Fermat's Little Theorem

Dr. Scot Anderson

January 26, 2020

Abstract

Theorem 1 (Fermat's Little Theorem) *Let p be a prime and $a \in Z^+$ such that $a \bmod p \neq 0$. Then*

$$a^{p-1} \equiv 1 \bmod p \tag{1}$$

Proof. Consider $Z_p = \{0, 1, ..., p-1\}$, we know that multiplying each element of Z_p by a modulo p just gives us Z_p in some order. Since $0 \times a \bmod p = 0$ we have the last $p-1$ numbers of Z_p multiplied by a as:

$$\begin{aligned} a \times Z_p \backslash \{0\} &= \{a, 2a, 3a, ..., (p-1)\, a\} \\ &\equiv \{a \bmod p, 2a \bmod p, ..., (p-1)\, a \bmod p\} \end{aligned} \tag{2}$$

If we multiply all the numbers in the set we have

$$\begin{aligned} a \times 2a \times 3a \times ... \times (p-1)\, a &= a^{p-1} (1 \times 2 \times ... \times (p-1)) \\ &= a^{p-1} (p-1)! \end{aligned} \tag{3}$$

and

$$a^{p-1} (p-1)! \equiv a \bmod p \times 2a \bmod p \times ... \times (p-1)\, a \bmod p \tag{4}$$

Because we know that all the terms in (4) map to some unique element in Z_p not 0 we have the following

$$a^{p-1} (p-1)! \equiv (1 \times 2 \times ... \times (p-1)) \bmod p \tag{5}$$

and

$$a^{p-1} (p-1)! \equiv (p-1)! \bmod p \tag{6}$$

Since $(p-1)$ is relatively prime to p (because p is prime) we can divide out $(p-1)!$ from each side of (6) to get the result:

$$a^{p-1} \equiv 1 \bmod p$$

■

Theorem 2 *An alternate form of Fermat's Little theorem: Let p be prime and $a \in Z^+$ such that $a \bmod p \neq 0$. Then*

$$a^p = a \bmod p$$

Definition 3 *Let $n \in Z^+$ then we define the totient function $\phi(n)$ is defined to be the number of positive integers less than n that are relatively prime to n. That is*

$$\phi(n) = \left\{x : x \in Z^+, x < n, \gcd(x, n) = 1\right\} \tag{7}$$

Lemma 4 *Let n be a prime number. Then*

$$\phi(n) = n - 1 \tag{8}$$

Theorem 5 *Given a composit number $n = p \times q$ where p, q are prime then*

$$\phi(n) = \phi(p_1) \times \phi(p_2) \tag{9}$$

Proof. Consider that the set of residues in Z_n is $\{0, 1, ..., pq - 1\}$. Now the residues that are not relatively prime to p are

$$\{p, 2p, ..., (q-1)\,p\} \tag{10}$$

and the residues that are not relatively prime to q are

$$\{q, 2q, ..., (p-1)\,q\} \tag{11}$$

Clearly the size of the two sets of residues not relatively prime to n are $(p-1)$ and $(q-1)$ plus the 0 element. So we have

$$\begin{aligned}\phi(n) &= pq - [(p-1) + (q-1) + 1] \\ &= pq - (p-1) - (q-1) - 1 \\ &= pq - p - q + 1 \\ &= p\,(q-1) - (q-1) \\ &= (p-1)\,(q-1)\end{aligned} \tag{12}$$

■

Theorem 6 (Euler's Theorem) *Let a and n be relatively prime positive numbers, then*

$$a^{\phi(n)} \equiv 1 \pmod{n} \tag{13}$$

Proof. First we not that if n is prime that the Theorem holds from Fermat's little Theorem. Namely (13) reduces to

$$a^{n-1} = 1 \bmod n \tag{14}$$

Consider the set of integers relatively prime to n:

$$R = \left\{x_1, ..., x_{\phi(n)}\right\}$$

Multiplying the set by a modulo n gives:

$$S = \left\{ax_1 \bmod n, ..., ax_{\phi(n)} \bmod n\right\}$$

We claim that S is a permutation of R. Consider that a and $x_i \in R$ are relatively prime to n. Then ax_i must also be relatively prime to n and $ax_i \bmod n \neq 0$. Thus all the members of S are relatively prime to n. There can be no duplicates in S because

$$ax_i \bmod n = ax_j \bmod n \rightarrow x_i \bmod n = x_j \bmod n$$

because there exists a a^{-1} in Z_n. But $x_i < n$ and $x_j < n$, so we must have that

$$x_i = x_j$$

and we have that there are no duplicates in S. Therefore S is a permutation of R. Consider

$$\prod_{i=1}^{\phi(n)} (ax_i \bmod n) = \prod_{i=1}^{\phi(n)} x_i$$

Then

$$\prod_{i=1}^{\phi(n)} ax_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n}$$

Which gives

$$a^{\phi(n)} \times \prod_{i=1}^{\phi(n)} x_i \equiv \prod_{i=1}^{\phi(n)} x_i \pmod{n}$$

Now since $\prod_{i=1}^{\phi(n)} x_i$ is relatively prime to n, we can cancel on each side to get the result

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

■

Theorem 7 *Alternate form of Euler's Theorem: Let a and n be relatively prime positive numbers, then*

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

Corollary 8 *Let $n = pq$ and m be integers where p and q are prime numbers and $0 < m < n$. Then*

$$m^{\phi(n)+1} = m^{(p-1)(q-1)+1} \equiv m \pmod{n}$$

Theorem 9 (CRT) *Let $S = \{m_1, ..., m_k\}$ and*

$$M = \prod_{i=1}^{k} m_i$$

where for all $m_i, m_j \in S, \gcd(m_i, m_j) = 1$ (that is they are pairwise relatively prime). We can represent any integer in Z_m by the $k-$tuple whose elements are in Z_{m_i}. That is we have a bijection:

$$A \longleftrightarrow (a_1, ..., a_k)$$

Proof. Define

$$a_i = A \bmod m_i$$

Let

$$M_i = M/m_i \text{ for } 1 \leq i \leq k$$

so that the following condition holds:

$$M_i = 0 \pmod{m_i}$$

Since M_i is relatively prime to m_i we define the following:

$$c_i = M_i \times \left(M_i^{-1} \bmod m_i\right) \text{ for } 1 \leq i \leq k$$

We claim that the following holds, but why we have no idea!

$$A \equiv \left(\sum_{i=1}^{k} a_i c_i\right) \bmod M$$

■