Lectures on Challenging Mathematics

Elements of Math Olympiads

Number Theory

Summer 2018

Zuming Feng
Phillips Exeter Academy and IDEA Math
zfeng@exeter.edu

Contents

1.15 Elementary proofs in number theory

1. Let p be an odd prime, and let m and n be positive integers such that $\gcd(m,n)=1$ and

$$\frac{m}{n}=1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}.$$

Prove that m is divisible by p. Is the statement true, if we replace p with any positive odd integer greater than 1?

2. Find the smallest positive integer k which is representable in the form $k=19^n-5^m$ for some positive integers m and n. An obvious choice for k is 14. But to prove that positive integers less than 14 are not representable in the form of 19^n-5^m is a bit more difficult.

   (a) Prove that we only need to consider two possible candidates 4 and 6.

   (b) Assume that $19^n-5^m=6$ for some positive integers n and m. First prove that both n and m are even. Then prove that there are no such numbers n and m.

   (c) Prove that 4 is not representable in the form of 19^n-5^m.

3. Assume that (x_0,y_0,z_0,w_0) is a quadruple of positive integers that satisfies the following equation:

$$x^2+y^2=3(z^2+w^2).$$

Show that one can find a *smaller* quadruple (x_1,y_1,z_1,w_1) of positive integers that satisfies the same equation, where $x_1^2<x_0^2$, $y_1^2<y_0^2$, $z_1^2<z_0^2$, and $w_1^2<w_0^2$. What conclusion can you draw from this fact? (Note that there are different ways to interpret the term *smaller*.)

This process is called *finite/infinite descent*. We will discuss this method in detail in our future series.

4. Show that the set of primes that divide at least one number of the form n^2+n-1, $n\geq 1$, is infinite.

5. Searching for primes remains a focal point in the field of number theory. A famous result on the distribution of primes is Bertrand's postulate, proposed by Bertrand in 1845 and proved by Chebyshev using elementary methods in 1850:

> If n is an integer greater than 1, then there is always at least one prime p such that $n<p<2n$.

Prove, without the assumption of this postulate, much weaker results:

   (a) For every positive integer n greater than 2, there is a prime p such that $n<p<n!$.

   (b) If $p_1=2$, $p_2=3$, $p_3=5$, ... is the sequence of prime numbers, then the n-th prime number, p_n, is less than or equal to $2^{2^{n-1}}$.