MOP 2018: MOD (06/18, B)

VICTOR WANG

Throughout these notes, p denotes a prime. See Ireland and Rosen, *A Classical Introduction to Modern Number Theory*, for a more comprehensive treatment.

1. Expand your comfort zone

You're probably comfortable with integers modulo p^k, but how about fractions modulo p^k? If their denominators are coprime to p, you have nothing to worry about.

Problem 1.1. Define the residue of a/b modulo p^k whenever a, b are integers with $p \nmid b$. Give two ways of doing arithmetic modulo p^k, and explain why they are consistent.

Problem 1.2 (Wolstenholme)**.** For $p > 3$, show that $v_p(\sum_{k=1}^{p-1} \frac{1}{k^2}) \geq 1$ and $v_p(\sum_{k=1}^{p-1} \frac{1}{k}) \geq 2$.

Are you more comfortable with $\mathbb{Z}$ and $\mathbb{R}[x]$ than $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{R}[x]/(x^2+1)\mathbb{R}[x]$? The point of the "slash" / is to identify objects "up to equivalence" or "modulo something". There are *quotient maps* $\mathbb{Z} \to \mathbb{Z}/n$ and $\mathbb{R}[x] \to \mathbb{R}[x]/(x^2+1)$ sending an integer or polynomial A to its *residue* $\overline{A}$ (sometimes written $[A]$), and we write $\overline{A} = \overline{B}$ or $[A] = [B]$ if A and B are in the same equivalence class. It's sometimes simpler or more economical to work with equivalence classes of objects, because we then don't have to write ? (mod ?) everywhere.

2. Polynomial expressions, factorization, and formal calculus

Definition 2.1. A *polynomial expression* $a_0 + a_1 x + \cdots \in R[x]$ is a finite list of coefficients $a_0, a_1, \cdots \in R$, with arithmetic following the formal rules of exponents. We use the phrase *expression* (or *formal* polynomial) to distinguish from polynomial *functions*.

Example 2.2. Although $\overline{n}^p = \overline{n}$ in $\mathbb{F}_p$ for all $n \in \mathbb{Z}$, the *expression* $x^p - x \in \mathbb{F}_p[x]$ is considered nonzero because $a_1 = -\overline{1}$ and $a_p = \overline{1}$ are nonzero in $\mathbb{F}_p$.

Problem 2.3. Prove that a polynomial $f \in \mathbb{F}_p[x]$ has at most $\deg f$ roots. Conclude that the identity $x^p - x = \prod_{n=0}^{p-1}(x - \overline{n})$ holds in $\mathbb{F}_p[x]$. How would you express this in $\mathbb{Z}[x]$?

Question 2.4. What are the most important properties of $\mathbb{F}_p := \mathbb{Z}/p$?

Problem 2.5. Give an example of a nonlinear irreducible polynomial in $\mathbb{F}_p[x]$. Prove that every polynomial in $\mathbb{F}_p[x]$ factors uniquely into irreducibles.

Question 2.6. If $d \mid p-1$, how many solutions does $n^d \equiv 1 \pmod{p}$ have? Can you prove that there exist primitive roots modulo p? What can you say about order d elements in the multiplicative group $(\mathbb{Z}/p)^\times$? How about dth powers?

Problem 2.7 (Frobenius)**.** How many nonzero terms does $(x+y+z)^{15} \in \mathbb{F}_2[x, y, z]$ have?

Problem 2.8 (Gauss's lemma, special case of "Irreducibility statement")**.** If $f(x) \in \mathbb{Z}[x]$ is *monic* and of the form $g(x)h(x)$ for *monic* $g, h \in \mathbb{Q}[x]$, show that $g, h \in \mathbb{Z}[x]$.

Problem 2.9. Prove that $\Phi_{p^k}(x) = x^{(p-1)p^{k-1}} + \cdots + x^{p^{k-1}} + 1$ is irreducible in $\mathbb{Q}[x]$.

Remark 2.10. See Yimin Ge's online article, "Elementary Properties of Cyclotomic Polynomials", for more on cyclotomic polynomials.

Problem 2.11. Define the (formal) *power series expansion at $x = a$* of a polynomial $f(x) \in R[x]$ as the binomial expansion in powers of $x-a$. The *formal derivative* $f'(a)$ is the $(x-a)^1$ coefficient. Show that $f(x)$ is of the form $g(x)(x-a)^2$ if and only if $f'(a) = 0$.

Problem 2.12 (Putnam?)**.** If p is odd, prove that the function $F(n) = 1 + 2n + 3n^2 + \cdots + (p-1)n^{p-2}$ is injective on residues modulo p.

Problem 2.13 (Dospinescu)**.** If $p > 5$, prove that $v_p(2 \cdot \sum_{k=1}^{p-1} \frac{1}{k} + p \cdot \sum_{k=1}^{p-1} \frac{1}{k^2}) \geq 4$.

Problem 2.14. Let $A(x) = \sum_{i=1}^{p-1} (\frac{i}{p}) x^i$ and $B(x) = \prod_{j=1}^{(p-1)/2} (x^{2j-1} - x^{p-2j+1})$ in $\mathbb{F}_p[x]$, for p odd. Given that $A(x) - \sigma B(x) \equiv 0 \pmod{x^p - 1}$ for some constant σ, prove that $\sigma = 1$.

Remark 2.15. This is the hard step in the evaluation of quadratic Gauss sums.

Remark 2.16. Although $\overline{x}^p - \overline{1} = (\overline{x} - \overline{1})^p$ in $\mathbb{F}_p[x]$, the non-reduced polynomial $\sum_{i=1}^{p-1} (\frac{i}{p}) x^i \in \mathbb{R}[x]$ is only divisible by $x-1$ in $\mathbb{R}[x]$, not even $(x-1)^2$, if $p \equiv 3 \pmod 4$.

3. "Continuity properties" of polynomials and exponentials

It may be best to avoid using the phrase "p-adic continuity" in contests unless you really know what it means. But, conceptually, the following facts are similar:

(1) $P(m) \equiv P(n) \pmod{m-n}$ for polynomials $P \in \mathbb{Z}[x]$ and integers $m \neq n$. If $a, b, P(x)$ have no p's in their denominators, "p-adic continuity" is reflected in the congruence $P(a + bp^k) \equiv P(a) \pmod{p^k}$. Sometimes, you can get more precise information (if you are given more, you can deduce more).

(2) For exponentials a^n with $a \equiv 1 \pmod p$, we similarly have $v_p(a^m - a^n) \geq v_p(m-n)$. More generally, if $v_p(a) = 0$ with $a^d \equiv 1 \pmod p$, we have $v_p(a^{dm} - a^{dn}) \geq v_p(m-n)$. More precise information comes from lifting the exponent (LTE). LTE can be proven inductively on k, but the statement and proof for $p = 2$ have to be modified a little.

Problem 3.1 (Romania?)**.** Let $f \in \mathbb{Z}[x]$. Let $a_0 = 0$ and $a_n = f(a_{n-1})$ for $n \geq 1$. Prove that $\gcd(a_m, a_n) = a_{\gcd(m,n)}$.

Problem 3.2 (ELMO 2013, Andre Arslan, one-dimensional version)**.** For what polynomials $P \in \mathbb{Z}[x]$ can a positive integer be assigned to every integer so that for every integer $n \geq 1$, the sum of the n^1 integers assigned to any n consecutive integers is divisible by $P(n)$?

Problem 3.3 (Folklore)**.** If $a_1, \ldots, a_n$ are rationals with $a_1^m + \cdots + a_n^m \in \mathbb{Z}$ for $m = 1, 2, \ldots$, show that $a_1, \ldots, a_n$ are in fact integers.

Problem 3.4. Let p be odd. If a is a primitive root modulo p, show that either a or $a + p$ is a primitive root modulo p^k for all $k \geq 2$.

Remark 3.5. We've shown that for p odd, $(\mathbb{Z}/p)^\times$ cyclic implies $(\mathbb{Z}/p^k)^\times$ cyclic.

Problem 3.6 (Dospinescu–Scholze)**.** Find all $f \in \mathbb{Z}[x]$ such that $f(p) \mid 2^p - 2$ for all odd p.

Problem 3.7 (Barry Powell, AMM E 2948)**.** Let $x, y > 1$ be coprime integers. Prove that $v_p(x^{p-1} - y^{p-1}) \equiv 1 \pmod 2$ for infinitely many p.

Theorem 3.8 (Skolem–Mahler–Lech theorem)**.** *The set of zeros $\{n : a_n = 0\}$ of a linear recurrence $a_0, a_1, a_2, \ldots$ valued in $\mathbb{C}$, or any other field containing $\mathbb{Q}$, is eventually periodic.*

4. Hensel's lemma

Hensel's lemma is an analog of Newton's method (from real calculus) for root-finding.

Question 4.1 (Hensel lifting)**.** If $f \in \mathbb{Z}[x]$ such that f has a root modulo p^k, under what natural conditions can you find a root modulo p^{k+1}? Is $k+1$ the best exponent possible?

Problem 4.2. Let p be odd. If $a \in \mathbb{Z}$ is a *nonzero* square modulo p, show that it's a square modulo p^k for all $k \geq 2$. Can you generalize this to higher powers?

Remark 4.3. The roots can be chosen so that the level $k+1$ root is a *lift* of the level k root. Hensel defined the *p-adic integers* $\mathbb{Z}_p$ to package all these *compatible lifts* together.

Problem 4.4 (USA TST 2010/1)**.** Let $P \in \mathbb{Z}[x]$ be such that $P(0) = 0$ and $\gcd(P(k))_{k \geq 0} = 1$. Show there are infinitely many n such that $\gcd(P(k+n) - P(k))_{k \geq 0} = n$.

Problem 4.5 (Calvin Deng)**.** Is $\mathbb{R}[x]/(x^2+1)^2$ isomorphic to $\mathbb{C}[y]/y^2$ as an $\mathbb{R}$-algebra?

5. Using symmetric sums: complex numbers vs. primitive roots

Problem 5.1. Let g be a primitive root modulo a prime p. Let ζ_{p-1} be a primitive complex $(p-1)$th root of unity. Compare $\sum_{i=1}^{p-1} i^r$, $\sum_{k=0}^{p-2} g^{rk}$, and $\sum_{k=0}^{p-2} \zeta_{p-1}^{rk} \in \mathbb{Z}$ modulo p.

Problem 5.2 (2013-2013 Winter OMO, W.)**.** Find the remainder when $\prod_{i=0}^{100}(1 - i^2 + i^4)$ is divided by 101.

Problem 5.3 (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 5.4 (W.)**.** Let $\omega = e^{2\pi i/5}$ and $p > 5$ be a prime. Show that $\frac{1+\omega^p}{(1+\omega)^p} + \frac{(1+\omega)^p}{1+\omega^p}$ is an integer congruent to $2 \pmod{p^2}$.

6. Global picture and motivation for mods

Besides the *real absolute value* $|x|_\infty := |x| := x \operatorname{sgn} x$ on $\mathbb{Q}$, there's a *p-adic absolute value* $|x|_p := p^{-v_p(x)}$ for every prime p, which satisfies not just the triangle inequality but something stronger: $|x+y|_p \leq \max(|x|_p, |y|_p)$. For any rational number $x \neq 0$, we have the *product formula* $|x|_\infty \prod_p |x|_p = 1$, as a consequence of *prime factorization*. Together with the *Chinese remainder theorem*, the product formula suggests that "local analysis" in $\mathbb{R}$ and $\mathbb{Z}/p^k$ will play a large role in understanding the "global objects" $\mathbb{Z}$ and $\mathbb{Q}$ of number theory.

Proposition 6.1. *A nonzero integer a is a perfect square if and only if $a > 0$ and $x^2 \equiv ay^2 \pmod{p^k}$ has a nonzero integer solution (x, y), with $\gcd(x, y) = 1$, for every prime power p^k.*

This is obvious by prime factorization, but it puts the following result into context.

Theorem 6.2 (Three-variable Hasse-Minkowski theorem over $\mathbb{Q}$)**.** *Let a, b, c be nonzero integers. Let $Q = ax^2 + by^2 + cz^2$. Then $Q = 0$ has a nonzero* integer *solution (x, y, z) if and only if both of the following conditions hold:*

- *$Q = 0$ has a nonzero* real *solution (x, y, z); and*
- *$Q \equiv 0 \pmod{p^k}$ has a nonzero integer solution (x, y, z), with $\gcd(x, y, z) = 1$, for every prime power p^k.*

Remark 6.3. See Serre, *A Course in Arithmetic*, for a better formulation of the result, as well as a generalization to any number of variables.

Problem 6.4 (Ostrowski's theorem)**.** Find all functions $f\colon \mathbb{Q} \to \mathbb{R}_{\geq 0}$ such that:

- f vanishes precisely at 0 (and is positive elsewhere);
- f is multiplicative, i.e. $f(ab) = f(a)f(b)$ for all a, b; and
- f satisfies the triangle inequality, i.e. $f(a+b) \leq f(a) + f(b)$ for all a, b.

Remark 6.5. Such functions are called *absolute values* on $\mathbb{Q}$.

7. Assorted problems

Problem 7.1 (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 7.2 (TST 2010/5)**.** Define the sequence $a_1, a_2, a_3, \ldots$ by $a_1 = 1$ and, for $n > 1$,

$$a_n = a_{\lfloor n/2 \rfloor} + a_{\lfloor n/3 \rfloor} + \ldots + a_{\lfloor n/n \rfloor} + 1.$$

Prove that there are infinitely many n such that $a_n \equiv n \pmod{2^{2010}}$.

Problem 7.3 (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 $n \geq 0$.

Problem 7.4 (ISL 2009 N6)**.** Fix a positive integer k. If there exists a constant $C \in \mathbb{Z}$ such that $\sum_{i=1}^{n} i^k (i-1)! \equiv C \pmod{n!}$ for $n = 1, 2, \ldots$, show that $k \equiv 2 \pmod 3$.

Problem 7.5 (Russia 2002)**.** Show that the numerator of the reduced fraction form of $H_n = 1/1 + 1/2 + \cdots + 1/n$ is infinitely often not a prime power.