Greatest Common Divisor

$\gcd(8, 12) = 4$

$\gcd(80, 30) = 10$

$8 = 2 \cdot 2 \cdot 2$
$12 = 3 \cdot 2 \cdot 2$

$80 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5$
$30 = 3 \cdot 2 \cdot 5$

Here's the approach the text takes:

$\gcd(8, 12) = 4$

$H = \{ m8 + n12 \mid m, n \in \mathbb{Z} \}$ is subgroup of $\mathbb{Z}$

$H = \{ \ldots 0, 4, 8, 12, 16, 20, 24, 28 \ldots \} = \langle 4 \rangle$

Definition $\gcd(r, s)$ = positive generator of $H = \{ mr + ns \mid m, n \in \mathbb{Z} \}$.

Definition r and s are **relatively prime** if $\gcd(r, s) = 1$ (i.e. if $H = \mathbb{Z}$).

(i.e. if there are integers m, n with $mr + ns = 1$.)

$9 = 3 \cdot 3 \cdot 3$
$50 = 2 \cdot 2 \cdot 5 \cdot 5$

Ex $\gcd(9, 50) = 1$

so 9 & 50 are rel. prime.

Note: $-11 \cdot 9 + 2 \cdot 50 = 1$.

Subgroups of finite cyclic groups

Now that we've got a grip on the subgroups of $\mathbb{Z}$, lets turn to subgroups of finite cyclic groups, i.e. those isomorphic to $\mathbb{Z}_n$.

An example illustrates the general principal.

$G = \mathbb{Z}_6$

$\langle 0 \rangle = \{0\}$ ← order $1 = \frac{6}{\gcd(6,0)}$

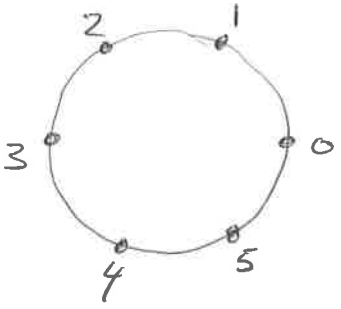
$\langle 1 \rangle = \{0,1,2,3,4,5,6\}$ ← size $6 = \frac{6}{\gcd(6,1)}$

$\langle 2 \rangle = \{0,2,4\}$ ← size $3 = \frac{6}{\gcd(6,2)}$

$\langle 3 \rangle = \{0,3\}$ ← size $2 = \frac{6}{\gcd(6,3)}$

$\langle 4 \rangle = \{0,4,2\}$ ← size $3 = \frac{6}{\gcd(6,4)}$

$\langle 5 \rangle$ $\{0,5,4,3,2,1\}$ ← size $6 = \frac{6}{\gcd(6,5)}$



This illustrates the following Theorem, proved in the text.

Theorem Suppose $G = \langle a \rangle$ is a cyclic group, $|G| = n$, and $H = \langle a^s \rangle \leq G$. Then $|H|$ ~~has~~ $\frac{n}{\gcd(n,s)}$ ~~elements~~.

Also, $\langle a^s \rangle = \langle a^t \rangle \iff \gcd(n,s) = \gcd(n,t)$

or with additive notation: $H = \langle sa \rangle$ has $\frac{n}{\gcd(n,s)}$ elements

and $\langle sa \rangle = \langle ta \rangle \iff \gcd(n,s) = \gcd(n,t)$.

Ex/ Consider $H = \langle 66 \rangle \leq \mathbb{Z}_{90} = \langle 1 \rangle$

$|H| = \frac{90}{\gcd(90,66)} = \frac{90}{6} = 15$

What are the generators of H? $H = \langle \underbrace{66 \cdot 1}_{s\,a} \rangle = \langle \underbrace{k \cdot 1}_{t\,a} \rangle$ k is a generator provided $\gcd(66,66) = \gcd(90,k)$

$s = 3 \cdot 2 \cdot 11$

$t = 3 \cdot 2$

66, 12, 24, 6, ...

$90 = 3 \cdot 3 \cdot 2 \cdot 5$

$66 = 3 \cdot 2 \cdot 11$ } gcd is 6

$90 = 2 \cdot 3 \cdot 3 \cdot 5$

1 → 6
2 → 12
4 → 24
8 → 48
7 → 42
11 → 66
13 → 78
14 → 84

Ex $H = \langle 66 \rangle \leq \mathbb{Z}_{90}$

$$|H| = \frac{90}{\gcd(90, 6)} = \frac{90}{6} = 15.$$

What are the generators of H?

Answer: $\langle k \rangle$ where $\gcd(90, 66) = \gcd(90, k)$

$$6 = \gcd(90, k)$$

$k = 2 \cdot 3 \cdot 1 = 6$
$k = 2 \cdot 3 \cdot 2 = 12$
$k = 2 \cdot 3 \cdot 4 = 24$
$k = 2 \cdot 3 \cdot 8 = 48$
$k = 2 \cdot 3 \cdot 7 = 42$

$90 = 2 \cdot 3 \cdot 3 \cdot 5$
$k = 2 \cdot 3$?

i.e. $H = \langle 66 \rangle = \langle 6 \rangle = \langle 12 \rangle = \langle 24 \rangle = \langle 48 \rangle = \langle 42 \rangle \ldots$

$H = \{ 0, \boxed{6}, \boxed{12}, 18, \boxed{24}, 30, 36, 42, \boxed{48}, 54, 60, \boxed{66}, 72$
$78, 84 \}$