Concepts of Math: Recitation 26 (Irina's Lecture)

December 2, 2015

Fermat's Little Theorem

In class we discussed two versions of Fermat's Little Theorem. First version: if p is a prime and a is not a multiple of p, then $a^{p-1} \equiv 1 \pmod{p}$. Second version: if p is a prime and $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$.

1. We can use Fermat's Little Theorem to compute the remainder from the division of a large number involving powers by a prime number. What is the the remainder from dividing 11^{902} by 31?

$$11^{902} = 11^{30\cdot 30+2} = (11^{30})^{30} \cdot 11^2 \equiv 1^{30} \cdot 121 \equiv -3 \equiv 28 \pmod{31}.$$

   The remainder is 28.

2. What is the the remainder from dividing 15^{250} by 17?

3. The contrapositive of Fermat's Little Theorem: if a^p is not congruent to a modulo p, then p is not a prime. This can be used to prove that certain numbers p are not primes. Let's show that 341 is not prime. Note that $7^3 = 343 \equiv 2 \pmod{341}$ and $2^{10} = 1024 \equiv 1 \pmod{341}$.

$$7^{341} = 7^{3\cdot 113+2} \equiv 2^{113} 7^2 \equiv 2^{110} \cdot 2^3 \cdot 7^2 \equiv 8 \cdot 49 \equiv 392 \equiv 51 \pmod{341}.$$

   We conclude that 341 is not prime.

4. Fermat Little Theorem implies that if p is prime, then p divides $2^p - 2$. Fermat conjectured that the converse is also true, meaning that p divides $2^p - 2$ only if p is prime, but he was wrong. Euler provided the counterexample $p = 341$. We just showed that $p = 341$ is not prime. Use the fact that $341 = 11 \cdot 31$ to prove that $2^{341} - 2$ is divisible by 341.

Homework 9 Hint

Please give the following hint for Problem 9 in Homework 9. By contradiction, suppose that the number of prime numbers of form $6n + 5$, where $n \in \mathbb{N}$, is finite. Denote all such prime numbers by $p_1, p_2, \dots, p_k$. Note that $p_1 = 11$. Consider the number $N = 6p_1p_2 \dots p_k + 5$. If N is prime, we achieved contradiction. Suppose that N is not prime. Consider the prime factorization of N. Prove that at least one of the prime factors of N is congruent to $-1 \pmod 6$ and reach contradiction.

Subtle work with congruence relations

In class we proved the following lemma: if p is a prime number and $a^2 \equiv 1 \pmod p$, then $a \equiv 1 \pmod p$ of $a \equiv -1 \pmod p$.

1. Show that this statement is not true when p is not prime. For example $5^2 \equiv 1 \pmod{12}$. However neither $5 \equiv 1 \pmod{12}$ nor $5 \equiv -1 \pmod{12}$ is true.

2. If there is time left, answer homework questions.