

**Math 104A, Number Theory, Fall 2002.**  
**Summary of Lecture 19.**

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

Last time we proved:

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

**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  $\phi(m) = \phi(p_1^{a_1}) \cdots \phi(p_k^{a_k}) = m(1 - 1/p_1) \cdots (1 - 1/p_k)$ .

*Proof of the Proposition.* Define  $J_m$  to be the set of elements  $\{0, 1, 2, \dots, m - 1\}$ . Define  $I_m$  to be the subset of  $J_m$  containing those elements  $x$  such that  $(m, x) = 1$ . If  $(m, n) = 1$ , define

$$F : J_{mn} \rightarrow J_m \times J_n$$

by

$$F(x) = (x \pmod{m}, x \pmod{n}),$$

where  $x \pmod{m}$  and  $x \pmod{n}$  are written in the standard residue system. (Note that  $x \pmod{m}$  is just the remainder when  $x$  is divided by  $m$ .) We claim that  $F$  has an inverse. Indeed, by the Chinese Remainder Theorem for every values of  $x$  and  $y$  we can find  $x$  satisfying

$$\begin{cases} x = y \pmod{m} \\ x = z \pmod{n} \end{cases}$$

and  $x$  is unique modulo  $mn$ . By expressing  $x$  in the standard residue system modulo  $mn$ , this means if we are given  $(y, z) \in J_m \times J_n$  then there exists  $x$  which is mapped by  $F$  to  $(y, z)$ . Moreover, by the uniqueness in the Chinese remainder theorem this is unique. Because it has an inverse, the map  $F$  sets up a bijection between  $J_{mn}$  and  $J_m \times J_n$ . We will now show that under this bijection  $I_{mn}$  is mapped onto  $I_m \times I_n$  and so the number of elements in these sets is the same, that is  $\phi(mn) = \phi(m) \cdot \phi(n)$ . To see this, we must first show that  $F$  maps  $I_{mn}$  to  $I_m \times I_n$ . Suppose  $(x, mn) = 1$  and  $F(x) = (y, z)$ . Then  $(x, m) = 1$  and so since  $x \equiv y \pmod{m}$  we have  $(y, m) = 1$ . Similarly  $(y, n) = 1$ . This shows  $F(I_{mn}) \subset I_m \times I_n$ . Conversely we will show that  $F^{-1}(I_m \times I_n) \subset I_{mn}$ . Indeed, suppose that  $F(x) = (y, z)$ ,  $(y, m) = 1$  and  $(z, n) = 1$ . Then since  $x \equiv y \pmod{m}$  we have  $(x, m) = 1$  and since  $x \equiv z \pmod{n}$  we have  $(x, n) = 1$ . This shows that  $F^{-1}(I_m \times I_n) \subset I_{mn}$ . Putting this together, we see that  $F(I_{mn}) = I_m \times I_n$ .

**Note:** In many cases Euler's theorem can be improved. For example, if  $m = 100$  we have  $100 = 4 \cdot 25$  and so  $\phi(100) = \phi(4) \cdot \phi(25) = 2 \cdot 20 = 40$ . However, if  $(a, 100) = 1$ , then  $(a, 4) = 1$  and  $(a, 25) = 1$  so

$$\begin{aligned} a^2 &\equiv 1 \pmod{4} && \Rightarrow && a^{20} &\equiv 1 \pmod{4}. \\ a^{20} &\equiv 1 \pmod{25} \end{aligned}$$

Hence  $a^{20} \equiv 1 \pmod{100}$ .

In practice when using large numbers and a computer, we use the method of squaring to compute powers modulo  $m$ . Euler's Theorem is used to compute roots modulo  $m$ .

**Efficient method to compute  $a^k \pmod{m}$  using a computer:** In fact if you have a computer, using Euler's theorem is not necessarily the most efficient way to compute  $a^k \pmod{m}$  if  $m$  is large because you first have to factorize  $m$ . A method which does not require you to factorize  $m$  is the method of successive squaring. Step 1: Compute the binary expansion of  $m$ , that is write  $m = 2^{m_r} + 2^{m_{r-1}} + \dots + 2^{m_1}$  where  $m_1 < m_2 < \dots < m_r$ .

Step 2: Use successive squaring to compute  $a^2 \pmod{m}$ ,  $a^{2^2} \pmod{m}$ ,  $a^{2^3} \pmod{m}$ , up to  $a^{2^{m_r}}$ .

**Example:**  $3^{52} \pmod{53}$ :

$$52 = 32 + 20 = 32 + 16 + 4.$$

Now modulo 53,

$$3^1 = 3$$

$$3^2 = 9$$

$$3^4 = 81 \equiv 28$$

$$3^8 \equiv 28^2 = 784 \equiv 42$$

$$3^{16} \equiv 42^2 = 1764 \equiv 15$$

$$3^{32} \equiv 15^2 = 225 \equiv 13$$

$$3^{52} \equiv 3^{32} \cdot 3^{16} \cdot 3^4 \equiv 13 \cdot 15 \cdot 28 \equiv 195 \cdot 28 \equiv 36 \cdot 28 = 1008 \equiv 1.$$