MOP 2018: ANALYTIC NUMBER THEORY (06/22, BK)

VICTOR WANG

1. Assorted problems

Problem 1.1 (2013-2014 Spring OMO). Characterize all pairs \((m, n)\) of integers such that \(x^3 + y^3 = m + 3n\cdot xy\) has infinitely many integer solutions \((x, y)\).

Problem 1.2. Prove by infinite descent that \((-\frac{3}{p}) = -1\) for odd primes \(p \equiv 2 \pmod{3}\).

Problem 1.3. Several different positive integers lie strictly between two successive squares. Prove that their pairwise products are also different.

Problem 1.4 (HMIC 2016/4). Let \(P\) be an odd-degree integer-coefficient polynomial. Suppose that \(xP(x) = yP(y)\) for infinitely many pairs \(x, y\) of integers with \(x \neq y\). Prove that the equation \(P(x) = 0\) has an integer root.

Problem 1.5 (Dan Schwarz, RMM 2010/1). For a finite nonempty set of primes \(P\), let \(m(P)\) denote the largest possible number of consecutive positive integers, each of which is divisible by at least one member of \(P\).

(1) Show that \(|P| \leq m(P)\), with equality if and only if \(\min(P) > |P|\).

(2) Show that \(m(P) < (|P| + 1)(2^{|P|} - 1)\).

Remark 1.6. See [ELMO 2013/3] for discussion on related “sieve-like” problems.

Problem 1.7 (Pell equation, special case of Dirichlet’s unit theorem). Let \(d\) be a positive squarefree integer. Prove that Pell’s equation, \(x^2 - dy^2 = 1\), has a nontrivial integer solution, \((x, y) \neq (\pm 1, 0)\).

Problem 1.8 (TST 2014). Let \(a_1, a_2, a_3, \ldots\) be a sequence of integers, with the property that every consecutive group of \(a_i\’s\) averages to a perfect square. More precisely, for every positive integers \(n\) and \(k\), the quantity

\[
\frac{a_n + a_{n+1} + \cdots + a_{n+k-1}}{k}
\]

is always the square of an integer. Prove that the sequence must be constant (all \(a_i\) are equal to the same perfect square).

Problem 1.9 (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.

Problem 1.10 (USAMO 2012/3). Determine which integers \(n > 1\) have the property that there exists an infinite sequence \(a_1, a_2, a_3, \ldots\) of nonzero integers such that the equality

\[
a_k + 2a_{2k} + \cdots + na_{nk} = 0
\]

holds for every positive integer \(k\).
Problem 1.11 (Miklos 2000/4). Let \( a < b < c \) be positive integers. Prove that there exist integers \( x, y, z \), not all zero, such that \( ax + by + cz = 0 \) and \( \max(|x|, |y|, |z|) \leq 1 + \frac{2}{\sqrt{3}} \sqrt{c} \), and show that the constant \( \frac{2}{\sqrt{3}} \) cannot be improved.

2. Equidistribution

Let \( \alpha \) be an irrational number. Let \( e(x) := e^{2\pi ix} \).

Problem 2.1. Show that \( \frac{1}{N} \sum_{n=1}^{N} e(an) \to 0 \) as \( N \to \infty \).

Problem 2.2. Show that \( \frac{1}{N} \sum_{n=1}^{N} e(an^2) \to 0 \) as \( N \to \infty \).

These results are part of the subject of “estimating exponential sums”.

3. Transcendence theory

Theorem 3.1 (Gelfond–Schneider theorem). If \( a \) and \( b \) are algebraic numbers with \( a \neq 0 \), \( a \neq 1 \), and \( b \) irrational, then any value of \( a^b \) is a transcendental number.

Theorem 3.2 (Lindemann–Weierstrass Theorem, Baker’s reformulation). If \( a_1, \ldots, a_n \) are nonzero algebraic numbers, and \( \alpha_1, \ldots, \alpha_n \) are distinct algebraic numbers, then \( a_1 e^{\alpha_1} + \cdots + a_n e^{\alpha_n} \neq 0 \).

Baker’s theorem (on “linear forms in logarithms”) generalizes both results above.

4. Ideas in Dirichlet’s theorem

Let \( \chi : (\mathbb{Z}/m) \times \to \mathbb{C} \times \) be a multiplicative character modulo \( m \). By abuse of notation, we extend it to a periodic multiplicative function \( \chi : \mathbb{Z} \to \mathbb{C} \times \) such that \( \chi(a) = 0 \) if and only if \( \gcd(a, m) > 1 \). The extension \( \mathbb{Z} \to \mathbb{C} \times \) is known as a Dirichlet character of modulus \( m \).

Definition 4.1. Define the Dirichlet L-function \( L(s, \chi) := \sum_{n \geq 1} \frac{\chi(n)}{n^s} \) when \( \Re(s) > 1 \).

Problem 4.2. Study \( L(s, \chi) \) for the two Dirichlet characters \( \chi \) of modulus \( m = 4 \), especially as \( s \to 1^+ \) in \( \mathbb{R} \), to prove Dirichlet’s theorem for primes congruent to 1 or 3 modulo 4.

A general modulus \( m \) requires more work. Below, assume \( \chi \) is nontrivial.

Problem 4.3. Extend the definition of \( L(s, \chi) \) from \( \Re(s) > 1 \) to \( \Re(s) > 0 \).

Now, here are the most difficult steps in Monsky’s elementary proof of Dirichlet’s theorem.

Problem 4.4. If \( \chi \) is real-valued, then \( f(x) := \sum_{n \geq 1} \chi(n) \frac{x^n}{1-x^n} \) is unbounded as \( x \to 1^- \).

Problem 4.5. If \( L(1, \chi) = 0 \), i.e. \( \sum_{n \geq 1} \frac{\chi(n)}{n} = 0 \), then \( f(x) \) is bounded as \( x \to 1^- \).

Consequently, \( L(1, \chi) \neq 0 \) for any (nontrivial) real-valued character \( \chi \). A standard argument, based on the product \( \prod_{\chi \mod m} L(s, \chi) \), shows that \( L(1, \chi) \neq 0 \) for complex-valued characters \( \chi \) too.

Following Dirichlet’s classical idea of finite Fourier analysis on \((\mathbb{Z}/m)^\times\) (generalizing the intended “second roots of unity filter” method above for \( m = 4 \)), the non-vanishing of all the values \( L(1, \chi) \) guarantees that for every residue class \( \overline{a} \in (\mathbb{Z}/m)^\times \), we have

\[
\sum_{p=1} \frac{1}{p^s} = \frac{1}{\phi(m)} \log \left( \frac{1}{s-1} \right) + O(1)
\]

as \( s \to 1^+ \).