## FERMAT'S LITTLE THEOREM AND EULER'S GENERALIZATION

LECTURE NOTES: MATH 422, CSUSM, SPRING 2009. PROF. WAYNE AITKEN

In this lecture, we cover Fermat Little Theorem, Euler's generalization of this theorem, and end with Wilson's theorem. Fermat's Little Theorem, and Euler's theorem are two of the most important theorems of modern number theory. Since it is so fundamental, we take the time to give two proofs of Fermat's theorem: (i) the induction based proof, and (ii) the permutation based proof. The second of these generalizes to give a proof of Euler's theorem. There is a third proof using group theory, but we focus on the two more elementary proofs.

# 1. Fermat's Little Theorem

One form of Fermat's Little Theorem states that if p is a prime and if a is an integer then

$$p \mid a^p - a.$$

For example 3 divides  $2^3 - 2 = 6$  and  $3^3 - 3 = 24$  and  $4^3 - 4 = 60$  and  $5^3 - 5 = 120$ . Similarly, 5 divides  $2^5 - 2 = 30$  and  $3^5 - 3 = 240$  et cetera.

Obviously  $a^p - a$  factors as  $a(a^{p-1} - 1)$ . So if  $p \nmid a$  then we have

$$p \mid a^{p-1} - 1$$

This gives another common form of Fermat's Little Theorem. For example, 3 divides  $5^2 - 1 = 24$  and  $4^2 - 1 = 15$  and  $2^2 - 1 = 3$ . Also, 5 divides  $2^4 - 1 = 15$  and  $3^4 - 1 = 80$  and  $4^4 - 1 = 255$ , and 7 divides  $2^6 - 1 = 63$  et cetera.

After Gauss introduced congruences, the theorem was typically written

$$a^p \equiv a \mod p$$

or, equivalently,

$$a \not\equiv 0 \mod p \implies a^{p-1} \equiv 1 \mod p$$
.

**Exercise 1.** Show that these two versions of Gauss's form of Fermat's Little Theorem are equivalent. In other words, show

version 
$$1 \iff \text{version } 2$$
.

Finally, using the more modern notion of a finite field  $\mathbb{F}_p$  with p elements, we can write the theorem as

$$a \in \mathbb{F}_p \implies a^p = a$$

or, equivalently,

$$a \in \mathbb{F}_p^{\times} \implies a^{p-1} = 1.$$

We will discuss three different proofs of Fermat's Little Theorem. The shortest is a proof using group theory: Suppose a is in the unit group  $\mathbb{F}_p^{\times}$ . By a theorem of group theory, if |G|is the order of the group, then  $a^{|G|}$  is the identity. The order of the unit group is p-1, so  $a^{p-1} = 1$ . This proof is very economical, but will only appeal to readers who have studied

Date: Spring 2008, Spring 2009. Modified April 12, 2009.

group theory. Furthermore, it is a relatively late proof, and uses concepts that were not available to Fermat, Euler, and Gauss.

### 2. INDUCTION BASED PROOF

The first of the two highlighted proofs of Fermat's Little Theorem uses induction and binomial coefficients.

**Theorem 1** (Fermat's Little Theorem). Let a be an integer, and let p be a prime. Then

$$a^p \equiv a \mod p.$$

*Proof.* Fix the prime p. First we prove the result for natural numbers n by induction. The base case is trivial:

$$0^p \equiv 0 \bmod p.$$

Now suppose  $n^p \equiv n \mod p$ . By the binomial theorem

$$(n+1)^{p} = n^{p} + {\binom{p}{1}}n^{p-1} + {\binom{p}{2}}n^{p-2} + \ldots + {\binom{p}{p-2}}n^{2} + {\binom{p}{p-1}}n + 1$$

The formula for the binomial coefficients is

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

and when  $1 \le k \le p-1$  we have p dividing the numerator, but not the denominator. Thus, for all  $1 \le k \le p-1$ ,

$$\binom{p}{k} \equiv 0 \mod p.$$

Hence

$$(n+1)^p \equiv n^p + 0 + \ldots + 0 + 1 \equiv n^p + 1 \mod p.$$

By induction, we have the result for all  $n \ge 0$ . For negative a, choose  $n \ge 0$  so that  $a \equiv n \mod p$ . Since the result holds for n, it holds for a as well. Thus the result holds for all  $a \in \mathbb{Z}$ .

#### 3. Permutation based proof

Now we give a second proof of Fermat's theorem. This involves permuting the order of factors of (p-1)!. Recall that a permutation map on a finite set is just a bijection from the set to itself.

For Fermat's theorem we only need the following lemma for m = p a prime. However, the general case is no harder to prove.

**Lemma 1.** Let m > 1 be an integer, and let  $a \in \mathbb{Z}_m^{\times}$ . Then the function  $\mu_a$  defined by the rule  $x \mapsto a \cdot x$  is a bijection  $\mathbb{Z}_m^{\times} \to \mathbb{Z}_m^{\times}$ .

*Proof.* Observe that

$$\mu_a(\mu_{a^{-1}}(x)) = \mu_a(a^{-1}x) = a(a^{-1}x) = x.$$

Similarly  $\mu_{a^{-1}}(\mu_a(x)) = x$ . Thus  $\mu_{a^{-1}}$  is the inverse of the function  $\mu_a$ . Since  $\mu_a$  has an inverse, it is a bijection.

**Corollary 2.** Let p be an prime. If  $a \in \mathbb{F}_p^{\times}$ , then  $a, 2a, \ldots, (p-1)a$  are distinct, and every element of  $\mathbb{F}_p^{\times}$  is in the sequence. In particular, this list is a permutation of the list  $1, 2, 3, \ldots, p-1$ .

*Proof.* The injectivity of  $\mu_a$  tells us that the terms are distinct, and the surjectivity tells us that every element of  $\mathbb{F}_p^{\times}$  is on the list.

**Exercise 2.** Make a table showing all the values of the functions  $\mu_3 : \mathbb{F}_5^{\times} \to \mathbb{F}_5^{\times}$ . Observe that multiplication by 3 (modulo 5) permutes  $\{1, 2, 3, 4\}$ .

**Exercise 3.** Make a table showing all the values of the functions  $\mu_4 : \mathbb{Z}_{15}^{\times} \to \mathbb{Z}_{15}^{\times}$ .

Here is the permutation based proof:

**Theorem 3** (Fermat's Little Theorem). Let p be a prime. If  $a \in \mathbb{F}_p^{\times}$  then  $a^{p-1} = 1$ .

*Proof.* Let  $u = 1 \cdot 2 \cdot 3 \cdots (p-1) = (p-1)!$  considered as an element of  $\mathbb{F}_p$ . Since u is the product of units, u is also a unit. By Corollary 2,

$$(a)(2a)(3a)\dots((p-1)a) = 1 \cdot 2 \cdot 3\dots(p-1) = u$$

since both sides are the product of the same elements, possibly in a different order.

Observe that

$$(a)(2a)(3a)\dots((p-1)a) = 1 \cdot 2 \cdot 3\dots(p-1)a^{p-1} = ua^{p-1}$$

(move all the a terms to the right). Thus

$$ua^{p-1} = u$$

Since u is a unit, we can multiply by its inverse. So  $a^{p-1} = 1$ .

## 4. Euler's Theorem

The famous mathematician Euler was fascinated with the number theoretic work of Fermat. In fact, Euler's interest in number theory is largely due to his study of Fermat's writings. Fermat did not leave a proof of his Little Theorem in his published writings, but Euler, once he learned of the statement, was able to figure out a proof. Next Euler thought about how to generalize this result to a modulus m that is not prime. His key idea was to develop his function  $\varphi(m)$ , and replace p-1 with  $\varphi(m)$ . This is motivated by the fact that  $\mathbb{Z}_p$  has p-1 units, but in general  $\mathbb{Z}_m$  has  $\varphi(m)$  units. The proof follows closely the permutation based version of the proof of Fermat's theorem.

**Lemma 2.** Let m > 1 be an integer and let  $u_1, \ldots, u_{\varphi(m)}$  be the (distinct) elements of  $\mathbb{Z}_m^{\times}$ . If  $a \in \mathbb{Z}_m^{\times}$  then the terms of the sequence  $a u_1, \ldots, a u_{\varphi(m)}$  are distinct, and every element of  $\mathbb{Z}_m^{\times}$  is in the sequence.

*Proof.* This follows from the fact that  $\mu_a$  is a bijection (Lemma 1).

**Theorem 4** (Euler's Theorem). Let m > 1 be an integer. If  $a \in \mathbb{Z}_m^{\times}$  then  $a^{\varphi(m)} = 1$ .

*Proof.* Let  $\mathbb{Z}_m^{\times} = \{u_1, \ldots, u_{\varphi(m)}\}$ . By the above lemma, and the commutative law of multiplication,

$$u_1 \cdots u_{\varphi(m)} = (a \, u_1) \cdots (a \, u_{\varphi(m)}) = a^{\varphi(m)} \cdot (u_1 \cdots u_{\varphi(m)}).$$

(The first equality is true since the second product has the same factors as the first, but typically in a different order. The second is true based on moving a to the front. Observe that there are  $\varphi(m)$  occurances of a since there are  $\varphi(m)$  units.) Let  $u = u_1 \cdots u_{\varphi(m)}$ . Observe that u is a unit by the closure property. Thus

$$u = a^{\varphi(m)}u.$$

Now multiply both sides by the inverse of u.

**Exercise 4.** Illustrate Euler's and Fermat's Little Theorem with several examples.

#### 5. WILSON'S THEOREM

In the permutation based proof of Fermat's theorem we used (p-1)! in the field  $\mathbb{F}_p$ . We didn't have to calculate its value, since it cancelled at the end of the proof. However, it is interesting to note that it is just -1. We begin with a short lemma.

**Lemma 3.** Let p > 2 be a prime and let  $a \in \mathbb{Z}_p^{\times}$ . Then  $a = a^{-1}$  if and only if a is 1 or -1.

*Proof.* One direction is clear. For the other, suppose that  $a = a^{-1}$ . Multiplying both sides by a gives  $a^2 = 1$ . In other words,  $a^2 - 1 = 0$ . This implies that (a - 1)(a + 1) = 0. Since  $\mathbb{F}_p$  is an integral domain, we have a - 1 = 0 or a + 1 = 0. Thus a = 1 or a = -1.

**Exercise 5.** Show that  $x \mapsto x^{-1}$  is a bijection of  $\mathbb{Z}_m^{\times}$ . Conclude from this that (p-1)! is its own multiplicative inverse in  $\mathbb{F}_p$ . The above lemma tells us that (p-1)! is either 1 or -1. The next exercise shows that is cannot be 1 but must be -1.

**Theorem 5** (Wilson's Theorem). Let p be a prime. Then  $(p-1)! \equiv -1 \mod p$ .

*Proof.* If p = 2 then it is clear, so assume p > 2. If we multiply all the elements of  $\mathbb{F}_p^{\times}$  together we get

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

Now reorder the elements of  $\mathbb{F}_p^{\times}$  as  $a_1, a_2, \ldots, a_{p-1}$  so that  $a_1 = 1$ , so that  $a_2 = -1$ , and, for i > 1, so that  $a_{2i-1}$  and  $a_{2i}$  are multiplicative 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 1 and -1. Consider the product:

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

By the commutative law of multiplication in  $\mathbb{F}_p$ ,

$$(p-1)! = 1 \cdot 2 \cdots (p-1) = a_1 \cdots a_{p-1} = -1.$$

Example 1. Consider 6! modulo 7:

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

From a direct calculation 6! + 1 = 721 is seen to be divisible by 7.

Exercise 6. Illustrate Wilson's Theorem with a few additional examples.

**Exercise 7.** Prove the converse of Wilson's theorem.