TJUSAMO - Number Theory 2

Sohail Farhangi, Victoria Xia

December 10th, 2012

1 Review from Number Theory 1

1. Do there exist positive integers m, n such that $m^{20} + 11^n$ is a perfect square?
2. Find all pairs of prime numbers p, q such that $p^2 - p - 1 = q^3$.
3. Let m and n be nonnegative integers. Prove that $\frac{(2m)!(2n)!}{m!n!(m+n)!}$ is always an integer.

2 Residue Classes

The integers can be split into *residue classes modulo n* such that any two integers in the same residue class are congruent mod n, but no two integers from different classes are. When the elements of one residue class are added to or multiplied by the elements of another residue class, the resulting set of values are a subset of another residue class; this is why we are allowed to reduce before or after addition/multiplication when working in mods. However, be very careful with division.

2.1 Complete Sets of Residues

A set of n integers is said to be a *complete set of residues mod n* iff the elements of the set are such that there is exactly one from each residue class mod n. For example, if a is relatively prime to n, then the set $S = \{a, 2a, ..., (n-1)a, na\}$ is a complete set of residues mod n.

2.2 Inverses

Consider the congruence $ax \equiv 1 \pmod{n}$. What must be true about a and n if this congruence has a solution x? Does this condition guarantee there is always a solution? (In particular, what can we say about prime mods?)

If such an x exists, then x is *the inverse of a mod n*. Does the inverse have to be unique?

3 Useful Theorems

3.1 Fermat's Little Theorem

For prime p and integer a relatively prime to p, $a^{p-1} \equiv 1 \pmod{p}$.

3.1.1 Euler's Totient Function

Fermat's Little Theorem is not (necessarily) true if the modulus is not prime. Which step of the proof breaks down?

Euler makes a more general statement for any mod n: Given a relatively prime to n, $a^{\phi(n)} \equiv 1 \pmod{n}$, where $\phi(n)$ is *Euler's totient function*, defined to be the number of positive integers less than or equal to n that are relatively prime to n.

3.2 Wilson's Theorem and Symmetric Polynomials

For prime p, $(p-1)! \equiv -1 \pmod{p}$. The converse is also true. Can you see how to generalize this to symmetric polynomials? Consider the following equivalence:

$$\prod_{i=1}^{n}(x-a_i) \equiv x^p - x \pmod{p}$$

3.3 Chinese Remainder Theorem

If m and n are relatively prime positive integers, then the system $x \equiv a \pmod{m}$; $x \equiv b \pmod{n}$ has a unique solution mod mn. Note that this result easily extends to any number of linear congruences will relatively prime mods.

4 Problems

4.1 To Do Here

1. How many solutions does $ax \equiv b \pmod{n}$ have?

2. How many solutions are there to $x^2 \equiv y^2 + 1 \pmod{p}$?

3. How many solutions are there to $x^2 + y^2 \equiv 1 \pmod{p}$?

4. Let p be a prime with $p > 5$. Prove that $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$.

5. Consider the sequence $a_1, a_2, ...$ defined by $a_n = 2^n + 3^n + 6^n - 1$ for all positive integers n. Determine all positive integers that are relatively prime to every term of the sequence.

6. Determine if it is possible to arrange $1, 2, ..., 1000$ in a row such that the average of any pair of distinct numbers is not located in between the numbers.

7. Prove that for each prime $p \geq 7$, there exists a positive integer n and integers $x_1, ..., x_n, y_1, ..., y_n$ not divisible by p such that

$$\begin{aligned} x_1^2 + y_1^2 &\equiv x_2^2 \pmod{p} \\ x_2^2 + y_2^2 &\equiv x_3^2 \pmod{p} \\ &\cdots \\ x_n^2 + y_n^2 &\equiv x_1^2 \pmod{p} \end{aligned}$$

.

4.2 To Do At Home

1. Prove that for any integer $a \geq 2$, $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$.
2. Find all prime numbers p and q such that pq divides the product $(5^p - 2^p)(5^q - 2^q)$.
3. For any positive integers n and k, let $L(n,k)$ be the least common multiple of the k consecutive integers $n, n+1, ..., n+k-1$. Show that for any integer b, there exist integers n and k such that $L(n,k) > bL(n+1,k)$.
4. Let $n \geq 1$ be an odd integer. Determine all functions f from the set of integers to itself such that for all integers x and y the difference $f(x) - f(y)$ divides the difference $x^n - y^n$.