# Primitive Roots

Monday, October 13, 2025 9:49 AM

## Recall Cyclic Groups

Missing:
100# 1, ~~4~~, ~~6~~, 7, 13, 17, ~~18~~
200# 7, 14, 17, 18, 24, ~~28~~,
Ex #225 on 10/6, 10/8

Wed, October 15
500# 2, 6, 11, 14, 19, 21, 24, 26,
+B #524, 504

9] Thm:

Every subgroup of a cyclic group is cyclic.

10] Def$^n$. The generators of $\mathbb{Z}_n^*$ are called primitive elements of $\mathbb{Z}_n^*$ or primitive roots of $n$.

11] Thm: A positive integer $n$ has a primitive root iff $n = 2, 4, p^k$ or $2p^k$ where $p$ is an odd prime and $k \geq 1$.

e.g. $\mathbb{Z}_{50}^*$ $50 = 2 \cdot 5^2$ is cyclic $\Rightarrow$ it has $\varphi(20) = 8$ generators

$\mathbb{Z}_{100}^*$ is not cyclic, for $100 = 4 \cdot 5^2$

$\mathbb{Z}_{162}^*$ is cyclic, for $n = 2 \cdot 3^4$

$\mathbb{Z}_{16}^*$ is not cyclic, for $n = 2^4$, $2 \cdot 2^3$

$\mathbb{Z}_{12}^*$ is not cyclic, for $n = 4 \cdot 3$

12] Def$^n$. Let $G_1$ and $G_2$ be groups, and $\theta: G_1 \to G_2$ is a function. Then $\theta$ is said to be a group isomorphism if

① $\theta$ is a bijection, and

② $\theta(ab) = \theta(a)\,\theta(b)$, $\forall a, b \in G_1$.

In this case $G_1$ is said to be isomorphic to $G_2$, denoted $G_1 \cong G_2$.

Note: $\theta$ is a group homomorphism if ② holds.

In this case, $G_1$ is said to be isomorphic to $G_2$, $G_1 \cong G_2$.
Note: $\theta$ is a homomorphism if ② holds.

13] e.g.

$$\mathbb{Z}_4 \cong \mathbb{Z}_5^*$$

Proof: Let $\theta: \mathbb{Z}_4 \to \mathbb{Z}_5^*$ be a bijection defined by

| $a$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $\theta(a)$ | 1 | 2 | 4 | 3 |

e.g.

$$\mathbb{Z}_{17}^* \cong \mathbb{Z}_{16} \qquad \text{why?}$$

proof: Since $\langle 6 \rangle = \mathbb{Z}_{17}^*$

define $\theta: \mathbb{Z}_{16} \to \mathbb{Z}_{17}^*$ by

$$\theta(n) = 6^n$$

then $\theta$ is a group isomorphism.

$$\theta(i+j) = 6^{i+j} = 6^i \cdot 6^j = \theta(i) \cdot \theta(j)$$

14] e.g. (Exponential function for groups):

Let $a \in G$, then $\theta: \mathbb{Z} \to G$, defined by $\theta(n) = a^n$ is a group homomorphism.

For $\theta(i+j) = a^{i+j} = (a^i)(a^j)$

$$= \theta(i)\,\theta(j)$$

15] Prop: if $\theta : G_1 \to G_2$ is a homomorphism, then

① $\theta(e_1) = e_2$

② $(\theta(a))^{-1} = \theta(a^{-1})$

③ $\theta(a^n) = (\theta(a))^n \quad \forall\ n \in \mathbb{Z}$

16] Prop: if $\theta : G_1 \to G_2$ is a group isomorphism, then

① $\forall\ a \in G_1$, $\text{ord}(a) = \text{ord}(\theta(a))$

② if $G_1$ is abelian, then so is $G_2$.

③ if $G_1$ is cyclic, then so is $G_2$.