MSJ Math Club

Modular Arithmetic

4 February 2016

1 Introduction

Suppose we have three integers a, b, and n. We say that a is equivalent to b mod n if there exists an integer k such that $a - b = kn$. In other words, a and b give the same remainder when divided by n.

This statement is written more succinctly as:

$$a \equiv b \mod n$$

One can treat modular equivalence the same way one treats an equal sign in regular algebra for addition and multiplication.

$$a + c \equiv b + c \mod n$$
$$a \times c \equiv b \times c \mod n$$

For every number x such that $\gcd(x, n) = 1$, we can find a unique x^{-1} such that $xx^{-1} \equiv 1 \mod n$. Division is also possible in certain circumstances. If a is divisible by b and $\gcd(b, n) = 1$, then

$$\frac{a}{b} \equiv ab^{-1} \mod n$$

1.1 Totient theorem

Let $\phi(n)$ be the number of positive integers k less than n such that $\gcd(n, k) = 1$. This function is called the *totient* of n.

If $\gcd(a, n) = 1$, then we have that

$$a^{\phi(n)} \equiv 1 \mod n$$

2 Tips and Tricks

- Notice that $a^{\phi(n)-1}a \equiv 1 \mod n$. Look at the definition for the modular inverse.
- $\phi(n)$ is usually not the smallest exponent such that $a^{\phi(n)} \equiv 1$. But all numbers k for which $a^k \equiv 1$ are factors of $\phi(n)$ for obvious reasons.

3 Examples

1. Prove the totient theorem.
2. If a number x gives remainder 5 when divided by 12, what is its remainder when divided by 4? 3?
3. If $n \equiv 3 \mod 5$, $n \equiv 2 \mod 3$ and $n \equiv 54 \mod 7$, find n.
4. (classic) Evaluate $\underbrace{13^{13^{13^{\cdots}}}}_{2016} \mod 120$.

4 Practice Problems

1. Let n be a constant. Let $f(a)$ be the smallest k such that $a^k \equiv 1 \ (mod\ n)$. Show that $f(a)$ is always a factor of $\phi(n)$
2. (Classic) Let $\phi^0(n) = n$ and $\phi^k(n) = \phi(\phi^{k-1}(n))$. Find the smallest k such that $\phi^k(3^{1000}) = 1$
3. Find all primes p such that $p^2 + 2$ is also prime.
4. (Another overused SMT problem) Find the largest number k that divides $p^3 - 1$ for all $p > 5$.
5. (2011 AMC 10B) What is the hundreds digit of 2011^{2011}?
6. (1989 AIME) One of Euler's conjectures was disproved in the 1960s by three American mathematicians when they showed there was a positive integer such that $133^5 + 110^5 + 84^5 + 27^5 = n^5$. Find the value of n.
7. (2007 PuMAC) Find the last three digits of
$$2008^{2007^{\cdot^{\cdot^{\cdot^{2^1}}}}}.$$
.
8. (2007 HMMT) Find the number of 7-tuples $(n_1, \cdots, n_7)$ of integers such that
$$\sum_{i=1}^{7} n_i^6 = 96957.$$
9. (Balkan Mathematical Olympiad) Let n be a positive integer with $n \geq 3$. Show that $n^{n^{n^n}} - n^{n^n}$ is divisible by 1989.

5 Problem of the Week

Consider an arbitrary set of 2016 red points and 2016 blue points in which no three points are collinear. Is it possible to pair up the red points with the blue points by drawing line segments between them such that no two line segments intersect? Justify your claim.