Ch 4 - Cyclic Groups.

Q1 Is $U(n)$ cyclic?

Consider $U(9) = \{1,2,4,5,7,8\}$. Is $U(9)$ cyclic?

Let's calculate: $\langle 2 \rangle = \{2^k \mid k \in \mathbb{Z}\}$

$$2^0 = 1$$
$$2^1 = 2$$
$$2^2 = 4$$
$$2^3 = 8$$
$$2^4 \equiv 2 \cdot 8 \pmod 9 \equiv 16 \pmod 9 \equiv 7$$
$$2^5 \equiv 2 \cdot 7 \pmod 9 \equiv 14 \pmod 9 \equiv 5$$
$$2^6 \equiv 2 \cdot 5 \pmod 9 \equiv 1 \pmod 9 \equiv 1$$
$$\left.\begin{array}{l} 2^7 \equiv 2 \\ \vdots \end{array}\right\}$$

repeats. we also get repeats for the negative powers. Do you see this?

$$2^{-1} \equiv 5 \pmod 9 \equiv 5$$
since $2 \cdot 5 \equiv 10 \equiv 1 \pmod 9$

etc.

From the above $\langle 2 \rangle = \{1,2,4,5,7,8\} = U(9)$ since 2 generates everything in $U(9)$, we can conclude $U(9)$ is cyclic.

Consider $U(8) = \{1,3,5,7\}$. Is $U(8)$ cyclic?

$3^2 \equiv 9 \equiv 1 \pmod 8$ i.e., $\langle 3 \rangle = \{1,3\}$
$5^2 \equiv 25 \equiv 1 \pmod 8$ i.e., $\langle 5 \rangle = \{1,5\}$
$7^2 \equiv 49 \equiv 1 \pmod 8$ i.e., $\langle 7 \rangle = \{1,7\}$

Hence, $U(8)$ is not generated by any of its elements. Thus, $U(8)$ is not cyclic. So the answer to this question is $\boxed{\text{no in general, but sometimes! when?}}$

The full answer of <u>when</u> $U(n)$ is cyclic will be an interesting result. To solve this we will need a special function called the Euler φ-function (or totient function). Using this function we will get an elegant result called the primitive root

Theorem: $U(n)$ is cyclic iff $n = 1, 2, 4, p^k$ OR $2p^k$, where p is an odd prime and $k \geq 1$.

So for example $9 = 3^2$ so $U(9)$ is cyclic (as we have seen)

but $8 = 2^3$ which is not of any of the above forms so $U(8)$ is not cyclic (as we have seen)

Cool huh!?

Q2 Find all the cyclic subgroups of $U(9)$, and find a generator for each of these cyclic subgroups.

$\boxed{\text{SOL}}$:

Notice that we have already shown $U(9) = \langle 2 \rangle$ so it is cyclic.

By the <u>Fundamental Theorem of Cyclic Groups</u>:

since $U(9) = \langle 2 \rangle$ and $|U(9)| = |\langle 2 \rangle| = 6 = n$

for all $k \mid n$, $U(9)$ has a unique cyclic subgroup H of order k. In particular $H = \langle 2^{6/k} \rangle$.

So the divisors of 6 are: 1, 2, 3 and 6.

<u>cyclic subgroup of order 1</u>: (generated always by the identity) $\{\langle 1 \rangle = \{1\}\}$ but also $2^{6/1} \equiv 2^6 \equiv 1 \pmod 9$ hence

<u>cyclic subgroup of order 2</u>: generated by $2^{6/2} \equiv 2^3 \equiv 8 \pmod 9$ indeed: $\langle 8 \rangle = \{1, 8\}$

<u>cyclic subgroup of order 3</u>: generated by $2^{6/3} \equiv 2^2 \equiv 4 \pmod 9$ indeed: $\langle 4 \rangle = \{1, 4, 7\}$

cyclic subgroup of order 6 : (we alread know $\langle 2\rangle = U(9)$) but

$2^{6/6} \equiv 2^1 \equiv 2 \pmod 9$ indeed

$\langle 2\rangle = \{1,2,4,5,7,8\}$

Q3 find all the generators of $U(9)$

SOL: we already found $\langle 2\rangle = U(9)$ to get the other generators we could try to compute $\langle n\rangle$ for each $n \in U(9)$, but is there a better method in general? we have a result:

Let $|a| = n$. Then $\langle a\rangle = \langle a^j\rangle \longleftrightarrow \gcd(n,j) = 1$

here $|2| = 6$ Then $\langle 2\rangle = \langle 2^j\rangle \longleftrightarrow \gcd(6,j) = 1$

so $j = 1$ or 5

hence $2^5 \equiv 32 \pmod 9 \equiv 5 \pmod 9$ will also generate the group. indeed:

$\langle 5\rangle = \langle 2\rangle = \{1,2,4,5,7,8\} = U(9)$

so 2 and 5 are the <u>only</u> generators of $U(9)$

Q4 Find all the generators of the cyclic subgroup of order 3 in $U(9)$.

SOL: In Q2 we found $\langle 4\rangle = \{1,4,7\}$ so the only other possibility is that 7 generates this, indeed $\langle 7\rangle = \{1,4,7\}$. so only 4 and 7

we can also get this by the same method as Q3:

$|\langle 4\rangle| = 3$, $\gcd(3,j) = 1 \longleftrightarrow j = 1,2$ so $\langle 4^2\rangle = \langle 7\rangle = \langle 4\rangle = \{1,4,7\}$

Q5 Find all the generators of the subgroup of order 10 in $\mathbb{Z}_{30}$.

SOL: $\mathbb{Z}_{30}$ is a cyclic group. (always $\mathbb{Z}_n = \langle 1 \rangle$)

$\mathbb{Z}_{30} = \langle 1 \rangle$ and $|\mathbb{Z}_{30}| = |\langle 1 \rangle| = 30$.

By the Fundamental Thm. of Cyclic Groups there is exactly 1 (cyclic) subgroup of order 10 since $10 \mid 30$. This is generated by: $\langle (30/10) 1 \rangle$

(This is the result of the thm in additive notation. $\langle a^{n/k} \rangle$ is $\langle (n/k) a \rangle$ in additive notation)

hence

$$\langle (30/10) 1 \rangle = \langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27\}$$

to find the others use the same idea as Q3/Q4:

$$|3| = |\langle 3 \rangle| = 10 \quad \text{so} \quad \langle 3 \rangle = \langle \underbrace{j3}_{\text{(again additive notation)}} \rangle \longleftrightarrow \gcd(10, j) = 1$$

so $j = 1, 3, 7, 9$

$$\boxed{\langle 3 \rangle = \langle 9 \rangle = \langle 21 \rangle = \langle 27 \rangle}$$

so the generators are 3, 9, 21 and 27 for the subgroup of order 10 in $\mathbb{Z}_{30}$.

(Q6) How many generators does $\mathbb{Z}_p$ have if p is prime?

SOL:

Recall, $\mathbb{Z}_n = \langle j \rangle \longleftrightarrow \gcd(n,j) = 1$

$\mathbb{Z}_p = \langle j \rangle \longleftrightarrow \gcd(p,j) = 1$

well every $1 \leq j \leq p-1$ is relatively prime to p

so

$1, 2, 3, \dots, p-1$ are generators.

$\boxed{\text{Answer: } p-1}$

(Q7) How many generators does $\mathbb{Z}_{p^2}$ have if p is prime?

SOL:

what j are relatively prime with p^2?

It may be easier ~~ten~~ find the j's that are NOT relatively prime instead:

$$\left.\begin{array}{l} p \\ 2p \\ 3p \\ \vdots \\ (p-2)p \\ (p-1)p \\ pp = p^2 \equiv 0 \pmod{p^2} \end{array}\right\}$$

these are elements of $\mathbb{Z}_{p^2}$ that are not relatively prime with p^2 since the share factors with p^2.

How many are there?

total: p

how many elements in $\mathbb{Z}_{p^2}$? $|\mathbb{Z}_{p^2}| = p^2$ so

total number of generators is $\boxed{p^2 - p}$

(Q8) How many generators does $\mathbb{Z}_{p^r}$ have if p is prime?

SOL: same idea as Q7:

$$\left.\begin{array}{l} p \\ 2p \\ 3p \\ \vdots \\ p^2 \\ (p+1)p \\ (p+2)p \\ \vdots \\ (p+p)p = 2p^2 \\ (2p+1)p \\ \vdots \\ (2p+p)p = 3p^2 \\ \vdots \\ p^{r-1}p = p^r \equiv 0 \pmod{p^r} \end{array}\right\}$$

all share factors with p^r

total of: p^{r-1}

total # of generators: $\boxed{p^r - p^{r-1}}$

(Q9) Use this idea from Q8 to find the number of generators for $\mathbb{Z}_{pq}$ where $p \neq q$ AND both p and q are prime.