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 $f_p = 2$.

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

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