INDIAN INSTITUTE OF TECHNOLOGY
KHARAGPUR

	Stamp / Signature of the Invigilator

EXAMINATION (End Semester)	**SEMESTER (Spring)**

Roll Number									**Section**		**Name**	

Subject Number	C	S	6	0	0	9	4	**Subject Name**	*Computational Number Theory*

Department / Center of the Student		**Additional sheets**	

Important Instructions and Guidelines for Students

1. You must occupy your seat as per the Examination Schedule/Sitting Plan.
2. Do not keep mobile phones or any similar electronic gadgets with you even in the switched off mode.
3. Loose papers, class notes, books or any such materials must not be in your possession, even if they are irrelevant to the subject you are taking examination.
4. Data book, codes, graph papers, relevant standard tables/charts or any other materials are allowed only when instructed by the paper-setter.
5. Use of instrument box, pencil box and non-programmable calculator is allowed during the examination. However, exchange of these items or any other papers (including question papers) is not permitted.
6. Write on both sides of the answer script and do not tear off any page. **Use last page(s) of the answer script for rough work.** Report to the invigilator if the answer script has torn or distorted page(s).
7. It is your responsibility to ensure that you have signed the Attendance Sheet. Keep your Admit Card/Identity Card on the desk for checking by the invigilator.
8. You may leave the examination hall for wash room or for drinking water for a very short period. Record your absence from the Examination Hall in the register provided. Smoking and the consumption of any kind of beverages are strictly prohibited inside the Examination Hall.
9. Do not leave the Examination Hall without submitting your answer script to the invigilator. **In any case, you are not allowed to take away the answer script with you.** After the completion of the examination, do not leave the seat until the invigilators collect all the answer scripts.
10. During the examination, either inside or outside the Examination Hall, gathering information from any kind of sources or exchanging information with others or any such attempt will be treated as **‘unfair means’**. Do not adopt unfair means and do not indulge in unseemly behavior.

Violation of any of the above instructions may lead to severe punishment.

Signature of the Student

To be filled in by the examiner

Question Number	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Total**
Marks Obtained											

Marks obtained (in words)	**Signature of the Examiner**	**Signature of the Scrutineer**

CS60094 Computational Number Theory, Spring 2017–2018

End-Semester Test

25–April–2018 CSE-107, 09:00am–12:00noon Maximum marks: 80

[*Write your answers in the question paper itself. Be brief and precise. Answer all questions. If you use any algorithm/result/formula covered in the class, just mention it, do not elaborate.*]

1. Consider the conic section defined by $C : f(X,Y) = 0$, where $f(X,Y) = X^2 - 2XY - 3Y^2 + 4X - 4Y - 5$. Treat C as a real curve (that is, let X,Y be real-valued variables).

(a) Prove that C is smooth at all finite rational points on the curve. **(4)**

Solution For the curve to have a singularity at some finite rational point (X,Y) on C, both the partial derivatives $\frac{\partial f}{\partial X}$ and $\frac{\partial f}{\partial Y}$ must vanish simultaneously at that point. We have

$$\begin{aligned}\frac{\partial f}{\partial X} &= 2X - 2Y + 4,\\ \frac{\partial f}{\partial Y} &= -2X - 6Y - 4.\end{aligned}$$

Thus $\frac{\partial f}{\partial X} = \frac{\partial f}{\partial Y} = 0$ implies that

$$\begin{aligned}X - Y &= -2,\\ X + 3Y &= -2.\end{aligned}$$

Solving these two linear equations gives $X = -2$ and $Y = 0$. But

$$f(-2,0) = 4 - 0 - 0 - 8 - 0 - 5 = -9 \neq 0,$$

that is, $(-2,0)$ is not a finite rational point on C.

(b) Find all the points at infinity on C. **(4)**

Solution The homogenization of the curve is

$$f^{(h)}(X,Y,Z) = X^2 - 2XY - 3Y^2 + 4XZ - 4YZ - 5Z^2 = 0.$$

Putting $Z = 0$ gives

$$\begin{aligned}X^2 - 2XY - 3Y^2 &= 0, \quad \text{that is,}\\ (X+Y)(X-3Y) &= 0, \quad \text{that is,}\\ X &= -Y, 3Y.\end{aligned}$$

Therefore, C contains two points at infinity: $[-1,1,0]$ and $[3,1,0]$.

(c) Let the projective curve corresponding to C be $C^{(h)} : f^{(h)}(X,Y,Z) = 0$. $C^{(h)}$ is smooth at a point at infinity on the curve if the three partial derivatives $\frac{\partial f^{(h)}}{\partial X}$, $\frac{\partial f^{(h)}}{\partial Y}$, and $\frac{\partial f^{(h)}}{\partial Z}$ do not vanish simultaneously at the point at infinity. Prove that the given curve is smooth at its points at infinity. **(4)**

Solution We have

$$f^{(h)}(X,Y,Z) = X^2 - 2XY - 3Y^2 + 4XZ - 4YZ - 5Z^2,$$

so

$$\begin{aligned}\frac{\partial f^{(h)}}{\partial X} &= 2X - 2Y + 4Z,\\ \frac{\partial f^{(h)}}{\partial Y} &= -2X - 6Y - 4Z,\\ \frac{\partial f^{(h)}}{\partial Z} &= 4X - 4Y - 10Z.\end{aligned}$$

The simultaneous vanishing of these three partial derivatives gives the system

$$\begin{aligned}X - Y + 2Z &= 0,\\ X + 3Y + 2Z &= 0,\\ 2x - 2Y - 5Z &= 0.\end{aligned}$$

The only solution of this system is $X = Y = Z = 0$, but $[0,0,0]$ is not a point in the projective plane (let alone being a point at infinity on C).

(d) Deduce that by a suitable transformation (that is, renaming) of the coordinates as

$$(X,Y) \leftarrow (\alpha X + \beta Y + \gamma, \alpha' X + \beta' Y + \gamma'),$$

where $\alpha, \beta, \gamma, \alpha', \beta', \gamma' \in \mathbb{R}$, the given curve C can be converted to the hyperbola $X^2 - Y^2 = 1$. **(4)**

Solution We have

$$X^2 - 2XY - 3Y^2 + 4X - 4Y - 5 = (X-Y)^2 - 4Y^2 + 4(X-Y) - 5.$$

The coordinate transformation

$$(X,Y) \leftarrow (X-Y, Y)$$

changes the equation of the curve to $X^2 - 4Y^2 + 4X - 5 = 0$, that is, $(X^2 + 4X + 4) - 4Y^2 = 9$, that is, $(X+2)^2 - (2Y)^2 = 3^2$, that is,

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

So we need another coordinate transformation

$$(X,Y) \leftarrow ((X+2)/3, (2Y)/3).$$

Combining together the two coordinate transformations gives

$$(X,Y) \leftarrow ((X-Y+2)/3, (2Y)/3)),$$

that is,

$$\alpha = 1/3, \quad \beta = -1/3, \quad \gamma = 2/3, \quad \alpha' = 0, \quad \beta' = 2/3, \quad \text{and} \quad \gamma' = 0.$$

2. Consider the elliptic curve $E : Y^2 = X^3 - X + 1$ defined over the finite field $\mathbb{F}_{11}$.

(a) Find all the finite $\mathbb{F}_{11}$-rational points on E. Show your calculations. **(6)**

Solution All the squares modulo 11 are:

$$\begin{array}{rcrcl}
 & & 0^2 & \equiv & 0 \pmod{11} \\
1^2 & \equiv & 10^2 & \equiv & 1 \pmod{11} \\
2^2 & \equiv & 9^2 & \equiv & 4 \pmod{11} \\
3^2 & \equiv & 8^2 & \equiv & 9 \pmod{11} \\
4^2 & \equiv & 7^2 & \equiv & 5 \pmod{11} \\
5^2 & \equiv & 6^2 & \equiv & 3 \pmod{11}
\end{array}$$

Now, we plug in different values of $X \pmod{11}$, and try to solve $Y^2 \equiv X^3 - X + 1 \pmod{11}$. The following table summarizes these calculations.

X	$X^3 - X + 1 \pmod{11}$	Number of solutions	Finite points
0	1	2	$(0,1),(0,10)$
1	1	2	$(1,1),(1,10)$
2	7	0	
3	3	2	$(3,5),(3,6)$
4	6	0	
5	0	1	$(5,0)$
6	2	0	
7	7	0	
8	10	0	
9	6	0	
10	1	2	$(10,1),(10,10)$

(b) What is the size of the group $E(\mathbb{F}_{11})$? **(2)**

Solution By Part (a), there are nine finite rational points on E. Considering the point at infinity, we have

$$|E(\mathbb{F}_{11})| = 9 + 1 = 10.$$

(c) E is naturally defined over the extension field $\mathbb{F}_{11^2} = \mathbb{F}_{121}$. Using Weil's theorem, determine the size of the group $E(\mathbb{F}_{11^2}) = E(\mathbb{F}_{121})$. Show your calculations. **(4)**

Solution Let t be the trace of Frobenius at $p = 11$. We have

$$10 = |E(\mathbb{F}_p)| = p + 1 - t = 12 - t,$$

that is, $t = 2$. The two solutions of the quadratic equation

$$W^2 - tW + p = W^2 - 2W + 11 = 0$$

are $\alpha = 1 + \mathrm{i}\sqrt{10}$ and $\beta = 1 - \mathrm{i}\sqrt{10}$. Therefore the trace of Frobenius at $p^2 = 11^2$ is

$$\alpha^2 + \beta^2 = 2 \times (1 - 10) = -18,$$

that is,

$$|E(\mathbb{F}_{p^2})| = 11^2 + 1 - (-18) = 140.$$

3. In this exercise, we factor $n = 3869$ using Dixon's method. Complete the details of the following steps in a possible run of Dixon's method. Take the factor base $B = \{2, 3, 5, 7\}$.

(a) [*Relation generation*] The following six relations are generated for randomly chosen values of $a \in \mathbb{Z}_n$. Compute $a^2 \pmod{n}$, and write its factorization over B, for the given values of a (two cases are shown). **(4)**

a	$a^2 \pmod{n}$
752	$630 = 2 \times 3^2 \times 5 \times 7$
2136	$945 = 3^3 \times 5 \times 7$
2007	$420 = 2^2 \times 3 \times 5 \times 7$
880	$600 = 2^3 \times 3 \times 5^2$
3032	$280 = 2^3 \times 5 \times 7$
1432	$54 = 2 \times 3^3$

(b) [*System generation*] Take $\mathbb{Z}_2$-valued variables u, v, w, x, y, z. Raise the six relations respectively to the u, v, w, x, y, z-th powers, and multiply. Write down the 4×6 linear system of congruences obtained modulo 2. **(4)**

Solution The exponents of $2, 3, 5, 7$ in the selected product of relations are $u + 2w + 3x + 3y + z$, $2u + 3v + w + x + 3z$, $u + v + w + 2x + y$, and $u + v + w + y$, respectively. All these exponents are desired to be even, so we have the following system of linear equations modulo 2.

$$\begin{aligned} u + x + y + z &= 0, \\ v + w + x + z &= 0, \\ u + v + w + y &= 0, \\ u + v + w + y &= 0, \end{aligned}$$

that is,

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} u \\ v \\ w \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

(c) [*Linear algebra*] Apply Gaussian elimination to the coefficient matrix M of the linear system from Part (b), in order to identify the free variables. Express the dependent variables in terms of the free variables. Finally, write the column vector $\begin{pmatrix} u & v & w & x & y & z \end{pmatrix}^{\mathrm{t}}$ as a linear combination of the free variables. The coefficients of the free variables constitute a basis of the null space of M. **(4)**

Solution We convert the coefficient matrix to the row-reduced echelon form. At every step, the pivot is highlighted.

Solution
$$\begin{pmatrix} \boxed{1} & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & \boxed{1} & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

It follows that w, x, y, z are free variables, and the dependent variables are $u = x + y + z$ and $v = w + x + z$. We therefore have

$$\begin{pmatrix} u \\ v \\ w \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x+y+z \\ w+x+z \\ w \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} w + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} x + \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} y + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} z.$$

(d) [*Split n by a non-trivial Fermat congruence*] Find a non-zero combination of the free variables, that splits n. Work out, in the rough space, a combination that works, and show the corresponding computations. **(4)**

Solution Here, we get the Fermat congruence $\alpha^2 \equiv \beta^2 \pmod{n}$ for all of the 16 values of w, x, y, z. For students, it suffices to show only one non-trivial split.

$wxyz$	α	β	$\gcd(\alpha - \beta, n)$	$wxyz$	α	β	$\gcd(\alpha - \beta, n)$
0000	1	1	3869	1000	100	630	53
0001	2969	1801	73	1001	89	3780	1
0010	1223	420	73	1010	2361	1508	1
0011	3780	3780	3869	1011	400	2520	53
0100	3424	3424	3869	1100	2000	993	53
0101	2735	180	73	1101	2670	1199	1
0110	1869	993	73	1110	3207	662	1
0111	2089	2089	3869	1111	3843	610	53

Let us see a sample calculation for the choice $wxyz = 0110$. The dependent variables for these choices are $u \equiv x + y + z \equiv 0 \pmod{2}$, and $v \equiv w + x + z \equiv 1 \pmod{2}$, that is, $uvwxyz = 010110$. Therefore $\alpha \equiv 2136 \times 880 \times 3032 \equiv 1869 \pmod{3869}$. The exponents of $2, 3, 5, 7$ on the other side of congruence are halves of $u + 2w + 3x + 3y + z = 6$, $2u + 3v + w + x + 3z = 4$, $u + v + w + 2x + y = 4$, and $u + v + w + y = 2$, that is, $\beta \equiv 2^3 \times 3^2 \times 5^2 \times 7 \equiv 993 \pmod{3869}$. We have $\gcd(1869 - 993, 3869) = 73$.

4. (a) Let $E = E_{A,B}$ be an elliptic curve defined by the equation $Y^2 = X^3 + AX + B$ over a field K which is not algebraically closed, and which has $\mathrm{char}(K) \notin \{2,3\}$. For such an elliptic curve $E_{A,B}$, denote the set of polynomials on E as $K[E] = K[X,Y]/(Y^2 - X^3 - AX - B)$. Prove that a polynomial $f(x,y) \in K[E]$ can be written *uniquely* in the canonical form. **(5)**

Solution As $E_{A,B}$ is quadratic and monic in y, the polynomial function can be expressed as $f(x,y) = v(x) + yw(x)$ with $v(x), w(x) \in K[x]$. We prove the uniqueness of this expression by contradiction. Let $f(x,y) = v_1(x) + yw_1(x) = v_2(x) + yw_2(x)$ be two canonical forms of f, that is, $(v_1(x) - v_2(x)) + y(w_1(x) - w_2(x)) = 0$.

Setting $v(x) = v_1(x) - v_2(x)$, $w(x) = w_1(x) - w_2(x)$, we have $v(x) + yw(x) = 0$. Multiplying both sides by $v(x) - yw(x)$, we get $v^2(x) - s(x)w^2(x) = 0$, where $s(x) = y^2 = x^3 + Ax + B$. Notice that $\deg_x(v^2(x))$ and $\deg_x(w^2(x))$ are both even. But $\deg_x(s(x))$ is odd. Thus, we have a contradiction unless $v(x) = w(x) = 0$.

(b) Let $K(E)$ denote the set of rational functions on the elliptic curve $E_{A,B}$. Prove that a rational function $r(x,y) \in K(E)$ with no finite poles is a polynomial. (**Hint:** Express $r(x,y)$ in the canonical form $a(x) + yb(x)$ with $a(x), b(x) \in K(x)$, and show that neither $a(x)$ nor $b(x)$ has finite poles. You may make use of the fact that if $r(x,y)$ does not have finite poles, the conjugate $\overline{r(x,y)} = a(x) - yb(x)$ also does not have finite poles.) **(5)**

Solution Write $r(x,y) \in K(E)$ without poles in the canonical form $r(x,y) = a(x) + yb(x)$ with $a(x), b(x) \in K(x)$.

As $r(x,y)$ (or in brief r) has no finite poles, $\overline{r} = a - yb$ too has no finite poles $\Rightarrow r + \overline{r} = 2a$ does not have finite poles $\Rightarrow r - a = yb$ does not have finite poles $\Rightarrow (yb)^2 = sb^2$ has no finite poles.

Assume that b has a pole of multiplicity $m \geqslant 1 \Rightarrow b^2$ has a pole of multiplicity $2m \geqslant 2$. But sb^2 does not have a finite pole, so s has a zero of multiplicity $2m \geqslant 2$. This contradicts the smoothness of the elliptic curve $E_{A,B}$.

5. Let n be a positive integer, and let $k = \lfloor \log_2 n \rfloor + 1$, which implies that $2^k > n$. Provide a proof of the fact that n always has an expansion of the form

$$n = u_0 + u_1 \cdot 2 + u_2 \cdot 4 + \cdots + u_k \cdot 2^k$$

with $u_0, u_1, \ldots, u_k \in \{-1, 0, 1\}$, and with at most $\frac{1}{2}k$ of the u_i non-zero. **(5)**

Solution The proof is presented as an algorithm for writing n in the desired form. We start by writing n in binary:

$$n = u_0 + u_1 \cdot 2 + u_2 \cdot 4 + \cdots + u_{k-1} \cdot 2^{k-1}. \tag{1}$$

Working from left to right, we look for the occurrence of two or more consecutive non-zero coefficients u_i. For example, suppose $u_s = u_{s+1} = \cdots = u_{s+t-1} = 1$, and $u_{s+t} = 0$, for some $t \geqslant 1$. Then, we can replace $2^s + 2^{s+1} + \cdots + 2^{s+t-1} + 0 \cdot 2^{s+t} = 2^s(1 + 2 + 4 + \cdots + 2^{t-1}) = 2^s(2^t - 1) = -2^s + 2^{s+t}$.

Repeating this procedure gives us an expansion of n with no consecutive non-zero u_i. This expansion can go up to 2^k (as opposed to the original expansion which goes up to 2^{k-1}). Thus, at most $\frac{1}{2}k$ of the u_i are non-zero.

6. A non-supersingular elliptic curve E over $\mathbb{F}_{2^m}$ consists of all the solutions $(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ of the equation $y^2 + xy = x^3 + ax^2 + b$, where a and b are in $\mathbb{F}_{2^m}$ and $b \neq 0$, together with the point at infinity denoted by $\mathscr{O}$. Let $P = (x,y)$, $P_1 = (x_1,y_1)$, and $P_2 = (x_2,y_2)$ be finite rational points on E. Assume that $P_2 = P_1 + P$. Prove that the x-coordinate x_3 of $P_1 + P_2$ can be computed in terms of the x-coordinates of P, P_1, and P_2 as **(5)**

$$x_3 = \begin{cases} \left(\dfrac{x_1}{x_1+x_2}\right)^2 + \dfrac{x_1}{x_1+x_2} + x & \text{if } P_1 \neq P_2, \\ x_1^2 + \dfrac{b}{x_1^2} & \text{if } P_1 = P_2. \end{cases}$$

Solution From the chord-and-tangent rule of addition on elliptic-curve points, we have

$$x_3 = \begin{cases} \left(\dfrac{y_1+y_2}{x_1+x_2}\right)^2 + \dfrac{y_1+y_2}{x_1+x_2} + x_1 + x_2 + a & \text{if } P_1 \neq P_2, \\ x_1^2 + \dfrac{b}{x_1^2} & \text{if } P_1 = P_2. \end{cases}$$

Hence, for the case $P_1 = P_2$, the result is straightforward.

As $P_1 = (x_1,y_1)$ and $P_2 = (x_2,y_2)$ are on the curve, we have $y_1^2 + x_1y_1 = x_1^3 + ax_1^2 + b$ and $y_2^2 + x_2y_2 = x_2^3 + ax_2^2 + b$, so

$$x_3 = \frac{x_1y_2 + x_2y_1 + x_1x_2^2 + x_2x_1^2}{(x_1+x_2)^2}. \tag{2}$$

The x-coordinate of $P_2 - P_1$ is

$$x = \frac{x_1y_2 + x_2(x_1+y_1) + x_1x_2^2 + x_2x_1^2}{(x_1+x_2)^2}. \tag{3}$$

Adding (2) and (3), we obtain the desired result.

7. Consider the elliptic curve $E : Y^2 = (X-1)(X-2)(X-3)$ defined over $\mathbb{F}_5$. Answer the following parts in the context of this curve.

(a) Assuming that $\mathbb{F}_5$ is represented by the set $\{0,1,2,-2,-1\}$, annotate the points on the elliptic curve. **(3)**

$P_1 = (0,2)$

$P_2 = (-1,1)$

$P_3 = (-2, \underline{\quad 0 \quad})$

$P_4 = (-1, \underline{\quad -1 \quad})$

$P_5 = (0, \underline{\quad -2 \quad})$

$P_6 = (1, \underline{\quad 0 \quad})$

$P_7 = (2, \underline{\quad 0 \quad})$

$P_8 = \underline{\quad \mathcal{O} \quad}$

(b) Show that the rational function $f(x) = (x-1) \in \mathbb{F}_5(E)$ has divisor $\operatorname{div}(f) = 2[P_6] - 2[\mathcal{O}]$. **(3)**

Solution The function f has neither a zero nor a pole if $x \neq 1$. The uniformizer at $P_6 = (1,0)$ is y. Write $f(x,y) = x - 1 = \frac{y^2}{(x-2)(x-3)}$. Hence, the degree of f at P_6 is 2, and the result follows from the fact that the sum of the (signed) multiplicities of the zeros and the poles of a rational function is zero.

(c) Prove that the order of the point P_2 in $E(\mathbb{F}_5)$ is 4. **(2)**

Solution $2P_2 = P_7$, and $2P_7 = \mathcal{O}$.

(d) Using Miller's algorithm, find the rational functions f_{P_2} and f_{P_4}, such that $\operatorname{div}(f_{P_2}) = 4[P_2] - 4[\mathscr{O}]$, and $\operatorname{div}(f_{P_4}) = 4[P_4] - 4[\mathscr{O}]$. **(4)**

Solution We have $f_{P_2} = \dfrac{(y+2x+1)^2}{(x-2)} = x^2 + 4y$, and $f_{P_4} = \dfrac{(y-2x-1)^2}{(x-2)} = x^2 - 4y$.

(e) Compute the Weil pairing $e_4(P_2, P_4)$ from the formula

$$e_4(P_2,P_4) = \frac{f_{P_2}(P_4+S)}{f_{P_2}(S)} \Bigg/ \frac{f_{P_4}(P_2-S)}{f_{P_4}(-S)}$$

by taking $S = P_4$. Note that the definition holds for any $S \notin \{\mathscr{O}, P_2, -P_4, P_2 - P_4\}$.

(**Hint:** Ensure that the functions f_{P_2} and f_{P_4} are in normal forms.) **(4)**

Solution By taking $S = P_4$, we have

$$e_4(P_2,P_4) = \frac{f_{P_2}(2P_4)}{f_{P_2}(P_4)} \Bigg/ \frac{f_{P_4}(P_2-P_4)}{f_{P_4}(-P_4)}.$$

Now, $P_4 = (-1,-1) \Rightarrow 2P_4 = P_7 = (2,0)$, $-P_4 = P_2 = (-1,1)$, $P_2 - P_4 = 2P_2 = P_7 = (2,0)$. Therefore $e_4(P_2,P_4) = \dfrac{f_{P_2}(2,0)}{f_{P_2}(-1,-1)} \Bigg/ \dfrac{f_{P_4}(2,0)}{f_{P_4}(-1,1)} = \left(\dfrac{4}{-3}\right) \Bigg/ \left(\dfrac{4}{-3}\right) = 1.$

FOR LEFTOVER ANSWERS OR ROUGH WORK

FOR ROUGH WORK

FOR ROUGH WORK