Euler's Theorem

DEFINITION: Let n be a positive integer. The **Euler phi-function** $\phi(n)$ is defined to be the number of positive integers not exceeding n that are relatively prime to n.

EXAMPLES:

1. Let $n = 1$. Since the only positive integer not exceeding 1 that is relatively prime to 1 is 1, we have

$$\phi(1) = 1$$

2. Let $n = 2$. Since the only positive integer not exceeding 2 that is relatively prime to 2 is 1, we have

$$\phi(2) = 1$$

3. Let $n = 3$. Since the only positive integers not exceeding 3 that are relatively prime to 3 are 1 and 2, we have

$$\phi(3) = 2$$

4. Let $n = 4$. Since the only positive integers not exceeding 4 that are relatively prime to 4 are 1 and 3, we have

$$\phi(4) = 2$$

5. Let $n = 5$. Since the only positive integers not exceeding 5 that are relatively prime to 5 are $1, 2, 3$, and 4, we have

$$\phi(5) = 4$$

REMARK: It immediately follows from the definition that $\phi(p) = p - 1$ if p is a prime number.

THEOREM 1: Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ be the prime-power factorization of the positive integer n. Then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right)$$

EXAMPLES:

1. Let $n = 4 = 2^2$, then

$$\phi(4) = 4\left(1 - \frac{1}{2}\right) = 2$$

2. Let $n = 5$, then

$$\phi(5) = 5\left(1 - \frac{1}{5}\right) = 4$$

3. Let $n = 2^3\, 3^2\, 7 = 504$, then

$$\begin{aligned}
\phi(504) &= 2^3\, 3^2\, 7\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right) \\
&= \left(2^3 - \frac{2^3}{2}\right)\left(3^2 - \frac{3^2}{3}\right)\left(7 - \frac{7}{7}\right) \\
&= (8 - 4)\,(9 - 3)\,(7 - 1) \\
&= 4 \cdot 6 \cdot 6 \\
&= 144
\end{aligned}$$

THEOREM 2 (Euler's Theorem): If m is a positive integer and a is an integer with $(a, m) = 1$, then

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

REMARK: Note that Fermat's Little Theorem follows immediately from Euler's Theorem, since $\phi(m) = m - 1$ if m is a prime number.

We can use Euler's Theorem to find inverses modulo m. If a and m are relatively prime, we know that

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

Hence, $a^{\phi(m)-1}$ is an inverse of a modulo m.

EXAMPLE: We know that

$$2^{\phi(9)-1} = 2^{6-1} = 2^5 = 32 \equiv 5 \pmod{9}$$

is an inverse of 2 modulo 9.

We can solve linear congruences using this observation. To solve

$$ax \equiv b \pmod{m}$$

where $(a, m) = 1$, we multiply both sides of this congruence by $a^{\phi(m)-1}$ to obtain

$$a^{\phi(m)-1}ax \equiv a^{\phi(m)-1}b \pmod{m}$$

Therefore, the solutions are those integers x such that

$$x \equiv a^{\phi(m)-1}b \pmod{m}$$

EXAMPLE: Find all solutions of the following congruence

$$3x \equiv 7 \pmod{10}$$

Solution 1: We first note that $(3, 10) = 1$. Therefore we can apply the Corollary from Section 4.2. Since $s = 7$ is a particular solution of $3s \equiv 1 \pmod{10}$, we get

$$x \equiv bs \equiv 7 \cdot 7 \equiv 49 \equiv 9 \pmod{10}$$

Solution 2: We have

$$x \equiv a^{\phi(10)-1} \cdot 7 \equiv 3^3 \cdot 7 \equiv 189 \equiv 9 \pmod{10}$$

because $\phi(10) = 4$.