Chapter: Euler's Generalization of Fermat's theorem

Euler's theorem.

Lemma Let $n>1$ and $\gcd(a,n)=1$. If $a_1, a_2, \ldots, a_{\phi(n)}$ are the +ve integers less than n and relatively prime to n, then

$$aa_1, aa_2, \ldots, aa_{\phi(n)}$$

are congruent modulo n to $a_1, a_2, \ldots, a_{\phi(n)}$ in some order.

Pf. Consider the given set of integers

$$aa_1, aa_2, \ldots, aa_{\phi(n)}$$

Claim $aa_i \not\equiv aa_j \pmod{n}$ $\quad 1 \le i, j \le \phi(n)$ $\quad i \neq j$

Pf Suppose $aa_i \equiv aa_j \pmod{n}$

$$\Rightarrow a_i \equiv a_j \pmod{n}$$

This is impossible as $a_i \neq a_j$ for $i \neq j$.

$\because$ $\gcd(a_i, n)=1$ and $\gcd(a,n)=1$ $\quad \forall\ 1 \le i \le \phi(n)$

$\therefore$ $\gcd(aa_i, n)=1$ $\quad \forall\ 1 \le i \le \phi(n)$

For a particular aa_i $\exists$ a unique integer b $(0 \le b < n)$ s.t.

$$aa_i \equiv b \pmod{n}$$

$\therefore$ $\gcd(b,n) = \gcd(aa_i, n) = 1$

Hence b must be one of the integers $a_1, a_2, \ldots, a_{\phi(n)}$

Thm (Euler's theorem) If $n>1$ and $\gcd(a,n)=1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$

Pf. **Case I** $n=1$. Then $\gcd(a,1)=1$ and $\phi(1)=1$

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

Case II $n>1$ Let $a_1, a_2, \ldots, a_{\phi(n)}$ be the positive integers less than n and relatively prime to n.

$\therefore \gcd(a,n)=1$

$\therefore aa_1, aa_2, \ldots, aa_{\phi(n)}$ are congruent modulo n to $a_1, a_2, \ldots, a_{\phi(n)}$ (not necessarily in the same order) i.e.

$$aa_1 \equiv a_1' \pmod{n}$$
$$aa_2 \equiv a_2' \pmod{n}$$
$$\vdots$$
$$aa_{\phi(n)} \equiv a_{\phi(n)}' \pmod{n}$$

where $a_1', a_2', \ldots a_{\phi(n)}'$ are integers $a_1, a_2, \ldots a_{\phi(n)}$ in some order. Multiplying these congruences

$$(aa_1)(aa_2)\cdots(aa_{\phi(n)}) \equiv a_1'a_2'\cdots a_{\phi(n)}' \pmod{n}$$
$$\equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n}$$

$$\Rightarrow a^{\phi(n)}(a_1 a_2 \cdots a_{\phi(n)}) \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n}$$

$\because \gcd(a_i, n)=1 \quad \forall i \quad 1 \le i \le \phi(n)$

$\therefore \gcd\left((a_1 a_2 \cdots a_{\phi(n)}), n\right) = 1$

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

Cor: (Fermat's thm) If p is a prime and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$

Pf $\because p \nmid a$ and p is prime

$\therefore \gcd(a, p) = 1$

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

$\therefore$ Using previous thm

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

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

Example Find the last two digits of 3^{256}.

Sol This is equivalent to finding the smallest non-negative integer to which 3^{256} is congruent modulo 100. Take $a=3$ and $n=100$

$\gcd(3, 100) = 1$, $\phi(100) = \phi(2^2 \cdot 5^2) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 40$

By Euler's thm

$$3^{\phi(100)} \equiv 1 \pmod{100}$$

$$\Rightarrow 3^{40} \equiv 1 \pmod{100}$$

Now $3^{256} = 3^{6 \cdot 40 + 16} = (3^{40})^6 3^{16} \equiv 3^{16} \pmod{100}$

$3^4 = 81$

$3^8 = (3^4)^2 = (81)^2 \equiv 61 \pmod{100}$

$3^{16} = (3^8)^2 = (61)^2 \equiv 21 \pmod{100}$

$\therefore 3^{256} \equiv 21 \pmod{100}$

i.e. the last two digits in the decimal expansion of 3^{256} are 21.