

Math 104A, Number Theory, Fall 2002.
Summary of Lecture 17.

Several students in the class contributed to the content of this lecture!

Last time we proved:

Theorem 4.1.1. (The little Fermat theorem.) Let p be a prime. Then $a^p \equiv 1 \pmod{p}$ for all integers a . In particular if $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

This time we ask what happens if p is replaced by a number which is not prime.

Example. Modulo 9,

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 7, \quad 2^5 \equiv 5, \quad 2^6 \equiv 1, \\ 2^7 \equiv 2, \quad 2^8 \equiv 4.$$

We see that $2^8 \not\equiv 1 \pmod{9}$ while $2^6 \equiv 1 \pmod{9}$.

Definition 4.2.1 For $m \geq 2$, $\phi(m)$ is the number of numbers between 0 and m which are relatively prime to m . This is the same as the number of invertible elements in a complete residue system modulo m . ϕ is called *Euler's Totient function*.

Theorem 4.3.1. (Euler's Theorem.) If $(a, m) = 1$ then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Note: since $\phi(9) = 6$, we get $2^6 \equiv 1 \pmod{9}$.

Proof of Theorem 4.3.2. Let $b_1, b_2, \dots, b_{\phi(m)}$ be the numbers between 0 and m which are relatively prime to m , that is invertible modulo m . Suppose $(a, m) = 1$, and let r_j be the remainder when ab_j is divided by m . We claim that the list of numbers $r_1, r_2, \dots, r_{\phi(m)}$ is just the list $b_1, b_2, \dots, b_{\phi(m)}$ possibly written in a different order. To see this, one can either use modulo arithmetic or not. Without using modulo arithmetic, note that each of the r_j s is one of the b_k s because since $(b_j, m) = 1$ and $(a, m) = 1$, $(ab_j, m) = 1$, but $ab_j = mq + r_j$ so $(r_j, m) = 1$. Since r_j is between 0 and m it equals one of the b_k s. Furthermore, the r_j s are all different from each other, for if $r_j = r_k$ then $m \mid (ab_j - ab_k) = a(b_j - b_k)$. But since $(a, m) = 1$, $m \mid (b_j - b_k)$, but b_j and b_k are both strictly between 0 and m , so $|b_j - b_k| < m$ and hence m can only divide this difference if $b_j = b_k$. Since there are the same number of r_j s as b_j s, the r_j s are just a re-ordering of the b_j s. The proof using modulo arithmetic is given in the book.

Remark. We saw in the proof of Euler's Theorem that if $b_1, \dots, b_{\phi(m)}$ is a list of invertible elements in a complete residue system modulo m , then so is $ab_1, \dots, ab_{\phi(m)}$. The question arose in the lecture whether $a, a^2, \dots, a^{\phi(m)}$ also gives all the invertible elements modulo m . We see that this does happen for $a = 2$ modulo 9. However, modulo 9 we have

$$4^1 \equiv 4, \quad 4^2 \equiv 7, \quad 4^3 \equiv 1.$$

We only get half of the elements in the complete residue system.

We note that $\phi(p) = p - 1$ and $\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$.

Proposition. If m and n are relatively prime then $\phi(mn) = \phi(m)\phi(n)$. Hence if $m = p_1^{a_1} \cdots p_k^{a_k}$ with p_1, \dots, p_k distinct primes, then $\phi(m) = \phi(p_1^{a_1}) \cdots \phi(p_k^{a_k}) = m(1 - 1/p_1) \cdots (1 - 1/p_k)$.