S.-T. Yau College Student Mathematics Contests 2020

Algebra and Number Theory

Solve every problem.

Problem 1. Let F be a field of characteristic zero. Consider the polynomial ring $F[x_1, \ldots, x_n]$.

(a) Prove Newton's identity over the field F

$$p_k - p_{k-1}e_1 + \cdots + (-1)^{k-1}p_1e_{k-1} + (-1)^k ke_k = 0,$$

where

$$e_k(x_1, \ldots, x_n) = \sum_{1 \leq i_1 < \cdots < \text{ß}_k \leq n} x_{i_1} \cdots x_{i_k}$$

for $1 \leq k \leq n$, $e_0 = 1$, $e_k = 0$ when $k > n$, and

$$p_k(x_1, \ldots, x_n) = x_1^k + \cdots + x_n^k.$$

(b) Prove that over the field of F of characteristic zero, an $n \times n$ matrix A is nilpotent if and only if the trace of A^k is equal to zero for all $k = 1, 2 \ldots$

Hint: use Part (a).

(c) Prove that over the field of F of characteristic zero, two $n \times n$ matrix A and B have the same characteristic polynomial if and only if the trace of A^k and trace of B^k are equal for all $k = 1, 2 \ldots$

Hint: use Part (a).

Problem 2.

(a) Let M be a finitely generated R-module and $\mathfrak{a} \subset R$ an ideal. Suppose $\phi : M \longrightarrow M$ is an R-module map such that $\phi(M) \subseteq \mathfrak{a}M$. Prove that there is a monic polynomial $p(t) \subset R[t]$ with coefficients from $\mathfrak{a}$ such that $p(\phi) = 0$.

Hint: $p(t)$ is basically just the characteristic polynomial.

(b) If M is a finitely generated R-module such that $\mathfrak{a}M = M$ for some ideal $\mathfrak{a} \subset R$, then there exits $x \in R$ such that $1 - x \in \mathfrak{a}$ and $xM = 0$.

Problem 3. Let $R = F[x, y]/(y^2 - x^2 - x^3)$ for some field F.

(a) Prove that R is an integral domain.

(b) Compute the normalization of R (*i.e.*, the integral closure of R in its field of fraction).

Problem 4. Let p and ℓ be two prime numbers and $[\ell_x]$ denote the ℓ-th cyclotomic polynomial $1 + x + \cdots + x^{\ell-1}$.

(a) Prove that $[\ell_x]$ is an irreducible element of $\mathbb{Q}[x]$.

(b) Show that $[\ell_x]$ is divisible by $x - 1$ in $\mathbb{F}_p[x]$ if $p = \ell$. Here $\mathbb{F}_p$ is the finite field $\mathbb{Z}/p\mathbb{Z}$.

(c) Suppose $p \neq \ell$. let a be the order of p in $\mathbb{F}_\ell$. Show that a is the first value of m for which the group $\mathrm{GL}_m(\mathbb{F}_p)$ of invertible $m \times m$ matrices with entries from $\mathbb{F}_p$ contains an element of order ℓ.

Hint: Derive and use the formula for the number of elements in $\mathrm{GL}_m(\mathbb{F}_p)$.

Problem 5. Let $p \geq 3$ be a prime number and let $\mathbb{Z}_p$ be the ring of p-adic integers.

(a) Show that an element in $1 + p\mathbb{Z}_p$ is a p-th power in $\mathbb{Z}_p$ if and only if it lives in $1 + p^2\mathbb{Z}_p$.

(b) Let $\mathbb{Z}_p^\times$ denote the group of units in $\mathbb{Z}_p$. Show that there exist $a, b, c \in \mathbb{Z}_p^\times$ such that $a^p + b^p = c^p$ if and only if

$$\sum_{i=1}^{p-1} i^{p-2} t^i \equiv 0 \pmod{p}$$

for some integer $t \in \{2, 3, \ldots, p-1\}$. (In particular, this condition holds for $p = 7$ by taking $t = 3$. Therefore, Fermat's Last Theorem does not hold for $\mathbb{Z}_7$.)

Problem 6. Recall that a metric space is called *spherically complete* if any decreasing sequence of closed balls has nonempty intersection.

Let p be a prime number and let $\mathbb{Q}_p$ be the field of p-adic numbers. For every integer $n \geq 1$, consider the finite extension $\mathbb{Q}_p(\mu_{p^n})$ of $\mathbb{Q}_p$ generated by all p^n-th roots of unity. Let $\mathbb{Q}_p(\mu_{p^\infty}) = \cup_{n\geq 1}\mathbb{Q}_p(\mu_{p^n})$. All of these algebraic extensions of $\mathbb{Q}_p$ are equipped with the unique norm $|\cdot|$ extending the usual p-adic norm on $\mathbb{Q}_p$.

Question: Which of the following are spherically complete? Explain why.

(a) $\mathbb{Q}_p$;

(b) $\mathbb{Q}_p(\mu_{p^n})$;

(c) $\mathbb{Q}_p(\mu_{p^\infty})$;

(d) $\widehat{\mathbb{Q}_p(\mu_{p^\infty})}$, the completion of $\mathbb{Q}_p(\mu_{p^\infty})$.

Hint: Show that there exists a sequence $a_1, a_2, \ldots \in \widehat{\mathbb{Q}_p(\mu_{p^\infty})}$ such that $|a_1| > |a_2| > \cdots$ and $\lim |a_i| > 0$, and such that the closed balls

$$B_i := \left\{x \in \widehat{\mathbb{Q}_p(\mu_{p^\infty})} \;:\; |x - a_1 - a_2 - \cdots - a_i| \leq |a_i|\right\}$$

have empty intersection.