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. Number Theory
   1.1 Modular arithmetic (part 1) ............................................. 3
   1.2 Perfect numbers, Mersenne primes, and the sum of divisors ............. 5
   1.3 Number theory practice set 1 ........................................... 6
   1.4 Modular arithmetic (part 2) ............................................. 7
   1.5 The first look at the Frobenius Coin theorem ............................. 8
   1.6 Number theory practice set 2 ........................................... 9
   1.7 Modular arithmetic (part 3) ............................................. 10
   1.8 Establishing the Frobenius Coin theorem (part 1) ......................... 11
   1.9 Number theory practice set 3 ........................................... 13
   1.10 Establishing the Frobenius Coin theorem (part 2) ......................... 14
   1.11 Pythagorean triples and parametric solutions ............................. 15
   1.12 Number theory practice set 4 ........................................... 16
   1.13 Modular arithmetic (part 4) ............................................. 17
   1.14 Diophantine equations (part 1) ........................................ 18
   1.15 Elementary proofs in number theory .................................... 19
   1.16 Number theory practice set 5 .......................................... 20
   1.17 Diophantine equations (part 2) ........................................ 21
   1.18 Number theory practice set 6 .......................................... 22
   1.19 A direct proof of the Fundamental Theorem of Arithmetic ................ 23
   1.20 Diophantine equations (part 3) ........................................ 24
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 $k = 19^m - 5^m$ 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 $19^m - 5^m$ is a bit more difficult.

   (a) Prove that we only need to consider two possible candidates 4 and 6.
   (b) Assume that $19^m - 5^m = 6$ 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 $19^m - 5^m$.

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 $x_1 < x_0$, $y_1 < y_0$, $z_1 < z_0$, and $w_1 < w_0$. 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 $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, \ldots is the sequence of prime numbers, then the $n$-th prime number, $p_n$, is less than or equal to $2^{2n-1}$.