# Solutions to January 2003 Examination. MATH444.

**Question 1.** *Part (a) is a straightforward variation of questions both on the example sheets and in lectures. Parts (b),(c) are harder variations of three medium-level-difficulty questions on the exercise sheets, but are not similar to any examples in lectures.*

**(a).** The point $(x,y)$ on $f(X,Y)=Y^2-(X-1)^4(X^3+1)=0$ is singular if $f(x,y)=0$, $(\partial f/\partial X)(x,y)=-4(x-1)^3(7x^3-3x^2+4)=0$ and $(\partial f/\partial Y)(x,y)=2y=0$. An immediate common solution is $x=1,y=0$, so that $(1,0)$ is a singular point [note that the question did *not* ask "find all singular points on the curve" and so it is not necessary to justify here the fact that $(1,0)$ is the only singular point]. $f(X+1,Y+0)=Y^2-X^4((X+1)^3+1)=Y^2+$ terms of higher degree, and so there are two tangents at $(1,0)$, namely $Y-0=0$ twice; that is: $Y=0$ twice.

The curve $\mathcal{C}:Y^2=(X-1)^4(X^3+1)$ can be written as $(Y/(X-1)^2)^2=(X^3+1)$, so that the birational transformation $(X,Y)\mapsto(X,Y/(X-1)^2)$ [with inverse $(X,Y)\mapsto(X,Y(X-1)^2)$] maps $\mathcal{C}$ to the curve $Y^2=X^3+1$, which is of the required form. **[8 marks]**

**(b).** Let $\mathcal{C}_0:Y^2=4X^6+2X^5+X^2+6X+1$. Then the birational transformation $(X,Y)\mapsto(2X,4Y)$ [with inverse $(X,Y)\mapsto(X/2,Y/4)$] maps $\mathcal{C}_0$ to the curve $\mathcal{C}_1:(Y/4)^2=4(X/2)^6+2(X/2)^5+(X/2)^2+6(X/2)+1$; multiplying both sides by 16 rearranges this as: $\mathcal{C}_1:Y^2=X^6+X^5+4X^2+48X+16$, which is of the first required form.

Starting at $\mathcal{C}_0$ again, the birational transformation $(X,Y)\mapsto(1/X,Y/X^3)$ [with inverse: $(X,Y)\mapsto(1/X,Y/X^3)$] maps $\mathcal{C}_0$ to the curve $\mathcal{C}_2:(Y/X^3)^2=4(1/X)^6+2(1/X)^5+(1/X)^2+6(1/X)+1$, and on multiplying both sides by $X^6$, we get: $\mathcal{C}_2:Y^2=4+2X+X^4+6X^5+X^6$, which is the same as $\mathcal{C}_2:Y^2=X^6+6X^5+X^4+2X+4$, which is of the second required form.

Then the birational transformation $(X,Y)\mapsto(X+1,Y)$ [with inverse $(X,Y)\mapsto(X-1,Y)$] maps $\mathcal{C}_2$ to the curve $\mathcal{C}_3:Y^2=(X-1)^6+6(X-1)^5+(X-1)^4+2(X-1)+4$; that is: $\mathcal{C}_3:Y^2=X^6-14X^4+36X^3-39X^2+22X-5$, which is of the third required form. **[7 marks]**

**(c).** Let $\mathcal{D}_1:Y^2=-X^4+2X^2-2$. The birational transformation $(X,Y)\mapsto(X,Y/i)$ [with inverse $(X,Y)\mapsto(X,iY)$] maps $\mathcal{D}_1$ to the curve $\mathcal{D}_2:(iY)^2=-X^4+2X^2-2$; that is $\mathcal{D}_2:Y^2=X^4-2X^2+2$. Rewrite $\mathcal{D}_2$ as $Y^2=X^4-2X^2+2=(X^2-1)^2+1$, which is the same as: $\mathcal{D}_2:(Y+X^2-1)(Y-(X^2-1))=1$, or $\mathcal{D}_2:(Y+X^2-1)(Y+X^2-1-2((X(Y+X^2-1)/(Y+X^2-1))^2-1))=1$, from which it is clear that that the birational transformation $(X,Y)\mapsto(Y+X^2-1,X(Y+X^2-1))$ [with inverse $(X,Y)\mapsto(Y/X,X-(Y/X)^1+1)$] maps $\mathcal{D}_2$ to $\mathcal{D}_3:X(X-2((Y/X)^2-1))=1$, which can be rearranged as: $2Y^2=X^3+2X^2-X$. Finally, the birational transformation $(X,Y)\mapsto(2X,4Y)$ [with inverse $(X,Y)\mapsto(X/2,Y/4)$] maps $\mathcal{D}_3$ to $\mathcal{D}_4:2(Y/4)^2=(X/2)^3+2(X/2)^2-(X/2)$; that is: $Y^2=X^3+4X^2-4X$, as required. **[6 marks]**

This is not possible over $\mathbf{R}$, since $Y^2=-X^4+2X^2-2$ is the same as $Y^2=-(X^2-1)^2-1$, which has no points over $\mathbf{R}$, whereas $Y^2=X^3+AX^2+BX$ has infinitely many (for $X$ sufficiently large). Since there is no birational transformation over $\mathbf{R}$ there must also be none over $\mathbf{Q}(\sqrt{2})$. However, the map $(X,Y)\mapsto(1/X,Y/X^2)$ [with inverse $(X,Y)\mapsto(1/X,Y/X^2)$] maps our curve to $(Y/X^2)^2=-(1/X)^4+2(1/X)^2-2$, which is the same as $Y^2=-2X^4+2X^2-1$. Since the coefficient of $X^4$ is a square in $\mathbf{Q}(\sqrt{-2})$, the same procedure as before will clearly take us to the form $Y^2=X^3+AX^2+BX$, and so it is possible over $\mathbf{Q}(\sqrt{-2})$. **[4 marks]**

**Question 2.** *Parts (a),(b) are straightforward variations of problems on exercise sheets. Parts (c).(d) are unseen, although they have seen the $x\mapsto x^3$ injective trick in another context.*

**(a).** Let $x_0=a_0=3$. Then $|x_0^2+2|_{11}=11^{-1}$. Look for $x_1=a_0+11a_1$ such that $|x_1^2+2|_{11}\leqslant 11^{-2}$. This is satisfied if: $(3+11a_1)^2\equiv -2 \pmod{11^2} \iff 2\cdot 3\cdot 11a_1\equiv -2-3^2 \pmod{11^2} \iff 6a_1\equiv -1 \pmod{11} \iff a_1\equiv -2\equiv 9 \pmod{11}$. So, now define: $a_1=9$ and $x_1=a_0+11a_1=102$. Check that indeed $|x_1^2+2|_{11}=|10406|_{11}=11^{-2}$.

Now, look for $x_2=a_0+11a_1+11^2a_2$ such that $|x_2^2+2|_{11}\leqslant 11^{-3}$. This is satisfied if: $(102+11^2a_2)^2\equiv -2 \pmod{11^3} \iff 2\cdot 102\cdot 11^2a_2\equiv -2-10404\equiv -10406 \pmod{11^3} \iff 204a_2\equiv -86 \pmod{11} \iff 6a_2\equiv 2 \pmod{11} \iff a_2\equiv 4 \pmod{11}$. So, now define: $a_2=4$ and $x_2=102+11^2a_1=586$. Check that indeed $|x_2^2+2|_{11}=|343398|_{11}=|11^3\cdot 258|_{11}=11^{-3}$. **[5 marks]**

Suppose there were an $x\in\mathbf{Z}$ such that $|x^2-11|_{11}<11^{-2}$, and let $|x|_{11}=11^r$, for some $r\in\mathbf{Z}$. Then $|x^2|_{11}=11^{2r}$. Note that $|-11|_3=|11|_{11}=11^{-1}$, so that $|x^2|_{11}\neq|-11|_{11}$, which means [from the

general property for any $p$-adic valuation that, if $|a|_p \neq |b|_p$ then $|a+b|_p = \max(|a|_p, |b|_p)]$ that $|x^2-11|_{11} = \max(11^{2r}, 11^{-1})$. If $r<0$ then $11^{2r} < 11^{-1}$ and so this maximum will be $11^{-1}$; if $r \geqslant 0$ then $11^{2r} > 11^{-1}$ and so this maximum will be $11^{2r}$. In either case, we must always have $|x^2-11|_{11} \geqslant 11^{-1}$, and so it never happens that $|x^2-11|_{11} < 11^{-2}$. **[3 marks]**

**(b).** First find the 5-adic expansion of $7/3$. Note that $|7/3|_5 = 1$, so the 5-adic expansion is of the form: $7/3 = a_0, a_1a_2\ldots = a_0 + 5a_1 + 5^2a_2 + \ldots$. So, $7 = 3(a_0 + 5a_1 + 5^2a_2 + \ldots)$. This gives $7 \equiv 3a_0 \pmod 5$, so that $a_0 = 4$. Hence, $7 \equiv 3\cdot 4 + 3\cdot 5a_1 \pmod{5^2}$, which implies $-5 \equiv 3\cdot 5a_1 \pmod{5^2}$, and so $-1 \equiv 3a_1 \pmod 5$, giving $a_1 = 3$. Similarly, $a_2 = 1$, $a_3 = 4$, $a_4 = 1$. At this point, we suspect that $7/3 = 4, \overline{31}$. We can confirm this by letting $x = 4, \overline{31}$. Then $x - 4 = 0, \overline{31}$ and so $5^2(x-4) = (x-4) - 3\cdot 5 - 1\cdot 5^2$, so that $24x = 56$; that is: $x = 7/3$, as required. Finally, $7/15 = (1/5)\cdot(7/3)$, so that the 5-adic expansion of $7/15$ is the same as that of $7/3$, but moved one place to the left; that is: $7/15 = 43, \overline{13}$. **[6 marks]**

**(c).** Compute $1, \overline{2} = 1 + 2p + 2p^2 + 2p^3 + \ldots = 1 + 2p(1 + p + p^2 + \ldots) = 1 + 2p/(1-p) = (1+p)/(1-p)$. So, $1, \overline{2} = -9/8 \iff (1+p)/(1-p) = -9/8 \iff 8(1+p) = -9(1-p) \iff p = 17$.

Compute $11, \overline{1} = p^{-1} + 1 + p + p^2 + p^3 + \ldots = p^{-1}(1 + p + p^2 + \ldots) = p/(1-p)$. So, $11, \overline{1} = -1/110 \iff p/(1-p) = -1/110 \iff -p(1-p) = -110 \iff p^2 - p - 110 = 0 \iff (p+10)(p-11) = 0 \iff p = -10$ or $11$. So we must have $p = 11$ since $p$ is prime. **[5 marks]**

**(d).** Note that 3 is coprime to $p-1$, and so there exist $\lambda, \mu \in \mathbf{Z}$ such that $(p-1)\lambda + 3\mu = 1$. Now, suppose that $v^3 = w^3$ in $\mathbf{F}_p^*$. Then $v^{3\mu} = w^{3\mu}$. Also $(p-1)\lambda$ is a multiple of the order of the group $\mathbf{F}_p^*$ and so $v^{(p-1)\lambda} = w^{(p-1)\lambda}$ (since both are equal to 1). Multiplying these last two equations gives: $v^{(p-1)\lambda+3\mu} = w^{(p-1)\lambda+3\mu}$, and so $v = w$. We have shown that $v^3 = w^3$ implies $v = w$, and so the map $v \mapsto v^3$ is injective, and hence surjective (and hence bijective), from $\mathbf{F}_p^*$ to $\mathbf{F}_p^*$. Hence $\mathbf{F}_p^* = (\mathbf{F}_p^*)^3$ and so $\mathbf{F}_p^*/(\mathbf{F}_p^*)^3$ has only one element.

Let $d \in \mathbf{Q}_p$ satisfy $|d|_p = 1$. By the above, there exists $x_0 \in \mathbf{Z}$ such that $x_0^3 \equiv d \pmod p$. This is the same as $|f(x_0)|_p < 1$, where $f(x) = x^3 - d$. But from the fact that $d$ is not divisible by $p$ and $x_0^3 \equiv d \pmod p$ it follows that $x_0$ is not divisible by $p$, and so $|x_0|_p = 1$, giving that $|f'(x_0)|_p = |3x_0^2|_p = 1$. Therefore, $|f(x_0)|_p < |f'(x_0)|_p^2$ and so, by Hensel's Lemma, there exists a solution in $\mathbf{Q}_p$ to $x^3 - d$; that is, $d$ is a cube in $\mathbf{Q}_p^*$; that is: $d = 1$ in $\mathbf{Q}_p^*/(\mathbf{Q}_p^*)^3$. Any $e \in \mathbf{Q}_p$ satisfying $|e|_p = p^{3r}$, do some $r$, must therefore also be a cube in $\mathbf{Q}_p^*$, since $|(p^r)^3 e|_p = 1$. We can therefore divide up all members of $\mathbf{Q}_p^*$ into: $e$ such that $|e|_p = p^{3r}$, $e$ such that $|e|_p = p^{3r+1}$ and $e$ such that $|e|_p = p^{3r+2}$, which give the only 3 distinct elements of $\mathbf{Q}_p^*/(\mathbf{Q}_p^*)^3$. **[6 marks]**

**Question 3.** *All parts of this question are unseen, but using general skills from exercise sheets.*

**(a).** To compute $2P$, we first compute the tangent to $\mathcal{C} : Y^2 = X(X^2 + 4k^4)$ at $P = (2k^2, 4k^3)$. This has slope: $\ell = (3\cdot(2k^2)^2 + 4k^4)/(2\cdot 4k^3) = 2k$, and it goes through the point $P$, so that the equation of the tangent is: $Y = 2kX$. Substituting this into $Y^2 = X(X^2 + 4k^4)$ gives: $4k^2X^2 = X(X^2 + 4k^4)$, and so: $X(X - 4k^2X + 4k^4) = 0$; that is: $X(X - 2k^2)^2 = 0$, and so the line $Y = 2kX$ meets $\mathcal{C}$ at the points: $(2k^2, 4k^3), (2k^2, 4k^3), (0,0)$. So, $(2k^2, 4k^3) + (2k^2, 4k^3) + (0,0) = \mathbf{o}$, giving: $2P = -(0,0) = (0,0)$. It follows that $3P = (2k^2, -4k^3)$ and $4P = \mathbf{o}$, so that $P$ is of order 4. The group generated by $P$, namely $\{\mathbf{o}, P, 2P, 3P\}$, is then a subgroup of $\mathcal{C}(\mathbf{F}_p)$, giving $4|\#\mathcal{C}(\mathbf{F}_p)$ by Lagrange's Theorem, as required. **[7 marks]**

**(b).** The points $\{\mathbf{o}, (0,0), (\ell, 0), (-\ell, 0)\} \in \mathcal{D}(\mathbf{Q})$ are all 2-torsion, and form a subgroup of of $\mathcal{D}(\mathbf{Q})$ [check: each element is self inverse; closure is clear from the fact that the sum of any two of the points of order 2 gives the third point of order 2]. So, again by Lagrange's Theorem, $4|\#\mathcal{D}(\mathbf{F}_p)$. **[4 marks]**

**(c).** It is not possible for $m = 0$ or $4 = 0$ in $\mathbf{F}_p$, since then $\mathcal{E}$ would not be an elliptic curve. First note that $\left(\frac{-m}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{m}{p}\right)$, so that it is not possible for all of $\left(\frac{-1}{p}\right) = -1, \left(\frac{m}{p}\right) = -1$ and $\left(\frac{-m}{p}\right) = -1$, and so at least one of these must equal 1 (since none are 0). If $\left(\frac{-1}{p}\right) = 1$ then $-1 = a^2$ for some $a \in \mathbf{F}_p$, and so $\mathcal{E}$ can be written as: $Y^2 = X(X^2 - (2am)^2)$ which by (b) gives that $\mathcal{E}(\mathbf{F}_p)$ has 3 points of order 2 and $4|\#\mathcal{E}(\mathbf{F}_p)$. If $\left(\frac{m}{p}\right) = 1$ or $\left(\frac{-m}{p}\right) = 1$ then $m = \pm k^2$ for some $k \in \mathbf{F}_p$, and so $\mathcal{E}$ can be written as: $Y^2 = X(X^2 + 4k^4)$ which by (a) gives that $\mathcal{E}(\mathbf{F}_p)$ has a point order 4 and $4|\#\mathcal{E}(\mathbf{F}_p)$. **[7 marks]**

**(d).** The fact that $p \equiv 3 \pmod 4$ gives $\left(\frac{-1}{p}\right) = -1$ so that, for any $u$, $\left(\frac{-u(u^2+n)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{u(u^2+n)}{p}\right) = -\left(\frac{u(u^2+n)}{p}\right)$. Now, let $u \neq 0, u \in \mathbf{F}_p$. If $u$ is a root of $X^2 + n$ then so is $-u$, giving the two points $(u,0), (-u,0) \in \mathcal{F}(\mathbf{F}_p)$. If $u$ is not a root of $X^2 + n$ then $u(u^2+n) \neq 0$ and from the identity we have just shown, exactly one of $\left(\frac{-u(u^2+n)}{p}\right)$ and $\left(\frac{u(u^2+n)}{p}\right)$ is equal to 1 and the other is equal to $-1$. Without

loss of generality, say that $\left(\frac{u(u^2+n)}{p}\right) = 1$ and $\left(\frac{-u(u^2+n)}{p}\right) = -1$. Then there exists $v \neq 0, v \in \mathbf{F}_p$ such that $v^2 = u(u^2+n)$, but there does not exist $v$ such that $v^2 = -u(u^2+n)$. This gives the two points $(u,v)$ and $(u,-v)$ in $\mathcal{F}(\mathbf{F}_p)$ with $X$-coordinate $u$ and no points in $\mathcal{F}(\mathbf{F}_p)$ with $X$-coordinate $u$. So, in all cases, there are two points in $\mathcal{F}(\mathbf{F}_p)$ with $X$-coordinate $u$ or $-u$. Divide the $p-1$ nonzero elements of $\mathbf{F}_p$ into pairs $u, -u$, each pair contributing two members of $\mathcal{F}(\mathbf{F}_p)$; this gives so far a total of $p-1$ members of $\mathcal{F}(\mathbf{F}_p)$ with nonzero $X$-coordinate. When we also include the points $\mathbf{o}, (0,0) \in \mathcal{F}(\mathbf{F}_p)$, then we finally obtain $\#\mathcal{F}(\mathbf{F}_p) = p+1$, as required. Since $p \equiv 3 \pmod 4$, it is immediate that $4|(p+1)$; that is: $4|\#\mathcal{F}(\mathbf{F}_p)$, as required. **[7 marks]**

**Question 4.** *Part (a) requires regurgitation of one of the easier proofs from lectures (middle of the course). Part (b) is a variation of examples from the example sheets. Part (c) is unseen and somewhat tricky.*
**(a).** The Nagell-Lutz Theorem states that, if $(x,y)$ is a $\mathbf{Q}$-rational torsion point on $\mathcal{E} : Y^2 = X^3 + AX + B$, where $A, B \in \mathbf{Z}$, then $x, y \in \mathbf{Z}$ and $y = 0$ or $y^2|\Delta$, where $\Delta = 4A^3 + 27B^2$.
**Proof (from lectures).** We are given the result that $x, y \in \mathbf{Z}$. If $y = 0$ then the result is satisfied; otherwise, $(x,y)$ is not 2-torsion and we can consider $(x_2, y_2) = 2(x,y)$, with $(x_2, y_2) \neq \mathbf{o}$, and so $x_2, y_2 \in \mathbf{Q}$. But $(x_2, y_2)$ is also a torsion point, so $x_2, y_2 \in \mathbf{Z}$. Now, the line tangent to $\mathcal{E}$ at $(x,y)$ has slope $(3x^2+A)/(2y)$, from which we immediately get: $x_2 = \big((3x^2+A)/(2y)\big)^2 - 2x$. Now, we know $x_2, x \in \mathbf{Z}$ and so $\big((3x^2+A)/(2y)\big)^2 \in \mathbf{Z}$. It follows that $4y^2|(3x^2+A)^2$ and so $y^2|(3x^2+A)^2 = \psi_1(x)$. Also, $y^2 = x^3 + Ax + B = \psi_2(x)$. Using the identity given on the exam paper, $y^2|(\phi_1(x)\psi_1(x) + \phi_2(x)\psi_2(x)) = \Delta$, as required. **[10 marks]**
**(b).** The discriminant of $X^3 - X - 1$ is $4 \cdot (-1)^3 + 27 \cdot (-1)^2 = 23$, and so $\widetilde{\mathcal{C}} : Y^2 = X^3 - X - 1$ is an elliptic curve for all $p \neq 2, 23$. The only element of $\widetilde{\mathcal{C}}(\mathbf{F}_3)$ is $\mathbf{o}$, and so $\widetilde{\mathcal{C}}(\mathbf{F}_3)$ has order 1. Since the torsion subgroup of $\mathcal{C}(\mathbf{Q})$ injects into this group, its order must divide 1 and so equal 1. Hence the torsion subgroup of $\mathcal{C}(\mathbf{Q})$ is precisely $\{\mathbf{o}\}$.

The discriminant of $X^3 - X + 1$ is $4 \cdot (-1)^3 + 27 \cdot (-1)^2 = 23$, and so again $\widetilde{\mathcal{D}} : Y^2 = X^3 - X + 1$ is an elliptic curve for all $p \neq 2, 23$. The elements of $\widetilde{\mathcal{D}}(\mathbf{F}_3)$ are: $\mathbf{o}, (0, \pm 1), (1, \pm 1), (-1, \pm 1)$, and so $\widetilde{\mathcal{D}}(\mathbf{F}_3)$ has order 7. The elements of $\widetilde{\mathcal{D}}(\mathbf{F}_5)$ are: $\mathbf{o}, (0, \pm 1), (1, \pm 1), (-1, \pm 1), (-2, 0)$, and so $\widetilde{\mathcal{D}}(\mathbf{F}_5)$ has order 8. Since the torsion subgroup of $\mathcal{D}(\mathbf{Q})$ injects into both of these groups, its order must divide $\gcd(7,8) = 1$ and so equal 1. Hence the torsion subgroup of $\mathcal{D}(\mathbf{Q})$ is again precisely $\{\mathbf{o}\}$. [Alternatively, Nagell-Lutz can be used for these examples] **[9 marks]**
**(c).** The disciminant of $X^3 - k^2X + k^3$ is $4 \cdot (-k^2)^3 + 27 \cdot (k^3)^2 = 23k^6$. If $(x,y)$ is a $\mathbf{Q}$-rational torsion point on $\mathcal{E} : Y^2 = X^3 - k^2X + k^3$, then we know by Nagell-Lutz that $x, y \in \mathbf{Z}$ with $y^2|23k^6$ and so $|y|^2 \leq 23|k|^6$; that is: $|y| \leq \sqrt{23}|k|^3 = (4.79583\ldots)|k|^3 < 5|k|^3$.

Imagine $|x| \geq 3|k|^2$. We cannot have $k = 0$ since then the discriminant would be 0 and $\mathcal{E}$ would not be an elliptic curve. The cases $k = \pm 1$ have already been dealt with in $(b)$, when it the torsion group of $\mathcal{E}(\mathbf{Q})$ was shown to be trivial. So, we can take $|k| > 1$, giving $|k|^2 < |k|^4$ and $|k|^3 < |k|^6$. Imagine $|x| \geq 3|k|^2$. Then:

$|x^2 - k^2| \geq |x^2| - |k^2| \geq 9|k|^4 - |k^2| > 9|k|^4 - |k^4| = 8|k|^4$, and so:
$|y|^2 = |x(x^2-k^2) + k^3| \geq |x(x^2-k^2)| - |k^3| = |x||x^2-k^2| - |k^3| > 3|k|^2 8|k|^4 - |k|^6 = 23|k|^6$,

a contradiction, since we have already shown that $|y|^2 \leq 23|k|^6$. This contradiction arose from imagining that $|x| \geq 3|k|^2$, and so we must have $|x| < 3|k|^2$, as required. **[6 marks]**

**Question 5.** *The proof in part (a) is tricky bookwork from lectures. Part (b) is unseen.*
**(a).** Let $r \in \mathbf{Q}^*/(\mathbf{Q}^*)^2, r \in \operatorname{im} q, r \in \mathbf{Z}, r$ square free. We want to prove that $r|b_1$. Suppose $r = q(u,v)$, where $(u,v) \in \mathcal{D}(\mathbf{Q})$, which must exist since $r \in \operatorname{im} q$. Then: $r = q(u,v) = u = u^2 + a_1u + b_1$ in $\mathbf{Q}^*/(\mathbf{Q}^*)^2$ [since $u(u^2 + a_1u + b_1) = v^2$]. So, $r, u, u^2 + a_1u + b_1$ are all the same modulo squares, which means we can write:

$$u^2 + a_1u + b_1 = rs^2, \quad u = rt^2, \quad \text{for some } s, t \in \mathbf{Q}.$$

Hence: $(rt^2)^2 + a_1(rt^2) + b_1 = rs^2$. Let $t = \ell/m$, where $\ell, m \in \mathbf{Z}$ and $\gcd(\ell, m) = 1$. Then: $r^2\ell^4/m^4 + a_1r\ell^2/m^2 + b_1 = rs^2$, and so: $r^2\ell^4 + a_1r\ell^2m^2 + b_1m^4 = r(m^2s)^2$. Now, $a_1, b_1, r, \ell, m \in \mathbf{Z}$, so the LHS of this last equation is in $\mathbf{Z}$, and so the RHS is also in $\mathbf{Z}$; that is: $r(m^2s)^2 \in \mathbf{Z}$. Since $r$ is square free, we must therefore have $m^2s \in \mathbf{Z}$. Define: $n = m^2s \in \mathbf{Z}$. Then our equation becomes:

$$r^2\ell^4 + a_1r\ell^2m^2 + b_1m^4 = rn^2, \quad \text{for some } \ell, m, n \in \mathbf{Z},\ \gcd(\ell, m) = 1. \qquad (\dagger)$$

We want to show that $r|b_1$, and we know that $r$ is square free. It is sufficient to show, for any prime $p$, that $p|r \Rightarrow p|b_1$.

Imagine $p|r$ and $p \not| b_1$, for some prime $p$. Then $p|r^2\ell^4, a_1 r\ell^2 m^2, rn^2$ and so by (†), $p|b_1 m^4$, which in turn gives: $p|m$ [since $p \not| b_1$]. Hence, since now $p|r$ and $p|m$, we have: $p^2|r^2\ell^4, a_1 r\ell^2 m^2, b_1 m^4$, and so by (†), $p^2|rn^2$, which in turn gives: $p|n$ [since $r$ is square free]. Hence, since now $p|r, m, n$, we have: $p^3|a_1 r\ell^2 m^2, b_1 m^4, rn^2$, and so by (†), $p^3|r^2\ell^4$, which in turn gives: $p|\ell$ [since $r$ is square free]. This is a contradiction, since $p|\ell$ and $p|m$ but $\gcd(\ell, m) = 1$.

The above assumption that $p|r$ and $p \not| b_1$ let to a contradiction, and so it is impossible for any prime $p$ to satisfy $p|r$ and $p \not| b_1$. This is the same as saying that $p|r \Rightarrow p|b_1$ for any prime $p$. Since $r$ is square free, we conclude that $r|b_1$, as required **[16 marks]**

**(b).** Let $P$ be a point of order $m$ on $\mathcal{C}(\mathbf{Q})$, where $m$ is odd. Then, since $\phi$ is a homomorphism, $P' = \phi(P)$ satisfies: $mP' = m\phi(P) = \phi(mP) = \phi(\mathbf{o}) = \mathbf{o}$, and so the order of $P'$ divides $m$ and is at most $m$. Let $j$ be the order of $P'$. Imagine that $j < m$. Then $\phi(jP) = j\phi(P) = jP' = \mathbf{o}$, so $jP \in \ker\phi$ and $jP \neq \mathbf{o}$ since $j < m$ and $P$ has order $m$. But this is a contradiction, since $jP \in \langle P\rangle$, and so $jP$ has order dividing $m$, which means that $jP$ has odd order and yet the only members of $\ker\phi$ are $\mathbf{o}$ and $(0,0)$. This contradiction arose from imagining that $j < m$; hence $j \geq m$; since also $j|m$, the only possibility is $j = m$; that is, the order of $P'$ is $m$, as required.

Let $Q$ be a point of order $n$ on $\mathcal{C}(\mathbf{Q})$, where $n$ is even. As before, since $\phi$ is a homomorphism, $Q' = \phi(Q)$ satisfies: $nQ' = n\phi(Q) = \phi(nQ) = \phi(\mathbf{o}) = \mathbf{o}$, and so the order of $Q'$ divides $n$ and is at most $n$. Let $j$ be the order of $Q'$. Imagine that $j < n/2$. Then $\phi(jQ) = j\phi(Q) = jQ' = \mathbf{o}$ and $\phi(2jQ) = 2j\phi(Q) = 2jQ' = \mathbf{o}$, so $jQ, 2jQ \in \ker\phi$ and $jQ, 2jQ \neq \mathbf{o}, jQ \neq 2jQ$ since $j, 2j < n$ and $Q$ has order $n$. But this is a contradiction, since the only members of $\ker\phi$ are $\mathbf{o}$ and $(0,0)$. This contradiction arose from imagining that $j < n/2$; hence $j \geq n/2$; since also $j|n$, we must have $j = n/2$ or $j = n$; that is, the order of $Q'$ is $n$ or $n/2$, as required **[9 marks]**

**Question 6.** *Examples like this have appeared on the exercise sheets, but these descents via isogeny are probably the hardest thing in the course, since they require bringing together most of the techniques learnt throughout the course. I thought it was sufficient, therefore, to give a standard descent-via-isogeny as an entire question.*

Let $\mathcal{C} : Y^2 = X(X^2 + aX + b) = X(X^2 + 3X + 7)$, where $a = 3, b = 7$, and isogenous curve $\mathcal{D} : Y^2 = X(X^2 + a_1X + b_1) = X(X^2 - 6X - 19)$, where $a_1 = -6, b_1 = -19$, with the usual isogeny $\phi : \mathcal{C}(\mathbf{Q}) \to \mathcal{D}(\mathbf{Q}) : (x, y) \mapsto (y^2/x^2, y - 7y/x^2)$, and dual isogeny $\hat{\phi} : \mathcal{D}(\mathbf{Q}) \to \mathcal{C}(\mathbf{Q}) : (u, v) \mapsto (\frac{1}{4}v^2/u^2, \frac{1}{8}(v + 19v/u^2))$. **[3 marks]**

The map $q : \mathcal{D}(\mathbf{Q})/\phi(\mathcal{C}(\mathbf{Q})) \to \mathbf{Q}^*/(\mathbf{Q}^*)^2 : (u, v) \mapsto u$, for $(u, v) \neq (0, 0)$, with $q : (0, 0) \mapsto b_1$ and $q : \mathbf{o} \mapsto 1$, is an injection with im$q$ contained in $\{d : d \text{ is square free and } d|b_1\} = \{\pm1, \pm19\}$. Also, $\mathbf{o} \mapsto 1$, $(0, 0) \mapsto -19$, so that $\{1, -19\} \subset \text{im}q \subset \{\pm1, \pm19\}$. **[3 marks]**

There is only one coset to check, represented by $-1$, say. We know that $-1 \in \text{im}q$ iff there are integers $\ell, m, n$, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1) \cdot \ell^4 + a_1\ell^2m^2 + (b_1/(-1)) \cdot m^4 = n^2$ that is: $-\ell^4 - 6\ell^2m^2 + 19m^4 = n^2$. Rewrite as: $-(\ell^2 + 3m^2)^2 + 28m^4 = n^2$. Reducing modulo 7 gives $-(\ell^2 + 3m^2)^2 \equiv n^2$ (modulo 7). If $n$ were coprime to 7, then this would give: $((\ell^2 + 3m^2)/n)^2 = -1$ in $\mathbf{F}_7$, contradicting the fact that $-1$ is not a quadratic residue modulo 7. So, $7|n$ and so $7|(\ell^2 + 3m^2)$ also. This means that $7^2|(\ell^2 + 3m^2)^2$ and $7^2|n^2$, which can be combined with $-(\ell^2 + 3m^2)^2 + 28m^4 = n^2$ to give: $7^2|28m^4$ and so $7|4m^4$, giving $7|m$. Combining $7|m$ with $7|(\ell^2 + 3m^2)$ gives that $7|\ell$. This contradicts the fact that $\gcd(\ell, m) = 1$. Hence our equation is impossible in $\mathbf{Q}_7$, and so impossible in $\mathbf{Q}$. Hence $-1 \notin \text{im}q$. **[6 marks]**

We conclude that im$q = \{1, -19\}$, and so $\mathcal{D}(\mathbf{Q})/\phi(\mathcal{C}(\mathbf{Q}))$ is generated by $(0, 0)$. **[1 mark]**

The map $\hat{q} : \mathcal{C}(\mathbf{Q})/\hat{\phi}(\mathcal{D}(\mathbf{Q})) \to \mathbf{Q}^*/(\mathbf{Q}^*)^2 : (x, y) \mapsto x$, for $(x, y) \neq (0, 0)$, with $\hat{q} : (0, 0) \mapsto b$ and $\hat{q} : \mathbf{o} \mapsto 1$, is an injection with im$\hat{q}$ contained in $\{d : d \text{ is square free and } d|b\} = \{\pm1, \pm7\}$. Also, $\mathbf{o} \mapsto 1$ and $(0, 0) \mapsto 7$, so that $\{1, 7\} \subset \text{im}\hat{q} \subset \{\pm1, \pm7\}$. **[3 marks]**

There is only one coset to check, represented by $-1$, say. We know that $-1 \in \text{im}\hat{q}$ iff there are integers $\ell, m, n$, not all 0, and with $\gcd(\ell, m) = 1$, such that: $(-1) \cdot \ell^4 + a\ell^2m^2 + (b/(-1)) \cdot m^4 = n^2$; that is: $-\ell^4 + 3\ell^2m^2 - 7m^4 = n^2$. Multiply both sides by 4 and rewrite as: $-(2\ell^2 - 3m^2)^2 - 19m^4 = 4n^2$. This is impossible in $\mathbf{R}$ (the left hand side is $\leqslant 0$ and the right hand side is $\geqslant 0$, and equality only occurs when

$2\ell^2 - 3m^2 = m^4 = n^2 = 0$, implying $\ell = m = n = 0$, which is not allowed). [A mod 19 argument would also work here.] Hence $-1 \notin \mathrm{im}\hat{q}$. **[4 marks]**

We conclude that $\mathrm{im}\hat{q} = \{1, 7\}$, and so $\mathcal{C}(\mathbf{Q})/\hat{\phi}(\mathcal{D}(\mathbf{Q}))$ is generated by $(0, 0)$. **[1 mark]**

Finally, since multiplication by 2 in $\mathcal{C}(\mathbf{Q})$ is $\hat{\phi} \circ \phi$, we have that $\mathcal{C}(\mathbf{Q})/2\mathcal{C}(\mathbf{Q})$ is generated by: generators for $\mathcal{C}(\mathbf{Q})/\hat{\phi}(\mathcal{D}(\mathbf{Q}))$ [namely: $(0, 0)$] together with the images under $\hat{\phi}$ of generators for $\mathcal{D}(\mathbf{Q})/\phi(\mathcal{C}(\mathbf{Q}))$ [namely, $\hat{\phi}\big((0, 0)\big) = \mathbf{o}$]. Conclusion: $\mathcal{C}(\mathbf{Q})/2\mathcal{C}(\mathbf{Q})$ is generated by $(0, 0)$, and so is isomorphic to $C_2$. We also know that $\mathcal{C}(\mathbf{Q})/2\mathcal{C}(\mathbf{Q})$ is isomorphic to $\mathcal{C}_{tors}(\mathbf{Q})/2\mathcal{C}_{tors}(\mathbf{Q}) \times C_2^r$, which is isomorphic to $\mathcal{C}(\mathbf{Q})[2] \times C_2^r$, where $\mathcal{C}(\mathbf{Q})[2]$ is the 2-torsion group and $r$ is the rank. The 2-torsion points on $\mathcal{C} : Y^2 = X(X^2 + 3X + 7)$ are $\mathbf{o}$ together with the points of the form $(x, 0)$, where $x$ is a root of $X(X^2 + 3X + 7)$, that is: $(0, 0)$, $(-\frac{3}{2} + \frac{\sqrt{-19}}{2}, 0)$ and $(-\frac{3}{2} - \frac{\sqrt{-19}}{2}, 0)$, of which only $\mathbf{o}$ and $(0, 0)$ are in $\mathcal{C}(\mathbf{Q})[2]$, giving that $\mathcal{C}(\mathbf{Q})[2]$ is isomorphic to $C_2$. Combining this with the facts (already found) that $\mathcal{C}(\mathbf{Q})/2\mathcal{C}(\mathbf{Q})$ is isomorphic both to $C_2$ and to $\mathcal{C}(\mathbf{Q})[2] \times C_2^r$, give that $\mathcal{C}(\mathbf{Q})$ has rank 0. **[4 marks]**

**Question 7.** *Parts (a),(b),(c) are easy variations of a question on one of the examples sheets; this is intended to be an easy question accessible to the weaker students, although it is not quick to answer, since there are quite a few computations.*

In all of the following, each step multiplies numbers $\leqslant N$ (followed by a possible reduction modulo $N$), and so we are guaranteed that everything can be done on an 9-digit calculator, since $N^2$ has only 9 digits.

**(a).** First compute (modulo $N = 10001$): $2^1 \equiv 2$, $2^2 \equiv 4$, $2^4 \equiv 16$, $2^8 \equiv 256$, $2^{16} \equiv 5530$, $2^{32} \equiv 7843$, $2^{64} \equiv 6499$ (where each of these was obtained be squaring the previous one, and reducing modulo $N$). Now, we write 68 in base 2: $68 = 4 + 64$ and so $2^{68} \equiv 2^4 2^{64} \equiv 16 \cdot 6499 \equiv 3974$ modulo $N$, so that $2^{68} - 1 \equiv 3973$ modulo $N$.

Now, compute $\gcd(3973, N)$ by Euclid's Algorithm: $10001 = 2 \cdot 3973 + 2055$; $3973 = 1 \cdot 2055 + 1918$; $2055 = 1 \cdot 1918 + 137$, $1918 = 14 \cdot 137 + 0$. So, 137 is a factor of $N$. Compute $10001/137 = 73$, giving the factorisation $N = 10001 = 73 \cdot 137$. **[8 marks]**

**(b).** The line tangent to $\mathcal{E}$ at $P = (1, 1)$ has slope $y'$ given by $2yy' = 3x^2 + 2$, with $x = 1, y = 1$; that is, the slope is $5/2$. This tangent line also goes through $(1, 1)$ and so has equation: $Y = (5/2)X - 3/2$. Note that $2 \cdot 5001 = 10002 \equiv 1$, so that 5001 is the inverse of 2 mod $N$, and the the tangent line has equation: $Y = (5 \cdot 5001)X - 3 \cdot 5001 \equiv 5003X - 5002$. The $x$-coordinate of $2P$ is therefore $5003^2 - (1 + 1) \equiv 7505$, and the $y$-coordinate is: $-(5003 \cdot 7505 - 5002) = -37542513 \equiv 1241$, so that $Q = 2P \equiv (7505, 1241)$ (modulo $N = 10001$). We now wish to double the point $Q = 2P$, and so again the first step is to find the line tangent to $\mathcal{E}$ at $Q$. This has slope $y'$ given by $2 \cdot 1241 \cdot y' = 3 \cdot 7505^2 + 2$, and so we need to compute $(3 \cdot 7505^2 + 2)/(2 \cdot 1241)$ (modulo $N = 10001$), for which the first step is to find the inverse of $2 \cdot 1241 \equiv 2482$ (modulo $N = 10001$). Using Euclid's Algorithm: $10001 = 4 \cdot 2482 + 73$; $2482 = 34 \cdot 73 + 0$. So, we cannot find the inverse of 2482 (modulo $N = 10001$), and this step has given us a factor 73 of $N$. Similarly to before, compute $10001/73 = 137$, again giving the factorisation $N = 10001 = 73 \cdot 137$. **[9 marks]**

**(c).** Since $N = 73 \cdot 137$, we have $\phi(N) = 72 \cdot 136 = 9792$. Computing the gcd of $d = 4451$ and $\phi(N)$, we see: $9792 = 2 \cdot 4451 + 890$; $4451 = 5 \cdot 890 + 1$, so that $\gcd(9792, 4451) = 1$. Reversing the steps: $1 = 4451 - 5 \cdot 890 = 4451 - 5 \cdot (9792 - 2 \cdot 4451) = -5 \cdot 9792 + 11 \cdot 4451$ Hence, 11 is the inverse of 4451 modulo 9792. The decoding operation is therefore $X \mapsto X^{11} \bmod N$. Computing $6847^{11} = ((6847^2)^2)^2 \cdot (6847^2 \cdot 6847) \equiv (6722^2)^2 \cdot (6722 \cdot 6847) \equiv 766^2 \cdot 932 \equiv 6698 \cdot 932 \equiv 1912$. (modulo $N = 10001$). Also: $2577^{11} = ((2577^2)^2)^2 \cdot (2577^2 \cdot 2577) \equiv (265^2)^2 \cdot (265 \cdot 2577) \equiv 218^2 \cdot 2837 \equiv 7520 \cdot 2837 \equiv 2107$ (modulo $N = 10001$). The decoded message is therefore: 1912, 2107; that is: SLUG. **[8 marks]**

---