Math 455.1 • April 4, 2009

## Fermat's Little Theorem

For the RSA encryption system, we shall need the following result

**Theorem 1 (Fermat's Little Theorem).** Let p be a prime. Then for each integer a not divisible by p,

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

*Proof.* Let a be an integer for which  $p \nmid a$ .

For each j = 1, 2, ..., p - 1, let

$$r_j = (ja) \mod p$$
,

so that  $0 \leq r_j < p$ , that is,  $0 \leq r_j \leq p - 1$ .

We are going to prove that  $(r_1, r_2, \ldots, r_{p-1})$  is a permutation of  $(1, 2, \ldots, p-1)$ . For each  $j = 1, 2, 3, \ldots, p-1$ , we have  $j a \not\equiv 0 \pmod{p}$  (why?), that is,  $r_j \neq 0$ . Thus  $r_1, r_2, \ldots, r_{p-1}$  all belong to the set  $\{1, 2, 3, \ldots, p-1\}$ .

Next, if  $1 \leq j, k \leq p-1$  with  $j \neq k$ , then  $r_j \neq r_k$ . (Why?) Thus  $\{r_1, r_2, \ldots, r_{p-1}\}$  is a set of p-1 numbers that is a subset of the set  $\{1, 2, 3, \ldots, p-1\}$ . Hence these two sets are the same:

$$\{r_1, r_2, \dots, r_{p-1}\} = \{1, 2, 3, \dots, p-1\}$$

Since both sets have p-1 elements, then  $(r_1, r_2, \ldots, r_{p-1})$  is a permutation of  $(1, 2, \ldots, p-1)$ .

In other words, each of the p-1 numbers  $a, 2a, 3a, \ldots, (p-1)a$  is congruent modulo p to *exactly one* of the p-1 numbers  $1, 2, 3, \ldots, p-1$ . Hence

$$a \cdot (2a) \cdot (3a) \cdots ((p-1)a) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}.$$

In other words,

$$(p-1)! a^{p-1} \equiv (p-1)! \pmod{p}.$$
 (\*)

Now each of the factors  $1, 2, 3, \ldots, p-1$  of (p-1)! is relatively prime to p and so, by the Congruence Cancellation Law, may be cancelled from both sides of (\*). After the cancellations, what remains is

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

as desired.  $\Box$ 

The following corollary is, in fact, equivalent to Fermat's Little Theorem.

**Corollary 1.** Let p be a prime. The for every integer a,

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

Fermat's Little Theorem may be used to calculate efficiently, modulo a prime, powers of an integer not divisible by the prime.

**Example 1.** Calculate  $2^{345} \mod 11$  efficiently using Fermat's Little Theorem. *Solution.* The number 2 is not divisible by the prime 11, so

$$2^{10} \equiv 1 \pmod{11}$$

by Fermat's Little Theorem. By the division algorithm,

$$345 = 34 \cdot 10 + 5.$$

Since  $2^{345} = 2^{34 \cdot 10 + 5} = (2^{10})^{34} \cdot 2^5$ , then

$$2^{345} \equiv 1^{34} \cdot 2^5 \equiv 1 \cdot 32 \equiv 10 \pmod{11}.$$

Thus  $2^{345} \mod 11 = 10$ .

The result actually needed for RSA encryption is the following corollary to Fermat's Little Theorem.

**Corollary 2 (Euler's Corollary).** Let p and q be distinct primes. Then for each integer a not divisible by either p or q,

$$a^{(p-1)(q-1)} \equiv 1 \pmod{p\,q}$$

*Proof.* This is an exercise.  $\Box$ 

Both Fermat's Little Theorem and Euler's Corollary are special cases of a more general result. To formulate the generalization, we need the following definition.

**Definition 1. Euler's phi function**  $\phi \colon \mathbb{N}^* \to \mathbb{N}^*$  is defined by the rule that, for each positive integer n,

 $\phi(n) = \#\{k : 1 \le k < n \text{ and } k \text{ is relatively prime to } n\}.$ 

For example,  $\phi(2) = \#\{1\} = 1$ ,  $\phi(3) = \#\{1,2\} = 2$ ,  $\phi(4) = \#\{1,3\} = 2$ ,  $\phi(6) = \#\{1,5\} = 2$ , and  $\phi(12) = \#\{1,5,7,11\} = 4$ .

Then the generalization is as follows.

**Theorem 2 (Euler's Theorem).** Let m be an integer with m > 1. Then for each integer a that is relatively prime to m,

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

We will not prove Euler's Theorem here, because we do not need it.

Fermat's Little Theorem is a special case of Euler's Theorem because, for a prime p, Euler's phi function takes the value  $\phi(p) = p - 1$ . Note that, for a prime p, saying that an integer a is relatively prime to p is equivalent to saying that p does not divide a.

Euler's Corollary is also a special case of Euler's Theorem because, for distinct primes p and q, Euler's phi function takes the value  $\phi(pq) = (p-1)(q-1)$ .

Copyright © 2009 by Murray Eisenberg. All rights reserved.