Novice Number Theory

Andre Kessler

September 29, 2010

1 Prime Mods

Suppose you have numbers a, b, c, each relatively prime to p, such that

$$ab \equiv ac \pmod{p}$$

This, however, implies that $ab - ac \equiv 0 \pmod{p}$. Pulling out the factor of a, we see $a(b - c) \equiv 0 \pmod{p}$. Since a is relatively prime to p, we need $b - c \equiv 0 \pmod{p}$ and therefore $b \equiv c \pmod{p}$.

2 Composite Mods

If the modulus is prime, then we can divide out common factors from each side. If it is composite, however, we can't necessarily do that. For example, consider $20 \equiv 2 \pmod{6}$. If we divide out a 2 on each side, we get $10 \equiv 1 \pmod{6}$, which is **not true**.

3 The Idea

Consider the set

$$S = \{1, 2, 3, \ldots, p - 1\}$$

consisting of the nonzero residues in mod p. Now suppose we multiply each element by a.

$$\{a, 2a, 3a, \ldots, (p - 1)a\}$$

Every element in this set must be distinct, because we can simply divide out the common factor of a in this prime mod. But there are only $p - 1$ nonzero residues mod p, so this must be a permutation of S.

4 Invertibility

In particular, because $\{a, 2a, 3a, \ldots, (p - 1)a\}$ is a permutation of $\{1, 2, 3, \ldots, p - 1\}$, there must exist some number a^{-1} such that $aa^{-1} \equiv 1 \pmod{p}$.

5 Theorems

5.1 Fermat's Little Theorem

In particular, because $\{a, 2a, 3a, \ldots, (p - 1)a\}$ is a permutation of $\{1, 2, 3, \ldots, p - 1\}$, the product of all the elements of the first set is the product of all the elements of the second set. Equating the two, we get

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p$$

Canceling $1 \cdot 2 \cdot 3 \cdots (p-1)$ from each side, recalling that this is a prime mod, we are left with

$$a^{p-1} \equiv 1 \pmod p$$

5.2 Wilson's Theorem

Consider $1 \cdot 2 \cdot 3 \cdots (p-1) = (p-1)! \pmod p$. By invertibility, we can pair together inverses and cancel them in pairs. This continues until we are left with the only two elements which are their own inverse: 1 and -1. As their product is -1, we have that

$$(p-1)! \equiv -1 \pmod p$$

6 Problems

1. (1 point) Find $3^{111890} \pmod{1009}$.
2. (1 points) Compute the remainder when 2009! is divided by 2011.
3. (2 point) Find the greatest common factor of $n! + 1$ and $(n+1)!$, in terms of n.
4. (2 points) Compute the remainder when 2008! is divided by 2011.
5. (2 points) Compute $9^{10^{11}} \pmod{101}$.
6. (2 points) Find the last "digit" of 13^{1024} in base 31.
7. (3 points) Find the last three digits of 7^{9999}.
8. (3 points) Determine all positive integers less than or equal to 100 such that $n^4 - n^2 + 57$ is divisible by 73.

7 More Problems

1. Let $p = 4k+1$ be a prime. Prove that $p | k^k - 1$.
2. Prove that there are infinitely many primes 1 mod 4.
3. Let ${}^k a = \underbrace{a^{a^{\cdots^{a}}}}_{k \text{ times}}$. Prove that the last n digits of ${}^k a$ will become constant for sufficiently large k. Find the exact integer k in terms of n after which the last n digits become constant.
4. Prove that there is a prime that is 1 mod n between 1 and n^n.