Question. Do the relatively prime elements of $(Z_k, *)$ form a group?

What does rel prime mean

$\{r \mid GCD(k,r) = 1\}$

Group Prop
- $*$ is assoc ✓
- identity ✓ 1 is rel prime to K
- inverse
- closed ✓ r, s are rel prime to K

r*s is rel prime to K
why?

r is relatively to K
What is r^{-1}?

Subgroups $G \supseteq H$ $h_1 * h_2 \in H$

$1 \in H$

$h \in H \Rightarrow h^{-1} \in H$

$(Z, +)$

What are the subgroups of $(Z, +)$?

Even are a subgroup:
odd are not. Closed under +, 0 ∉ odd

$(nZ, +)$ is a subgroup. Even $2Z$

$Z = 1Z$

$3Z = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$

Question are nZ the only subgroups of Z?

Extended GCD $(a, b \in N)$

~~let GCD(a,b)~~

GCD(0,0) not defined
GCD(0,5) = 5

Extended GCD ($a, b \in \mathbb{N}$)

```
def GCD(a,b):
    if (a%b)==0:
        return b
    :
    return GCD(b, a%b)
```

GCD(0,0) not defined

GCD(0,5) = 5

Goal $g = GCD(a,b)$ $\exists\ s,t \in \mathbb{Z}$, s.t. $g = sa + tb$

```
def EGCD(a,b):
    if (a%b)==0:
        return (b,0,1)
    else
        temp = EGCD(b, a%b)
        return (temp[0], temp[2], temp[1] - (a//b) * temp[2])
```

returns (g, s, t)

g = sa + tb.

```
# b = s*a + t*b
# r = a%b
temp = (g, k, q)
= EGCD(b, r)
```

① $kb + qr = g$

② $sa + tb = g$

③ $r = a - wb$

$a = wb + r$

① + ③

$\Rightarrow$

$kb + q(a - wb) = g$

$qa + (k - wq)b = g$

$w = a//b$

What is a^{-1} in $(\mathbb{Z}_k^*, *)$ $\quad \mathbb{Z}_k^* = \{y \in \mathbb{Z}_k \mid GCD(k,y) = 1\}$

$GCD(k,y) = 1$ $\exists$ s, t s.t. $sk + ty = 1$

Take $\bmod k$ $\quad 0 + (ty) \bmod k = 1$

Solution to Quest 1

Solution to Quest 1

Question 2?

$G \subseteq \mathbb{Z}_n$ G is a subgroup $\neq \{0\}$

Pick $k = \min\{y \in G \mid y > 0\}$ $\mathbb{N}$ is well-ordered.

A well-ordered set is a set with a partial order s.t. every non-empty subset has a smallest element.

$\mathbb{N}$ is well-ordered & every non-empty subset of a well-ordered set is well-ordered

G has a smallest positive value call it v

Let $w \in G$, $w > 0$. $w \geq v$ Why?

$w = qv + r$. If $r = 0$, w is a multiple of v

if $r \neq 0$, $v > r > 0$, $r \in G$ $r = w - qv$

impossible so $r = 0$

$G = v\mathbb{Z}$

Let G be a group and H a subgroup.

Let $g \in G$, what does gH look like?

$gH = \{gh_1, gh_2, \ldots, gh_k\}$ where $H = \{h_1, \ldots, h_k\}$

are these all different?

$gh_i = gh_k$

$g^{-1}gh_i = g^{-1}gh_k$

$h_i = h_k$

is $gH = H$ iff $g \in H$

What about $gH = kH$

$g \in gH$ $ge = g$ $k \in kH$

$g = kh$ for some $h \in H$

$k^{-1}g \in H$

$z \in gH$ & $z \in kH$ claim $gH = kH$

$z = gh_1$ $z = kh_2 = gh_1$

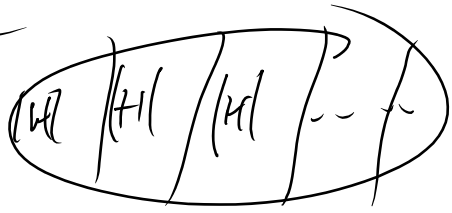
$g = kh_2h_1^{-1}$

$gh_3 = k(h_2h_1^{-1}h_3)$ $k = gh_1h_2^{-1}$

$kh_4 = gh_1h_2^{-1}h_4$ $gH = kH$

gH is a called a coset. $|gH| = |H|$

Cosets form a partition



$G = \bigcup_{g \in G} gH$ $g \in gH$

$\frac{|G|}{|H|}$ = an integer

$|G|$ is a prime the only subgroups of G are $\{e\}$ and G.

---

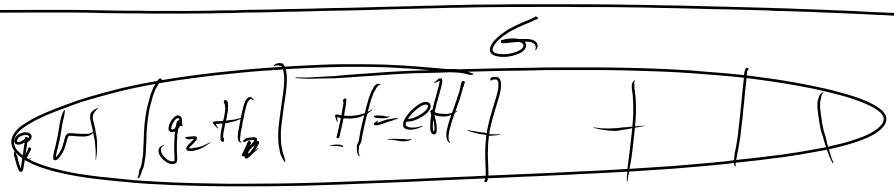
order(H) | order(G) if $H \leq G$

$g \in G$, order(g) | order(G) $\{1, g, g^2, \ldots, g^{k-1}, g^k = 1\}$

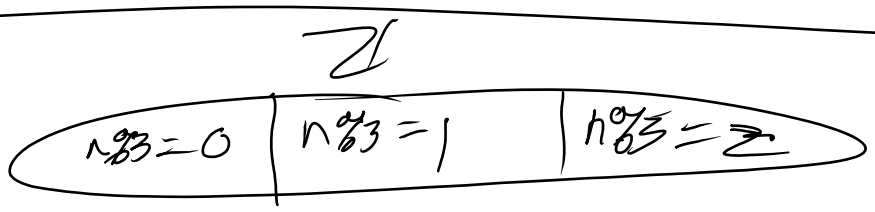
order$(\{1, g, \ldots, g^{k-1}\}) = k =$ order(g)

order(g) | order(G)

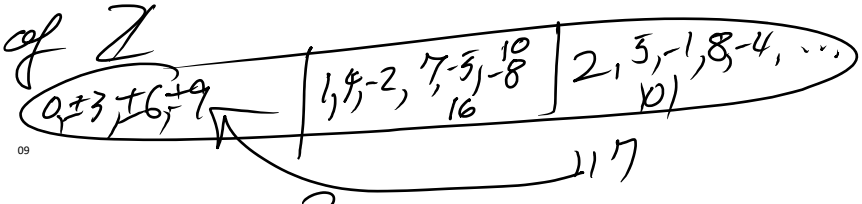
$H < G$



$\mathbb{Z}_3$

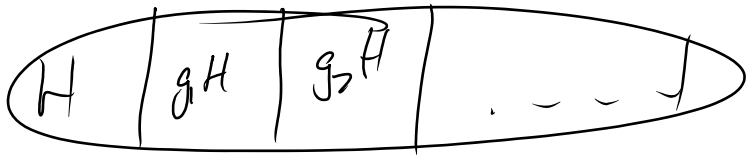


$3\mathbb{Z}$ is a subgroup of $\mathbb{Z}$



09

$\{0,1,2\}$



$g_1H \cdot g_2H = g_1g_2H$?

$gH \cdot kH = gkH$

$gh_1 \cdot kh_2 = gkh_3$