When checking whether a set G is a group, check whether it :

1. *Is closed under the operation:* Let $a, b \in G$. Is $a * b \in G$?

2. *Is associative:* Let $a, b, c \in G$. Does $a * (b * c) = (a * b) * c$?

3. *Has an identity:* Is there an element $e \in G$ such that for all $a \in G$, $e * a = a = a * e$?

4. *Has inverses:* Let $a \in G$. Is there an element $b \in G$ such that $a * b = e = b * a$?

1. Is $\mathbb{Z}_5$ under $\times$ mod 5 a group?

2. Write out the Cayley table for $U(12)$. Is $U(12)$ a group?

September 13, 2002

$\mathbb{Z}_5$ under $\times$ mod 5

1. **Closed?** Yes: the definition of multiplication mod 5 is that you always end up with a number in the set $\{0, 1, 2, 3, 4\}$.

2. **Associative?** Yes: modular multiplication is of course associative, since you can do it by simply multiplying the integers (which is associative) and then taking the result mod 5.

3. **Identity?** For all $a \in \mathbb{Z}_5$, $a \cdot 1 = a$ mod 5 and $1 \cdot a = a$ mod 5, so 1 acts as a multiplicative identity mod 5.

4. **Inverses?** For each $a \in \mathbb{Z}_5$, is there an a^{-1} such that $a \cdot a^{-1} = 1$? No! $0 \cdot b \neq 1$ for any b, so 0 does not have a multiplicative inverse!

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

$\cdot$ mod 12	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

1. **Closed under multiplication mod 12?** We can see by looking at the Cayley table that for any $a, b \in U(12), ab \in U(12)$.

2. **Associative?** Since multiplication is associative, and since $a mod 12 \cdot b mod 12 = (ab) mod 12$, multiplication mod 12 is also associative.

3. **Identity?** Multiplying by 1 mod 12 leaves every number unchanged, and so 1 is the identity.

4. **Inverses?** By looking at the Cayley table, I can see that each number has a unique inverse:

   $$(1)^{-1} = 1 \qquad (5)^{-1} = 5 \qquad 7^{-1} = 7 \qquad 11^{-1} = 11$$

   Notice: each number is its own inverse!