Fermat's Theorem

Two theorems that play important roles in public-key cryptography are Fermat's theorem and Euler's theorem.

Fermat's theorem states the following: If p is prime and a is a positive integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p} \tag{8.2}$$

Proof:

Consider a set of positive integers less than **p:{1,2,3.....p-1}** and multiply each element by a mod p, to get a set **X={a mod p,2a modp,3a mod p,......(p-1)a mod p}**

None of the elements of X is equal to zero, because p does not divide a.

No two of the integers in X are equal.

To see this, assume that $ja \equiv ka \pmod{p}$, where $1 \le j < k \le p-1$

Because a is relatively prime to p, we can eliminate a from both sides, resulting in $\mathbf{j \equiv k \pmod{p}}$

This last equality is impossible, because j and k are both positive integers less than p

Therefore we know that the p-1 elements of X are all positive integers with no two elements equal

We can conclude the X consists of the set of integers :{1,2,3.....p-1}in some order

Multiplying the numbers in both sets (p and X) and take the results mod p yield

$$a \times 2a \times 3a \ldots\ldots (p-1)a \equiv [(1 \times 2 \times 3 \ldots\ldots (p-1)] \pmod{p}$$

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

We can cancel the $((p-1)!$ term because it is relatively prime to p

This yields Equation (8.2), which completes the proof.

Eg: a= 7, p = 19

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

$7^{19-1} = 7^{18}$

$7^2 = 7 \times 7 = 49 \pmod{19} = 11$

$7^4 = 7^2 \times 7^2 = 11 \times 11 = 121 \bmod 19 = 7$

$7^8 = 7^4 \times 7^4 = 7 \times 7 = 49 \pmod{19} = 11$

$7^{16} = 7^8 \times 7^8 = 11 \times 11 = 121 \bmod 19 = 7$

$7^{18} = 7^{16} \times 7^2 = 7 \times 11 = 77 \bmod 19 = 1$

An alternative form of fermat's theorem, If p is prime and a is a positive integer, then

$$a^p \equiv (a \bmod p)$$

Eg: p=5,a=3

$a^p = 3^5 = 243 \bmod 5 = 3$

Euler's totient function

Euler's totient function, written Φ(n), and defined as the number of positive integers less than and relatively prime to n.

By convention, $\Phi(1)= 1$

Euler's totient function is represented as $\Phi(n)=n-1$,

$$\Phi(pq)= (p-1)(q-1)$$

It is defined as the number of positive integers less than n and relatively prime to n.

$\Phi(1) = 1$
$\Phi(5) = 1, 2, 3, 4 = 4$
$\Phi(4) = 1, 3 =2$
$\Phi(20) =1, 3, 7, 9, 11, 13, 17, 19 = 8$
$= \Phi(5) * \Phi(4)$
$= 4 * 2 = 8$

The value $\phi(1)$ is without meaning but is defined to have the value 1.

It should be clear that, for a prime number p,

$$\phi(p) = p - 1$$

Now suppose that we have two prime numbers p and q with $p \neq q$. Then we can show that, for $n = pq$,

$$\phi(n) = \phi(pq) = \phi(p) \times \phi(q) = (p - 1) \times (q - 1)$$

To see that $\phi(n) = \phi(p) \times \phi(q)$, consider that the set of positive integers less that n is the set $\{1, \ldots, (pq - 1)\}$. The integers in this set that are not relatively prime to n are the set $\{p, 2p, \ldots, (q - 1)p\}$ and the set $\{q, 2q, \ldots, (p - 1)q\}$. Accordingly,

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

Euler's Theorem

Euler's theorem states that for every a and n that are relatively prime:

$$a^{\Phi(n)} \equiv 1(\text{mod } n)$$

Proof: Equation is true if n is prime, because in that case, $\phi(n) = (n - 1)$ and Fermat's theorem holds. However, it also holds for any integer n. Recall that $\phi(n)$ is the number of positive integers less than n that are relatively prime to n. Consider the set of such integers, labeled as

$$R = \{x_1, x_2, \ldots, x_{\phi(n)}\}$$

That is, each element x_i of R is a unique positive integer less than n with $\gcd(x_i, n) = 1$. Now multiply each element by a, modulo n:

$$S = \{(ax_1 \bmod n), (ax_2 \bmod n), \ldots, (ax_{\phi(n)} \bmod n)\}$$

The set S is a permutation[6] of R, by the following line of reasoning:

1. Because a is relatively prime to n and x_i is relatively prime to n, ax_i must also be relatively prime to n. Thus, all the members of S are integers that are less than n and that are relatively prime to n.

2. There are no duplicates in S. Refer to Equation (4.5). If $ax_i \bmod n = ax_j \bmod n$, then $x_i = x_j$.

Therefore,

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

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

$$a^{\phi(n)} \times \left[\prod_{i=1}^{\phi(n)} x_i\right] = \prod_{i=1}^{\phi(n)} x_i (\text{mod } n)$$

$$a^{\phi(n)} = 1 (\text{mod } n)$$

which completes the proof. This is the same line of reasoning applied to the proof of Fermat's theorem.

$a = 3; n = 10; \phi(10) = 4 \quad a^{\phi(n)} = 3^4 = 81 = 1 \pmod{10} = 1 \pmod{n}$
$a = 2; n = 11; \phi(11) = 10 \quad a^{\phi(n)} = 2^{10} = 1024 = 1 \pmod{11} = 1 \pmod{n}$

As is the case for Fermat's theorem, an alternative form of the theorem is also useful:

$$a^{\phi(n)+1} \equiv a \pmod{n} \tag{8.5}$$

Again, similar to the case with Fermat's theorem, the first form of Euler's theorem [Equation (8.4)] requires that a be relatively prime to n, but this form does not.