Euler thm.

If $a \in \mathbb{Z}$ and $\gcd(a, n) = 1$ then

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

Chinese rem. thm

If $m_1, \dots, m_r$ s.t $\gcd(m_i, m_j) = 1$ for $i \neq j$

and $a_1, \dots, a_r \in \mathbb{Z}$ then

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \quad \vdots \\ x \equiv a_r \mod m_r \end{cases}$$

admits a unique solution mod $m_1 \dots m_r$

Put $m = m_1 \dots m_r$

and for $i = 1, \dots, r$ put $N_i = \frac{m}{m_i}$

and

$$x = a_1 N_1^{\varphi(m_1)} + \dots + a_r N_r^{\varphi(m_r)}$$

Then x is a solution. Indeed for every i

$$m_i \mid N_j \quad \text{for } i \neq j$$

so

$$x \equiv a_i N_i^{\varphi(m_i)} \mod m_i \qquad \gcd(N_i, m_i) = 1$$

Euler thm: $\equiv 1 \mod m_i$

$$x \equiv a_i \mod m_i \quad \text{for } i = 1, \dots, r.$$

$\blacksquare$

Example

$$\begin{cases} x \equiv 1 \mod 7 \\ x \equiv 3 \mod 8 \\ x \equiv 1 \mod 9 \end{cases} \qquad m = 7 \cdot 8 \cdot 9 = 504$$

$N_1 = \frac{504}{7} = 72$

$N_2 = \frac{504}{8} = 63$

$N_3 = \frac{504}{8} = 56$

$x = 1 \cdot 72^{\varphi(7)} + 3 \cdot 63^{\varphi(8)} + 1 \cdot 56^{\varphi(9)} = 379$

unique sol. mod 504

$\varphi(7) = 6$

$\varphi(8) = 2^2(2-1) = 4$

$\varphi(9) = 3(3-1) = 6$

Structure of $\mathbb{Z}_m^\times$

Commutative group.

Groups

G finite group $|G| = m$

Then for $g \in G$ we define the order of g

$\operatorname{ord}(g) = \min\{n > 0 \mid g^n = e\}$

$\operatorname{ord}(g) \mid m$

Def. exponent of G

$\exp(G) = \text{lcm}\,\{\text{ord}(g) \mid g \in G\}$

$\exp(G) \mid n$

$\forall g \in G \qquad \text{ord}(g) \mid \exp(G) \mid n$

A group G is cyclic if $\exists\, g \in G$ s.t. $\text{ord}(g) = |G|$ ↪ generator of G

$G = \{e, g, g^2, \dots, g^{k-1}\} \qquad k = \text{ord}(g)$
$= \langle g \rangle$

$\mathbb{Z}_n^\times$ is not in general cyclic.

$\mathbb{Z}_8^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$

$\bar{1}^2 = \bar{1} \qquad \bar{3}^2 = \bar{1} \qquad \bar{5}^2 = \bar{1} \qquad \bar{7}^2 = \bar{1}$

$\rightsquigarrow$ is not cyclic.

Thm. $\mathbb{Z}_n^\times$ is cyclic $\iff n = 2, 4, p^k, 2p^k$ for p an odd prime $k \geq 0$.

Want to prove the case $n = p$

An integer $a \in \mathbb{Z}$ is called a primitive root mod p if $\bar{a}$ generates $\mathbb{Z}_p^\times$.

For example 2 is a primitive root mod 5

$\langle \bar{2} \rangle = \{\bar{1}, \bar{2}, \bar{4}, \bar{3}\} = \mathbb{Z}_5^\times$

but 2 <u>not</u> a primitive root mod 7

$\langle \bar{2} \rangle = \{ \bar{1}, \bar{2}, \bar{4} \}$ $\qquad 2^3 = 8 \equiv 1 \mod 7$

$\mathrm{ord}(\bar{2}) = 3 \qquad |\mathbb{Z}_7^*| = 6$

<u>Artin primitive root conjecture</u> : if $a > 1$ is not a square then it is a primitive root mod p for infinitely many p.

<u>Thm.</u> classification of finite ab. gps.

If G is finite and abelian then

$$G \simeq \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_k} \quad (*)$$

$$(\bar{1}, \bar{1}, \dots, \bar{1})$$

where $n_1, \dots, n_k$ are integers such that $n_1 \cdots n_k = |G|$.

$\mathbb{Z}_n, +$ is cyclic, generated by $\bar{1}$

all elements in $\mathbb{Z}_n$ is a multiple of 1.

G is cyclic $\iff$ $\gcd(n_i, n_j) = 1$ for $i \neq j$

the exponent of G

$$\exp(G) = \mathrm{lcm}(n_i \mid i = 1, \dots, k)$$

The element $(\bar{1}, \dots, \bar{1})$ has order $= \exp(G)$

in $\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$.

Prop.

If G is a finite ab. group then $\exists\, g \in G$ s.t.

ord g = $\exp(G)$.

Other description of $\mathbb{Z}_n^\times$

$\mathbb{Z}_n^\times = \{$ invertible elements in $\mathbb{Z}_n \}$

$= \{ \bar{a} \in \mathbb{Z}_n \mid \gcd(a, n) = 1 \}$

$= \{$ generators of $\mathbb{Z}_n \}$.

Pf: $\mathbb{Z}_n = \langle \bar{1} \rangle$

$\bar{a} \in \mathbb{Z}_n$ is a generator (i.e. $\langle \bar{a} \rangle = \mathbb{Z}_n$)

$\exists\, k \in \mathbb{Z}$ s.t. $k\bar{a} = \bar{1}$

$\bar{k}\,\bar{a} = \bar{1} \rightsquigarrow \bar{a}$ is invertible.

Prop. $\forall\, \bar{m} \in \mathbb{Z}_n$

$$\mathrm{ord}(\bar{m}) = \frac{n}{\gcd(m,n)}$$

Proof.

$$m \cdot \frac{n}{\gcd(m,n)} = \underbrace{\frac{m}{\gcd(m,n)}}_{\in \mathbb{Z}} \cdot n \equiv 0 \mod n$$

$\rightsquigarrow \dfrac{n}{\gcd(m,n)}$ is a multiple of ord (m)

Moreover if $km \equiv 0 \mod n \rightsquigarrow$

$n \mid km \qquad \dfrac{n}{\gcd(n,m)} \,\Big|\, k\dfrac{m}{\gcd(n,m)} \rightsquigarrow \dfrac{n}{\gcd(n,m)} \,\Big|\, k.$

relatively prime

<u>Consequence</u> for every divisor d of n there are exactly $\varphi(d)$ elements in $\mathbb{Z}_n$ having order d.

<u>Proof</u>

$n = dm$

$\operatorname{ord}(\bar{m}) = d$ in $\mathbb{Z}_n$ and for every k prime to d

$$o(\overline{km}) = \frac{n}{\gcd(km, n)} = o(m)$$

$$\gcd(km, n) = \gcd(km, dm) = m \underbrace{\gcd(k,d)}_{=1} \quad \boxtimes$$

<u>Corollary</u> : (Gauss)

$$\sum_{d \mid n} \varphi(d) = n$$