MOP 2018: HARD IDEAS (06/18, K)

VICTOR WANG

Abstract. We discuss problems with a *hard* rather than *soft* aesthetic. "Hardness" refers only to style, not to difficulty; the problems here vary wildly in difficulty.

1. Elementary number theory

Problem 1.1 (MIT Problem-Solving Seminar)**.** Can you find two positive integers a, b with $b - a > 1$ such that for all integers $a < k < b$, we have $\gcd(a, k) > 1$ or $\gcd(k, b) > 1$?

Problem 1.2 (Nagell–Ljunggren equation, special case)**.** Find all integers $x, n > 1$ such that $(x^n - 1)/(x - 1)$ is an *even* perfect square.

Problem 1.3 (David Yang)**.** Find all $k \geq 2$ such that there exist infinitely many pairs $(x, y) \in \mathbb{N}^2$ such that $(x + i)(y + i)$ is a perfect square for each $i = 1, 2, \dots, k$.

Problem 1.4 (MIT Problem-Solving Seminar)**.** Let $f(x) = a_0 + a_1 x + \cdots \in \mathbb{Z}[[x]]$ with $a_0 \neq 0$. Suppose that $f'(x) f(x)^{-1} \in \mathbb{Z}[[x]]$. Prove or disprove that $a_0 \mid a_n$ for all $n \geq 0$.

There are at least three approaches to the following problem.

Problem 1.5 (Artin–Hasse exponential)**.** For p a prime, prove that the coefficients of

$$E_p(x) = \exp\left(x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \frac{x^{p^3}}{p^3} + \cdots\right) \in \mathbb{Q}[[x]]$$

are rational numbers with denominators coprime to p.

Remark 1.6. An equivalent combinatorial formulation is that the number of elements of S_n (permutations on n letters) of p-power order is divisible by $p^{v_p(n!)}$. More generally, a finite group G has $\#\{x \in G : x^d = 1\} \equiv 0 \pmod{\gcd(d, \#G)}$ by a theorem of Frobenius.

2. Elementary field and Galois theory

Problem 2.1. Find a field K and a linear recurrence $a_0, a_1, a_2, \dots$ valued in K such that the set of zeros $\{n : a_n = 0\}$ is *not* eventually periodic.

Remark 2.2. If $K \supseteq \mathbb{Q}$, then the Skolem–Mahler–Lech theorem gives eventual periodicity.[1]

Problem 2.3. Prove the fundamental theorem of algebra algebraically.

Problem 2.4 (Vandermonde, Galois)**.** Let α be an algebraic number and let $\beta \in \mathbb{Q}[\alpha]$ be a $\mathbb{Q}$-coefficient polynomial expression $P(\alpha)$ in α that remains invariant when α is replaced with any conjugate of α. Prove that $\beta \in \mathbb{Q}$.

Problem 2.5. Solve a general cubic and quartic equation in radicals, using finite Fourier analysis on certain abelian group quotients of S_3 and S_4, respectively.

[1] See Tao's blog exposition if you're interested.

There are at least two different ways to solve the following problem.

Problem 2.6 (Heard from Yang)**.** Find all integers $n \geq 2$ such that $\sqrt[n]{2}$ can be written as a finite $\mathbb{Q}$-linear combination of roots of unity.

For the next problem, let $K/\mathbb{Q}$ be a number field with a $\mathbb{Q}$-*algebra automorphism*[2] $\sigma \colon K \to K$ that is *cyclic Galois* of order d, so that $\sigma^d = \mathrm{Id}$ and for any element $\alpha \in K$, the list $\alpha, \sigma\alpha, \ldots, \sigma^{d-1}\alpha$ contains all the roots of the minimal polynomial of α over $\mathbb{Q}$.

Problem 2.7 (Hilbert's theorem 90)**.** If $K/\mathbb{Q}$ is *cyclic* as specified above, prove that $\alpha \in K$ satisfies $\prod_{k=0}^{d-1} \sigma^k \alpha = 1$ if and only if there exists nonzero $z \in K$ such that $\alpha = z/\sigma z$.

3. Elementary algebraic number theory

Problem 3.1. Prove that $a_0 \mid a_n$ (affirmatively) in Problem 1.4 if $f \in \mathbb{Z}[x]$.

Problem 3.2 (USA TST 2010/9)**.** Determine whether or not there exists a positive integer k such that $p = 6k+1$ is a prime and $\binom{3k}{k} \equiv 1 \pmod{p}$.

Problem 3.3 (W.)**.** For $\omega = \zeta_5$ and $p > 5$ a prime, show that $\frac{1+\omega^p}{(1+\omega)^p} + \frac{(1+\omega)^p}{1+\omega^p} \in 2 + p^2\mathbb{Z}$.

Problem 3.4. Prove that $\prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (\zeta_n^k + \zeta_n^{-k})$ is $\pm 2^e$ for some integer $e \geq 0$.

Problem 3.5 (Ring of integers, $\mathcal{O}_{\mathbb{Q}(\zeta_p)}$, in pth cyclotomic field is $\mathbb{Z}[\zeta_p]$)**.** Let p be a prime. If $a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$ is an algebraic integer, where $a_i \in \mathbb{Q}$, then $a_i \in \mathbb{Z}$ for all i.

Theorem 3.6 (Gauss)**.** $\sum_{n=0}^{p-1} \zeta_p^{n^2}$ *is* $\sqrt{p}$ *if* $p \equiv 1 \pmod 4$, *and* $i\sqrt{p}$ *if* $p \equiv 3 \pmod 4$.

4. Elementary algebraic geometry

Let K be a field. In scheme theory, a *closed point* of $A = K[X_1, \ldots, X_n]$ is a (surjective) K-linear ring map $A \twoheadrightarrow L$ from A to a *field* L containing K. Why is this a good definition?

Problem 4.1 (Hilbert's nullstellensatz)**.** L/K is *finite* for any closed point $A \to L$.

Problem 4.2 (Lüroth's theorem)**.** If E is a *field* between K and $K(T)$, then $E = K(U)$ for some $U \in E$. (Here $K(T)$ denotes the field of rational expressions in T.)

5. Some combinatorics and geometry for Gen Z

Problem 5.1 (Reference: Newman)**.** If $X \subseteq \mathbb{Z}$ and $a_1, \ldots, a_n \in \mathbb{Z}$ are such that the translated "tiles" $X + a_1, \ldots, X + a_n$ partition $\mathbb{Z}$, prove that X is periodic. If $n = p$ is *prime*, prove that $\{a_1, \ldots, a_n \pmod{p^e}\} = p^{e-1}\mathbb{Z}/p^e\mathbb{Z}$ for some integer $e \geq 1$.

Problem 5.2 (USA Dec TST for IMO 2014: Neighbors of neighbors)**.** Let $G = (V, E)$ be a graph with no isolated vertices. Show that $\sum_{v \in V} |N^2(v)| \geq \sum_{v \in V} |N(v)|$.

Problem 5.3 (Heard from Allen Liu)**.** Let A be a (rectangular) matrix with all entries 0 or 1. If p is a prime such that $p > 4(\operatorname{rank}_{\mathbb{F}_p} A)^2$, then show that $\operatorname{rank}_{\mathbb{Q}} A < 2 \operatorname{rank}_{\mathbb{F}_p} A$.

Problem 5.4 (Robi Bhattacharjee, inspired by sphere packing?)**.** Let $e_1, \ldots, e_n$ be the standard basis of $\mathbb{R}^n$. Let V be a subspace of $\mathbb{R}^n$, and for each i, choose $v_i \in V$ such that the distance between v_i and e_i is as small as possible. Must $v_1, v_2, \ldots, v_n$ span all of V?

Problem 5.5. Let L be a set of lines in $\mathbb{R}^3$. A point $p \in \mathbb{R}^3$ is called a *joint* if p lies on (at least) three *non-coplanar* lines $\ell_1, \ell_2, \ell_3 \in L$. Prove that there are at most $2017|L|^{3/2}$ joints.

[2] meaning a $\mathbb{Q}$-linear isomorphism preserving multiplication and the identity