~~§1.6 - Cyclic Groups~~

~~1.6 - Cyclic Groups~~

~~Thm. Every cyclic group is abelian.~~

~~pf: Let $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. Then $a^{n_1} a^{n_2} = a^{n_1+n_2} = \dots$~~

(<u>Division Algorithm for $\mathbb{Z}$</u>) If m is a positive integer and n is any integer, then there exist unique integers q and r such that

$$n = mq + r \quad \text{and} \quad 0 \leq r < m$$

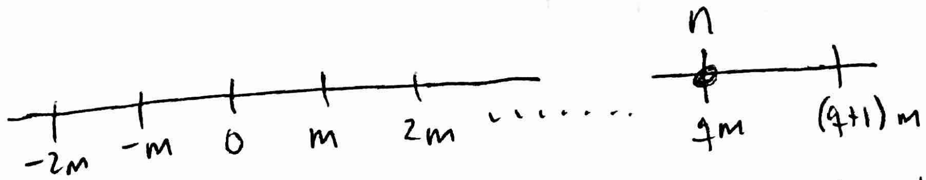
<u>pf:</u> One the real axis, mark off the multiples of m and the position of n. Now either

① n falls on a multiple qm of m and r can be taken to be 0

<u>or</u>

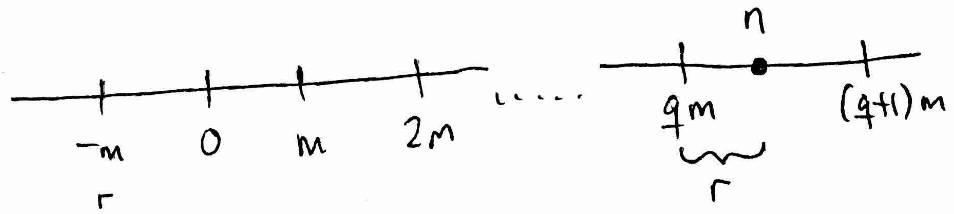
② n falls between two multiples of m.

<u>case 1:</u>

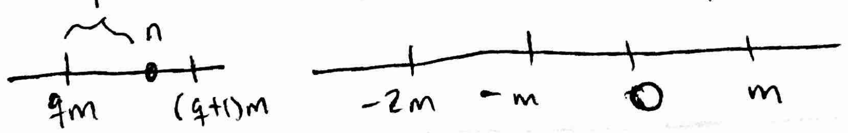


In case 2, let qm be the first multiple of m to the left on n. r is shown in the following diagrams.

<u>case 2:</u>
$q \geq 0$



<u>case 2:</u>
$q < 0$



24''

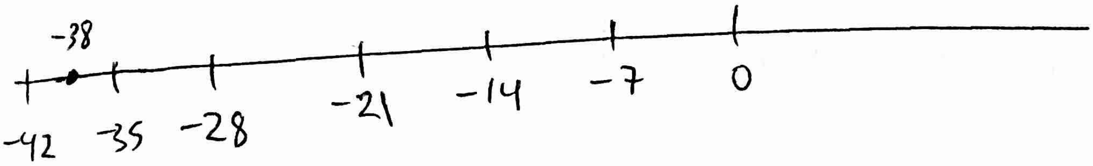
Note that $0 \le r < m$. In case 1, uniqueness of m & r is clear. In case 2, there is a unique multiple qm of m to the left of n at a distance less than m from n. $\boxed{/\!/}$

---

ex: Find the quotient q and remainder r when 38 is divided by 7.

$$38 = 7(\underset{q}{\underset{\uparrow}{5}}) + \underset{r}{\underset{\uparrow}{3}}$$

ex: Do the same when dividing -38 by 7.



$$-38 = 7(-6) + 4$$

$$q = -6, \quad r = 4$$