathbf{d}}$ denote the line which meets C at $\underline{\mathbf{o}}$ and $\mathbf{d}$.
Let $\mathbf{c}$ be the third point of intersection between C and $\ell_{\underline{\mathbf{o}},\mathbf{d}}$.
Define $\mathbf{a} + \mathbf{b} = \mathbf{c}$.

For associativity we need the following technical lemma.

Lemma: Let $P_1, \ldots, P_8$ be such that no 4 points lie on a line and no 7 points lie on a conic. Then there exists a unique point P_9 which is a 9th point of intersection of any two cubics passing through $P_1, \ldots, P_8$.

In order to prove associativity, consider the following diagram.



Here, r, s, t, ℓ, m, n are lines. On each line, the labelled points are the points of intersection between C and that line. From the definition of addition:

$$\mathbf{a} + \mathbf{b} = \mathbf{e},$$

and so:

$$(\mathbf{a} + \mathbf{b}) + \mathbf{c} = \text{3rd point of intersection on } \ell_{\underline{\mathbf{o}},\mathbf{f}}.$$

Similarly:

$$\mathbf{b} + \mathbf{c} = \mathbf{v},$$
$$\mathbf{a} + (\mathbf{b} + \mathbf{c}) = \text{3rd point of intersection on } \ell_{\underline{\mathbf{o}},\mathbf{w}}.$$

To show $(\mathbf{a} + \mathbf{b}) + \mathbf{c} = \mathbf{a} + (\mathbf{b} + \mathbf{c})$, it is sufficient to show that $\mathbf{f} = \mathbf{w}$. Let $F_1 = \ell mn$ and $F_2 = rst$, both of which are cubic curves.

C and F_1 have 8 common points: $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}, \mathbf{u}, \mathbf{v}, \underline{\mathbf{o}}$.

C and F_2 also have these 8 common points: $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}, \mathbf{u}, \mathbf{v}, \underline{\mathbf{o}}$.

From the Lemma, the 9th point of intersection of C and F_1 must be the same as the 9th point of intersection of C and F_2; that is, $\mathbf{f} = \mathbf{w}$, as required.

(ii) [New: 5 marks. *They have not actually applied the point addition formula above except for an elliptic curve in standard form.*]

In affine coordinates the equations is $x^3 + y^3 + 1 = 0$, that is $y^3 = -x^3 - 1$. Cubing is a bijection on $\mathbb{F}_5$ and so the affine points are easily found to be

$$(1, 2), (2, 1), (3, 3), (4, 0), (0, 4).$$

We have $\mathbf{a} = (2, 1), \mathbf{b} = (3, 3)$. The line joining $\mathbf{a}$ and $\mathbf{b}$ is $y = 2x - 3$. By inspection the other point on this line is $\mathbf{d} = (4, 0)$. The line joining $\mathbf{d} = (4, 0)$ and $\underline{\mathbf{o}} = (1, 2)$ is $y = x + 1$. By inspection no other affine point satisfies this equation. Now the point at infinity is $(-1, 1, 0)$ and this does not lie on the projective line $Y = X + Z$. So our line must be tangent to the

curve at one of the two points. By calculus the gradient at a point (x, y) is $\frac{dy}{dx} = -\frac{x^2}{y^2}$ and indeed the gradient at $\underline{\mathbf{o}}$ is $-\frac{1}{4} \equiv 1$. So the third point of intersection is $\underline{\mathbf{o}}$. So overall $\mathbf{a}+\mathbf{b} = \underline{\mathbf{o}}$.

(b) [New, but solving different equations using Hensel's lemma is in the problem sheets]

(i) [4 marks] (This argument is due to Kevin Buzzard.) The quotient group of $(\mathbb{Z}/(p\mathbb{Z}))^\star$ modulo cubes either has order 3 or 1, depending upon whether $p \equiv 1$ or $p \equiv 2 \bmod 3$. In the latter case all non-zero residues are cubes. In the former case, let α and β respectively be the images of 3 and 5 in this quotient. So, written additively, $\alpha, \beta \in \{0, 1, 2\}$. If either of them are zero then one of 3 or 5 is a cube. Otherwise we $(\alpha, \beta) = (1, 2), (2, 1), (1, 1), (2, 2)$. In the first two cases $\alpha+\beta = 0$ and so $3{\cdot}5$ is a cube. In the second two cases $2\alpha+\beta = 0$ and so $3^2{\cdot}5$ is a cube.

(ii) [1 mark] In this case the equation becomes $3x^3 = 1 \bmod p$ and since 3 is a cube so is $1/3$. Now apply Hensel's lemma to get a solution in $\mathbb{Q}_p$.

(iii) [1 mark] Here the equation is $(-x)^3 = 5 \bmod p$ and since 5 is a cube we can solve this as before.

(iv) [3 marks] Here the equation becomes $3(7x)^3+4{\cdot}5^3 = 5{\cdot}7^3$ and so $3(7x)^3 = 5{\cdot}7^3-4{\cdot}5^3 = 3^5{\cdot}5$. (Note $7^3 - 4 \cdot 5^2 = 343 - 100 = 243 = 3^5$.) Multiplying by 3^2 we get $(21x)^3 = 3^6 \cdot 15 \bmod p$, and since 15 is a cube we can solve this as before.

(v) [1 mark] Here we can write the equation as $3^2 \cdot 3x^3 = 3^2 \cdot 5 \bmod p$, that is $(3x)^3 = 45 \bmod p$, which we can solve.

2. (a) [10 marks] Let R be a commutative ring with an identity. Let F and G be formal groups defined over R and let $f(T) \in TR[[T]]$ be a homomorphism from F to G.
   (i) Assume $g(T) \in TR[[T]]$ is such that $f(g(T)) = g(f(T)) = T$. Prove that $g(T)$ is a homomorphism from G to F.
   (ii) Let ω_F and ω_G be the normalised invariant differentials on F and G, respectively. Show that $\omega_G \circ f = f'(0)\omega_F$.
   [*You may assume that every invariant differential on F is of the form $a\omega_F$ for some $a \in R$.*]
   (iii) Deduce that for any prime p there exists $a, b \in R[[T]]$ such that $[p](T) = pa(T)+b(T^p)$. (Here $[p](T)$ denotes the multiplication by p map in the formal group F.)

   (b) [9 marks] Now let R be a commutative ring with an identity and consider the formal multiplicative group
$$\hat{G}_m(X, Y) = X + Y + XY.$$
   (i) Let p be prime and $[p](T)$ be the multiplication by p map on the formal group $\hat{G}_m(X, Y)$. Find explicitly $a(T), b(T) \in R[[T]]$ such that $[p](T) = pa(T) + b(T^p)$.
   (ii) With $[p](T)$ as in part (b)(i), assume now that R is a field of characteristic zero. Write down explicitly a series $g(T) \in TR[[T]]$ with $[p](g(T)) = g([p](T)) = T$, justifying your answer.
   (iii) Let $n \geqslant 1$ be an integer. Using your construction in part (b)(ii), show that the rational number
$$\frac{\frac{1}{p}\left(\frac{1}{p}-1\right)\left(\frac{1}{p}-2\right)\cdots\left(\frac{1}{p}-n+1\right)}{n!}$$
   when written in reduced form has denominator a power of p.

   (c) [6 marks] Let P be the point $(1, -1)$ on the elliptic curve $y^2 = x^3 + 5x - 5$. Using the Elliptic Curve Method, factorise 2491 by attempting to calculate $4P$.

Solution: (a) (i) [3 marks. *This argument is mentioned in lectures but is not in the actual lecture notes.*]

We have $f(F(X, Y)) = G(f(X), f(Y))$, since f is a homomorphism. Evaluating $g(T)$ on both sides and using that $g(f(T)) = T$ we get that $F(X, Y) = g(G(f(X), f(Y))$. Now put $X = g(X_1)$ and $Y = g(Y_1)$ and use that $f(g(T)) = T$ to get $F(g(X_1), g(Y_1) = g(G(X_1, Y_1))$.

(ii) [4 marks. Bookwork.]

First, note that $\omega_G \circ f\big(F(T, S)\big) = \omega_G\big(G(f(T), f(S))\big) = \omega_G \circ f(T)$, so that $\omega_G \circ f$ is an invariant differential on F. From the italicised hint, it follows that $\omega_G \circ f = a\ \omega_F$, for some $a \in R$. Since ω_F, ω_G are normalised, $(1 + \cdots)\mathrm{d}f(T) = a(1 + \cdots)\mathrm{d}T$, and so $(1 + \cdots)f'(T)\mathrm{d}T = a(1 + \cdots)\mathrm{d}T$; equating constant terms gives $a = f'(0)$, as required.

(iii) [3 marks. Bookwork.]

Let ω be the normalised invariant differential on F. Since $[p](T) = pT + \ldots$, it satisfies $[p]'(0) = p$. Applying the previous result to $[p]$, a homomorphism from F to itself, gives: $\omega \circ [p] = [p]'(0)\omega = p\omega$, and so

$$p\omega(T) = \omega \circ [p](T) = (1 + \ldots)\mathrm{d}([p](T)) = (1 + \ldots)[p]'(T)\mathrm{d}T.$$

Hence $[p]'(T) \in p\, R_T$. Each term $a_n T^n$ in $[p](T)$ must then satisfy $p|na_n$ in R, and so $p|n$ in $\mathbb{Z}$ or $p|a_n$ in R, as required.

(b) (i) [3 marks. *New: this is an illustration of Corollary 4.13 (part (a)(ii)) in the notes but looking at the proof will not help much.*]

The group operation is just $(1+X)(1+Y)-1$ (key observation) and so $[p](T) = (1+T)^p - 1$. Now we know $(1+T)^p - 1 \equiv 1 + T^p - 1 \equiv T^p \bmod p$. So we can take $b(T) = T$ (so $b(T^p) = T^p$) and

$$a(T) = \frac{(1+T)^p - (1+T^p)}{p}.$$

(ii) [3 marks: *New.*]

Intuitively one sees that $g(T) = (1+T)^{1/p} - 1$ should work. For indeed it can be expanded as a series

$$\sum_{n=1}^{\infty} \binom{1/p}{n} T^n \in TR[[T]].$$

Note all the binomial coefficients lie in R since it must contain a copy of $\mathbb{Q}$. Moreover

$$[p](g(T)) = (1 + (1+T)^{1/p} - 1)^p - 1 = T,\ g([p](T)) = (1 + (1+T)^p - 1)^{1/p} - 1 = T.$$

(iii) [3 marks: *New.*]
The rational number is our binomial coefficient from (ii). Now if in (ii) we take instead $R = \mathbb{Z}[1/p]$ so that $p \in R^*$ then Lemma 4.7 in the lecture notes tells us a unique $g(T) \in TR[[T]]$ exists with $[p](g(T)) = T$. Now such $g(T)$ must also be the unique functional inverse taking R to be the field of fractions $\mathbb{Q}$ of $\mathbb{Z}[1/p]$. Thus our $g(T)$ must be the power series written above, and so all the coefficients of this series lie in $\mathbb{Z}[1/p]$.

(c) [6 marks: *Similar.*]

The gradient of the tangent at a point (x, y) on the curve is $\frac{dy}{dx} = \frac{3x^2+5}{2y}$. So at $P = (1, -1)$ we get gradient -4. Hence the tangent line is $y = -4x + 3$. Putting into the equation of the curve gives

$$(-4x+3)^2 = x^3 + 5x - 5$$

and so

$$x^3 - (-4x)^2 + \cdots = 0.$$

Looking at the coefficient of x^2 we get $1 + 1 + x_3 = 16$ where (x_3, y_3) is the third point of intersection of the tangent line with the curve. So this point is $(14, -4 \cdot 14 + 3) = (14, -53)$. Hence $2P = (14, 53)$. (Note this point has order 2 modulo 53 which tells us already that $4P$ is the identity modulo 53 and the doubling will break down modulo any multiple of 53.)

The gradient of the tangent at $2P$ is

$$\frac{3 \cdot 14^2 + 5}{2 \cdot 53}.$$

So we need to attempt to compute the inverse of 53 modulo 2491and some long division then reveals $2491 = 53 \cdot 47$.

3. (a) [9 marks] Compute the Mordell-Weil group of the curve $y^2 = x(x^2 + x - 1)$.

(b) [16 marks] Let p be a prime number such that $s = p - 2$ is also prime. Consider the elliptic curve

$$\mathcal{E}_p : y^2 = x(x-2)(x-p).$$

(i) Show that the rank of $\mathcal{E}_p$ is at most 2.

(ii) When $p \equiv 3 \bmod 8$ show that the rank of $\mathcal{E}_p$ is at most 1. [*It may help to observe that the curve* $v^2 = u(u^2 + 42u + 289)$ *has the point* $(17/16, 1207/64)$.]

(iii) What is the rank of $\mathcal{E}_{19}$? Briefly justify your answer.

Solution:

(a) [*Routine and similar to questions in lectures and notes.*] Following notation in the lecture notes, we have $a = 1$, $b = -1$, $a_1 = -2a = -2$, $b_1 = a^2 - 4b = 5$. Thus $\mathcal{D} : v^2 = u(u^2 - 2u + 5)$.

So for $\mathcal{H}/\phi(\mathcal{G})$ we need to consider $r \in \{\pm 1, \pm 5\}$, and we have $q(0) = 1$, $q((0,0)) = b_1 = 5$. For $r = -1$ we have $W_{-1} : -\ell^4 - 2\ell^2 m^2 - 5m^4 = n^2$. But we see this has no non-trivial solutions since always $LHS \leqslant 0$ and $RHS \geqslant 0$.

Hence $\mathcal{H}/\phi(\mathcal{G}) = \langle (0,0) \rangle \cong C_2$.

For $\mathcal{G}/\hat{\phi}(\mathcal{H})$ we need to consider $r \in \{\pm 1\}$, and $\hat{q}(0) = 1$, $\hat{q}((0,0)) = b = -1$. So $\mathcal{G}/\hat{\phi}(\mathcal{H}) = \langle (0,0) \rangle$.

Overall $\mathcal{G}/2\mathcal{G}$ is generated by $(0,0)$ and $\hat{\phi}((0,0)) = \underline{o}$, so is C_2. Since the two torsion of our curve is C_2 we get rank $1 - 1 = 0$.

For the torsion subgroup, the reduction is smooth mod p provided $b_1 = 5 \neq 0 \mod p$. So we can look modulo 3 and find the points are $\{(0,1), (0,0), (1,1), (1,2), (2,1), (2,2)\}$. So the torsion has order 2 or 6. But aside from the point $(0,0)$ on the curve there is the obvious point $(1,1)$. So the torsion subgroup must have order 6. (Now we don't know whether $(1,1)$ has order 3 or 6 (it has order 3) but this is not necessary to answer the question.)

Hence the Mordell-Weil group is isomorphic to C_6.

(b) [*Part (i) is fairly straightforward and similar to other questions. The method used for (ii) has been seen before in many other exam questions, but the execution of this method is quite delicate. Part (iii) is an original argument not seen before. The notation s for* $p - 2$ *is introduced in the question just to make marking it easier for me.*]

(i) [8 marks] We have $x(x-2)(x-p) = x(x^2 - (2+p)x + 2p)$ and so $a = -(p+2), b = 2p, a_1 = -2a = 2(p+2)$ and $b_1 = a^2 - 4b = (p+2)^2 - 8p = (p-2)^2 = s^2$. Thus $\mathcal{D} : v^2 = u(u^2 + 2(p+2)u + (p-2)^2)$.

So for $\mathcal{H}/\phi(\mathcal{G})$ we need to consider $r | s^2$, that is $\{\pm 1, \pm s\}$, and we have $q(0) = 1$, $q((0,0)) = b_1 = 1$. So we know that this quotient is C_2^a where $0 \leqslant a \leqslant 2$.

For $\mathcal{G}/\hat{\phi}(\mathcal{H})$ we need to consider $r | 2p$ and so in $\{\pm 1, \pm 2, \pm p\}$, and $\hat{q}(0) = 1$, $\hat{q}((0,0)) = b = 2p$. But notice that $a = -(p+2) < 0$ and $b = 2p > 0$ so by the usual argument we can rule out negative r (since $LHS \leqslant 0$ and $RHS \geqslant 0$ etc). But also we have that $q((2,0)) = 2$ and $q((p,0)) = p$ and so this quotient is C_2^2.

Overall $\mathcal{G}/2\mathcal{G}$ is generated by a C_2^2 and "$\hat{\phi}(C_2^a)$" the latter having rank between 0 and 2. (Note that though $\hat{\phi}((0,0)) = \underline{o}$ it was already trivial in the first quotient.) Thus we have at most a

C_2^{a+2}, that is at most a C_2^4. Now the two torsion of the curve is C_2^2 and so the rank is at most 2.

(ii) [6 marks] To reduce the rank we need to consider $\mathcal{H}/\phi(\mathcal{G})$. We should try and prove that one of the following homogenous spaces has no suitable points:

$r = -1$: Here $\hat{W}_{-1} : -\ell^4 + 2(s+4)\ell^2 m^2 - s^2 m^4 = n^2$.

$r = s$: Here $\hat{W}_s : s\ell^4 + 2(s+4)\ell^2 m^2 + s m^4 = n^2$.

But from the hint when $p = 19$ the equation $\hat{W}_{17}$ does have a solution. So this indicates we should prove that $\hat{W}_{-1}$ has no suitable solution.

Note that when ℓ and m are both even then n is. So at least one of ℓ and m must be odd.

Assume $p \equiv 3 \bmod 8$ and so $s \equiv 1 \bmod 8$. Suppose first ℓ and m are both odd. Then $\ell^4, m^4 \equiv 1 \bmod 16$ and $\ell^2 m^2 = 1, 9 \bmod 16$. Also $s^2 \equiv 1 \bmod 16$ and $2(s+4) \equiv 10$ or $26 \equiv 10 \bmod 16$. Note that always $2(s+4)\ell^2 m^2 \equiv 10$ or $90 \equiv 10 \bmod 16$. So we get

$$\hat{W}_{-1} : -1 + 10 - 1 = n^2 \bmod 16$$

which is impossible as 8 is not a square modulo 16.

Next assume ℓ is odd and m is even. Then $\ell^2 m^2 \equiv 0$ or $4 \bmod 16$ and $m^4 \equiv 0 \bmod 16$. Hence $2(s+4)\ell^2 m^2 \equiv 0$ or $8 \bmod 16$. So we have

$$\hat{W}_{-1} : -1 + 0 - 0 = n^2 \bmod 16 \text{ or } -1 + 8 - 0 \equiv n^2 \bmod 16$$

which is impossible as the squares modulo 16 are $0, 1, 4, 9$.

Finally assume ℓ is even and m is odd. Since $s^2 \equiv 1 \bmod 16$ the equation $\hat{W}_{-1}$ modulo 16 is symmetrical in ℓ and m and the preceding argument applies.

So we conclude that $\hat{W}_{-1}$ has no suitable solutions, and hence $\mathcal{H}/\phi(\mathcal{G})$ has 2-rank either 0 or 1, which reduces our rank bound to 1. [Added: An alternative argument starts with $\ell^4 + 2(2+p)\ell^2 m^2 - (p-2)^2 m^2 = n^2$ and reduces it modulo p to get $-(\ell - 2m^2) = n^2 \bmod p$. As $p \equiv 3 \bmod 8$ we have -1 is not a square modulo p, and hence find in particular that $\ell - 2m^2 \equiv 0 \bmod p$. Then we see that unless $p|m$ we can write $2 = (\ell/m)^2 \bmod p$ and this contradicts that 2 is not a square modulo p etc.]

(iii) [2 marks] The rank is 1. We are told by the hint that $\hat{W}_{17}$ has a solution, which should prove the rank is 1 except that the theory in the lecture notes does not guarantee that $\hat{\phi}((17/16, 1207/64))$ is independent of the other points we already have in $\mathcal{G}/2\mathcal{G}$. However, if we let $Q = \hat{\phi}((17/16, 1207/64))$ and suppose this point has finite order m then

$$[m][2](17/16, 1207/64) = [m]\phi(\hat{\phi}((17/16, 1207/64))) = [m]\phi(Q) = \phi([m]Q) = \phi(\underline{o}) = \underline{o}$$

which shows $(17/16, 1207/64)$ has order dividing $2m$. But this is impossible since it is not integral. [Added: In fact Sheet 4 Question 3 of the revised sheets for 2021-22 guarantees independence.]