IMPERIAL

MATH70064

BSc, MSci and MSc EXAMINATIONS (MATHEMATICS)
May 2024

This paper is also taken for the relevant examination for the
Associateship of the Royal College of Science

Elliptic Curves

Date: Wednesday, May 1, 2024

Time: 14:00 – 16:30 (BST)

Time Allowed: 2.5 hours

This paper has 5 Questions.

Please Answer All Questions in 1 Answer Booklet

Candidates should start their solutions to each question on a new sheet of paper.

Supplementary books may only be used after the relevant main book(s) are full.

Any required additional material(s) will be provided.

Allow margins for marking.

Credit will be given for all questions attempted.

Each question carries equal weight.

DO NOT OPEN THIS PAPER UNTIL THE INVIGILATOR TELLS YOU TO

© 2024 Imperial College London

You can assume any theorem proved in the course as well as the following facts.

A: *Quadratic Reciprocity:* Let p, q be two distinct odd prime numbers. Then

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

where $(\frac{p}{q})$ is the Legendre symbol, i.e. if p is a quadratic residue modulo q, then $(\frac{p}{q}) = 1$, otherwise $(\frac{p}{q}) = -1$.

B: *Mazur's theorem:* For any elliptic curve E defined over $\mathbb{Q}$, the torsion subgroup $E(\mathbb{Q})_{\text{tor}}$ is of the form

$$\mathbb{Z}/N\mathbb{Z},\ 1 \leq N \leq 10,\ \mathbb{Z}/12\mathbb{Z}$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z},\ 1 \leq N \leq 4.$$

1. Consider the projective plane conic: $11X^2 + 23Y^2 - Z^2 = 0$.

   (a) Prove it has infinitely many solutions in $\mathbb{P}^2(\mathbb{Q}_{11})$. (4 marks)

   (b) Does it have solutions in $\mathbb{P}^2(\mathbb{Q}_{23})$? Justify your answers. (6 marks)

   (c) Does it have solutions in $\mathbb{P}^2(\mathbb{Q}_2)$? Justify your answers. (6 marks)

   (d) Does it have solutions in $\mathbb{P}^2(\mathbb{R})$? Justify your answers. (2 marks)

   (e) Does it have solutions in $\mathbb{P}^2(\mathbb{Q})$? Justify your answers. (2 marks)

   (Total: 20 marks)

2. Study the torsion subgroup $E(\mathbb{Q})_{\text{tor}}$ of $E(\mathbb{Q})$ of the following elliptic curves.

   (a) $E : y^2 = x^3 + 4x$.

      (i) Please list all the torsion points in $E(\mathbb{Q})_{\text{tor}}$. (7 marks)

      (ii) Determine the structure of $E(\mathbb{Q})_{\text{tor}}$. (3 marks)

   (b) $E : y^2 = x^3 + 7^7x + 3$.

      (i) Find a prime number p such that $E(\mathbb{Q})_{\text{tor}}$ injects into $\overline{E}(\mathbb{F}_p)$, where $\overline{E}$ is the reduction of E modulo p. (4 marks)

      (ii) Determine the structure of $E(\mathbb{Q})_{\text{tor}}$. (6 marks)
      (*Hint: use Mazur's theorem.*)

   (Total: 20 marks)

3. (a) Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbb{Q}$.

(i) Find a, b such that E passes through the points $P = (0, 1)$ and $Q = (-1, 2)$. (2 marks)

(ii) Compute $P + Q$. (2 marks)

(iii) Prove that E has infinitely many $\mathbb{Q}$-rational points (3 marks)

(iv) Determine whether the reduction of E modulo 2 is singular or not. (2 marks)

(b) Let $p > 3$ be prime. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbb{Z}_p$. Recall that $E(\mathbb{Q}_p)^{(0)}$ is the subgroup of $E(\mathbb{Q}_p)$ consisting of points whose reduction modulo p are non-singular. Assume $|a|_p = 1/p$ and $|b|_p \leq 1/p^2$.

(i) Show that there exists $u \in \mathbb{Z}_p^\times$ such that if we put $x = au$, then $x^3 + ax + b$ is a square. (*Hint: use Hensel's lemma and the fact that there are only* $(p-1)/2$ *choices of non-zero squares mod* p.) (4 marks)

(ii) Show that $E(\mathbb{Q}_p) \neq E(\mathbb{Q}_p)^{(0)}$. (3 marks)

(iii) Show that if $P, Q \in E(\mathbb{Q}_p)$ but $P, Q \notin E(\mathbb{Q}_p)^{(0)}$, then $P + Q \in E(\mathbb{Q}_p)^{(0)}$. (4 marks)

(Total: 20 marks)

4. Consider the elliptic curve $E : y^2 = x(x - 2)(x - 10)$ defined over $\mathbb{Q}$.

(a) Find the three non-trivial 2-torsion points of E. (3 marks)

Now let T_1, T_2, T_3 be the non-trivial 2-torsion points with x-coordinates e_1, e_2, e_3 respectively, such that $e_1 \geq e_2 \geq e_3$. Recall the following map appearing in the 2-descent method

$$\delta : E(\mathbb{Q}) \to (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2) \times (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2) \times (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)$$

defined by $\delta(x, y) = (x - e_1, x - e_2, x - e_3)$ if (x, y) is not 2-torsion and

$$\begin{aligned}
\delta(T_1) &= ((e_1 - e_2)(e_1 - e_3), (e_1 - e_2), (e_1 - e_3)),\\
\delta(T_2) &= (e_2 - e_1, (e_2 - e_1)(e_2 - e_3), e_2 - e_3),\\
\delta(T_3) &= (e_3 - e_1, e_3 - e_2, (e_3 - e_1)(e_3 - e_2)),\\
\delta(\mathcal{O}) &= (1, 1, 1).
\end{aligned}$$

(b) Show that $(1, 2, 2)$ is not contained in the image of δ.
(*Hint:* 2 *is not a square modulo* 5.) (8 marks)

(c) Show that $(1, 5, 5)$ is not contained in the image of δ. (5 marks)

(d) Assume $\#E(\mathbb{Q})/2E(\mathbb{Q}) = \#\mathrm{Im}(\delta) = 8$. What is the rank of $E(\mathbb{Q})$? (2 marks)

(e) Give an example of an elliptic curve defined over $\mathbb{Q}$, whose 2-torsion points are not all defined over $\mathbb{Q}$. (2 marks)

(Total: 20 marks)

5. (a) Let $p \equiv 3 \mod 4$ be a prime and $D \in \mathbb{F}_p^\times$.

(i) Let $(\mathbb{F}_p^\times)^2 := \{g^2 : g \in \mathbb{F}_p^\times\}$. Show that the map $(\mathbb{F}_p^\times)^2 \to (\mathbb{F}_p^\times)^2$ sending $g^2 \mapsto g^4$ is bijective. (3 marks)

(ii) Show that $v^2 - U^2 = -4D$ has $(p-1)$ solutions (U, v) in $\mathbb{F}_p \times \mathbb{F}_p$.
(*Hint: try to make the change of variables* $v + U = x$ *and* $v - U = y$.) (4 marks)

(iii) Combine (i) and (ii) to show that the equation

$$C : v^2 = u^4 - 4D$$

has $(p-1)$ solutions (u, v) in $\mathbb{F}_p \times \mathbb{F}_p$. (2 marks)

(iv) Let $E/\mathbb{F}_p$ be the elliptic curve

$$y^2 = x^3 + Dx.$$

Consider the map

$$\phi : C \to E, \quad \phi(u, v) = \left(\frac{u^2 + v}{2}, \frac{u(u^2 + v)}{2}\right).$$

Show the above map is well-defined and use it to prove $\#E(\mathbb{F}_p) = p + 1$. (5 marks)

(b) Let $p \equiv 2 \mod 3$ be an odd prime.

(i) Show that $x \mapsto x^3$ defines a bijection of sets from $\mathbb{F}_p$ to $\mathbb{F}_p$. (3 marks)

(ii) Let $E/\mathbb{F}_p$ be the elliptic curve

$$E : y^2 = x^3 + 1.$$

Show that $\#E(\mathbb{F}_p) = p + 1$.
(*Hint: there are* $\frac{p+1}{2}$ *quadratic residues (including 0) mod* p.) (3 marks)

(Total: 20 marks)

BSc and MSci EXAMINATIONS (MATHEMATICS)

May 2024

This paper is also taken for the relevant examination for the Associateship.

Math70064

Elliptic Curves (Solutions)

Setter's signature	Checker's signature	Editor's signature
.....	.....	.....

1. (a) Note that this projective plane conic is non-singular, which means it either has no solution or has infinitely many in $\mathbb{P}^2(\mathbb{Q}_{11})$. So it suffices to find one solution. Put $X = 0, Y = 1$. Then we need to solve the equation $f(Z) = Z^2 - 23 = 0$. Note that $f(1) \equiv 23 \mod 11$ and $f'(1) = 2$. So we have $|f(1)|_{11} < |f'(1)|_{11}$. By Hensel's lemma, there exists an $\alpha \in \mathbb{Z}_{11}$ such that $\alpha^2 = 23$ in $\mathbb{Z}_{11}$. So $[0; 1; \alpha]$ is a solution to $11X^2 + 23Y^2 - Z^2 = 0$ in $\mathbb{P}^2(\mathbb{Q}_{11})$.

sim. seen ⇓

4, A

(b) No, it does not have solutions in $\mathbb{P}^2(\mathbb{Q}_{23})$. Suppose $[x; y; z]$ is a solution with $x, y, z \in \mathbb{Z}_{23}$. We may assume the maximum of the 23-adic norms of x, y, z is 1. If $|x|_{23} < 1$, then $|z|_{23} < 1$. But $|23y^2|_{23} = |11x^2 - z^2|_{23} \leq 23^{-2}$, which implie $|y|_{23} < 1$. This contradicts our assumption. So we must have $|x|_{23} = 1$. The same reason shows that $|z|_{23} = 1$. But then reducing modulo 23, the equation $11X^2 - Z^2 = 0 \mod 23$ admits a non-zero solution. We may assume $x = 1$. Then we have $z^2 = 11 \mod 23$. The quadratic reciprocity shows that $(\frac{11}{23})(\frac{23}{11}) = (-1)^{55} = -1$. As $(\frac{23}{11}) = 1$, we see that $(\frac{11}{23}) = -1$. So 11 is not a quadratic residue modulo 23. Contradiction.

sim. seen ⇓

6, B

(c) No, there is no solution in $\mathbb{P}^2(\mathbb{Q}_2)$. Suppose $[x; y; z]$ is a solution. We may assume the maximum of the 2-adic norms of x, y, z is 1. Reducing modulo 4, we get

$$X^2 + Y^2 + Z^2 = 0 \mod 4.$$

As squares are congruent to either 0 or 1 modulo 4, we get a contradiction.

sim. seen ⇓

6, B

(d) Yes, for example $[1/\sqrt{11}; 0; 1]$ is a solution.

sim. seen ⇓

2, A

(e) No, since there is no solution in $\mathbb{P}^2(\mathbb{Q}_2)$.

sim. seen ⇓

2, A

2. (a) (i) Let (x, y) be a torsion point. Then by the theorem of Lutz–Nagell, we have either $y = 0$ or $y^2|256$. When $y = 0$, we need to solve the equation $x^3+4x = 0$. It has only one solution $x = 0$. When $y^2|256$, we see that $y^2 = 1, 4, 16, 64, 256$. One can check the only possible solutions are $(x, y) = (2, \pm 4)$. So the torsion subgroup contains at most 4 points: $(0, 0), (2, 4), (2, -4), \mathcal{O}$. By the doubling formula, we see that $2(2, 4) = (0, 0)$. Obviously, $2(0, 0) = \mathcal{O}$. So the torsion subgroup contains exactly the 4 points: $(0, 0), (2, 4), (2, -4), \mathcal{O}$.

meth seen ⇓

7, A

(ii) As the point $(2, 4)$ is of order 4, the torsion subgroup is isomorphism to $\mathbb{Z}/4$.

meth seen ⇓

3, A

(b) (i) As $7 \nmid \Delta = 4 \times 7^{21} + 27 \times 9$, we then have an injection $E(\mathbb{Q})_{\text{tor}} \hookrightarrow \bar{E}(\mathbb{F}_7)$, where $\bar{E} : y^2 = x^3 + 3$ is the reduction of E modulo 7.

sim. seen ⇓

4, C

(ii) The squares modulo 7 are $0, 1, 2, 4$. So we have

sim. seen ⇓

x	0	1	2	3	4	5	6
x^3+3	3	4	4	2	4	2	2
$\#y$	0	2	2	2	2	2	2

So $\#\bar{E}(\mathbb{F}_7) = 12 + 1 = 13$. And $\bar{E}(\mathbb{F}_7) \cong \mathbb{Z}/13$. But by Mazur's theorem, there is no point of order 13 in $E(\mathbb{Q})_{\text{tor}}$. This means $E(\mathbb{Q})_{\text{tor}} = 0$.

6, C

3. (a) (i) We need to solve the equations $\begin{cases} 1 = b \\ 4 = -1 - a + b. \end{cases}$ seen ⇓

We can get $a = -4, b = 1$. 2, A

(ii) Write $(x, y) = (x_P, y_P) + (x_Q, y_Q)$. Let $m = \frac{y_P - y_Q}{x_P - x_Q} = -1$. Then by the doubling formula, we have $x = \frac{-2y_Py_Q + (x_P + x_Q)(x_Px_Q + a) + 2b}{(x_P - x_Q)^2} = 2$ and $y = -(mx + (y_Q - mx_Q)) = 1$. seen ⇓ 2, A

(iii) It suffices to find a point which is not torsion. By the theorem of Lutz–Nagell, if a point (x, y) is torsion, then either $y = 0$ or $y^2 | 4a^3 + 27b^2$. We can just consider the point $P = (1, 2)$. As 4 does not divide $-4^4 + 27$, the point P is not torsion. seen ⇓ 3, B

(iv) The reduction of E modulo 2 is $\bar{E} : y^2 = x^3 + 1$, which has a singular point $(0, 1)$. So it is singular. seen ⇓

(b) (i) Write $x = au$. Then $x^3 + ax + b = p^2((a^2u + b)/p^2 + au^3(a^2/p^2))$. So we need to find u such that $(a^2u + b)/p^2 + au^3(a^2/p^2) = T^2$ for some $T \in \mathbb{Z}_p$. By Hensel's lemma, we only need to prove $T^2 = (a^2u + b)/p^2 + au^3(a^2/p^2) \mod p$ has a non-trivial solution. As $|a|_p = 1/p$, we have $(a^2u + b)/p^2 + au^3(a^2/p^2) = (a^2u + b)/p^2 \mod p$. We have $(p - 1)$-choices of $u \mod p$. There are $(p-1)/2$-choices of non-zero squares $\mod p$. If $|b|_p < 1/p^2$, then $(a^2u + b)/p^2 \mod p$ is always non-zero. Since $p - 1 > (p - 1)/2$, there must exist some u such that $(a^2u + b)/p^2$ is a non-zero square $\mod p$. If $|b|_p = 1/p^2$, then there only exist $(p - 2)$-choices of u such that $(a^2u + b)/p^2 \mod p$ is non-zero. As $p > 3$, we see that $p - 2 > (p - 1)/2$. So there still exists some u such that $(a^2u + b)/p^2$ is a non-zero square $\mod p$. 2, A meth seen ⇓ 4, D

(ii) The reduction of E modulo p is given by $\bar{E} : y^2 = x^3$. The only singular point is $(0, 0)$. By (i), we can find some $u \in \mathbb{Z}_p^\times$ such that $(au)^3 + a^2u + b = y_0^2$ for some $y_0 \in \mathbb{Z}_p$. As $|(au)^3 + a^2u + b|_p < 1$, we see that $|y_0|_p < 1$. So the reduction of the point (au, y_0) modulo p is just $(0, 0)$, which implies $E(\mathbb{Q}_p) \neq E(\mathbb{Q}_p)^{(0)}$. meth seen ⇓ 3, A

(iii) Note that it suffices to show that if we have three collinear points, at most two of them can have x-coordinate (and thus y-coordinate) in $p\mathbb{Z}_p$. Now suppose that there is a line $y = mx + c$ meeting the curve at three such points. Then the three x-coordinates x_1, x_2, x_3 of this intersection are the roots of $x^3 + ax + b - (mx + c)^2 = 0$. So $x_1 + x_2 + x_3 = m^2$, which means $m \in p\mathbb{Z}_p$. Then $c = y - mx$ is also in $p\mathbb{Z}_p$. But we also have $x_1x_2 + x_2x_3 + x_1x_3 = a - mc$. As $|m|_p, |c|_p \leq 1/p$, we have $|x_1x_2 + x_2x_3 + x_1x_3|_p = |a - mc|_p = |a|_p = 1/p$. But our assumption that $|x_1|_p, |x_2|_p, |x_3|_p < 1$ implies that $|x_1x_2 + x_2x_3 + x_1x_3|_p \leq 1/p^2$. A contradiction. sim. seen ⇓ 4, D

4. (i) The three non-trivial 2-torsion points are $(0,0),(2,0),(10,0)$. seen ⇓

3, A

(ii) We see that $T_1=(10,0), T_2=(2,0), T_3=(0,0)$ and $e_1=10, e_2=2, e_3=0$. Explicitly, the δ-map meth seen ⇓

$$\delta : E(\mathbb{Q}) \to (\mathbb{Q}^\times/(\mathbb{Q}^\times)^2)^3$$

is defined by $\delta(x,y)=(x-10,x-2,x)$ if $y\neq 0$ and

$$\begin{aligned}\delta(10,0)&=(80,8,10)=(5,2,10),\\ \delta(2,0)&=(-8,-16,2)=(-2,-1,2),\\ \delta(0,0)&=(-10,-2,20)=(-10,-2,5),\\ \delta(\mathcal{O})&=(1,1,1).\end{aligned}$$

We know that $\mathrm{Im}(\delta)$ is contained in the subgroup $\{(\delta_1,\delta_2,\delta_3) \mid \delta_1\delta_2\delta_3=1\}$. So we can ignore the third coordinate. Also $\mathrm{Im}(\delta)$ is contained in the subgroup whose entries are in $\{\pm1,\pm2,\pm5,\pm10\}$.

In order to determine $\mathrm{Im}(\delta)$, we need to determine for which $b_1,b_2 \in \{\pm1,\pm2,\pm5,\pm10\}$ the equations

$$x-10=b_1u^2, \quad x-2=b_2v^2, \quad x=b_1b_2w^2$$

have a rational solution.

In order to do that, we need to solve the following equations

$$\begin{cases} b_2v^2-b_1u^2=8\\ b_1b_2w^2-b_1u^2=10.\end{cases}$$

Let $(b_1,b_2)=(1,2)$. Then we have

$$\begin{cases} 2v^2-u^2=8\\ 2w^2-u^2=10.\end{cases}$$

Write $w=\frac{W}{Z}, u=\frac{U}{Z}, v=\frac{V}{Z}$ for $W,U,V,Z\in\mathbb{Z}$ not all 0 and without common factors. Then we get $2W^2-U^2=10Z^2, 2V^2-U^2=8Z^2$. Since 2 is not a square modulo 5, we must have $5|W, 5|U$, which imply $5|Z$ and $5|V$. A contradiction. 8, D

(iii) Let $(b_1,b_2)=(1,5)$. Choose W,U,V,Z as above. Then we get $5V^2-U^2=8Z^2$ and $5W^2-5V^2=2Z^2$. This will imply $5|W,U,V,Z$. A contradiction. 5, B

(iv) As there are four 2-torsion points, we have $\#E(\mathbb{Q})/2E(\mathbb{Q})=\#\mathrm{Im}(\delta)=4\times 2^r$, where r is the rank of E. So $r=1$. 2, C

(v) For example, $E: y^2=x^3+x$. 2, A

5. (a) (i) We first prove the injection, i.e. if $u^4 = v^4$, then $u^2 = v^2$. Note that $u^{p-1} = 1, v^{p-1} = 1$. As $p \equiv 3 \mod 4$, we then have $u^{p-1} = u^{4(\frac{p-3}{4})}u^2 = v^{4(\frac{p-3}{4})}u^2 = 1 = v^{p-1}$. So $u^2 = v^2$. Now since $\mathbb{F}_p$ is finite, an injection from $(\mathbb{F}_p^\times)^2$ to $(\mathbb{F}_p^\times)^2$ must be a bijection. unseen ⇓ | 3, M

(ii) Make the change of variables $v + U = x$ and $v - U = y$, which is invertible as $p > 2$. Then it suffices to show the equation $xy = -4D$ has $(p-1)$ solutions in $\mathbb{F}_p \times \mathbb{F}_p$. This is true as $-4D$ is in $\mathbb{F}_p^\times$ (which means x, y must be units). unseen ⇓ | 4, M

(iii) Let $U = u^2$. Then by (i), we know that $v^2 - u^4 = -4D$ has the same number of solutions as $v^2 - U^2 = -4D$. By (ii), we know that $v^2 - U^2 = -4D$ has $(p-1)$ solutions. So we are done. unseen ⇓ | 2, M

(iv) To show the map ϕ is well-defined, we need to prove $(\frac{u(u^2+v)}{2})^2 = (\frac{u^2+v}{2})^3 + D(\frac{u^2+v}{2})$ for any $(u, v) \in C$. Using $v^2 = u^4 - 4D$, this then follows from direct calculations. unseen ⇓

Now we show the map ϕ is injective. For any $(u, v) \in C$, we see that $u^2 + v \neq 0$. Otherwise, we have $4D = u^4 - v^2 = u^4 - u^4 = 0$, which is a contradiction. Now let $(u_1, v_1), (u_2, v_2) \in C$. Suppose $\phi(u_1, v_1) = \phi(u_2, v_2)$. Then by taking the quotient of the y-coordinate by the x-coordinate, we see that $u_1 = u_2$. This also implies $v_1 = v_2$.

It is easy to see that $(0, 0)$ and the point at infinity $\mathcal{O}$ are in $E(\mathbb{F}_p)$. And both of them are not in the image of ϕ. Now let (x_0, y_0) be any other point in $E(\mathbb{F}_p)$. We can construct a point $(u_0, v_0) \in C$ such that $\phi(u_0, v_0) = (x_0, y_0)$. As x_0 is not 0, we can define $u_0 := \frac{y_0}{x_0}$ and $v_0 := 2x_0 - u_0^2$. Then $u_0^4 - v_0^2 = \frac{y_0^4}{x_0^4} - (2x_0 - \frac{y_0}{x_0})^2 = \frac{4y_0^2 - 4x_0^3}{x_0} = 4D$. So we must have $\#E(\mathbb{F}_p) = (p-1) + 2 = p + 1$. | 5, M

(b) (i) We first prove it is injective. Let $x_0, x_1 \in \mathbb{F}_p^\times$. Suppose $x_1^3 = x_2^3$. Note that $x_1^{p-1} = 1, x_2^{p-1} = 1$. We then have $x_1^{p-1} = x_1^{3(\frac{p-2}{3})}x_1 = x_2^{3(\frac{p-2}{3})}x_1 = 1 = x_2^{p-1}$. So $x_1 = x_2$. If $x^3 = 0$, then $x = 0$. This shows that $x \mapsto x^3$ is an injection from $\mathbb{F}_p$ to $\mathbb{F}_p$. As $\mathbb{F}_p$ is finite, this map is an bijection. unseen ⇓ | 3, M

(ii) Let $X = x^3$. By (i), we just need to show $y^2 = X + 1$ has $(p+1)$ solutions in $\mathbb{P}^2(\mathbb{F}_p)$. Note that there are $(p+1)/2$ quadratic residues (including 0) modulo p. So $y^2 = X + 1$ has $2(\frac{p-1}{2}) + 1 = p$ solutions in $\mathbb{A}^2(\mathbb{F}_p)$. Then $y^2 = X + 1$ has $(p+1)$ solutions in $\mathbb{P}^2(\mathbb{F}_p)$ after taking the point at infinity into account. unseen ⇓ | 3, M

Review of mark distribution:

Total A marks: 32 of 32 marks
Total B marks: 20 of 20 marks
Total C marks: 12 of 12 marks
Total D marks: 16 of 16 marks
Total marks: 100 of 80 marks
Total Mastery marks: 20 of 20 marks

MATH70064 Elliptic Curves

Question	Marker's comment
1	Most students did quite well. But the answers should be written in a more complete way. For example, in Question 1(b), we should first assume [x:y:z] is a solution such that the maximum of the 23-adic norms of x,y,z is 1. Then discuss whether x,y,z can be units or not. Some students just omit this part.
2	Most students did quite well. The common error is that the point at infinity is often ignored when students count the number of torsion rational points.nbsp;
3	Most students did quite well in the part (a) of Question 3. The common error lies in that there is a sign difference between the y-coordinate of the point P+Q and the y-coordinate of the third intersection point.Part (b) is relatively difficult. But the second question of part (b) should be a direct consequence of the first question of part (b).nbsp;
4	Question 4 is concerned with the 2-descent method. The students should understand how it works. The common error comes from part (b) and (c). To solve the equations concerning rational numbers u,v,w, one should first write u=U/Z,v=V/Z,w=W/Z such that U,V,Z,W are integers and have no common factors. Then you can consider its reduction modulo p.
5	Question 5 was answered better than I expected. The fourth question of part (a) might be relatively difficult. One needs to use this map to count the number of F_p-points. But the point (0,0) and the point at infinity are often ignored.nbsp;