

## EULER'S PHI AND EULER'S THEOREM

MATH 372. FALL 2005. INSTRUCTOR: PROFESSOR AITKEN

The goal of this handout is to discuss Euler's phi function culminating in a proof of Euler's theorem. As a corollary we have Fermat's Little Theorem. (There were two other proofs of Fermat's Little Theorem given in class. But the proof here is the only one you need to know for the test.)

### 1. EULER'S PHI FUNCTION AND UNITS

**Definition 1.** Let  $n > 1$  be an integer. Then  $\phi(n)$  is defined to be the number of positive integers less than or equal to  $n$  that are relatively prime to  $n$ . The function  $n \mapsto \phi(n)$  is called *Euler's phi function* or the *totient function*.

*Example 1.* The integers less than or equal to 12 that are relatively prime to 12 are 1, 5, 7, 11. Thus  $\phi(12) = 4$ .

In earlier notes we proved the following:

**Theorem 1.** Let  $m$  be a positive integer and let  $a \in \mathbb{Z}$ . Then  $\bar{a} \in \mathbb{Z}_m$  is a unit if and only if  $(a, m) = 1$ .

**Corollary 1.** Let  $m > 1$  be an integer. The number of units in  $U_m$  is equal to  $\phi(m)$ .

**Proposition 1.** Suppose that  $m$  and  $n$  are positive integers such that  $(m, n) = 1$ . Let  $a \in \mathbb{Z}$ . Then  $[a]_{mn}$  is a unit if and only if both  $[a]_m$  and  $[a]_n$  are units.

*Proof.* First suppose that  $[a]_{mn}$  is a unit. Then  $(a, mn) = 1$ . Claim:  $(a, m) = 1$ . To see this, observe that any common divisor of  $a$  and  $m$  is a common divisor of  $a$  and  $mn$ , and the largest such divisor is 1. Likewise  $(a, n) = 1$ . Thus  $[a]_n$  and  $[a]_m$  are both units.

Suppose that  $[a]_n$  and  $[a]_m$  are both units. Thus  $(a, m) = 1$  and  $(a, n) = 1$ . In an effort to get a contradiction, suppose  $(a, mn) = d > 1$ . Let  $p$  divide  $d$ . So  $p$  divides  $a$  and  $mn$ . Since  $p \mid mn$  then  $p \mid m$  or  $p \mid n$ . In the first case,  $p$  is a common divisor of  $a$  and  $m$  contradicting the assumption that  $(a, m) = 1$ . In the second case,  $p$  is a common divisor of  $a$  and  $n$  contradicting the assumption that  $(a, n) = 1$ . In either case we get a contradiction. So  $(a, mn) = 1$ . Thus  $[a]_{mn}$  is a unit.  $\square$

### 2. UNITS AND THE CHINESE REMAINDER THEOREM

Recall the following form of the Chinese Remainder Theorem:

**Theorem 2** (Chinese Remainder Theorem). Let  $m$  and  $n$  be relatively prime positive integers. Then the rule  $[a]_{mn} \mapsto ([a]_m, [a]_n)$  defines a bijection (a one-to-one and onto function)  $\mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ .

The following shows what happens to units under this map.

---

*Date:* Fall 2005. Version of November 4, 2005.

**Theorem 3.** *Let  $m$  and  $n$  be relatively prime positive integers. When we restrict the function  $[a]_{mn} \mapsto ([a]_m, [a]_n)$  to units in  $U_{mn}$ , we get a bijection  $U_{mn} \rightarrow U_m \times U_n$ . Thus the sets  $U_{mn}$  and  $U_m \times U_n$  have the same number of elements.*

*Remark.* For those of you with a background in abstract algebra:  $U_{mn} \rightarrow U_m \times U_n$  is an isomorphism between groups.

*Proof.* Suppose that  $[a]_{mn}$  is a unit. So by Proposition 1 both  $[a]_m$  and  $[a]_n$  are units. Thus  $[a]_{mn} \mapsto ([a]_m, [a]_n)$  defines a function  $U_{mn} \rightarrow U_m \times U_n$ .

This function is injective (one-to-one) on the domain  $U_{mn}$  since it is injective on the larger domain  $\mathbb{Z}_{mn}$ .

To show surjectivity (onto) let  $([b]_m, [c]_n)$  be an arbitrary element of  $U_m \times U_n$ . Since the rule  $[a]_{mn} \mapsto ([a]_m, [a]_n)$  considered as a function  $\mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$  is surjective, there is an  $a \in \mathbb{Z}$  so that  $[a]_{mn} \mapsto ([b]_m, [c]_n)$ . By the way the function is defined,  $[a]_m = [b]_m$  and  $[a]_n = [c]_n$ . Thus  $[a]_m$  and  $[a]_n$  are units. By Proposition 1,  $[a]_{nm}$  must also be a unit. So we have found an element of  $U_{mn}$  mapping to the arbitrary  $([b]_m, [c]_n)$ . Thus the function is surjective (onto).  $\square$

**Corollary 2** (Multiplicative Law). *If  $m$  and  $n$  are relatively prime integers greater than one, then  $\phi(mn) = \phi(m)\phi(n)$ .*

*Proof.* There are  $\phi(mn)$  elements of  $U_{mn}$ . The number of ordered pairs in  $U_m \times U_n$  is  $\phi(m)\phi(n)$ . Since there is a bijection from  $U_{mn}$  to  $U_m \times U_n$ , the sets have the same number of elements.  $\square$

### 3. USEFUL FACTS

Let  $p$  be a prime. It is easy to see that  $\phi(p) = p - 1$  since every positive integer less than  $p$  is relatively prime to  $p$ . This generalizes from  $p^1$  to  $p^k$  as follows.

**Proposition 2.** *Let  $k$  be a positive integer. If  $p$  is a prime, then  $\phi(p^k) = p^k - p^{k-1}$ .*

*Proof.* Clearly  $(a, p^k) > 1$  if and only if  $a$  is a multiple of  $p$  since all common divisors of  $a$  and  $p^k$  must be powers of  $p$ . The multiples of  $p$  less than or equal to  $p^k$  are  $p, 2p, 3p, \dots, p^{k-1}p$ . Observe that there are  $p^{k-1}$  such multiples. If we remove them from  $1, 2, 3, \dots, p^k$ , we are left with  $p^k - p^{k-1}$  integers.  $\square$

With a simple induction argument, one can generalize Corollary 2.

**Proposition 3.** *If  $m_1, \dots, m_r$  are pairwise relatively prime integers greater than one, then*

$$\phi(m_1 \cdots m_r) = \phi(m_1) \cdots \phi(m_r).$$

*Remark.* Once we have a prime power factorization of  $m$ , we can use the preceding two propositions to compute  $m$  as follows:

**Proposition 4.** *If  $m > 1$  is an integer, and  $m = p_1^{e_1} \cdots p_r^{e_r}$  where each  $p_i$  is a prime and each  $e_i$  is positive, then*

$$\phi(m) = \phi(p_1^{e_1}) \cdots \phi(p_r^{e_r}) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_r^{e_r} - p_r^{e_r-1})$$

*Example 2.* Since  $150 = 2^1 \cdot 3^1 \cdot 5^2$ , we have  $\phi(150) = (2 - 1)(3 - 1)(25 - 5) = 40$ . So  $U_{150}$  is a group with 40 elements.

#### 4. EULER'S THEOREM

**Lemma 1.** *Let  $m > 1$  be an integer and let  $\overline{a_1}, \dots, \overline{a_{\phi(m)}}$  be the (distinct) elements of  $U_m$ . If  $\overline{a} \in U_m$  then the terms of the list  $\overline{a}\overline{a_1}, \dots, \overline{a}\overline{a_{\phi(m)}}$  are distinct, and every element of  $U_m$  is on the list.*

*Proof.* Suppose the elements are not distinct:  $\overline{a}\overline{a_i} = \overline{a}\overline{a_j}$  with  $i \neq j$ . Multiply both sides by the inverse of  $\overline{a}$  (which exists since  $\overline{a}$  is a unit). So  $\overline{a_i} = \overline{a_j}$ , a contradiction. So the elements are distinct.

Let  $\overline{b} \in U_m$  be given. Then  $\overline{a}^{-1}\overline{b}$  is in  $U_m$  by closure, so is equal to  $\overline{a_i}$  for some choice of  $i$ . Observe that  $\overline{a}\overline{a_i} = \overline{a}\overline{a}^{-1}\overline{b} = \overline{b}$ . So  $\overline{b}$  is the  $i$ th term on the list.  $\square$

**Theorem 4** (Euler's Theorem). *Let  $m > 1$  be an integer. If  $\overline{a} \in U_m$  then  $\overline{a}^{\phi(m)} = \overline{1}$ . In other words, if  $a$  is an integer relatively prime to  $m$  then*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

*Proof.* Let  $U_m = \{\overline{a_1}, \dots, \overline{a_{\phi(m)}}\}$ . By the previous lemma

$$\overline{a_1} \cdots \overline{a_{\phi(m)}} = (\overline{a}\overline{a_1}) \cdots (\overline{a}\overline{a_{\phi(m)}}) = \overline{a}^{\phi(m)} \cdot \overline{a_1} \cdots \overline{a_{\phi(m)}}.$$

(The first equality is true since the second product has the same terms as the first, but usually in a different order). Let  $\overline{A} = \overline{a_1} \cdots \overline{a_{\phi(m)}}$ . Observe that  $\overline{A}$  is a unit by closure. The above equality can be written as

$$\overline{A} = \overline{a}^{\phi(m)}\overline{A}.$$

Now multiply both sides by the inverse of  $\overline{A}$ .  $\square$

Fermat's Little Theorem is just a special case of Euler's Theorem. (Of course, the *original* proof of Fermat's Little Theorem was earlier: Fermat lived before Euler did).

**Corollary 3** (Fermat's Little Theorem). *Let  $p$  be a prime. If  $\overline{a} \in U_p$ , then  $\overline{a}^{p-1} = \overline{1}$ . In other words, if  $a$  is an integer not divisible by  $p$  then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

*Proof.* Recall that  $\phi(p) = p - 1$ . Also,  $(a, p) = 1$  if and only if  $p \nmid a$ .  $\square$

**Theorem 5** (Fermat's Little Theorem part 2). *Let  $p$  be a prime. If  $a \in \mathbb{Z}$  then*

$$a^p \equiv a \pmod{p}.$$

*Proof.* If  $a$  is not divisible by  $p$ , multiply both sides of the congruence of the above congruence by  $a$ .

If  $a$  is divisible by  $p$  then both sides are congruent to 0, so they are congruent to each other.  $\square$

#### 5. WILSON'S THEOREM

**Lemma 2.** *Let  $p > 2$  be a prime and let  $\overline{a} \in U_p$ . Then  $\overline{a} = \overline{a}^{-1}$  if and only if  $\overline{a}$  is  $\overline{1}$  or  $\overline{-1}$ .*

*Proof.* One direction is obvious. For the other, suppose that  $\overline{a} = \overline{a}^{-1}$ . Multiplying both sides by  $\overline{a}$  gives  $\overline{a}^2 = \overline{1}$ . In other words,  $a^2 \equiv 1 \pmod{p}$ . This implies that  $p \mid a^2 - 1 = (a+1)(a-1)$ . Since  $p$  is a prime, this implies that  $p \mid (a+1)$  or  $p \mid (a-1)$ . In the first case,  $a \equiv -1 \pmod{p}$ . In the second case  $a \equiv 1 \pmod{p}$ . So  $\overline{a}$  is either  $\overline{-1}$  or  $\overline{1}$ .  $\square$

**Theorem 6** (Wilson's Theorem). *Let  $p$  be a prime. Then  $(p - 1)! \equiv -1 \pmod{p}$ .*

*Proof.* If  $p = 2$  then it is obvious. So assume  $p > 2$ . If we multiply every element of  $U_p$  together we get

$$\overline{1} \cdot \overline{2} \cdots \overline{p-1} = \overline{1 \cdot 2 \cdots (p-1)} = \overline{(p-1)!}.$$

Now reorder the elements of  $U_p$  as  $\overline{a_1}, \overline{a_2}, \dots, \overline{a_{p-1}}$  so that  $\overline{a_1} = \overline{1}$ , so that  $\overline{a_2} = \overline{-1}$  and, for  $i > 1$ , so that  $\overline{a_{2i-1}}$  and  $\overline{a_{2i}}$  are inverses to each other. We can do this by the previous lemma: an element and its inverse pair up to give two distinct elements except for  $\overline{1}$  and  $\overline{-1}$ . If we multiply every element of  $U_p$  together we get

$$\overline{a_1} \cdot \overline{a_2} \cdots \overline{a_{p-1}} = \overline{1} \cdot \overline{-1} \cdot (\overline{a_3} \cdot \overline{a_4}) \cdots (\overline{a_{p-2}} \cdot \overline{a_{p-1}}) = \overline{-1}$$

since the elements in parentheses give a product of  $\overline{1}$ .

Putting the two calculations together gives  $\overline{(p-1)!} = \overline{-1}$ . So  $(p-1)! \equiv -1 \pmod{p}$ .  $\square$

*Example 3.* Consider  $6!$  modulo  $7$ :

$$6! \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 1 \cdot 6 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \equiv 1 \cdot -1 \cdot (1) \cdot (1) \equiv -1 \pmod{7}.$$

From a direct calculation  $6! + 1 = 721 = 7(103)$ , so  $6! \equiv -1 \pmod{7}$ .

DR. WAYNE AITKEN, CAL. STATE, SAN MARCOS, CA 92096, USA  
*E-mail address:* `waitken@csusm.edu`