EECS 70 Discrete Mathematics and Probability Theory
Fall 2014 Anant Sahai

Discussion 5W

1. Simplifying Some "Little" Exponents

For the following problems, you must both calculate the answers and show your work.

(a) What is $7^{3,000,000,000} \mod 41$?

(b) What is $2^{2014} \mod 11$?

(c) What is $2^{(5^{2014})} \mod 11$?

2. CRT Decomposition

In this problem we will find $3^{302} \mod 385$.

(a) Write 385 as a product of prime numbers in the form $385 = p_1 \times p_2 \times p_3$.

(b) Use Fermat's Little Theorem to find $3^{302} \mod p_1$, $3^{302} \mod p_2$, and $3^{302} \mod p_3$.

(c) Let $x = 3^{302}$. Use part (b) to express the problem as a system of congruences. Solve the system using the Chinese Remainder Theorem. What is $3^{302} \mod 385$?

3. Just a Little Proof

Suppose that p and q are distinct odd primes and a is an integer such that $\gcd(a, pq) = 1$. Prove that $a^{(p-1)(q-1)+1} \equiv a \pmod{pq}$.

4. Euler's Theorem

Euler's Theorem states that, if n and a are coprime,

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

where $\phi(n)$ (known as Euler's Totient Function) is the number of integers less than n which are coprime to n (including 1). Let's try to prove Euler's Theorem.

(a) Let the numbers less than n which are coprime to n be $m_1, m_2, \cdots, m_{\phi(n)}$. Prove that $am_i \equiv m_j \pmod{n}$. That is, when you multiply a number coprime to n and a, you get a number coprime to n.

(b) Prove that if $am_i \equiv am_j \pmod{n}$, then $m_i = m_j$. That is, if two of the numbers coprime to n multiply to the same number with a, then they must have been the same number originally.

(c) Using the two parts above, argue that $am_1, am_2, \cdots, am_{\phi(n)}$ is a permutation of $m_1, m_2, \cdots, m_{\phi(n)}$.

(d) Prove Euler's Theorem. (Hint: Try multiplying the sets.)