S.-T. Yau College Student Mathematics Contests 2026

Algebra and Number Theory
(5 problems)

Problem 1. *Let p be a prime, $n \geq 1$ an integer with $\gcd(n,p)=1$, and write*

$$\Gamma_0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{p} \right\}, \qquad \alpha = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}.$$

Prove that the double coset $\Gamma_0(p)\alpha\Gamma_0(p)$ decomposes into a disjoint union of right cosets:

$$\Gamma_0(p)\alpha\Gamma_0(p) = \bigsqcup_{\gamma \in \mathcal{R}} \Gamma_0(p)\gamma,$$

where $\mathcal{R} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \;\middle|\; ad = n,\ a > 0,\ 0 \leq b < d,\ \gcd(a,b,d) = 1 \right\}$.

Problem 2. *Let p be a prime, and let $\mathbb{F}_p$ denote the field of p elements. Consider the equation $Y^2 = X^3+1$ over $\mathbb{F}_p$, and denote by N_p its number of solutions in $\mathbb{F}_p$:*

$$N_p := \#\{(x,y) \in \mathbb{F}_p^2 \mid y^2 = x^3 + 1\}.$$

In the following, we want to show the following inequality

$$|N_p - p| \leq 2\sqrt{p}.$$

For $m \in \mathbb{Z}_{\geq 1}$, let $\mathsf{X}_m = \mathsf{X}_m(\mathbb{F}_p^\times)$ be the group of (complex) characters of $\mathbb{F}_p^\times$ of order dividing m. For χ a character of $\mathbb{F}_p^\times$, set

$$\chi(0) = \begin{cases} 1, & \text{if } \chi = 1; \\ 0, & \text{otherwise.} \end{cases}$$

For χ and μ two characters of $\mathbb{F}_p^\times$, write $J(\chi,\mu)$ the Jacobi sum attached to them:

$$J(\chi,\mu) := \sum_{a+b=1} \chi(a)\mu(b) \in \mathbb{C}.$$

Recall that we have $|J(\chi,\mu)| = \sqrt{p}$ if the characters χ, μ and $\chi\mu$ are all non-trivial.

(1) *Assume $p = 3$ or $p \equiv 2 \pmod 3$. Show that $N_p = p$, and thus $|N_p - p| \leq 2\sqrt{p}$ in this case.*

(2) *Assume $p \equiv 1 \pmod m$. Let $a \in \mathbb{F}_p$. Write $N(X^m = a)$ the number of solutions of the equation $X^m = a$. Show that*

$$N(X^m = a) = \sum_{\chi \in \mathsf{X}_m} \chi(a).$$

(3) *Suppose $p \equiv 1 \pmod 3$. Show that we still have $|N_p - p| \leq 2\sqrt{p}$.*

Problem 3. *Let K be a number field, with $\mathcal{O}_K$ its ring of integers. Let $\overline{K}$ be an algebraic closure of K, and denote by $\mathcal{O}_{\overline{K}}$ the set of algebraic integers, i.e., the set of elements of $\overline{K}$ that are integral over $\mathcal{O}_K$. Let $a, b \in \mathcal{O}_K$. Show that the following two conditions are equivalent:*

(1) *the two elements a and b are coprime to each other, in the sense that the ideal $(a,b) \subset \mathcal{O}_K$ generated by a, b is $\mathcal{O}_K$;*

(2) *there exists some $u \in \mathcal{O}_{\overline{K}}$ so that $au + b \in \mathcal{O}_{\overline{K}}^\times$.*

Problem 4. *Let $a \in \mathbb{Z}$ be square-free and let $\alpha = \sqrt[3]{a}$ be a root of $f(x) = x^3 - a$. Recall that the discriminant* $\mathrm{Disc}(f) = -27a^2$. *Denote $K = \mathbb{Q}(\alpha)$. Show that the ring of integers $\mathcal{O}_K$ has integral basis*

$$\{1, \alpha, \alpha^2\} \quad \text{if } a \not\equiv \pm 1 \pmod 9, \text{ and}$$
$$\left\{1, \alpha, \ (1 \pm \alpha + \alpha^2)/3\right\} \quad \text{if } a \equiv \pm 1 \pmod 9.$$

Problem 5. *Let p be a prime number. Let $K/\mathbb{Q}_p$ be a finite extension of $\mathbb{Q}_p$, the field of p-adic numbers.*

(1) *Show that for any fixed integer $d \geq 1$, K has only finitely many non-isomorphic finite extensions of degree d.*

(2) *Assume $(d, p) = 1$. Suppose that K has a finite Galois extension L/K of degree d which is totally ramified, show that K contains a primitive d-th root of unity and that L/K must be cyclic.*

(3) *Assume $(d, p) = 1$. Compute the number of non-isomorphic Galois totally ramified extensions of K of degree d.*