Preliminaries

Remember that, if n is a positive integer, then $U(n)$ is the multiplicative group of residue classes modulo n that have no factor in common with n.

Examples

- $U(7) = \{1, 2, 3, 4, 5, 6\}$ group operation is mult mod 7
  $|U(7)| = 6$
- $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ $|U(15)| = 8$
  ~~0~~ 1 ~~2~~ ~~3~~ 4 ~~5~~ ~~6~~ 7 8 ~~9~~ ~~10~~ 11 ~~12~~ 13 14
- $U(12) = \{1, 5, 7, 11\}$ $|U(12)| = 4$
  ~~0~~ 1 ~~2~~ ~~3~~ ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11
- $U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$ $|U(30)| = 8$

Euler's Function ϕ

Definition: $\phi(n)$ is the number of elements in $U(n)$.

- $\phi(7) =$ 6
- $\phi(15) =$ 8
- $\phi(12) =$ 4
- $\phi(30) =$ 8

Proposition: If p is prime, then $\phi(p) = p - 1$.

$U(p) = \{1, 2, \ldots, p-1\}$. $|U(p)| = p-1$.

Fermat's (Little) Theorem

Theorem: Let p be a prime and let a be an integer not divisible by p. Then

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

Proof: $U(p)$ has $p-1$ elements

$a \in \mathbb{Z}$, $p \nmid a$. $[a] \in U(p)$.

$[a]^k = [1] \iff \text{order}(a) \mid k$. ★★

$\text{order}[a] = \#\langle [a] \rangle \leq U(p)$.

$|U(p)| = p-1$.

$\#\langle [a] \rangle \mid p-1$.

$\text{order}(a) \mid p-1$.

$[a]^{p-1} = [1]$ means $a^{p-1} \equiv 1 \bmod p$.

$U(7)$:

$a = 2$ $\quad 2^6 \equiv 64 \equiv 1 \ (7)$

$3^6 \equiv 9 \cdot 9 \cdot 9 \equiv 81 \cdot 9 \bmod 7$

$81 \equiv 77 + 4 \equiv 4 \bmod 7$ $\quad 81 \cdot 9 \equiv 4 \cdot 9 \equiv 36 \bmod 7$

$36 \equiv 1 \bmod 7$.

Euler's Theorem

Theorem: Let n be a positive integer and let a be an integer with no factor in common with n. Then

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

Proof: $[a] \in U(n)$ since $\gcd(a,n) = 1$.

$\text{order}(a) \mid |U(n)|$

which by definition means $\text{order}(a) \mid \varphi(n)$.

$[a]^{\varphi(n)} = [1]$ in $U(n)$

$a^{\varphi(n)} \equiv 1 \mod n.$

$U(12) = \{1, 5, 7, 11\}$. $\varphi(12) = 4$.

$5^4 \equiv 25^2 \equiv 1^2 \equiv 1 \mod 12.$

$7^2 \equiv 1 \mod 12$ $(49 \equiv 1 \mod 12)$

$7^4 \equiv 1 \mod 12$ $(1^2 \equiv 1 \mod 12.$

$11^2 \equiv 121 \equiv 1 \mod 12$ $11^4 \equiv 1 \mod 12.$