

NOTES FOR MATH 310  
LECTURE 6

VIVEK DHAND

1. THE EULER  $\phi$  FUNCTION

A natural question to ask at this point is: how many elements of  $\mathbb{Z}_n$  have multiplicative inverses? By a theorem proved in class, this is the same as asking how many integers  $1 \leq a \leq n - 1$  have  $(a, n) = 1$ .

Let  $\phi(n)$  denote the number integers  $a$  such that  $1 \leq a \leq n - 1$  and  $(a, n) = 1$ . For example, we have shown that:

$$\phi(p) = p - 1$$

if  $p$  is prime.

**Proposition.**  $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$ .

*Proof.* Note that  $(a, p^k) = p^r$  for some  $0 \leq r \leq k$ . Therefore  $(a, p^k) = 1$  if and only if  $r = 0$ , which means that  $p \nmid a$ . So we need the number of  $1 \leq a \leq p^k$  with  $p \nmid a$ . This is the same as the number of multiples of  $p$  that are between 1 and  $p^k$ . If we arrange these  $p^k$  integers into  $p$  columns, we see that all the multiples of  $p$  lie in the same column, so there are  $p^{k-1}$  of them. Therefore, there are

$$p^k - p^{k-1}$$

integers  $1 \leq a \leq p^k$  such that  $p \nmid a$ . □

**Lemma.** Let  $a, m, n \in \mathbb{Z}$ .  $(a, mn) = 1$  if and only if  $(a, m) = 1$  and  $(a, n) = 1$ .

*Proof.* If

$$mnu + av = 1$$

then

$$m(nu) + av = 1$$

$$n(mu) + av = 1$$

If

$$ms + at = 1, \quad nu + av = 1$$

then

$$1 = ms(nu + av) + at = mn(su) + a(msv + t)$$

□

**Theorem.** If  $(m, n) = 1$ , then  $\phi(mn) = \phi(m)\phi(n)$ .

*Proof.* We know  $mu + nv = 1$  for some  $u, v \in \mathbb{Z}$ . By the Chinese remainder theorem, there is a unique  $t \in \mathbb{Z}_{mn}$  such that

$$t \equiv a \pmod{m}$$

$$t \equiv b \pmod{n}$$

We claim that  $(t, mn) = 1$  if and only if  $(a, m) = 1$  and  $(b, n) = 1$ . Note that, since  $t \equiv a \pmod{m}$ , we have  $(t, m) = (a, m)$ , and since  $t \equiv b \pmod{n}$ , we have  $(t, n) = (b, n)$ .

Suppose that  $(a, m) = 1$  and  $(b, n) = 1$ . Then  $(t, m) = 1$  and  $(t, n) = 1$ , and by the previous proposition,  $(t, mn) = 1$ .

Suppose that  $(t, mn) = 1$ . Then  $(t, m) = (t, n) = 1$ , so  $(a, m) = 1$  and  $(b, n) = 1$ .

Now  $\phi(mn)$  counts how many  $t \in \mathbb{Z}_{mn}$  have  $(t, mn) = 1$ . This is the same as counting those  $a \in \mathbb{Z}_m$  such that  $(a, m) = 1$  (which is  $\phi(m)$ ) and for each such  $a$ , those  $b \in \mathbb{Z}_n$  such that  $(b, n) = 1$  (which is  $\phi(n)$ ). In other words, we are counting  $\phi(n)$  elements for each one of the  $\phi(m)$  elements, for a total of  $\phi(m)\phi(n)$  elements.

□

We can now derive a formula for the function  $\phi$ :

**Theorem.** Let  $n > 1$  be an integer and let  $n = p_1^{a_1} \dots p_k^{a_k}$  be its prime factorization. Then:

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

*Proof.* Note that  $(p^a, q^b) = 1$  for any two distinct primes  $p$  and  $q$ . Therefore,

$$\begin{aligned} \phi(p_1^{a_1} \dots p_k^{a_k}) &= \phi(p_1^{a_1}) \dots \phi(p_k^{a_k}) \\ &= p_1^{a_1-1}(p_1 - 1) \dots (p_k^{a_k-1})(p_k - 1) \\ &= p_1^{a_1} \dots p_k^{a_k} \frac{(p_1 - 1) \dots (p_k - 1)}{p_1 \dots p_k} \\ &= n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right) \end{aligned}$$

□

**Example.**  $\phi(120) = \phi(8)\phi(3)\phi(5) = 4 \cdot 2 \cdot 4 = 32$ .

**Example.**  $\phi(2^n) = 2^{n-1}(2 - 1) = 2^{n-1}$ .

## 2. EULER'S THEOREM

**Theorem.** Let  $n > 1$  be an integer and suppose  $(a, n) = 1$ . Then

$$a^{\phi(n)} = 1 \text{ in } \mathbb{Z}_n$$

*Proof.* Let  $\phi(n) = k$  and list all the elements of  $\mathbb{Z}_n$  that have multiplicative inverses:

$$A = \{b_1, \dots, b_k\}$$

Now multiply all the elements by  $a$ :

$$B = \{ab_1, \dots, ab_k\}$$

Since  $(a, n) = 1$  and  $(b_i, n) = 1$ , we conclude that  $(ab_i, n) = 1$  for all  $1 \leq i \leq k$ . Therefore,  $B$  is a subset of  $A$ . If  $ab_i = ab_j$ , then

$$a(b_i - b_j) = 0$$

so  $b_i - b_j = 0$  and  $b_i = b_j$ . This shows that  $B$  has  $k$  elements, so  $A = B$ .

Let  $m = b_1 \dots b_k$ . Similarly, the product of all the elements of  $B$  is:

$$(ab_1) \dots (ab_k) = a^{\phi(n)} b_1 \dots b_k = a^{\phi(n)} m$$

Therefore,

$$a^{\phi(n)} m = m$$

in  $\mathbb{Z}_n$ . Since  $(m, n) = 1$ , we can divide by it:

$$a^{\phi(n)} = 1$$

in  $\mathbb{Z}_n$ .

□

**Example.** Find  $4^{12003} \pmod{9999}$

First find the prime factorization of 9999:

$$9999 = 9 \cdot 11 \cdot 101$$

Now calculate  $\phi(9999)$ :

$$\phi(9999) = \phi(9)\phi(11)\phi(101) = 6 \cdot 10 \cdot 100 = 6000$$

Note that  $(4, 9999) = 1$  because  $(4, 9) = (4, 11) = (4, 101) = 1$ . Therefore, in  $\mathbb{Z}_{9999}$ :

$$4^{6000} = 1$$

Squaring both sides, we see that

$$4^{12000} = 1$$

Therefore

$$4^{12003} = 4^{12000} 4^3 = 4^3 = 64$$

in  $\mathbb{Z}_{9999}$ .