PROBLEMS FOR AFTERNOON SESSION (GARLAT 2026)

DEBANJANA KUNDU

1. Elliptic Curves over $\mathbb{Q}$

Problem 1.1. Let $d \in \mathbb{Z} \setminus \{0\}$ and let E be an elliptic curve given by the cubic equation

$$X^3 + Y^3 = dZ^3$$

with $\mathcal{O} = [1, -1, 0]$.

(1) Show that E is a smooth curve.
(2) Find the Weierstrass equation for E.

Problem 1.2. Consider the curve

$$C/\mathbb{Q} : V^2 = U^4 + 1 \quad \text{and} \quad \mathsf{E}/\mathbb{Q} : y^2 = x^3 - 4x.$$

(1) Find an invertible rational map $\psi : C \to \mathsf{E}$ defined over $\mathbb{Q}$.
(2) Where does it send $(U, V) = (0, \pm 1)$?

Problem 1.3. A positive integer n is called a *congruent number*, if there exists a right-angled triangle with *rational* sides such that its area is n.

Define the following two sets

$$C_n \coloneqq \{(a, b, c) \in \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q} \ : \ a^2 + b^2 = c^2, \ ab/2 = n\}$$
$$E_n \coloneqq \{(x, y) \in \mathbb{Q} \times \mathbb{Q} \ : \ y^2 = x^3 - n^2 x, \ y \neq 0\}.$$

Show that there is a one-to-one correspondence between C_n and E_n given by the following two mutually inverse maps

$$\psi : (a, b, c) \mapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a} \right),$$
$$\phi : (x, y) \mapsto \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y} \right).$$

Problem 1.4. In this exercise, we will work with the specific elliptic curve

$$\mathsf{E} : y^2 = x^3 - x = x(x-1)(x+1).$$

(1) What is the structure of $\mathsf{E}(\mathbb{Q})[2]$?
(2) Define the map

$$\delta : \mathsf{E}(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$
$$\mathsf{P} = (x_0, y_0) \mapsto \delta(\mathsf{P}) = \begin{cases} (1,1,1) & \text{if } \mathsf{P} = \mathcal{O} \\ (x_0, x_0 - 1, x_0 + 1) & \text{if } y_0 \neq 0 \\ (-1,-1,1) & \text{if } \mathsf{P} = (0,0) \\ (1,2,2) & \text{if } \mathsf{P} = (1,0) \\ (-1,-2,2) & \text{if } \mathsf{P} = (-1,0). \end{cases}$$

Date: July 15, 2026.

(a) Check that δ is a homomorphism of groups.
(b) Show that if $\delta(\mathsf{P}) = (\delta_1, \delta_2, \delta_3)$ then $\delta_1 \times \delta_2 \times \delta_3 = 1$ in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.
(c) What is the kernel of δ?
(d) Let $\mathsf{P} = (x_0, y_0) \in \mathsf{E}(\mathbb{Q})$. Write

$$x_0 = au^2, \quad x_0 - 1 = bv^2, \quad x_0 + 1 = cw^2, \quad y_0^2 = abc(uvw)^2,$$

such that $a, b, c \in \mathbb{Z}$ are square-free and abc is a square in $\mathbb{Z}$, whereas $u, v, w \in \mathbb{Q}$. Show that an odd prime does not divide abc.
(e) Use this to show that each δ_i can be represented by elements in $\{\pm 1, \pm 2\} =: \Gamma'$.
(f) Let us denote the image of $\mathsf{E}(\mathbb{Q})/2\mathsf{E}(\mathbb{Q})$ under the map δ by $\delta(\mathsf{E})$. Show that $\delta(\mathsf{E})$ embeds in

$$\Gamma_{\mathsf{E}} = \{(\delta_1, \delta_2, \delta_3) \in \Gamma' \times \Gamma' \times \Gamma' \ : \ \delta_1 \times \delta_2 \times \delta_3 = 1 \text{ modulo squares}\}.$$

(g) Conclude that $\mathsf{E}(\mathbb{Q})/2\mathsf{E}(\mathbb{Q})$ is finite.
(3) What is the discriminant Δ_{E}?
(4) Find an upper bound on the rank of $\mathsf{E}(\mathbb{Q})$ in terms of the number of distinct prime divisors of Δ_{E}.
(5) Define the *homogeneous space*

$$C(\delta_1, \delta_2) : \begin{cases} -1 = \delta_2 Y^2 - \delta_1 X^2 \\ -2 = \delta_2 Y^2 - \delta_1 \delta_2 Z^2. \end{cases}$$

This is the intersection of two conics. Further define

$$\mathcal{H} \coloneqq \{C(\delta_1, \delta_2) \ : \ \delta_1, \delta_2 \in \Gamma'\}.$$

Some homogeneous spaces in $\mathcal{H}$ have rational points that correspond to $\mathsf{P} \in \mathsf{E}(\mathbb{Q})$, whereas other homogeneous spaces do not have points.
(a) If $(\delta_1, \delta_2, \delta_3) \in \delta(\mathsf{E})$, show that $C(\delta_1, \delta_2)$ has a point with rational coordinates.
(b) If $C(\delta_1, \delta_2)$ has a rational point then find the corresponding point P in $\mathsf{E}(\mathbb{Q})$.
(c) Show that $\delta(\mathsf{E})$ is a subgroup of Γ_{E}.
(6) Use the above exercise to conclude the size of $\delta(\mathsf{E})$.
(7) Use (4) to find the rank of E.
(8) Define the 2-*Selmer group* as

$$\mathrm{Sel}_2(\mathsf{E}/\mathbb{Q}) \coloneqq \{C(\delta_1, \delta_2) \text{ with points over } \mathbb{R} \text{ and } \mathbb{Q}_p \text{ for all primes } p\}.$$

The Selmer group is the set of all homogeneous spaces that are solvable everywhere locally.
(a) What is the size of the 2-Selmer group?
(b) Show that the 2-Selmer group contains (a subgroup isomorphic to) $\mathsf{E}(\mathbb{Q})/2\mathsf{E}(\mathbb{Q})$.
(9) Define the *Shafarevich–Tate group* as the quotient of $\mathrm{Sel}_2(\mathsf{E}/\mathbb{Q})$ by its subgroup $\mathsf{E}(\mathbb{Q})/2\mathsf{E}(\mathbb{Q})$.
(a) Write a description of $Ш_2(\mathsf{E}/\mathbb{Q})$ as a subgroup of $\mathcal{H}$.
(b) What is the size of $Ш_2(\mathsf{E}/\mathbb{Q})$?

The above problem is an example of *2-descent*. This is a general technique to show the finiteness of $\mathsf{E}(\mathbb{Q})/2\mathsf{E}(\mathbb{Q})$ when an elliptic curve is written as $y^2 = (x - e_1)(x - e_2)(x - e_3)$ with $e_i \in \mathbb{Z}$ and $e_1 + e_2 + e_3 = 0$. This is a special case of the weak Mordell–Weil Theorem.

Problem 1.5. The purpose of this exercise is to justify the name 'descent'.

(1) [Parameterization of Pythagorean triples] Suppose that x, y, z are relatively prime positive integers such that

$$x^2 + y^2 = z^2.$$

Then one of x, y is even. Suppose that it is x. Then there exist positive integers m, n such that

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2.$$

Moreover, $\gcd(m, n) = 1$ and $m \not\equiv n \pmod 2$.

(2) Consider the equation

$$a^4 + b^4 = c^2. \tag{$\star$}$$

(a) Suppose there exist non-zero integer solutions (a, b, c). Show that (without loss of generality)

$$a^2 = 2mn, \quad b^2 = m^2 - n^2, \quad c = m^2 + n^2.$$

Conclude that n is even and m is odd.

(b) Set $n = 2q$. Show that m, q must both be squares.

(c) Set $m = t^2$ and $q = u^2$ for positive t, u and rewrite

$$b^2 = m^2 - n^2 = t^4 - 4u^4.$$

Conclude that

$$t^2 = r^4 + s^4,$$

for some r, s with $\gcd(r, s) = 1$.

(d) Show that $t < c$. Use this to arrive at a contradiction to the existence of non-trivial integer solutions (a, b, c).

(3) Suppose we do not know that $(\star)$ does not have non-zero integer solutions. Consider the curves from Problem 1.2

$$C : V^2 = U^4 + 1 \text{ and } \mathsf{E} : y^2 = x^3 - 4x.$$

(a) In view of $(\star)$, we may start with the following point on C

$$(U, V) = \left(\frac{a}{b}, \frac{c}{b^2}\right)$$

Show that it maps to the point Q such that

$$x(\mathsf{Q}) = \left(\frac{t}{rs}\right)^2.$$

(b) Find $x(\mathsf{Q}) \pm 2$. In particular note that both these expressions are rational squares.

(c) Define the map

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

$$\mathsf{P} = (x_0, y_0) \mapsto \delta(\mathsf{P}) = \begin{cases} (1, 1, 1) & \text{if } \mathsf{P} = \mathcal{O} \\ (x_0, x_0 - 2, x_0 + 2) & \text{if } y_0 \neq 0 \\ (-4, -2, 2) & \text{if } \mathsf{P} = (0, 0) \\ (2, 8, 4) & \text{if } \mathsf{P} = (2, 0) \\ (-2, -4, 8) & \text{if } \mathsf{P} = (-2, 0). \end{cases}$$

Show that $\mathsf{Q} = 2\mathsf{P}$ for some $\mathsf{P} \in \mathsf{E}(\mathbb{Q})$.

(d) Explicitly find the polynomial $f(T) = u_0 + u_1 T + u_2 T^2$ in $\mathbb{Q}[T]$ such that

$$f(0)^2 = x(\mathsf{Q}), \quad f(2)^2 = x(\mathsf{Q}) - 2, \quad f(-2)^2 = x(\mathsf{Q}) + 2.$$

Show that

$$x(\mathsf{Q}) - T \equiv f(T)^2 \pmod{T^3 - 4T}.$$

Deduce that

$$\left(\frac{1}{u_2}\right)^2 = \left(\frac{u_1}{u_2}\right)^3 - 4\left(\frac{1}{u_2}\right)^2.$$

(e) Show that the point

$$\mathsf{P} = (x_1, y_1) = \left(\frac{u_1}{u_2}, \frac{1}{u_2}\right)$$

satisfies $2\mathsf{P} = \mathsf{Q}$.

(f) Use the inverse transformation found in Problem 1.2 from $\mathsf{E} \to \mathbb{C}$ to find the solution on C corresponding to P. *This new solution will be in terms of* (r, s, t). *Given any rational point* P *on* $\mathsf{E}(\mathbb{Q})$ *we can define a non-negative real valued function* $\hat{h}$ *called* canonical height *such that* $\hat{h}(n\mathsf{P}) = n^2 n\mathsf{P}$ *for all* n. *In this exercise, we showed that Fermat's procedure can be interpreted as starting with a rational point on* E *and halving it. This decreases the height by a factor of 4; so the process must stop. Once again, this means we could not have started with a non-trivial solution.*

(4) Show that 2 is not a congruent number.

Problem 1.6. Prove or disprove the following assertion: 1 is a congruent number.

Problem 1.7. Let p be a prime and define

$$\mathsf{E}_p : y^2 = x^3 + p^2.$$

Show that $\mathsf{E}(\mathbb{Q})_{\text{tor}} \simeq \mathbb{Z}/3\mathbb{Z}$.

Problem 1.8. More generally, let k be any non-zero integer (assume it to be 6-th power free). Consider the family of Mordell-curves

$$\mathsf{E}_k : y^2 = x^3 + k.$$

Predict (and prove) the torsion structure of $\mathsf{E}_k(\mathbb{Q})$.

Problem 1.9. (1) Consider Montgomery family of elliptic curves (over $\mathbb{Q}$) given by

$$M_{A,B} : BY^2 = X^3 + AX^2 + X \text{ such that } A, B \in \mathbb{Q} \text{ and } B(A^2 - 4) \neq 0.$$

Perform a change of variables and write this in short Weierstrass form.

(2) Next consider the family of elliptic curve in the twisted Edwards form given by

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2 \text{ where } a, d \in \mathbb{Q}^\times \text{ and } a \neq d.$$

Set $A = \frac{2(a+d)}{a-d}$ and $B = \frac{4}{a-d}$. Show that $E_{a,d}$ and $M_{A,B}$ are birationally equivalent. *See* [1, Theorem 3.2] *if you are interested in learning more.*

2. Elliptic Curves over $\mathbb{C}$

Problem 2.1. For any elliptic curve E, denote the n-torsion subgroup $\mathsf{E}[n]$ to be the set of points on an elliptic curve of order dividing n. In other words,

$$\mathsf{E}[n] = \{\mathsf{P} \in \mathsf{E} \ : n\mathsf{P} = \mathcal{O}\},$$

where $\mathcal{O}$ is the identity element under the elliptic curve group law (corresponding to the point at infinity). We write $\mathsf{P} \in \mathsf{E}$ to mean $\mathsf{P} \in \mathsf{E}(\mathbb{C})$.

For any n, show that $\mathsf{E}[n]$ is isomorphic to the direct sum $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by giving an explicit map. *We can say that* $\mathsf{E}[n]$ *is generated by two 'basis' elements* P *and* Q *and every element of* $\mathsf{E}[n]$ *can be written as* $\alpha\mathsf{P} + \beta\mathsf{Q}$ *for a unique pair of elements* $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$.

Problem 2.2. An *isogeny* of elliptic curves $\mathsf{E}_1, \mathsf{E}_2$ is a non-zero holomorphic group homomorphism (equivalently, an algebraic homomorphism)

$$\phi : \mathsf{E}_1 \longrightarrow \mathsf{E}_2.$$

An *endomorphism* of an elliptic curve E is an isogeny from E to itself. The *endomorphism ring* of E, denoted $\mathrm{End}(\mathsf{E})$, is the set of all endomorphisms of E, with addition being defined point-wise and multiplication being defined by composition.

(1) Show that the set of all endomorphisms is indeed a ring.
(2) Show that the multiply-by-n map, which sends a point $\mathsf{P} \in \mathsf{E}$ to $n\mathsf{P} \in \mathsf{E}$, is an endomorphism.

Problem 2.3. Consider the curve

$$\mathsf{E} : y^2 = x^3 + x.$$

(1) Show that $\phi : (x, y) \to (-x, iy)$ is an endomorphism.
(2) 2-torsion points
   (a) Find the set of points $\mathsf{E}[2]$.
   (b) Set the notation $\mathbb{Q}(\mathsf{E}[n])$ to mean the field generated over $\mathbb{Q}$ by the x and y coordinates of all the points in $\mathsf{E}[n]$. Show that $\mathbb{Q}(\mathsf{E}[2]) = \mathbb{Q}(i)$.
   (c) Write $G = \mathrm{Gal}(\mathbb{Q}(\mathsf{E}[2])/\mathbb{Q}) = \{e, \iota\}$, where ι denotes the complex conjugation. Let P and Q denote the two generators of $\mathsf{E}[2]$. Find $\iota(\mathsf{P})$ and $\iota(\mathsf{Q})$ in term of P and Q.
   (d) Write the matrix associated to ι and denote it by M_ι.
   (e) Show that the map

$$\rho_2 : \mathrm{Gal}(\mathbb{Q}(\mathsf{E}[2])/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$$

   given by $e \mapsto I_2$ and $\iota \mapsto M_\iota$ is a one-to-one homomorphism.
(3) 3-torsion points
   (a) Show that

$$\mathsf{P} = (x_0, y_0) \text{ has order three} \iff 3x_0^2 + 6x_0 - 1 = 0.$$

   (b) Find the set of points $\mathsf{E}[3]$.
   (c) Show that the field generated by the coordinates of the set of points above is a (non-abelian) Galois extension of order 16.
(4) 4-torsion points
   (a) Show that

$$\mathsf{P} = (x_0, y_0) \text{ has order four} \iff x_0^6 + 5x_0^4 - 5x_0^2 - 1 = 0.$$

   (b) Find the complete set of points of order four on E.
   (c) What is the field generated by these points?
(5) n-torsion points: In this exercise we will show that the field extension

$$K_n \coloneqq \mathbb{Q}(i)(\mathsf{E}[n])$$

   is an abelian (Galois) extension of $\mathbb{Q}(i)$.
   (a) Show that if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mathsf{E}[n])/\mathbb{Q})$ and $\mathsf{P} \in \mathsf{E}[n]$ then $\sigma(\mathsf{P}) \in \mathsf{E}[n]$; i.e., σ induces a permutation on the set $\mathsf{E}[n]$. Further show that each $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mathsf{E}[n])/\mathbb{Q})$ gives a group isomorphism from $\mathsf{E}[n]$ to itself.
   (b) Fix generators P and Q for $\mathsf{E}[n]$. From above, we can write define a matrix

$$M_\sigma = \begin{pmatrix} \alpha_\sigma & \beta_\sigma \\ \gamma_\sigma & \delta_\sigma \end{pmatrix}$$

where $\sigma(\mathsf{P}) = \alpha_\sigma \mathsf{P} + \gamma_\sigma \mathsf{Q}$ and $\sigma(\mathsf{P}) = \beta_\sigma \mathsf{P} + \delta_\sigma \mathsf{Q}$. Show that the map

$$\rho_n : \mathrm{Gal}(\mathbb{Q}(\mathsf{E}[n])/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

given by $\sigma \mapsto M_\sigma$ is a one-to-one homomorphism. *Such a map ρ_n is called a Galois representation.*

(c) Show that $K_n/\mathbb{Q}$ is a Galois extension. Hence, conclude that $K_n/\mathbb{Q}(i)$ is Galois.

(d) Consider a different endomorphism

$$\phi : \mathsf{E} \longrightarrow \mathsf{E}.$$

This gives a homomorphism $\phi : \mathsf{E}[n] \to \mathsf{E}[n]$ to which we can associate a matrix, say A_ϕ. Show that if $\sigma \in \mathrm{Gal}(K_n/\mathbb{Q}(i))$ and $\mathsf{P} \in \mathsf{E}(K_n)$ then

$$\sigma(\phi(\mathsf{P})) = \phi(\sigma(\mathsf{P})).$$

(e) You may use the following facts without proof
- The matrix $A_\phi \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.
- Matrices that commute with A_ϕ also commute with one another.

Conclude that all matrices in the set

$$\{\rho_n(\sigma) \ : \ \sigma \in \mathrm{Gal}(K_n/\mathbb{Q}(i))\}$$

commute with one another.

(f) Conclude that $\mathrm{Gal}(K_n/\mathbb{Q}(i))$ is abelian.

(6) Now, view $\mathsf{E}(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ and choose $\Lambda = [\omega_1, \omega_2]$. Take

$$\mathsf{P} = \frac{\omega_1}{n} \text{ and } \mathsf{Q} = \frac{\omega_2}{n}$$

as the generators of $\mathsf{E}[n]$. Show that $K_n/\mathbb{Q}(i)$ can be generated by using special values of meromorphic functions.

Problem 2.4. Consider the elliptic curve

$$\mathsf{E} : y^2 = x^3 - 2.$$

(1) Show that $\phi : (x, y) \to (\zeta x, -y)$ is an endomorphism, where $\zeta = \frac{-1+\sqrt{-3}}{2}$ is a primitive cube root of unity.
(2) Find the set $\mathsf{E}[2]$.
(3) Show that $G = \mathrm{Gal}(\mathbb{Q}(\mathsf{E}[2])/\mathbb{Q})$ is non-abelian of order six.
(4) Let σ (resp. τ) be the order three (resp. two) element in G. Compute the matrices M_σ, M_τ with respect to two fixed 'basis' elements P and Q.
(5) Is ρ_2 surjective?

3. Elliptic Curves over Finite Fields

Throughout this section, we write $\mathbb{F}_q$ to denote a finite field with $q = p^k$ elements where $k \geq 1$.

Problem 3.1. Define

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} +1 & \text{if } x \text{ is a square in } \mathbb{F}_q^\times \\ -1 & \text{if } x \text{ is not a square in } \mathbb{F}_q^\times \\ 0 & \text{if } x = 0. \end{cases}$$

(1) Show that if q is odd then $\left(\frac{x}{\mathbb{F}_q}\right) = x^{(q-1)/2}$ as an element of $\mathbb{F}_q$.

Let $\mathsf{E} : y^2 = x^3 + Ax + B$ be an elliptic curve defined over $\mathbb{F}_q$.

(2) Show that

$$\#\mathsf{E}(\mathbb{F}_q) = 1 + q + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q} \right).$$

Problem 3.2. Consider the rational elliptic curve

$$\mathsf{E} : y^2 = x^3 + 3.$$

(1) Find a point $\mathsf{P} \in \mathsf{E}(\mathbb{Q})$.
(2) Calculate the discriminant Δ_{E}.
(3) Calculate the size of $\widetilde{\mathsf{E}}(\mathbb{F}_5)$ and $\widetilde{\mathsf{E}}(\mathbb{F}_7)$.
(4) Let p be a prime such that $p \nmid 2\Delta_{\mathsf{E}}$. Consider the *reduction modulo p map*

$$\mathsf{E}(\mathbb{Q})_{\text{tors}} \longrightarrow \widetilde{\mathsf{E}}(\mathbb{F}_p).$$

Show (abstractly) that this homomorphism is one-to-one.
(5) Conclude that $\#\mathsf{E}(\mathbb{Q})_{\text{tors}}$ is trivial. In particular, E has infinitely many rational points.

Problem 3.3. Consider the elliptic curve

$$\mathsf{E} : y^2 = x^3 - 43x + 166.$$

(1) Calculate Δ_{E}.
(2) Calculate $\#\widetilde{\mathsf{E}}(\mathbb{F}_3)$.
(3) Use the Nagell-Lutz theorem to find a point $\mathsf{P} \in \mathsf{E}(\mathbb{Q})$ which might have finite order.
(4) Show that $\#\mathsf{E}(\mathbb{Q})_{\text{tors}}$ is non-trivial and calculate its size.

Problem 3.4. Consider the elliptic curves

$$\mathsf{E} : y^2 = x^3 + 1.$$

Show that $\widetilde{\mathsf{E}}/\mathbb{F}_5$ is an elliptic curve but $\widetilde{\mathsf{E}}/\mathbb{F}_3$ is not. *The notation means that in the first case we consider* $\mathsf{E} \pmod 5$ *and in the second case we take* $\mathsf{E} \pmod 3$.

Problem 3.5. Find the reduction type at $p \geq 5$ for the following elliptic curves defined over $\mathbb{Q}$ by looking at reduction modulo p curve $\widetilde{\mathsf{E}}$ and determining the slopes of their tangent line(s) at a point of singularity.

(1) $\mathsf{E} : y^2 = x^3 + px^2 + 1$.
(2) $\mathsf{E} : y^2 = x^3 + x^2 + p$.
(3) $\mathsf{E} : y^2 = x^3 + p$.

Problem 3.6. Fix an odd prime $p \equiv 2 \pmod 3$.

(1) Show that every element of $\mathbb{F}_p$ has a unique cube-root in $\mathbb{F}_p$.
(2) If $a \in \mathbb{F}_p^{\times}$, show that $\mathsf{E} : y^2 = x^3 + a$ is supersingular.

Problem 3.7. Let a prime $p > 2$ and an elliptic curve $\mathsf{E} : y^2 = x(x-1)(x-\lambda)$ with $\lambda \in \mathbf{F}_q$.

(1) Let $n \in \mathbb{Z}_{>0}$. Show that

$$\sum_{x \in \mathbb{F}_q} x^n = \begin{cases} 0 & \text{if } q-1 \nmid n, \\ -1 & \text{if } q-1 \mid n. \end{cases}$$

(2) Show that

$$\sum_{x \in \mathbb{F}_q} (x(x-1)(x-\lambda))^{(q-1/2)} = -a_q(\mathsf{E}).$$

Conclude that $a_q(\mathsf{E})$ is the coefficient of x^{q-1} of the polynomial $(x(x-1)(x-\lambda))^{(q-1/2)}$.

(3) Show that $a_q(\mathsf{E}) = 0$ if and only if $a_p(\mathsf{E}) = 0$ in a field of characteristic p.
(4) Consider the polynomial $((x-1)(x-\lambda))^{(p-1)/2}$. Then, $a_p(\mathsf{E})$ appears as a coefficient of what power of x? Using the binomial theorem, express $a_p(\mathsf{E})$ as a polynomial in λ.
(5) Show that $\mathsf{E} : y^2 = x^3 + x$ over $\mathbb{F}_p$ is supersingular if and only if $p \equiv 3 \pmod 4$.

In the course of the next few exercises we prove a special case of the theorem of Hasse.
Theorem (Gauss): Let M_p denote the number of projective solutions to the equation

$$X^3 + Y^3 + Z^3 = 0$$

with $X, Y, Z \in \mathbb{F}_p$. Then

- $M_p = p + 1$ if $p \not\equiv 1 \pmod 3$
- $M_p = p + 1 + A$ if $p \equiv 1 \pmod 3$ where A, B are integers satisfying $4p = A^2 + 27B^2$ and $A \equiv 1 \pmod 3$. *This A is unique.*

Problem 3.8. We first see an application of this result.
(1) Show that the Fermat curve $C/\mathbb{Q} : X^3 + Y^3 = 1$ is birationally equivalent to $\mathsf{E}/\mathbb{Q} : y^2 = x^3 - 432$ using the transformation

$$\psi : C \longrightarrow \mathsf{E} \text{ given by } (X, Y) \mapsto \left(\frac{12}{X+Y}, \frac{36(X-Y)}{X+Y} \right).$$

(2) Show that the theorem of Gauss implies Hasse's theorem for E.

We will now prove the theorem above via several exercises.

Problem 3.9. Suppose we are in the case that $3 \nmid p - 1$.
(1) Check that $x \mapsto x^3$ is an isomorphism from $\mathbb{F}_p^\times$ to itself.
(2) Conclude that every element of $\mathbb{F}_p$ has a unique cube root.
(3) Conclude that $M_p = p + 1$. [Hint: we are counting projective solutions]

Problem 3.10. Suppose we are in the case that $3 \mid p - 1$. Write $p = 3m + 1$. *For simplicity you may take $p = 13$.*
(1) Consider the homomorphism $x \to x^3$. Find the image of this homomorphism and denote it by R. Further, find the kernel of this homomorphism. *The elements of R are called cubic residues.*
(2) Find the other (two) cosets of R in $\mathbb{F}_p^\times$ and denote them by S and T. Conclude that

$$\mathbb{F}_p = \{0\} \sqcup R \sqcup S \sqcup T.$$

(3) We introduce a new symbol: let $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$ be subsets of $\mathbb{F}_p$. We write $[\mathcal{X}\mathcal{Y}\mathcal{Z}]$ to denote the *number* of triples $(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ satisfying $x + y + z = 0$.
   (a) Show (abstractly) that the number of projective solutions of $X^3 + Y^3 + Z^3 = 0$ where $XYZ \neq 0$ is $\frac{9[RRR]}{m}$. *Do not explicitly calculate $[RRR]$.*
   (b) Show that the number of projective solutions of $X^3 + Y^3 + Z^3 = 0$ with one coordinate zero is 9.
   (c) From the above two exercises conclude that

$$M_p = 9 \left(\frac{[RRR]}{m} + 1 \right).$$

   (d) Check that

$$\begin{aligned} [RR\mathbb{F}_p] &= [RR\{0\}] + [RRR] + [RRS] + [RRT] \\ &= [RR\{0\}] + [RRR] + [SST] + [TTS] \\ &= m^2. \end{aligned}$$

(e) Similarly, check

$$\begin{aligned}[\mathbb{F}_p TS] &= [\{0\}TS] + [RTS] + [STS] + [TTS] \\ &= m^2.\end{aligned}$$

(f) Check that $[\{0\}TS] = 0$ and $[RR\{0\}] = m$. Conclude that

$$m + [RRR] = [RTS].$$

Further conclude that $M_p = \frac{9[RTS]}{m}$.

(4) Let $\zeta = e^{2\pi i/p}$. Define

$$\alpha_R = \sum_{r\in R} \zeta^r, \quad \alpha_S = \sum_{s\in S} \zeta^s, \quad \alpha_R = \sum_{t\in T} \zeta^t.$$

(a) Show that $\alpha_R + \alpha_S + \alpha_T = -1$.

(b) *If you are working with $p = 13$, you may prove this directly:* Show that

$$\begin{aligned}\alpha_R\alpha_S + \alpha_S\alpha_T + \alpha_T\alpha_R &= -m \\ \alpha_R^2 + \alpha_S^2 + \alpha_T^2 &= 1 + 2m.\end{aligned}$$

(b') *Alternatively:* Write N_x to denote the umber of pairs $(s,t) \in S \times T$ such that $s+t = x$.

(i) Show that

$$\alpha_S\alpha_T = \sum_{x\in\mathbb{F}_p} N_x\zeta^x.$$

(ii) Show that $N_x = N_{rx}$ for $r \in R$. *In other words, N_x only depends on the coset R, S, T in which x lies.*

(iii) Conclude that $mN_x = [ST\mathcal{Z}]$ if x is a coset representative of $\mathcal{Z} = \{R, S, T\}$. *We may therefore write $[ST\mathcal{Z}] = mN_{\mathcal{Z}}$.*

(iv) Show that

$$\begin{aligned}\alpha_S\alpha_T &= N_R\alpha_R + N_S\alpha_S + N_T\alpha_T, \\ \alpha_T\alpha_R &= N_R\alpha_S + N_S\alpha_T + N_T\alpha_R, \\ \alpha_R\alpha_S &= N_R\alpha_T + N_S\alpha_R + N_T\alpha_S.\end{aligned}$$

(v) Show that

$$\begin{aligned}\alpha_R\alpha_S + \alpha_S\alpha_T + \alpha_T\alpha_R &= -m \\ \alpha_R^2 + \alpha_S^2 + \alpha_T^2 &= 1 + 2m.\end{aligned}$$

(c) Show that

$$3\alpha_R\alpha_S\alpha_T = N_R + (3N_R - m)m.$$

Define $k \coloneqq 3N_R - m$.

(5) Set $A = 3k - 2 \equiv 1 \pmod 3$. Show that

$$M_p = p + 1 + A.$$

(6) Define $F(t) = (t - \alpha_R)(t - \alpha_S)(t - \alpha_T)$. Calculate $D(F)$ which is the discriminant of the polynomial $F(t)$.

(7) Set

$$\beta_* = 1 + 3\alpha_* \text{ for } * \in \{R, S, T\}.$$

Define $G(t) = (t-\beta_R)(t-\beta_S)(t-\beta_T)$. Calculate $D(G)$ from the formula of the discriminant of a cubic.

(8) Show that $D(F) = (27)^2 D(F)$.

(9) Set $B = N_S - N_T$. Conclude that

$$4p = A^2 + 27B^2.$$

(10) Show that A is uniquely determined by the conditions $A \equiv 1 \pmod 3$ and $4p = A^2 + 27B^2$.

References

[1] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters. Twisted Edwards curves. In *International conference on cryptology in Africa*, pages 389–405. Springer, 2008.

Department of Mathematics and Statistics, University of Regina, Saskatchewan, Canada
Email address: debanjana.kundu@uregina.ca