MOP 2018: DIOPHANTINE EQUATIONS (06/21, B)

VICTOR WANG

1. Polynomial Diophantines

Many things, like Fermat's last theorem, are much easier for polynomials.

2. Prime Factorization

Observing the exponents in the prime factorization of a number can yield much useful information. The following examples illustrate this:

Example 2.1. Find the number of triples of integers (x, y, z) such that $xyz = 720$.

Example 2.2 (Four numbers theorem)**.** If $ab = cd$ for positive integers a, b, c, d, show that there exist positive integers x, y, z, w such that $a = xy$, $b = zw$, $c = xz$, and $d = yw$, where $\gcd(y, z) = 1$.

Example 2.3. If two numbers a and b are relatively prime, and ab is a perfect kth power, then a and b are both perfect kth powers.

The following is an example of how the above can be applied:

Example 2.4. Solve $y^2 = x^3 - x$ over the integers.

3. Algebraic manipulation, factorization, and bounding

Modular arithmetic, prime factorization, algebraic conjugates, and other ideas from number theory are often combined with manipulation and/or bounding to great success.

Example 3.1. Suppose that $a \equiv 1 \pmod{p}$. Show that $a^p \equiv 1 \pmod{p^2}$.

Example 3.2. Find all pairs of integers (x, y) with $0 < x < y$ and $x^y = y^x$.

Example 3.3. Solve $y^2 = x^2 + y^3x - 1$ over the positive integers. How about over all integers?

Problem 3.4 (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.

Factoring is one of the most useful manipulations. For example, it lets us parameterize the Pythagorean triples as follows:

Theorem 3.5. *Suppose (a, b, c) is a Pythagorean triple. Then $(a, b, c) = (k \cdot 2mn, k(m^2 - n^2), k(m^2 + n^2))$ or $(k(m^2 - n^2), k \cdot 2mn, k(m^2 + n^2))$ for some positive integer k and some relatively prime integers m, n.*

Problem 3.6. Solve $x^2 + y^2 = 2z^2$ over the positive integers in every way you can.

Problem 3.7. Solve $1/x + 1/y = 1/z$ over the positive integers.

Problem 3.8. Solve $1/x^2 + 1/y^2 = 1/z^2$ over the positive integers.

4. Infinite Descent

The method of infinite descent is essentially an extremal argument: given a solution (sometimes we take it to be minimal), we try to reduce it to either restrict the possible minimal solutions or show that there are no (nontrivial) solutions in the first place.

Example 4.1. Show that $\sqrt{2}$ is irrational.

A special type of infinite descent is known as Vieta jumping, or root flipping, where we use in particular that for a quadratic with integer coefficients, either both roots are integers or both roots are not integers (i.e. if one root is an integer, the other must be as well).

Example 4.2 (IMO 1988/6)**.** Let a, b be positive integers such that $ab+1 \mid a^2+b^2$. Prove that $(a^2+b^2)/(ab+1)$ is a perfect square.

Problem 4.3 (ISL 2009)**.** Find all positive integers n such that there exists a sequence of positive integers $a_1, a_2, \ldots, a_n$ satisfying

$$a_{k+1} = \frac{a_k^2+1}{a_{k-1}+1} - 1$$

for every k with $2 \le k \le n-1$.

5. Test your classifier

Problem 5.1 (St. Petersburg)**.** Prove that the equation $3^k = m^2+n^2+1$ has infinitely many solutions in positive integers.

Problem 5.2. Find infinitely many integral solutions of $(x^2+x+1)(y^2+y+1) = z^2+z+1$.

Problem 5.3 (Nick's Math Puzzles 110; AMM?)**.** Several different positive integers lie strictly between two successive squares. Prove that their pairwise products are also different.

Problem 5.4 (China)**.** Let $x < y$ be positive integers and

$$P = \frac{x^3-y}{1+xy}.$$

Find all integer values that P can take.

6. Things Fermat actually proved

Problem 6.1. If x, y are positive integers, prove that x^2-y^2 and x^2+y^2 cannot both be perfect squares.

Problem 6.2. Given 4 squares in arithmetic progression, show that they must all be equal.

Problem 6.3. Prove that $x^4+y^4=z^2$ has no solutions in positive integers.

Problem 6.4. Prove that $x^4-y^4=z^2$ has no solutions in positive integers.

Problem 6.5. Find all integer solutions to $x^4-x^2y^2+y^4=z^2$.

Problem 6.6. Find all integer solutions to $x^4+x^2y^2+y^4=z^2$.

Do you know how Gauss originally used "induction on primes" to prove quadratic reciprocity (QR)? Reference: L. Carlitz, "A Note on Gauss' First Proof of the Quadratic Reciprocity Theorem" (heard from MathOverflow question on QR proofs).

Problem 6.7. Prove by infinite descent that $(\frac{-3}{p}) = -1$ for odd primes $p \equiv 2 \pmod 3$.

7. Norms, units, and rational approximation

Problem 7.1 (2013-2014 Spring OMO)**.** Characterize all pairs (m, n) of integers such that $x^3 + y^3 = m + 3nxy$ has infinitely many integer solutions (x, y).

Problem 7.2 (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, $(x, y) \neq (\pm 1, 0)$. Furthermore, given $m \in \mathbb{Z}_{>0}$, prove that infinitely many solutions of Pell's equation satisfy $(x, y) \equiv (1, 0) \pmod{m}$.

Problem 7.3 (Nice special case of negative Pell equation)**.** Let $p > 2$ be a prime. Prove that $p \equiv 1 \pmod 4$ if and only if there exist integers x, y such that $x^2 - py^2 = -1$.

Problem 7.4 (Units of norm -1?)**.** Let $d \equiv 1 \pmod 4$ be a squarefree positive integer. Show that $x^2 - dy^2 = -1$ is solvable in $\mathbb{Z}$ if and only if $x^2 - dy^2 = -4$ is.

Problem 7.5 (From Alison Miller's 2010 notes; AMM?)**.** If a, b are non-square positive integers, prove that $ax^2 - by^2 = \pm 1$ cannot both be solvable in integers x, y.

Problem 7.6 (Dirichlet)**.** Solve $x^3 + 2y^3 + 4z^3 - 6xyz = 1$ over the positive integers.

Problem 7.7. If $p = a^2 + nb^2 = c^2 + nd^2$ for a prime p and positive integers a, b, c, d, n, with $n > 1$, show that $a = c$.

Problem 7.8 (nnosipov, AoPS)**.** Find the least positive constant c for which

$$\frac{m}{n} < \sqrt{34} < \frac{m}{n} + \frac{c}{mn}$$

has infinitely many solutions in positive integers m, n.

Problem 7.9 (IMO 1996/4)**.** The positive integers a and b are such that the numbers $15a + 16b$ and $16a - 15b$ are both squares of positive integers. What is the least possible value that can be taken on by the smaller of these two squares?

Theorem 7.10 (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 7.11. See Serre, *A Course in Arithmetic*, for a better formulation of the result, as well as a generalization to any number of variables.

8. Things I used to know how to do

Problem 8.1 (IMO 1982/4)**.** Prove that if n is a positive integer such that the equation

$$x^3 - 3xy^2 + y^3 = n$$

has a solution in integers x, y, then it has at least three such solutions. Show that the equation has no solutions in integers for $n = 2891$.

Problem 8.2 (ISL 1984; special case of Erdős–Selfridge theorem)**.** Can the product of five consecutive positive integers be a perfect square?

Problem 8.3 (ISL 2001 N2)**.** Find the greatest value of the real constant m such that $m \leq x/y$ for any positive integers x, y, z, u satisfying $x \geq y$, $x + y = z + u$, and $2xy = zu$.

Problem 8.4 (Wilson+)**.** Find all primes p such that $(p-1)! + 1$ is a perfect power of p.

Problem 8.5 (Brazil 2010/6)**.** Solve $3^a - 1 = 2b^2$ over the positive integers.

Problem 8.6 (China 2010 Quiz 1/3)**.** Find all positive integers $m, n \geq 2$ such that $m+1 \equiv 3 \pmod 4$ is a prime number and for some prime number p and nonnegative integer a,

$$\frac{m^{2^n-1} - 1}{m-1} = m^n + p^a.$$

Problem 8.7 (Russia 2011 11-7)**.** For an integer a, let $P(a)$ be a largest prime positive divisor of $a^2 + 1$. Prove that there exist infinitely many triples of distinct positive integers (a, b, c) such that $P(a) = P(b) = P(c)$.

Problem 8.8 (Russia 2005 11-4)**.** Integers $x > 2$, $y > 1$, $z > 0$ satisfy $x^y + 1 = z^2$. If p denotes the number of different prime divisors of x and q denotes the number of prime divisors of y, prove that $p \geq q + 2$.

Problem 8.9 (Victor Wang)**.** Solve $y^2 = 8x^4 - 8x^2 + 1$, $y^2 = 20x^4 - 4x^2 + 1$, and $y^2 = 2x^4 - 2x^2 + 1$ over the integers.

Problem 8.10 (nnosipov, AoPS)**.** Are there rational numbers x, y, z such that $x^2 - y^2 = 2011 = z^2 - x^2$?

Problem 8.11 (nnosipov, AoPS)**.** For some positive integers x and y, the number x^2 is divisible by $2xy + y^2 - 1$. Prove that $2x$ divides $y^2 - 1$.

Problem 8.12 (Bulgaria 2005/6)**.** Let a, b, c be positive integers such that ab divides $c(c^2 - c + 1)$ and $a + b$ is divisible by $c^2 + 1$. Prove that $\{a, b\} = \{c, c^2 - c + 1\}$.

Problem 8.13 (MOP 2010 Team Contest; China?)**.** Find all positive integer solutions to

$$(a+b)^x = a^y + b^y.$$

9. Tricky things for inspired teens

Problem 9.1 (IMO 2001/6)**.** Let $a > b > c > d$ be positive integers satisfying $ac + bd = (b + d + a - c)(b + d + c - a)$. Prove that $ab + cd$ is composite.

Problem 9.2 (MOP 2010 Team Contest)**.** Let $a > b > c > d$ be positive integers satisfying $ac + bd = (b + d + a - c)(b + d + c - a)$. Compute the smallest possible number of total prime factors of $(ab + cd)(ac + bd)(ad + bc)$ (i.e. $p^i \parallel (ab + cd)(ac + bd)(ad + bc)$ adds i to the count).

Problem 9.3 (Nagell–Ljunggren equation, special case)**.** Find all integers $x, n > 1$ such that $(x^n - 1)/(x - 1)$ is an *even* perfect square.

Problem 9.4 (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 $i = 1, 2, \ldots, k$.

Problem 9.5 (Euler?)**.** Show that there are infinitely many *Diophantine quadruples*: positive integers (a_1, a_2, a_3, a_4) such that $a_i a_j + 1$ is a perfect square for all $1 \leq i < j \leq 4$.

Problem 9.6 (Kiran Kedlaya, PEN?)**.** Given positive integers x, y, z such that $(xy+1)(yz+1)(zx + 1)$ is a perfect square, show that each of $xy + 1, yz + 1, zx + 1$ is a perfect square itself.