Boston University MA341 Number Theory
Summer I 2009 Kalin Kostadinov

Lecture 5 (02 June 2009)

Fermat, Euler, and the Theorems of Number Theory

Theorem 1. *(Fermat's Little Theorem) Let p be a prime number and a an integer relatively prime with p. Then* $a^{p-1} \equiv 1 \pmod{p}$.

Proof. With the data in the theorem, consider the set of integers

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

We contend that the numbers in this set represent all possible non-zero remainders modulo p. To prove this, it is enough to show that no two numbers in the set have the same remainder modulo p, since obviously none of them is divisible by p and there are exactly $p-1$ nonzero remainders, namely $0, 1, \ldots, p-1$.
Suppose two numbers have the same remainder, say $ma \equiv na \pmod{p}$. Then $p|ma - na$, so $p|(m-n)a$, and since p is prime $p|a$ or $p|(m-n)$. Both of these are impossible, since we are given $\gcd(a, p) = 1$ and $0 < m - n < p$, thus our assumption lead to a contradiction and the claim is verified. Then

$$1 \cdot a \cdot 2 \cdot a \cdot 3 \cdot a \ldots (p-2) \cdot a \cdot (p-1) \cdot a \equiv 1 \cdot 2 \cdot 3 \ldots (p-2) \cdot (p-1) \pmod{p}$$

as both products have the same set of multipliers, but in possibly different order; after rearanging and canceling out $(p-2)!$ (which is certainly relatively prime with p) from both sides of the congruence, we get the statement of the theorem. □

For the next theorem, we introduce a notation: For a positive integer n, $\phi(n)$ will denote the number of integers in the interval $[1, n]$ that are relatively prime with n. For example $\phi(12) = 4$, since only $1, 5, 7, 11$ could be counted. For every prime p, $\phi(p) = p - 1$ and the next theorem is therefore a generalization of Fermat's theorem.

Theorem 2. *(Euler's ϕ-theorem) Let n be a positive integer and a an integer relatively prime with n. Then* $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. Not only the statement of theorem generalizes, but so does its proof. We leave the details as an exercise, only note that instead of all multiples of a, one should consider only the ones with a multiplier relatively prime with n. □

Both statements could be generalized further in the content of group theory. There meaning is that the *order* of an element in a finite group always is a divisor of the number of elements in the group.
There is third theorem, that has a somewhat similar content and proof to the above two, and we state it here.

Theorem 3. *(Wilson's theorem) Let n be an arbitrary positive integer. Then* $(n-1)! + 1 \equiv 0 \pmod{n}$ *if and only if n is prime.*