Number theory

Botong Wang

February 19, 2020

Diophantine equations

A **Pythagorean triples** consists of three positive integers a, b and c such that $a^2 + b^2 = c^2$.

Theorem (Euclid's formula)**.** *All primitive Pythagorean triples (after possibly exchanging a and b) are of the form*

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2,$$

for some positive integers m and n.

A consequence of Euclid's formula is a special case of Fermat's last theorem.

Theorem. *The equation*

$$x^4 + y^4 = z^2$$

has no nontrivial integer solution.

Pell's equation:

$$x^2 - Dy^2 = 1$$

where D is a positive integer that is not a perfect square.

Theorem (Lagrange's theorem)**.** *The Pell equation has infinitely many positive integer solutions, and the general solution (x_n, y_n) is computed from the relation*

$$(x_n, y_n) = (x_1 + y_1\sqrt{D})^n,$$

where (x_1, y_1) is the fundamental solution, that is, the minimal solution different from the trivial solution $(1, 0)$.

The proof of Lagrange's theorem is long but inspiring. A detailed discussion can be found here:

http://math.uga.edu/∼pete/4400pellnotes.pdf

The initial solution of Pell equation can be found using continued fraction expansion of $\sqrt{D}$. See *Putnam and beyond* section 5.3.3.

Modular arithmetics

Theorem (Fermat's little theorem)**.** *Let p be a prime number and n a positive integer. Then*

$$n^p \equiv n (\mathrm{mod}\ p).$$

Problems

1. Let $a_n = 10 + n^2$ for $n \geq 1$. For each n, let d_n denote the gcd of a_n and $a_n + 1$. Find the maximum value of d_n as n ranges through the positive integers.
Hint: show that the gcd divides 41.

2. Let p be an odd prime number. Show that if the equation $x^2 \equiv a (\mathrm{mod}\ p)$ has a solution, then $a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\ p)$. Conclude that there are infinitely many primes of the form $4m+1$.
Putnam and Beyond 762.

3. Prove that for every pair of positive integers m and n, there exists a positive integer p satisfying
$$\left(\sqrt{m} + \sqrt{m-1}\right)^n = \sqrt{p} + \sqrt{p-1}.$$
Putnam and Beyond 812.

4. Find all prime numbers of the form $1010 \cdots 101$ written in base 10.
Hint: suppose the number has $2n - 1$ digits. Then it is equal to $\frac{10^{2n}-1}{99}$. Notice that $10^{2n} - 1 = (10^n - 1)(10^n + 1)$. If the number is a prime number, then $10^n - 1 \leq 99$.

5. Prove that the equation
$$x^2 + y^2 + z^2 + 3(x + y + z) + 5 = 0$$
has no solutions in rational numbers.
Putnam and beyond 817.

6. Find all ordered pairs of positive integers a, b such that
$$\frac{1}{a} + \frac{1}{b} = \frac{3}{2018}.$$
Putnam 2018 (A-1).

7. Let $a_0 = 1$, $a_1 = 2$, and
$$a_n = 4a_{n-1} - a_{n-2}$$
for $n \geq 2$. Find an odd prime factor of a_{2015}.
Hint: use the general term formula from the previous lecture.

8. Prove that the sequence $2^n - 3$, $n \geq 1$, contains an infinite subsequence whose terms are pairwise relatively prime.
Putnam and beyond 765.

9. Let f be a polynomial with positive integer coefficients. Prove that if n is a positive integer, then $f(n)$ divides $f(f(n) + 1)$ if and only if $n = 1$.
Putnam 2007 (B-1).

10. Show that for each positive integer n,
$$n! = \prod_{i=1}^{n} \mathrm{lcm}\left\{1, 2, \cdots, \lfloor \frac{n}{i} \rfloor\right\}.$$
Here lcm denotes the least common multiple.
Putnam 2003 (B-3).

11. Prove that there are infinitely many squares of the form

$$1 + 2^{x^2} + 2^{y^2},$$

where x and y are positive integers.
Putnam and beyond 806.

12. Prove that $x^2 = y^3 + 7$ has no integer solutions.
Putnam and beyond 763.