Recall : u is a unit mod n when u^{-1} mod n exist, or equivalently when $(u,n) = 1$

$uu^{-1} \equiv 1 \pmod{n}$

- $1, -1$ are units
- u is a unit $\Rightarrow u^{-1}$ is also a unit
- u, v are units $\Rightarrow uv$ is a unit

Definition: $\phi(n)$ = number of units in $\mathbb{Z}_n$
(Euler's function)

$$= \left| \{ u : 1 \leq u \leq n-1 \text{ and } (u,n) = 1 \} \right| .$$

$\phi(8) = 4$

$\phi(9) = 6$

$\phi(10) = 4$

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

Back to Fermat's analog in $\mathbb{Z}_n$.

Claim: Suppose $(a,n)=1$, then we have

$$\{u : 1 \leq u \leq n-1 \text{ and } (u,n)=1\}$$
$$\equiv$$
$$\{au : 1 \leq u \leq n-1 \text{ and } (u,n)=1\}$$

in $\mathbb{Z}_n$.

e.g. $n=8$ and $a=3$

$$\{1,3,5,7\} \equiv \{3,9,15,21\} \pmod{8}$$

$n=10$ and $a=7$

$$\{1,3,7,9\} \equiv \{7,21,49,63\} \pmod{10}$$

Proof: $\{u : 1 \leq u \leq n-1 \text{ and } (u,n)=1\}$ has $\phi(n)$ elements, all units.

$(a,n)=1$ and $(u,n)=1 \Rightarrow (au,n)=1 \Rightarrow au$ is unit.

Also $au \equiv av \pmod{n} \iff u \equiv v \pmod{n}$

So, $\{au : 1 \leq u \leq n-1 \text{ and } (u,n)=1\}$ has $\phi(n)$ distinct elements, all units. ∎

Similar to Fermat's Theorem, we now have

Euler's Theorem: Suppose $(a,n)=1$, then we have $a^{\phi(n)} \equiv 1 \pmod{n}$.

- $n=p$ gives Fermat.

How to compute $\phi(n)$?

An example: $n=12$

$$(u,12)=1 \iff (u,4)=1 \text{ and } (u,3)=1$$

$$\begin{array}{ccc} \downarrow & & \downarrow \\ 1 \pmod{4} & & 1 \pmod{3} \\ 3 \pmod{4} & & 2 \pmod{3} \end{array}$$

$\Downarrow$ CRT

$1 \pmod{12}$

$5 \pmod{12}$

$7 \pmod{12}$

$11 \pmod{12}$

$$\phi(12) = \phi(4)\cdot\phi(3) = 4$$

Theorem: For $(m,n)=1$, we have

$$\phi(mn)=\phi(m)\cdot\phi(n)$$

Proof: $(u,mn)=1 \iff (u,m)=1$ and $(u,n)=1$

There are $\phi(m)$ values in $\mathbb{Z}_m$ and $\phi(n)$ values in $\mathbb{Z}_n$. By CRT, there are $\phi(m)\,\phi(n)$ units in $\mathbb{Z}_{mn}$.

- $\phi(1)=1$ by convention.

Corollary: $\phi(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k})=\phi(p_1^{\alpha_1})\cdot\phi(p_2^{\alpha_2})\cdot\ldots\cdot\phi(p_k^{\alpha_k})$

Now, it is remained to compute $\phi(p^k)$.

$(u,p^k)=1 \iff (u,p)=1$, i.e. $p\nmid u$.

$\{u : 1\leq u\leq p^k-1 \text{ and } (u,p^k)=1\}$

$=\{u : 1\leq u\leq p^k-1 \text{ and } p\nmid u\}$

$=\{u : 1\leq u\leq p^k-1\}-\{p, 2p, 3p, \ldots, (p^{k-1}-1)\cdot p\}$

Theorem: p prime, $k\geqslant 1$. Then,

$$\phi(p^k)=p^k-p^{k-1}=p^{k-1}\cdot(p-1)=p^k\cdot\left(1-\frac{1}{p}\right)$$

<u>Theorem:</u> $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Then

$$\phi(n) = \prod_{i=1}^{k} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1} \right)$$

$$= \prod_{i=1}^{k} p_i^{\alpha_i - 1}(p_i - 1)$$

$$= \prod_{i=1}^{k} p_i^{\alpha_i} \cdot \left(1 - \frac{1}{p_i} \right)$$

$$= n \cdot \prod_{i=1}^{k} 1 - \frac{1}{p_i} .$$

- Compute $\phi(42)$, $\phi(48)$, $\phi(60)$

$$\phi(42) = \phi(2 \cdot 3 \cdot 7)$$

$$= 42 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7}$$

$$= 12$$

$$\phi(48) = \phi(2^4 \cdot 3)$$

$$= 48 \cdot \frac{1}{2} \cdot \frac{2}{3}$$

$$= 16$$

$$\phi(60) = \phi(2^2 \cdot 3^1 \cdot 5^1)$$
$$= 2^{2-1} \cdot (2-1) \cdot 3^{1-1} \cdot (3-1) \cdot 5^{1-1} \cdot (5-1)$$
$$= 2 \cdot 2 \cdot 4$$
$$= 16$$

- Last two digits of $3^{2001} = ?$

$$3^{2001} \bmod (100) = ?$$

$$\phi(100) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40$$

$$\Rightarrow 3^{2001} \equiv (3^{40})^{50} \cdot 3 \equiv 1^{50} \cdot 3 \equiv 3 \pmod{100}$$

$\Rightarrow$ Last two digits 03.

- Prove $a^{12} \equiv 1 \pmod{42}$ for $(a, 42) = 1$.

$$\phi(42) = 12 \Rightarrow a^{12} \equiv 1 \pmod{42}$$

- Similarly,

$$a^{16} \equiv 1 \pmod{48} \quad \text{for} \quad (a, 48) = 1$$
$$a^{16} \equiv 1 \pmod{60} \quad \text{for} \quad (a, 60) = 1.$$

Next goal: to understand the structure of the units of $\mathbb{Z}_n$ better.

Start with $n = p$ prime and the following observation:

- units of $\mathbb{Z}_3$: $\{1, 2\} \equiv \{2, 2^2\} \pmod 3$
- units of $\mathbb{Z}_5$: $\{1, 2, 3, 4\} \equiv \{2, 2^2, 2^3, 2^4\} \pmod 5$
- units of $\mathbb{Z}_7$: $\{1, 2, 3, 4, 5, 6\} \not\equiv \{2, 2^2, 2^3, 2^4, 2^5, 2^6\}$

2 again

However $\{1, 2, 3, 4, 5, 6\} \equiv \{3, 3^2, 3^3, 3^4, 3^5, 3^6\}$

3 2 6 4 5 1

in $\mathbb{Z}_7$.

We make the following claim:

<u>Theorem</u>: p prime. There exists an integer g such that $\{1, 2, \ldots, p-1\} \equiv \{g, g^2, g^3, \ldots, g^{p-1}\}$

in $\mathbb{Z}_p$.

- g satisfying this condition will be called a primitive root.

We'll prove the theorem later. For now assume it is true if necessary.

<u>Theorem</u>: A unit u is a primitive root mod p if and only if the smallest positive integer k satisfying $u^k \equiv 1 \pmod p$ is $k = p-1$.

<u>Proof</u>: $\Rightarrow$: Suppose u is a primitive root, then $u, u^2, \dots, u^{p-2}$ must be different than u^{p-1} which is $1 \pmod p$ by Fermat. So, $u^k \not\equiv 1 \pmod p$ for $1 \le k \le p-2$ and $u^{p-1} \equiv 1 \pmod p$ by Fermat.

$\Leftarrow$: Suppose the smallest pos. int. k with $u^k \equiv 1 \pmod p$ is $k = p-1$.

$u, u^2, u^3, \dots, u^{p-1}$ are all distinct mod p since

$$u^i \equiv u^j \pmod p \Leftrightarrow u^{i-j} \equiv 1 \pmod p$$

shouldn't be $< p-1$

Therefore, $\{u, u^2, \dots, u^{p-1}\} \equiv \{1, 2, \dots, p-1\} \pmod p$.

Definition: Let u be a unit in $\mathbb{Z}_n$. We call the smallest positive integer k satisfying

$$u^k \equiv 1 \pmod{n}$$

the order of u modulo n, denoted by $\operatorname{ord}_n(u)$.

modulo p

- A primitive root is a unit of order $p-1$.

Theorem: g is a primitive root modulo p and $k \geq 0$ is an integer. Then,

$$g^k \equiv 1 \pmod{p} \iff p-1 \mid k$$

Proof: Write $k = (p-1)\cdot n + r$ with $0 \leq r < p-1$

$$g^k \equiv 1 \pmod{p} \iff g^{(p-1)\cdot n} \cdot g^r \equiv 1 \pmod{p}$$

$$\iff g^r \equiv 1 \pmod{p}$$

because $g^r \equiv 1 \pmod{p}$ and r positive $\Rightarrow r \geq p-1$.

$$\iff r = 0$$

$$\iff k = (p-1)\cdot n$$

$$\iff p-1 \mid k.$$

Next, we compute the orders of the units modulo p. More specifically $\mathrm{ord}_p(g^a)$ for $1 \leq a \leq p-1$.