MÈTODES GEOMÈTRICS EN TEORIA DE NOMBRES

Semestre de primavera de 2022

Problem Set 2

Submit the solutions of Exercises $1, 2, 3, 4$ at Campus Virtual by Sunday 13/3/2022 at 23:59.

Exercise 5 is optional, it is not necessary to submit its solution, and it will not be part of the evaluation (however, you can submit its solution if you wish!).

In all exercises below, K denotes a field and $\overline{K}$ its algebraic closure.

Exercise 1. Let $F(X,Y,Z) = Y^2Z - X^3 - X^2Z \in K[X,Y,Z]$, $G(X,Y,Z) = Y \in K[X,Y,Z]$, $P_1 = [0:0:1]$ and $P_2 := [-1:0:1]$. Compute the multiplicities $I(P_1; \mathcal{C}_F, \mathcal{C}_G)$ and $I(P_2; \mathcal{C}_F, \mathcal{C}_G)$.

Exercise 2. Show that:

(1) A homogeneous polynomial $F(X,Y) \in K[X,Y]$ of degree n decomposes as

$$F(X,Y) = \prod_{i=1}^{n} (a_i X - b_i Y)\,, \qquad \text{where } a_i, b_i \in \overline{K}.$$

(2) A conic $\mathcal{C}$ is smooth if and only if it is geometrically irreducible.

Hint: You need to show that $\mathcal{C}$ has a singular point P if and only if its defining polynomial $F(X,Y,Z)$ factorizes over $\overline{K}$ as the product of two linear factors. For the 'if' implication, you may assume without loss of generality that $F(X,Y,Z)$ is XY or X^2. For the 'only if' implication, assume that $P = [0:0:1]$, note the constraints this imposes on F, and apply part (1) of this exercise.

Exercise 3. Show that the cubic defined by the polynomial $F(X,Y,Z) = Y^2Z - X^3 \in K[X,Y,Z]$ is geometrically irreducible, but it is not smooth at $[0:0:1]$.

Hint: The key point is to show that $R = \overline{K}[x,y]/(y^2 - x^3)$ is a domain. To show this, identify R with a subring of $\overline{K}[T]$ by studying the kernel of the ring homomorphism

$$\Phi : \overline{K}[x,y] \to \overline{K}[T]$$

that maps x to T^2 and y to T^3.

Exercise 4. Show that a smooth projective plane curve $\mathcal{C}$ defined over K is geometrically irreducible.

Hint: Suppose that the defining polynomial $F(X,Y,Z)$ of $\mathcal{C}$ factorizes as $F = G \cdot H$, where $G, H \in \overline{K}[X,Y,Z]$. Recall that, by Bézout's theorem, the projective plane curves $\mathcal{C}_G$ and $\mathcal{C}_H$ intersect at at least one $\overline{K}$-rational point P. Show that P is not a smooth point of $\mathcal{C}$.

Exercise 5. Let L/K be a Galois extension and let G denote $\mathrm{Gal}(L/K)$.

(1) Show that

$$\sigma([a_0 : \cdots : a_d]) := [\sigma(a_0) : \cdots : \sigma(a_d)] \qquad \text{for } \sigma \in G \text{ and } [a_0 : \cdots : a_d] \in \mathbb{P}^d(L)$$

is a well-defined action of G on $\mathbb{P}^d(L)$.

(2) Let $v \in L^{d+1} \backslash \{(0, \ldots, 0)\}$ be such that for every $\sigma \in G$ there exists $\lambda_\sigma \in L^\times$ such that

$$\sigma(v) = \lambda_\sigma \cdot v \,.$$

Show that $\lambda_{\sigma\tau} = \lambda_\sigma \cdot \sigma(\lambda_\tau)$.

(3) Consider the map

$$\sum_{\tau \in G} \lambda_\tau \cdot \tau : L \to L \,.$$

(It is a nonzero map by Dedekind's theorem on independence of characters). Choose $\theta \in L$ such that $\gamma := \sum_{\tau \in G} \lambda_\tau \tau(\theta)$ is nonzero. Show that $\lambda_\sigma = \gamma/\sigma(\gamma)$ for all $\sigma \in G$, and deduce that $\sigma(\gamma \cdot v) = \gamma \cdot v$ for all $\sigma \in G$.

(4) Consider the set

$$\mathbb{P}^d(L)^G := \{P \in \mathbb{P}^d(L) : \sigma(P) = P \text{ for all } \sigma \in G\} \,.$$

Deduce from (3) that the natural inclusion

$$\mathbb{P}^d(K) \hookrightarrow \mathbb{P}^d(L)^G \,.$$

is a bijection.

(5) Let $\mathcal{C}$ be a plane projective curve defined over K. Show that the action of (1), for $d = 2$, restricts to an action on $\mathcal{C}(L)$. Consider the set

$$\mathcal{C}(L)^G := \{P \in \mathcal{C}(L) : \sigma(P) = P \text{ for all } \sigma \in G\} \,.$$

Deduce from (4) that

$$\mathcal{C}(L)^G = \mathcal{C}(K) \,.$$

MÈTODES GEOMÈTRICS EN TEORIA DE NOMBRES

Semestre de primavera de 2022

Problem Set 4

Submit the solutions of Exercises $1, 2, 3, 4$ at Campus Virtual by Sunday 10/4/2022 at 23:59.

Exercise 5 is optional, it is not necessary to submit its solution, and it will not be part of the evaluation (however, you can submit its solution if you wish!).

Exercise 1. Determine $\mathcal{Q}(\mathbb{Q})$, where $\mathcal{Q}$ is the cubic defined by the polynomial:

(1) $F(X,Y,Z) = X^3 + 2Y^3 - 4Z^3 \in \mathbb{Q}[X,Y,Z]$.

(2) $F(X,Y,Z) = (Y+Z)^3 - 2X^3 \in \mathbb{Q}[X,Y,Z]$.

Hint: For (1), study the divisibility by powers of 2 of an eventual solution, once assumed to be given by integral coordinates. For (2), note that $\mathcal{Q}$ is not geometrically irreducible and study the Galois action on the irreducible components.

Exercise 2. Let K be a field of characteristic $\neq 2$ and let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over K. Show that if $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(K)$ are such that $P_1 \neq -P_2$, then:

$$P_1 + P_2 = \big(m^2 - x_1 - x_2, -y_1 - m(m^2 - 2x_1 - x_2)\big)\ ,$$

where

$$m = \begin{cases} \frac{3x_1^2 + a}{2y_1} & \text{if } P_1 = P_2\,, \\ \frac{y_1 - y_2}{x_1 - x_2} & \text{if } P_1 \neq P_2\,. \end{cases}$$

Deduce that for every $P = (x, y)$ such that $2P \neq \mathcal{O}$, we have

$$2 \cdot P = \left(\frac{p'(x)^2}{4p(x)} - 2x, -y\left(1 + \frac{p'(x)}{2p(x)^2}\left(\frac{p'(x)^2}{4p(x)} - 3x\right)\right)\right)\ .$$

Hint: If P_1 and P_2 if are distinct, write an equation for the line through P_1 and P_2, and find the x-coordinate of the third point of intersection of this line with E. If the points P_1 and P_2 coincide, repeat the argument with the tangent to E at P_1.

Exercise 3. Let E be the elliptic curve $y^2 = x^3 + x + 2$ defined over $\mathbb{F}_5$. Determine the isomorphism class of the group of $\mathbb{F}_5$-rational points $E(\mathbb{F}_5)$.

Hint: Determine the set $E(\mathbb{F}_5)$ by exhaustive search and study the orders of its elements by applying the formulas of Exercise 2.

Exercise 4. Let K be a field of characteristic $\neq 2$. Let $a, b \in K$ be such that $b \neq 0$ and $a^2 - 4b \neq 0$.

(1) Show that
$$E_1 : y^2 = x^3 + ax^2 + bx\,, \qquad E_2 : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x\,.$$
are elliptic curves.

(2) Show that
$$\phi(x, y) = \left(\frac{y^2}{x^2}, y\frac{x^2 - b}{x^2}\right)$$
is an isogeny from E_1 to E_2.

(3) Determine $\ker(\phi)$.

Comment: For part (1), you may use the formula for the discriminant of a general cubic polynomial given at class. In part (2), for the sake of brevity, when checking that
$$\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2)\,,$$
you may just consider the general case in which $P_1, P_2 \notin \{(0,0), \mathcal{O}\}$. When one among P_1, P_2 lies in $\{(0,0), \mathcal{O}\}$, the general argument fails and an additional argument is needed; feel free to disregard this degenerate case.

Exercise 5. Let K be a field and let $\mathcal{Q}$ be the nodal curve
$$y^2 = x^3 + \alpha x^2\,, \qquad \text{with } \alpha \in K^\times\,.$$
Recall that the chord-and-tangent operation equips the set of nonsingular points of $\mathcal{Q}_{ns}(\overline{K})$ with a group structure. Show that:

(1) The map
$$\varphi\colon \mathcal{Q}_{ns}(\overline{K}) \to \overline{K}^\times\,, \qquad \varphi([r : s : t]) = \frac{s + \sqrt{\alpha}r}{s - \sqrt{\alpha}r}$$
is a group isomorphism.

(2) If $\mathcal{Q}$ is split multiplicative, then φ induces an isomorphism $\mathcal{Q}_{ns}(K) \simeq K^\times$.

(3) If $\mathcal{Q}$ is non-split multiplicative, then
$$\mathcal{Q}_{ns}(K) \simeq \{\beta \in K(\sqrt{\alpha})^\times : \beta \cdot \sigma(\beta) = 1\}\,,$$
where σ is the generator of $\mathrm{Gal}(K(\sqrt{\alpha})/K)$.

Hint: For part (1), once you have shown that φ is a bijection, to show that it is a group homomorphism it will suffice to see that if $P_1 = \varphi(u_1)$, $P_2 = \varphi(u_2)$, and $P_3 = \varphi(u_3)$ lie on a line, then $u_1 \cdot u_2 \cdot u_3 = 1$. For part (3), use that by Hilbert's 90th Theorem for every $\beta \in K(\sqrt{\alpha})$ such that $\beta \cdot \sigma(\beta) = 1$, there exist $r, s \in K$ such that
$$\beta = \frac{s + \sqrt{\alpha}r}{s - \sqrt{\alpha}r}\,.$$

MÈTODES GEOMÈTRICS EN TEORIA DE NOMBRES

Semestre de primavera de 2022

Problem Set 6

Submit the solutions of Exercises 1, 2, 3, 4 at Campus Virtual by Sunday 8/5/2022 at 23:59.

Exercise 1. Let $E : y^2 = f(x)$ be an elliptic curve defined over $\mathbb{F}_p$.

(1) Show that if $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol, then

$$\#E(\mathbb{F}_p) = p + 1 + \sum_{x\in\mathbb{F}_p} \left(\frac{f(x)}{p}\right).$$

(2) Let $n \in \mathbb{Z}_{\geq 1}$ be such that $p \nmid n$. Show that if $p \equiv 3 \pmod 4$ and $f(x) = x(x^2 - n^2) \in \mathbb{F}_p[x]$, then $\#E(\mathbb{F}_p) = p + 1$.

(3) Let $n \in \mathbb{Z}_{\geq 1}$. Show that the elliptic curve $E : y^2 = x(x^2 - n^2)$ defined over $\mathbb{Q}$ has complex multiplication and that $a_p(E) = 0$ for every prime p in a set of density $1/2$.

Hint: Recall that for $x \in \mathbb{F}_p$, the Legendre symbol is defined as

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \textit{if } x = 0, \\ 1 & \textit{if } x \in (\mathbb{F}_p^\times)^2, \\ -1 & \textit{otherwise.} \end{cases}$$

For (2), use that if $p \equiv 3 \pmod 4$, then $\left(\frac{-1}{p}\right) = -1$, and for (3) apply Dirichlet's density theorem.

Exercise 2. Let E be the elliptic curve $y^2 = x^3 + x + 2$ defined over $\mathbb{F}_5$. Determine $\#E(\mathbb{F}_{5^5})$.

Hint: Deduce from Exercise 3 of PS 4 that $a_5(E) = 2$. From the existence of $\alpha \in \overline{\mathbb{Q}}$ such that

$$\#E(\mathbb{F}_{5^n}) = 1 + 5^n - \alpha^n - \overline{\alpha}^n$$

find a recurrence relation between $a_{5^{n+1}}$, a_{5^n}, and $a_{5^{n-1}}$.

Exercise 3. Let $\mathbb{F}_q$ be a finite field of characteristic p. Let $F \in \mathbb{F}_q[X_1, \ldots, X_n]$ be a homogeneous polynomial of degree d and let

$$V := \{\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_q^n : F(\mathbf{a}) = 0\}.$$

For $\mathbf{a} \in \mathbb{F}_q^n$, define $G(\mathbf{a}) := F(\mathbf{a})^{q-1}$. Show that:

(1) $\#(\mathbb{F}_q^n \setminus V) \equiv \sum_{\mathbf{a}\in\mathbb{F}_q^n} G(\mathbf{a}) \pmod p$.

(2) For $\alpha \in \mathbb{Z}_{\geq 0}$, one has

$$\sum_{a \in \mathbb{F}_q} a^\alpha \equiv 0 \pmod{p}$$

unless α is a nonzero multiple of $q-1$.

(3) For $\alpha = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{Z}_{\geq 0})^n$, write $\mathbf{a}^\alpha = a_1^{\alpha_1} \cdots a_n^{\alpha_n}$. One has

$$\sum_{\mathbf{a} \in \mathbb{F}_q^n} \mathbf{a}^\alpha \equiv 0 \pmod{p}$$

unless $\alpha_1 + \cdots + \alpha_n \geq n(q-1)$.

(4) If $n > d$, then

$$\sum_{\mathbf{a} \in \mathbb{F}_q^n} G(\mathbf{a}) \equiv 0 \pmod{p}, \quad \#(\mathbb{F}_q^n \backslash V) \equiv 0 \pmod{p}, \quad \#V \equiv 0 \pmod{p}.$$

(5) $\#C(\mathbb{F}_q) = q + 1$ for every smooth conic C defined over $\mathbb{F}_q$.

Hint: For (2), express the sum in terms of a generator of $\mathbb{F}_q^\times$. For (3), observe that

$$\sum_{\mathbf{a} \in \mathbb{F}_q^n} \mathbf{a}^\alpha = \left(\sum_{a_1 \in \mathbb{F}_q} a_1^{\alpha_1} \right) \cdots \left(\sum_{a_n \in \mathbb{F}_q} a_n^{\alpha_n} \right)$$

and apply (2). For (5), use (4) to deduce that $C(\mathbb{F}_q) \neq \emptyset$ and apply the bijection between $C(\mathbb{F}_q)$ and $\mathbb{P}^1(\mathbb{F}_q)$ that we have seen in this case in the lectures.

Exercise 4. Show that every smooth plane cubic $\mathcal{Q}$ over a finite field $\mathbb{F}_q$ is an elliptic curve. Deduce that

$$|\#\mathcal{Q}(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Hint: A priori $\mathcal{Q}(\mathbb{F}_q)$ may be empty, so we can not take for granted that $\mathcal{Q}$ is an elliltic curve defined over $\mathbb{F}_q$. Argue, however, that there exists $n \in \mathbb{Z}_{\geq 1}$ such that $\mathcal{Q}(\mathbb{F}_{q^n}) \neq \emptyset$. Choose an arbitrary $\mathcal{O} \in \mathcal{Q}(\mathbb{F}_{q^n})$ and consider the group structure $(\mathcal{Q}(\overline{\mathbb{F}}_q), +)$ induced by the elliptic curve $(\mathcal{Q}, \mathcal{O})$ defined over $\mathbb{F}_{q^n}$. Consider the map

$$\phi : \mathcal{Q}(\overline{\mathbb{F}}_q) \to \mathcal{Q}(\overline{\mathbb{F}}_q), \qquad \phi(P) := \phi_q(P) - P,$$

where ϕ_q is the Frobenius endomorphism. Justify that ϕ is either constant or surjective. Show that the map cannot be constant, and that the first statement of the exercise follows from the surjectivity of ϕ. Deduce the second statement of the exercise from the Hasse–Weil theorem.

Comment: With Exercises 3 and 4, we have completed the proof of the Weil Conjectures for curves of genus 0 and 1.

MÈTODES GEOMÈTRICS EN TEORIA DE NOMBRES

Semestre de primavera de 2022

Problem Set 7

Submit the solutions of Exercises $1, 2$ at Campus Virtual by Sunday 22/5/2022 at 23:59.

Exercise 1. We say that $n \in \mathbb{Z}_{\geq 1}$ is a *congruent number* if there is a right triangle of rational sides and area n.

i) Show that n is a congruent number if and only if there exist $a, b, c \in \mathbb{Q}_{>0}$ such that

$$\left(\frac{a+b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 + n\,, \qquad \left(\frac{a-b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 - n\,.$$

ii) Let $E_n : y^2 = x(x^2 - n^2)$ be the elliptic curve defined over $\mathbb{Q}$. Show that n is a congurent number if and only if there exists an affine point $(x, y) \in E_n(\mathbb{Q})$ with $y \neq 0$.

iii) Show that $E_n(\mathbb{Q})_{\mathrm{tors}} = \{\mathcal{O}, (0,0), (n,0), (-n,0)\}$.

iv) Show that if n is a congruent number, then there exist infinitely many nonsimilar triangles of rational sides and area n.

Hint: For the 'if' implication of part (2), show that there exist there exist $a, b, c \in \mathbb{Q}_{>0}$ satisfying the relations of (1). To this aim, using the duplication formula, show that if u denotes the x-coordinate of $2 \cdot (x, y)$, then $u - n, u, u + n \in (\mathbb{Q}^\times)^2$. Determine a, b, c by imposing the square roots of $u - n, u, u + n$ to be $(a - b)/2$, $c/2$, and $(a + b)/2$, respectively. As for (3), use Exercise 1 of PS 6 to show that $\#E(\mathbb{Q})_{\mathrm{tors}} \mid p + 1$ for all but finitely many primes $p \equiv 3 \pmod 4$. Use Dirichlet's density theorem to deduce that $\#E(\mathbb{Q})_{\mathrm{tors}} = 4$

Exercise 2. Show that:

i) The elliptic curve $y^2 = x^3 - x$ has rank 0.

ii) The elliptic curve $E : y^2 = x^3 - 5x$ has rank 1.

Hint: Given elliptic curves

$$E : y^2 = x^3 + ax^2 + bx\,, \qquad \overline{E} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x\,,$$

where $a, b \in \mathbb{Z}$, $\overline{a} = -2a$ and $\overline{b} = a^2 - 4b$, we have defined maps

$$\alpha : E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2\,, \qquad \overline{\alpha} : \overline{E}(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2\,.$$

By the class of Monday 16/5/2022, we have

$$2^{r_E+2} = \#\alpha(E(\mathbb{Q})) \cdot \#\overline{\alpha}(\overline{E}(\mathbb{Q}))\,,$$

as well as we have the following method to compute $\alpha(E(\mathbb{Q}))$ *(for the computation of* $\overline{\alpha}(\overline{E}(\mathbb{Q}))$ *simply replace* a, b *by* $\overline{a}, \overline{b}$*). For* b_1 *a divisor (positive or negative) of* b*, consider the equation*

$$N^2 = b_1 M^4 + a M^2 e^2 + \frac{b}{b_1} e^4 \,. \tag{1}$$

In the above equation, consider a, b, b_1 *as given coefficients and* M, e, N *as the variables. Then*

$$\alpha(\Gamma) = \{b \pmod{(\mathbb{Q}^\times)^2}\} \cup \{b_1 \pmod{(\mathbb{Q}^\times)^2} : b_1 \mid b \text{ and } (1) \text{ has a solution with } M \neq 0\} \,.$$