MSJ Math Club

Number Theory 1: Modular Arithmetic and Totient

11 September 2014

1 Introduction

Definitions
We say that
$$a \equiv b \ (mod\ n)$$
if the remainder of a when divided by n is the same as the remainder of b when divided by n. This may be rewritten as
$$a = nk + b$$
where $k \in \mathbb{Z}$. As a result, we have that if $a \equiv b \ (mod\ n)$, then $aq \equiv bq \ (mod\ n)$ and $a + q \equiv b + q \ (mod\ n)$.
We wish to also define $(a, b) = gcd(a, b)$ and $[a, b] = lcm(a, b)$, which may be used in future handouts.

Lemma
If a and n are relatively prime, and $b \not\equiv c \ (mod\ n)$, then we have that $ab \not\equiv ac \ (mod\ n)$.

Proof
$(a, n) = 1$ and $(b, n) = 1$, so $(ab, n) = 1$ (since ab shares no prime factors with n).
Assume for sake of contradiction that $ab \equiv ac \ (mod\ n)$. Because $ab \equiv ac \ (mod\ n)$, $a(b - c) \equiv 0 \ (mod\ n)$, so $a(b - c)$ is divisible by n. Since $(a, n) = 1$, then $(b - c)$ must be divisible by n. That means that $b - c \equiv 0 \ (mod\ n)$, or equivalently, $b \equiv c \ (mod\ n)$.

Totient Theorem
If $\phi(n)$ is the number of positive integers q less than n such that $(q, n) = 1$, and if $(a, n) = 1$ then we have:
$$a^{\phi(n)} \equiv 1 \ (mod\ n)$$

Proof
Consider the set of numbers less than n that are relatively prime to n. Let us call them $q_1, q_2, \ldots, q_{\phi(n)}$. We see that for if $i \neq j$, then $aq_i \not\equiv aq_j \ (mod\ n)$, by the lemma. We also know that since $(a, n) = 1$ and $(q_i, n) = 1$, then $(aq_i, n) = 1$. Therefore, the set of all aq_i is the set of numbers relatively prime to n, since we have $\phi(n)$ different aq_i and $\phi(n)$ of numbers relatively prime to n. That means the set of all aq_i is also equivalent to the set of q_i. If we take the product of both sets, then we have:
$$q_1 q_2 \ldots q_{\phi(n)} \equiv aq_1 \ldots aq_{\phi(n)} \equiv x \ (mod\ n)$$
so
$$x \equiv xa^{\phi(n)} \ (mod\ n)$$
Since x is the product of a bunch of numbers relatively prime to n, x is relatively prime to n, and by the lemma:
$$a^{\phi(n)} \equiv 1 \ (mod\ n)$$

2 Tips and Tricks

- You should read the tips and tricks section on every handout.
- If you don't know what the Chinese Remainder Theorem is, you should look it up.
- Fermat's little theorem is a special case of the totient theorem. Set $n = p$ where p is a prime and you get Fermat's little theorem.
- If $n = p_1^{a_1} p_2^{a_2} \ldots$ then $\phi(n) = ((p_1 - 1)p_1^{a_1 - 1})((p_2 - 1)p_2^{a_2 - 1})((p_3 - 1)p_3^{a_3 - 1})((p_4 - 1)p_4^{a_4 - 1}) \ldots$
- For example we have $360 = 2^3 3^2 5$, so we have $\phi(360) = ((1)2^2)((2)3^1)((4)5^0) = 96$

3 Examples

1. Find $1^5 + 2^5 + 3^5 + 4^5 + 5^5 + ... + 10^5 \ (mod\ 11)$.
2. (classic) If $n \equiv 3 \ (mod\ 5)$, $n \equiv 2 \ (mod\ 3)$ and $n \equiv 54 \ (mod\ 7)$, find n
3. Evaluate the following: $5^{600} \ (mod\ 36)$, $70^{588} \ (mod\ 343)$, $6^{200} \ (mod\ 20)$.
4. (classic) Evaluate $\underbrace{7^{7^{7^{7^{\cdots}}}}}_{2014} \ (mod\ 120)$
5. Simplify $x^7 + 81x^6 + 62x^5 - 45x^4 + 33x^3 + 23x^2 + 41 \ (mod\ 5)$ into a polynomial (mod 5) of degree 4 and coefficients less that 5, given that $(x, 5) = 1$

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. Evaluate $45^{44^{43^{42^{\cdots}}}} \ (mod\ 1234)$
4. Find all primes p such that $p^2 + 2$ is also prime.
5. (Another overused SMT problem) Find the largest number k that divides $p^3 - 1$ for all $p > 5$.
6. (2011 AMC 10B) What is the hundreds digit of 2011^{2011}?
7. (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.
8. (2008 PuMAC) If $f(x) = x^{x^{x^x}}$, find the last two digits of $f(17) + f(18) + f(19) + f(20)$.
9. (2007 PuMAC) Find the last three digits of
$$2008^{2007^{\cdot^{\cdot^{\cdot^{2^1}}}}}.$$
.
10. (2007 HMMT) Find the number of 7-tuples $(n_1, \cdots, n_7)$ of integers such that
$$\sum_{i=1}^{7} n_i^6 = 96957.$$
11. (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.