Lectures on Challenging Mathematics

Introduction to Math Olympiads

Number Theory

Summer 2021

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

"Cogito ergo Sum" – "I think, therefore I am"

René Descartes (1596–1650)

"Success is not final, failure is not fatal, it is the courage to continue that counts."

Winston Churchill (1874–1965)

"I can see that without being excited, mathematics can look pointless and cold. The beauty of mathematics only shows itself to more patient followers."

Maryam Mirzakhani (1977–2017)

Contents

1.9 Revisiting modular arithmetic (part 3)

1. Solve the following equations:

   (a) $x^2 \equiv 1 \pmod{15}$ (b) $x^2 \equiv 1 \pmod{65}$
   (c) $x^2 \equiv -1 \pmod{15}$ (d) $x^2 \equiv -1 \pmod{65}$

   Specify the number of solutions for each equation. Explain how solving equations

   $x^2 \equiv 1 \pmod{3}$, $x^2 \equiv -1 \pmod{3}$,
   $x^2 \equiv 1 \pmod{5}$, $x^2 \equiv -1 \pmod{5}$,
   $x^2 \equiv 1 \pmod{13}$, $x^2 \equiv -1 \pmod{13}$,

   could have helped to predict the result.

   In Algebra, solving a quadratic equation is much harder than solving a linear equation—remember the so-called quadratic formula? In modular arithmetic, solving a linear equation is already challenging, and solving a quadratic equation is much more challenging. The most important result on this front is the *law of quadratic reciprocity*. It was conjectured by Euler and Legendre and first proved by Gauss, who referred to it as the "fundamental theorem" in his *Disquisitiones Arithmeticae*. This is a theorem you shall learn (and learn well) in a formal number theory course.

2. Consider the following statement:

   > There are $n-1$ consecutive integers such that it is possible to divide them into two disjoint sets A and B such that the product of numbers in A is congruent to the product of numbers in B modulo n.

   Determine if the statement is true for

   (a) $n = 13$ (b) $n = 19$.

3. Find all positive integers n greater than 1 such that there exist two complete sets of residue classes modulo n $\{a_1, a_2, \ldots, a_n\}$ and $\{b_1, b_2, \ldots, b_n\}$ such that $\{a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n\}$ is a complete set of residue classes modulo n.

4. (Continuation) Prove that for each positive integer n there exist two complete sets of residue classes modulo n $\{a_1, a_2, \ldots, a_n\}$ and $\{b_1, b_2, \ldots, b_n\}$ such that $\{a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n\}$ contains at least $n - 1$ distinct congruence classes modulo n.

5. Show that there are infinitely many n such that $n! - 1$ is divisible by at least two distinct primes.

1.13 Fermat's Little Theorem

1. Determine all positive integers n such that $n^6 - 1$ is divisible by each of 2, 3, 5, 7, and 13.

2. (a) Find the smallest positive integer m for each of the following congruence relations.
   (i) $2^m \equiv 1 \pmod{13}$ (ii) $2^m \equiv 1 \pmod{31}$
   (i) $5^m \equiv 1 \pmod{13}$ (ii) $5^m \equiv 1 \pmod{31}$
   (b) Explain why $\frac{1}{13}$ is a 6-digit repeating decimal.
   (c) Explain why $\frac{1}{31}$ is a 15-digit repeating decimal.

3. Let a and m be relatively prime integers. Prove that the sequence
$$a,\ a^2,\ a^3,\ \ldots \pmod{m}$$
is periodic and that $a^k \equiv 1 \pmod{m}$ for some integer k.

4. *Fermat's Little Theorem* states that if prime p is a prime and a is a positive integer relatively prime to p, then $a^{p-1} \equiv 1 \pmod{p}$.
   (a) Prove Fermat's Little Theorem by considering the set $\{a, 2a, 3a, \ldots, (p-1)a\}$.
   (b) Prove Fermat's Little Theorem inductively by using binomial expansion.

5. We intend to show that there are infinitely many primes of the form $4k + 1$. Complete the following statements.

   Assume on the contrary that there are only _____ many primes of the form $4k + 1$. Thus let P be the greatest prime of the form $4k + 1$. We consider the number $n = (P!)^2 + 1$. Let p be a _____ divisor of n. Clearly, p is _____ than P. (In particular, p is odd and _____ prime to _____.) Because p is a _____ of n, we have $(P!)^2 \equiv -1 \pmod{p}$. Because p is odd, _____ is an integer and so we can raise both sides to the $\left(\frac{p-1}{2}\right)^{\text{th}}$ power to obtain

$$\_\_\_\_\_ \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

   By _____ _____ Theorem, the _____ side of the above congruence is congruent to 1 modulo p. It therefore follows that $1 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Because p is odd, _____ must be even, implying that p is also of the form $4k + 1$, contradicting the assumption that P is the _____ prime of the form $4k + 1$. Therefore, our original assumption was false, hence there are _____ many primes of the form $4k + 1$.