Definition 1 ($\mathbb{Z}_n^*$)**.** We define the *group of units modulo* n by

$$\mathbb{Z}_n^* = \{g \in \mathbb{Z}_n : \gcd(g, n) = 1\}.$$

This set is a group under multiplication mod n (every element has a multiplicative inverse). Recall that this group has order $\phi(n)$ (Euler phi function).

It follows from the Chinese Remainder Theorem, that the study of $\mathbb{Z}_n^*$ can be reduced to the cases when n is a prime power, $n = p^\alpha$.

Recalls: if p is a prime, the group $\mathbb{Z}_p^*$ is cyclic (as is the multiplicative group of any finite field). A generator of this group is called a *primitive element* mod p; (also called *primitive root* mod p).

Study of $\mathbb{Z}_{p^\alpha}^*$, p an odd prime

Lemma 1. *Let p be an odd prime and assume that $g \in \mathbb{Z}_{p^\alpha}^*$ has order $\phi(p^\alpha)$ (i.e. g is a generator of this group). Then the following holds:*

$$\text{If } g^{\phi(p^\alpha)} \not\equiv 1 \bmod (p^{\alpha+1}) \text{ then } g \text{ has order } \phi(p^{\alpha+1} \text{ in the group } \mathbb{Z}_{p^{\alpha+1}}^*.$$

Lemma 2. *Let p be an odd prime. Assume that g is a primitive element mod p with the property that $g^{p-1} = 1 + mp$ where m is an integer not divisible by p. Then g is a primitive element mod p^α for all $\alpha \geq 1$.*

Lemma 3. *Let p be an odd prime. There exists a primitive root g modulo p with the property*

$$g^{p-1} = 1 + pm \text{ where } m \text{ is an integer not divisible by } p.$$

Theorem 4. *Let p be an odd prime. Then*

(1) *the group $\mathbb{Z}_{p^\alpha}^*$ is cyclic;*
(2) *the group $\mathbb{Z}_{2p^\alpha}^*$ is cyclic.*

Study of $\mathbb{Z}_{2^\alpha}^*$

Note that the group $\mathbb{Z}_{2^\alpha}^*$ has $2^{\alpha-1}$ elements. The order of every element in the group will be a power 2^β, $\beta \leq \alpha - 1$.

Lemma 5. *Assume that $\alpha \geq 3$. Then there is no element of order $2^{\alpha-1}$ in $\mathbb{Z}_{2^\alpha}^*$. More precisely,*

$$a^{2^{\alpha-2}} \equiv 1 \bmod 2^\alpha \quad \text{for all odd integers } a.$$

Lemma 6. *The element 5 has order $2^{\alpha-2}$ in the group $\mathbb{Z}_{2^\alpha}^*$.*

Lemma 7. *-1 is not a power of 5 in $\mathbb{Z}_{2^\alpha}^*$.*

Theorem 8. *If $\alpha \geq 3$, the group $\mathbb{Z}_{2^\alpha}^*$ is not cyclic.*

In fact, the group is isomorphic to the group $\mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$.

It follows with little effort that

Theorem 9. *The group $\mathbb{Z}_n^*$ is cyclic if and only if $n = 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime.*