

# CS 135

## Fermat's Little Theorem

Professor Bloom

March 18, 2009

### 1 Euler's Theorem

**Recall** that if  $a \in \mathbb{Z}_n^*$ , then there is some  $b \in \mathbb{Z}_n^*$  such that  $ab = 1$ , where multiplication is mod  $n$ .

**Proposition 1.1** *If  $a \in \mathbb{Z}_n^*$ , the function  $m_a : \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^*$  which maps  $x$  to  $(ax) \bmod n$  is injective (and hence bijective).*

*Proof.* Suppose that

$$ax \equiv ay \pmod{n}.$$

We show  $x = y$ . Multiply (mod  $n$ ) both sides by the multiplicative inverse  $b$  of  $a$ :

$$\begin{aligned}x &= 1 \cdot x \\ &= bax \\ &= bay \\ &= 1 \cdot y = y.\end{aligned}$$

**Theorem 1.2 (Euler's theorem)** *If  $a \in \mathbb{Z}_n^*$ , then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

*Proof.* By Proposition 1.1, the set  $\mathbb{Z}_n^*$  is the same as the set  $\{a \cdot x : x \in \mathbb{Z}_n^*\}$ . Thus the product (mod  $n$ ) of all elements in each set is the same. The product of all elements in  $\mathbb{Z}_n^*$  is

$$\prod \mathbb{Z}_n^*.$$

The product (mod  $n$ ) of all elements in the second can be written

$$a^{\varphi(n)} \cdot \prod \mathbb{Z}_n^*.$$

Thus,

$$\prod \mathbb{Z}_n^* = a^{\varphi(n)} \prod \mathbb{Z}_n^*.$$

By multiplying both sides by the multiplicative inverse of  $\prod \mathbb{Z}_n^*$ , we obtain the desired result:

$$a^{\varphi(n)} \equiv 1, \pmod{n}$$

where all products are mod  $n$ .

**Corollary 1.3 (Fermat's little theorem)** *If  $p$  is a prime and  $a \not\equiv 0 \pmod{p}$ , then*

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

*Proof.* When  $p$  is a prime,  $\varphi(p) = p - 1$ , so that this result follows from Euler's theorem.

**Proposition 1.4** *If  $p$  is a prime, then there are only two values of  $x \in \mathbb{Z}_p^*$  such that*

$$x^2 \equiv 1 \pmod{p}$$

*Proof.* Clearly, if  $x = 1$  or  $x = -1$ , then  $x^2 = 1$ . Now suppose that (mod  $p$ ),

$$x^2 = y^2.$$

Then, mod  $p$ ,

$$\begin{aligned} x^2 - y^2 &= (x + y)(x - y) \\ &= 0. \end{aligned}$$

Thus, either  $p \mid (x + y)$  or  $p \mid (x - y)$ , showing  $y = x$  or  $y = -x$ . When  $x = 1$ , we get the desired result.

**Theorem 1.5 (Wilson's theorem)** *If  $p$  is a prime,*

$$(p - 1)! \equiv -1 \pmod{p}$$

Note that  $(p - 1)!$  is the product of all elements in  $\mathbb{Z}_p^*$ . By Proposition 1.4, only 1 and  $-1 = p - 1$  have the property that their square is 1. For  $1 < x < p$ , there is  $y \neq x$  with  $xy = 1 \pmod{p}$ , since  $x$  has some multiplicative inverse, and it

can't be  $x$  itself, unless  $x = 1$  or  $x = p - 1$ . Thus, the product of all numbers in the range  $2 \leq x < p - 1$  is 1, since the product can be grouped into pairs  $x, x^{-1}$ . When  $p - 1$  is included, we get Wilson's theorem.

Is it the case that if  $a \perp n$  and  $a^{n-1} \cong 1 \pmod{n}$ , then  $n$  is prime? No. For example, if  $n = 351 = 3^3 \cdot 13$  and  $a = 298$ , then  $a^{350} \equiv 1 \pmod{351}$ .

**Definition 1.6** A *Carmichael number* is an integer  $n$  which is NOT prime but has the property that for all  $1 \leq a < n$  and  $a \perp n$ ,  $a^{n-1} \equiv 1 \pmod{n}$ .

## 2 Exercises

1. Read Rosen, Chap 3.7.
2. Write a Scheme program to find the smallest Carmichael number.
3. Find all Carmichael numbers  $< 5000$ .
4. Show that if  $n$  is not prime, then it is FALSE that

$$(n - 1)! \equiv -1 \pmod{n}$$

5. Conclude that Wilson's theorem gives a necessary and sufficient condition that a number is prime.
6. Use Scheme to find nonprimes as follows. Choose a random integer  $n > 10000$  (in Scheme, `(random 10000)`). Choose a random  $0 < a < n$  (in Scheme, `(random n)`). Compute  $a^{n-1} \bmod n$ . (use smart exponentiation mod  $n$ .) If the result is not 1,  $n$  is not prime. When you find such  $a, n$ , now see how many such  $a < n$  could have been counter examples. It is at least  $n/2$ .
7. Do problems 18, 19, page 245 in Rosen.
8. Use Fermat's little theorem to show  $2^{340} \equiv 1 \pmod{11}$ .
9. Find out something about Carmichael.
10. Find out something about Euler.
11. Find out something about Fermat.
12. Find out something about Wilson.
13. If you write a 2-3 page bio of any of the above people (and do a good job), you get 25 points on the next quiz.