Euler's Theorem

Euler not only proved Fermat's little theorem but also gave a generalization.

Definition: Let $n \in \mathbb{Z}^+$. The Euler phi-function $\varphi(n)$ is defined to be the number of positive integers not exceeding n that are relatively prime to n.

ex: $\varphi(1) = 1$

$\varphi(2) = 1$

$\varphi(3) = 2$

$\varphi(4) = 2$

$\varphi(5) = 4$

$\varphi(6) = 2$

Definition: A reduced residue system modulo n is a set of $\varphi(n)$ number of integers such that each element of the set is relatively prime to n, and no two different elements of the set are congruent modulo n.

ex: The set $\{1, 3, 5, 7\}$ is a reduced residue system modulo 8. The set $\{-3, -1, 1, 3\}$ is also such a set. $\{9, 11, 13, 15\}$ is another such set.

Theorem 6.13: If $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$ is a reduced residue system modulo n, and $a \in \mathbb{Z}^+$ is relatively prime to n, then the set $\{ar_1, ar_2, \ldots, ar_{\varphi(n)}\}$ is also a reduced residue system modulo n.

Proof: Exercise

ex: $\{1, 3, 5, 7\}$ is a reduced residue system modulo 8. Therefore, $\{3, 9, 15, 21\}$ is also a reduced residue system modulo 8.

Theorem 6.14: Euler's Theorem

Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ be such that $\gcd(a, m) = 1$. Then,

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

Proof: Exercise (very similar to the proof of Fermat's little theorem)

ex: $3^4 \equiv 1 \pmod 8$ because $\gcd(8, 3) = 1$ and $\varphi(8) = 4$.

This theorem can be used effectively to find inverses of an integer a modulo m when $\gcd(a,m)=1$. This is because

$$a \cdot a^{\varphi(m)-1} = a^{\varphi(m)} \equiv 1 \pmod{m}$$

and thus, $a^{\varphi(m)-1}$ is an inverse of a modulo m.

ex: We know $\varphi(9)=6$. Also, $\gcd(9,7)=1$.

$$\therefore \bar{7} = 7^{\varphi(9)-1} = 7^5$$
$$= (7^2)^2 \cdot 7$$
$$= 49^2 \cdot 7$$
$$\equiv 4^2 \cdot 7 \pmod{9}$$
$$\equiv 16 \cdot 7 \pmod{9}$$
$$\equiv (-2)(-2) \pmod{9}$$
$$\equiv 4 \pmod{9}$$

We can also use this theorem to solve linear congruences.

ex: Consider $3x \equiv 7 \pmod{10}$.

Then,
$$x \equiv 3^{\varphi(10)-1} \cdot 7 \pmod{10}$$
$$\equiv 3^{4-1} \cdot 7 \pmod{10}$$
$$\equiv 27 \cdot 7 \pmod{10}$$
$$\equiv (-3)(-3) \pmod{10} \equiv 9 \pmod{10}$$