MOP 2018: POLYNOMIALS (06/04, B; 06/08, BK)

VICTOR WANG

1. General business: analogies from number theory

Problem 1.1. What would Euclid do?

(1) Prove that $\mathbb{Z}$ has a *division algorithm* (using the notion of *size*). In other words, $\mathbb{Z}$ is a *Euclidean domain*.
(2) Prove *Bézout's identity*: if m, n are integers, then the set of integer linear combinations of m, n coincides with the set of integer multiples of some integer g. Conclude that g divides m and n, so that $g = \pm \gcd(m, n)$.
(3) Prove that if a positive integer $p > 1$ is *irreducible* (cannot be nontrivially factored), and $p \nmid a$, then a is *invertible* modulo p, i.e. there exists $r \in \mathbb{Z}$ with $ar \equiv 1 \pmod{p}$.
(4) Prove *Euclid's lemma*: if a positive integer $p > 1$ is irreducible, and $p \mid ab$ for some integers a, b, then either $p \mid a$ or $p \mid b$.
(5) Prove the *fundamental theorem of arithmetic*: every nonzero integer has a factorization into irreducible elements, *unique* up to *units* (invertible elements).
(6) Prove the *Chinese remainder theorem* [1].
(7) Repeat the above for one-variable polynomials over a field (such as $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$). How is the Chinese remainder theorem related to Lagrange interpolation?
(8) Disprove Bézout's identity when $\mathbb{Z}$ ("integers") is replaced by $\mathbb{Z}[x]$ ("integer-coefficient polynomials"). However, show that if $P(x), Q(x)$ are two integer-coefficient polynomials sharing no complex roots, then the set

$$\{p \in \mathbb{Z} \text{ prime} : p \mid \gcd(P(n), Q(n)) \text{ for some integer } n\}$$

is finite.
(9) Disprove Bézout's identity when $\mathbb{Z}$ ("integers") is replaced by $\mathbb{C}[t, x]$ ("two-variable polynomials over a field", or "$\mathbb{C}[t]$-coefficient polynomials").

Remark 1.2. In fact, $\mathbb{Z}[x]$ and $\mathbb{C}[t, x]$ still have unique factorization.[1]

Problem 1.3 (NT analog of USA TSTST 2016/1)**.** Let $A, B \in \mathbb{Z}[x]$ be polynomials. Suppose that $\frac{A}{B}$ is a polynomial in x modulo infinitely many primes p. Prove that $A = CB$ for some polynomial $C \in \mathbb{Q}[x]$.

Problem 1.4. Guess the statement of USA TSTST 2016/1.

Problem 1.5 (Polynomial Thue: USA TSTST 2014/4)**.** Let $F = \mathbb{R}$. Let $M \in F[x]$ be a nonzero polynomial of degree $d \geq 0$, and $C \in F[x]$ a polynomial relatively prime to M. Prove that there exist $A, B \in F[x]$ of degree at most $\frac{d}{2}$ such that $\frac{A(x)-C(x)B(x)}{M(x)} \in F[x]$.

[1]For a proof sketch, see Wikipedia on Gauss's lemma (polynomial).

2. Real business: continuity, differentiation, and real roots

Problem 2.1. To find the first n derivatives of a polynomial, look modulo $(x-a)^{n+1}$.

IVT and Rolle's theorem can often help to locate real roots [2, 3].

Problem 2.2 (Interlacing polynomials)**.** Let $P, Q \in \mathbb{R}[x]$ be polynomials of degrees $n, n-1$ with all real roots $r_1 \le \cdots \le r_n$ and $s_1 \le \cdots \le s_{n-1}$, respectively. We say that P, Q are *interlaced* if $r_i \le s_i \le r_{i+1}$ for $i = 1, \ldots, n-1$. Prove that P, Q are interlaced if and only if *every* $\mathbb{R}$*-linear combination* $sP + tQ$ has all real roots.

Problem 2.3 (Putnam 2014)**.** Show that for each positive integer n, all the roots of the polynomial $\sum_{k=0}^{n} 2^{k(n-k)} x^k$ are real numbers.

Problem 2.4 (Descartes' rule of signs)**.** For a polynomial $p \in \mathbb{R}[x]$, let $z(p)$ denote the number of positive zeros and $v(p)$ the number of sign changes.

(1) Show that $2 \mid z(p) - v(p)$.
(2) Prove that $z(p) \le v(p)$ by writing $p = (x-r)q$ for some positive real root r of $p(x)$ and inducting on $\deg p$.
(3) Prove that $z(p) \le v(p)$ by considering the derivative $p'(x)$ (assuming WLOG that $p(0) \neq 0$) and inducting on $\deg p$.

Problem 2.5 (MOP 2001)**.** Let $P(x)$ be a real-valued polynomial with $P(n) = P(0)$. Show that there exist at least n distinct (unordered) pairs of distinct real numbers $\{x, y\}$ such that $x - y \in \mathbb{Z}$ and $P(x) = P(y)$.

Problem 2.6. Read about the Kadison–Singer problem if you're interested [3].

3. Complex business, real or fake

Problem 3.1. Let n be a positive integer. Find the number of pairs $P, Q \in \mathbb{R}[X]$ such that $P^2 + Q^2 = X^{2n} + 1$ and $\deg P > \deg Q$.

Problem 3.2 (Putnam 1983 B6)**.** Given a positive integer n, find polynomials $p, q \in \mathbb{Z}[X]$ such that $p^2 + q^2 \equiv -1 \pmod{X^{2^n} + X^{2^n - 1} + \cdots + X + 1}$.

Problem 3.3 (MOP 1999)**.** Given $z_1, \ldots, z_n$ on the unit circle C such that $\prod |z - z_i| \le 2$ for all $z \in C$, prove that the z_i must be vertices of a regular n-gon.

Problem 3.4 (MOP 2007)**.** Let a be a real number. Prove that every nonreal root of $f(x) = x^{2n} + ax^{2n-1} + \cdots + ax + 1$ lies on the unit circle and f has at most 2 real roots.

Problem 3.5 (Gauss-Lucas theorem)**.** The roots of a complex polynomial's derivative lie in the convex hull of the roots of the polynomial itself.

Problem 3.6 (Evan O'Dorney, ESL 2011, technical?)**.** If $a + b + c = a^n + b^n + c^n = 0$ for some positive integer n and complex a, b, c, then two of a, b, c have the same magnitude.

References

[1] `http://web.evanchen.cc/handouts/CRT/CRT.pdf` [Cited on page 1.]
[2] HroK's blog: `https://artofproblemsolving.com/community/c2032` [Cited on page 2.]
[3] `https://www.quantamagazine.org/20151124-kadison-singer-math-problem/` [Cited on page 2.]