MOP 2018: POWER SERIES AND p-ADIC INTEGERS (06/13, K)

VICTOR WANG

1. Power series, actual or formal

Definition 1.1 (Power series, formal power series)**.**

Definition 1.2 (Laurent series, formal Laurent series, residue, formal residue)**.**

Definition 1.3 (Puiseux series, Hahn series)**.**

Problem 1.4 (Abel?)**.** Prove that $\sum_{k\geq 1}\frac{z^k}{k}$ converges for all $z\in\mathbb{C}\setminus\{1\}$ with $|z|\leq 1$.

Problem 1.5 (Putnam 1972)**.** The polynomial $p(x)$ has all coefficients 0 or 1, and $p(0)=1$. Show that if the complex number z is a root, then $|z|\geq(\sqrt{5}-1)/2$.

Problem 1.6 (SFTB, Proposition 9.A.21)**.** If $a_1,a_2,\dots\in\mathbb{Z}$, then formally

$$\exp\left(\sum_{n\geq 1}\frac{a_n}{n}T^n\right)=1+\sum_{n\geq 1}b_nT^n=\prod_{n\geq 1}(1-T^n)^{c_n}\in\mathbb{Q}[[T]]$$

for unique numbers $b_1,c_1,b_2,c_2,\dots\in\mathbb{Q}$. Furthermore, $b_n\in\mathbb{Z}$ for all n if and only if $c_n\in\mathbb{Z}$ for all n; if and only if $\sum_{d\mid n}\mu(\frac{n}{d})a_d\equiv 0 \pmod{n}$ for all n.

Problem 1.7. Prove that $\exp(T)=\prod_{n\geq 1}(1-T^n)^{-\mu(n)/n}\in\mathbb{Q}[[T]]$ (formally).

Problem 1.8 (USAMO 1988/5; AoPS)**.** For certain integers $b_k>0$, the polynomial product

$$(1-z)^{b_1}(1-z^2)^{b_2}(1-z^3)^{b_3}(1-z^4)^{b_4}(1-z^5)^{b_5}\cdots(1-z^{32})^{b_{32}}$$

has the surprising property that if we multiply it out and discard all terms involving z to a power larger than 32, what is left is just $1-2z$. Determine, with proof, b_{32}.

Problem 1.9 (MIT Problem-Solving Seminar)**.** Let $f(x)=a_0+a_1x+\cdots\in\mathbb{Z}[[x]]$ be a formal power series 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 1.10 (Calvin Deng)**.** Is $\mathbb{R}[x]/(x^2+1)^2$ isomorphic to $\mathbb{C}[y]/y^2$ as an $\mathbb{R}$-algebra?

2. p-adics

Reference: Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions.*

Problem 2.1. By analogy with (formal) power series and Laurent series, define the *p-adic integers*, $\mathbb{Z}_p$, and the *p-adic rationals*, $\mathbb{Q}_p$, in every way you can. You can draw looser inspiration from $[-1,1]$ and $\mathbb{R}$ as well, if you like.

Question 2.2. Should p^{9001} be considered larger or smaller, p-adically, than p^{666}?

Problem 2.3. Restate "Hensel lifting" in terms of $\mathbb{Z}_p$-solutions.

Problem 2.4. Characterize $\mathbb{Z}$ in $\mathbb{Z}_p$ and $\mathbb{Q}$ in $\mathbb{Q}_p$. Also characterize $\mathbb{Z}_p$ in $\mathbb{Q}_p$ in every way you can.

Problem 2.5 (Automorphisms of $\mathbb{Q}_p$)**.** Find all functions $f\colon \mathbb{Q}_p \to \mathbb{Q}_p$ such that $f(1) = 1$, $f(xy) = f(x)f(y)$, and $f(x+y) = f(x) + f(y)$. What if $\mathbb{Q}_p$ is replaced by $\mathbb{R}$?

Problem 2.6. Guess how to define the 10-*adic integers*, and find a pair of nonzero 10-adic integers multiplying (10-adically) to zero.

Problem 2.7. Prove that $v_2(\sum_{k=1}^{n} \frac{2^k}{k}) \to \infty$ as $n \to \infty$.

Problem 2.8 (Dwork's lemma)**.** Let $F(x) = \sum a_i x^i \in \mathbb{Q}_p[[x]]$ with $a_0 = 1$. Prove that $a_i \in \mathbb{Z}_p$ for all i if and only if $\frac{F(x^p)}{F(x)^p} \equiv 1 \pmod{p}$.

Problem 2.9 (Artin–Hasse exponential)**.** 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.

Problem 2.10. Prove that $E_p(x) = \prod_{\substack{n\geq 1 \\ \gcd(n,p)=1}} (1-x^n)^{-\mu(n)/n} \in \mathbb{Q}[[x]]$ (formally).

Theorem 2.11 (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.*

3. Global picture

For the sake of remaining completely elementary, the following statements are not optimized for mathematical aesthetics or generality.

Proposition 3.1. *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 3.2 (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 3.3. See Serre, *A Course in Arithmetic*, for a better formulation of the result, as well as a generalization to any number of variables.

Problem 3.4 (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.[1]

Problem 3.5 (Asked by Ting-Chun Lin after MOP 2018; see answer here)**.** Determine whether or not there exists a *non-rational* function $f\colon \mathbb{Q} \to \mathbb{Q}$ that is continuous in both the real sense and the p-adic sense for all primes p.

[1]Such functions are called *absolute values*.