S.-T. Yau College Student Mathematics Contests 2018

Algebra and Number Theory

Individual

This test has 5 problems and is worth 100 points. Carefully justify your answers.

Problem 1 (20 points).

(a) (6 points) Show that if $2^k - 1$ is a prime for some integer $k \geq 1$, then k is a prime.

(b) (6 points) Show that if $2^k + 1$ is a prime for some integer $k \geq 1$, then k is a power of 2.

(c) (8 points) Prove the following theorem of Goldbach: for integers $i, j \geq 0$ with $i \neq j$, the integers $2^{2^i} + 1$ and $2^{2^j} + 1$ are coprime.

Problem 2 (20 points). Let $K = \mathbb{Q}(\sqrt[3]{5})$ and let L be the Galois closure of K.

(a) (6 points) Prove that L has a unique subfield M satisfying $[M : \mathbb{Q}] = 2$. Prove that every prime number $p \equiv 1 \pmod 3$ splits in M.

(b) (6 points) Determine all prime numbers which are *ramified* in L.

(c) (8 points) Let $p \geq 7$ be a prime number. Let f_p be the inertia degree of a prime ideal of the ring of integers $\mathcal{O}_L$ of L above p. Recall that 5 is called a *cubic residue* mod p if $x^3 \equiv 5 \pmod p$ has a solution in $\mathbb{F}_p$. Prove the following decomposition law in L.

(i) If $p \equiv 1 \pmod 3$ and 5 is a cubic residue mod p, then p splits completely in L.

(ii) If $p \equiv 1 \pmod 3$ and 5 is *not* a cubic residue mod p, then $f_p = 3$.

(iii) If $p \equiv 2 \pmod 3$, then 5 is a cubic residue and $f_p = 2$. 1 [illegible]

Problem 3 (20 points). Prove that every group of order 99 is abelian.

Problem 4 (20 points). Let K be a field and let V be a finite-dimensional K-vector space.

(a) (6 points) Assume that K is infinite. Show that V is not the union of finitely many proper linear K-subspaces.

(b) (6 points) Assume that K is finite and V is non-zero. Let S be the set of affine hyperplanes of V. Let $g\colon V \to \mathbb{R}$ be a function. The Radon transform $Rg\colon S \to \mathbb{R}$ is defined by $(Rg)(\xi) = \sum_{x\in\xi} g(x)$ for $\xi \in S$. Show that $Rg = 0$ implies $g = 0$.

(c) (8 points) Let $v_1, \ldots, v_n, w_1, \ldots, w_n \in V$. Assume that for every K-linear map $f\colon V \to K$, $(f(v_1), \ldots, f(v_n))$ and $(f(w_1), \ldots, f(w_n))$ coincide up to permutation of the indices. Deduce that $(v_1, \ldots, v_n)$ and $(w_1, \ldots, w_n)$ coincide up to permutation of the indices. Here we make no assumptions on K.

Problem 5 (20 points). Let p be a prime number and let $v_p(\cdot)$ denote the p-adic valuation on $\mathbb{Q}_p$. Let $A = (a_{ij})_{1\le i,j\le n} \in \mathrm{M}_n(\mathbb{Q}_p)$ be an $n \times n$ matrix with entries in $\mathbb{Q}_p$. Assume that we know the following:

(1) $A^2 = p^{n+1} \cdot I_{n\times n}$;

(2) $v_p(a_{ij}) \ge i$ for all i, j.

Prove that $v_p(a_{ij}) \ge \max\{i, n+1-j\}$ and $a_{i,n+1-i} \in p^i\mathbb{Z}_p^\times$, i.e.

$$A \in \begin{pmatrix}
p^n\mathbb{Z}_p & p^{n-1}\mathbb{Z}_p & p^{n-2}\mathbb{Z}_p & \cdots & p^3\mathbb{Z}_p & p^2\mathbb{Z}_p & p\mathbb{Z}_p^\times \\
p^n\mathbb{Z}_p & p^{n-1}\mathbb{Z}_p & p^{n-2}\mathbb{Z}_p & \cdots & p^3\mathbb{Z}_p & p^2\mathbb{Z}_p^\times & p^2\mathbb{Z}_p \\
p^n\mathbb{Z}_p & p^{n-1}\mathbb{Z}_p & p^{n-2}\mathbb{Z}_p & \cdots & p^3\mathbb{Z}_p^\times & p^3\mathbb{Z}_p & p^3\mathbb{Z}_p \\
\vdots & \vdots & \vdots & \iddots & \vdots & \vdots & \vdots \\
p^n\mathbb{Z}_p & p^{n-1}\mathbb{Z}_p & p^{n-2}\mathbb{Z}_p^\times & \cdots & p^{n-2}\mathbb{Z}_p & p^{n-2}\mathbb{Z}_p & p^{n-2}\mathbb{Z}_p \\
p^n\mathbb{Z}_p & p^{n-1}\mathbb{Z}_p^\times & p^{n-1}\mathbb{Z}_p & \cdots & p^{n-1}\mathbb{Z}_p & p^{n-1}\mathbb{Z}_p & p^{n-1}\mathbb{Z}_p \\
p^n\mathbb{Z}_p^\times & p^n\mathbb{Z}_p & p^n\mathbb{Z}_p & \cdots & p^n\mathbb{Z}_p & p^n\mathbb{Z}_p & p^n\mathbb{Z}_p
\end{pmatrix}.$$

Hint. Consider the antidiagonal matrix

$$J = \begin{pmatrix}
0 & 0 & \cdots & 0 & p \\
0 & 0 & \cdots & p^2 & 0 \\
\vdots & \vdots & \iddots & \vdots & \vdots \\
0 & p^{n-1} & \cdots & 0 & 0 \\
p^n & 0 & \cdots & 0 & 0
\end{pmatrix}.$$

Probability and Statistics

Individual (5 problems)

Problem 1. A submarine is lost in some ocean. There are two (and only two) possible regions: A and B. Experts estimate the probability of being lost in A is 70%. On the other hand, for each search, the probability of finding this submarine is 40% if it is lost in A. This number is 80% for region B. Now we have independently searched region A 4 times and region B once, but still have not found the submarine yet. Now based on these informations, which region we should search next? And why?

Problem 2. A teacher and 12 students sit around a circle. In the beginning the teach holds a gift, he will randomly pass it to the left person or right person next to him, so as the other students each time. (For the gift, It is like a random walk between these people) The rule is that the gift will be eventually given to some student (not teacher) if he/she

is the last student who ever touches the gift.

Which student(s) have the highest probability to get this gift (i.e., win) ?

Problem 3. In a party, N people attend, each of them brings k gifts. When they leave, each of them randomly picks k gifts. Let X be the total number of gifts which are taken back by their owners. Let's fix k, please find the limiting distribution of $X\frac{1}{n}$ when $N \to \infty$.

Problem 4. Suppose that a random vector $\mathbf{x} = (x_1, ..., x_n)' \in R^n (n \geq 2)$ is distributed as a multivariate normal distribution $N(\mathbf{0}, \Sigma)$ with the following joint probability density function

$$f(\mathbf{x}) = \frac{1}{(2\pi)^{\frac{n}{2}} det(\Sigma)^{\frac{1}{2}}} \exp\left\{-\frac{1}{2}\mathbf{x}'\Sigma^{-1}\mathbf{x}\right\}, \quad \mathbf{x} \in R^n,$$

where Σ is an $n \times n$ positive definite matrix. Let the (i, j) element of $\Omega = \Sigma^{-1}$ be ω_{ij} $(1 \leq i, j \leq n)$. For $1 \leq i \neq j \leq n$, show that if $\omega_{ij} = 0$, then x_i and x_j are conditionally independent when the other elements of $\mathbf{x}$ are given.

Problem 5. Let$\mathbf{x}, \mathbf{y}$ be two independent random vectors in R^n $(n \geq 3)$. Assume that $P(\mathbf{y} = \mathbf{0}) = 0$ and $\mathbf{x}$ has a standard multivariate normal distribution, i.e., $\mathbf{x} \sim N(0, I_n)$.

(a) For any nonzero constant vector $\mathbf{a} \in R^n$ satisfying $||\mathbf{a}|| = (\mathbf{a}'\mathbf{a})^{1/2} = 1$, prove that

$$\sqrt{n-1}\frac{\mathbf{a}'\mathbf{x}}{\sqrt{||\mathbf{x}||^2 - (\mathbf{a}'\mathbf{x})^2}} \sim t_{n-1},$$

here t_{n-1} stands for a t distribution with $n - 1$ degrees of freedom.

(b) The sample correlation coefficient between $\mathbf{x} = (x_1, ..., x_n)'$ and $\mathbf{y} = (y_1, ..., y_n)'$ is defined as

$$r = \frac{\sum_{i=1}^n (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^n (x_i - \bar{x})^2}\sqrt{\sum_{i=1}^n (y_i - \bar{y})^2}}.$$

where $\bar{x} = \sum_{i=1}^n x_i/n, \bar{y} = \sum_{i=1}^n y_i/n$. Show that $\sqrt{n-2}\frac{r}{\sqrt{1-r^2}} \sim t_{n-2}$.

Algebra and Number Theory

Team

This test has 5 problems and is worth 100 points. Carefully justify your answers.

Problem 1 (20 points). Recall that a ring E is said to be *local* if for every $u \in E$, at least one of the elements u and $1-u$ is invertible. Let R be a ring and let M be an R-module.

(a) (8 points) Show that if $\mathrm{End}_R(M)$ is a local ring, then M is indecomposable.

(b) (12 points) Assume M indecomposable and of finite length. Prove the Fitting lemma: Every endomorphism u of M is either invertible or nilpotent. Deduce that $\mathrm{End}_R(M)$ is a local ring.

Problem 2 (20 points).

(a) (6 points) Let $n \geq 2$ be an integer. Show that there exists an integer m with $1 \leq m \leq n-1$ such that the binomial coefficient $\binom{n}{m}$ satisfies $\binom{n}{m} \geq 2^n/n$.

(b) (6 points) Let $0 \leq m \leq n$ be integers with $n \geq 1$. Show that for every prime number p,

$$v_p\left(\binom{n}{m}\right) \leq \log_p(n)$$

Here v_p is the p-adic valuation: $v_p(p^a b) = a$ for integers b prime to p and $a \geq 0$.

(c) (8 points) Let $n \geq 2$ be an integer and let $\pi(n)$ denote the number of prime numbers $p \leq n$. Deduce the following inequality of Chebyshev:

$$\pi(n) \geq \frac{n}{\log_2 n} - 1.$$

Problem 3 (20 points). Let $n \geq 1$ be an integer and let $\Phi_n(X) \in \mathbb{Q}[X]$ denote the n-th cyclotomic polynomial, i.e.

$$\Phi_n(X) := \prod_{\xi}(X - \xi),$$

where ξ runs through primitive n-th roots of unity in $\mathbb{C}$. Recall that $X^n - 1 = \prod_{d|n} \Phi_d(X)$ and $\Phi_n(X)$ belongs to $\mathbb{Z}[X]$. Let p be a prime number such that $p \nmid n$. Denote by $\overline{\Phi}_n$ the residue class of Φ_n in $\mathbb{F}_p[X]$. Prove the following statements:

(a) (8 points) The roots of $\overline{\Phi}_n = 0$ in the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$ are exactly the *primitive* n-th roots of 1 in $\overline{\mathbb{F}}_p$.

(b) (12 points) $\overline{\Phi}_n$ is irreducible in $\mathbb{F}_p[X]$ if and only if $(\mathbb{Z}/n\mathbb{Z})^\times$ is a cyclic group generated by the class of p.

Problem 4 (20 points). Let G be a finite group. Let V be a finite-dimensional complex representation of G and let $\chi\colon G \to \mathbb{C}$ be the associated character.

(a) (8 points) Show that there exists a subfield $L \subseteq \mathbb{C}$ containing the image of χ such that $L/\mathbb{Q}$ is a finite Galois extension. Show moreover that

$$B(\chi) = \prod_{\sigma \in \mathrm{Gal}(L/\mathbb{Q})} \prod_{g \in G} \sigma(\chi(g))$$

belongs to $\mathbb{Z}$.

(b) (12 points) Suppose that χ is irreducible and $\dim(V) \geq 2$. Show that there exists $g \in G$ with $\chi(g) = 0$. (*Hint.* One may apply the inequality of arithmetic and geometric means to $|B(\chi)|^2$.)

Problem 5 (20 points). Let F be a field, V an F-vector space of dimension d and $W \subseteq V$ a subspace. Let $f\colon W \to V$ be an F-linear map. Assume that the only subspace $W' \subseteq W$ such that $f(W') \subseteq W'$ is $\{0\}$.

(a) (6 points) Let $v \in V$ be a non-zero vector. Show that there exists a unique integer $k(v) \geq 0$ such that $v, f(v), f^2(v), \ldots, f^{k(v)-1}(v) \in W$ but $f^{k(v)}(v) \notin W$. Show moreover that $v, f(v), \ldots, f^{k(v)}(v)$ are linearly independent over F.

(b) (14 points) Prove that given $\lambda_1, \ldots, \lambda_d \in F$, there exists an F-linear extension of f to $\tilde{f}\colon V \to V$ such that the characteristic polynomial of $\tilde{f}$ is $\prod_{i=1}^{d}(\lambda - \lambda_i)$. (*Hint.* You may first treat the special case $V = \bigoplus_{i=0}^{k(v)} F f^i(v)$. For the general case, consider the subset $W_n \subseteq V$ of vectors $v \in V$ with $k(v) \geq n$ or $v = 0$.)