Q1. $\phi\left(\prod_{i=1}^{r} p_i^{a_i}\right) = \prod_{i=1}^{r} p_i^{a_i-1}(p_i-1).$

$\sum_{i=1}^{r}$

$$\phi(36) = \phi(2^2 \cdot 3^2)$$
$$= 2^1(2-1)\,3^1(3-1)$$
$$= 2 \cdot 3 \cdot 2 = 12.$$

Q2 $\phi(p) = p-1$, for p prime.

Q3 Claim $\phi(n) = \frac{n}{2} \iff n = 2^k$, for some $k \geq 1$.

Proof: "$\Leftarrow$" If we assume $n = 2^k$, $k \geq 1$

then $\phi(2^k) = 2^{k-1} \cdot (2-1)$
$$= 2^{k-1}$$
$$= \frac{2^k}{2}.$$

So $\phi(n) = n/2$.

"$\Rightarrow$" "$\phi(n) = \frac{n}{2} \Rightarrow n = 2^k$"

Try proving the contrapositive.

i.e. the statement "$\boxed{n \neq 2^k}$ for any k then

So we assume n is not a power of 2.

$\phi(n) \neq \frac{n}{2}$ "

ie. $n = 2^k \cdot m$, where $k \geq 0$, and $m > 1$ is an odd integer, ie. $2 \nmid m$.

Can use the fact that ϕ is multiplicative to show

$$\phi(2^k \cdot m) = \phi(2^k) \cdot \phi(m), \text{ since } \gcd(2^k, m) = 1$$
$$\geq 2^{k-1} \cdot 2 = 2^k$$

so $m \geq 3$ and so $\phi(m) \geq 2$.

as $\gcd(1, m) = \gcd(m-1, m) = 1$

So if $\boxed{\phi(n) = \phi(2^k m)} \geq 2^k = \frac{2^k m}{m} = \boxed{\frac{n}{m}}$

but $m \geq 3$ $\qquad \frac{n}{2} = 2^{k-1} m$

So $\phi(n) \neq \frac{n}{2}$

Oooops

$$\phi(n) = \phi(2^k m)$$
$$= \phi(2^k)\phi(m)$$
$$= 2^{k-1}\phi(m) < 2^{k-1} m = \frac{n}{2}$$

Since $m \geq 3$, we know $\phi(m) < m$

(the largest $\phi(m)$ could be would $m-1$ which happens when m is prime)

So in particular $\phi(n) \neq \frac{n}{2}$.

This completes the "$\Rightarrow$" proof.

Q4 $U(15) = \mathbb{Z}_{15}^{\times} = \{1, 2, 4, 7, 8, 11, 13, 14\}$

This is the group of integers, coprime to 15, under multiplication modulo 15.

In $U(15)$ simplify for $a, b \in U(15)$

$$a^{24} b^{15}$$

Think of applying Euler's theorem

$$\phi(15) = \phi(3 \cdot 5) = 2 \cdot 4 = 8$$

Euler's theorem says for any $a \in U(15)$

$$a^{8} \equiv 1 \pmod{15}$$

$24 = 3 \cdot 8$
$15 = 8 + 7$.

$$\begin{aligned} a^{24} b^{15} &= (a^8)^3 b^8 \cdot b^7 \\ &= 1^3 \cdot 1 \cdot b^7 \\ &= b^7 \\ &= b^{-1} \end{aligned}$$

$b^7 b = b^8 = 1$

Q6] What's the $\underbrace{\text{unit digit}}_{\text{Rightmost}}$ of 3^{100}?

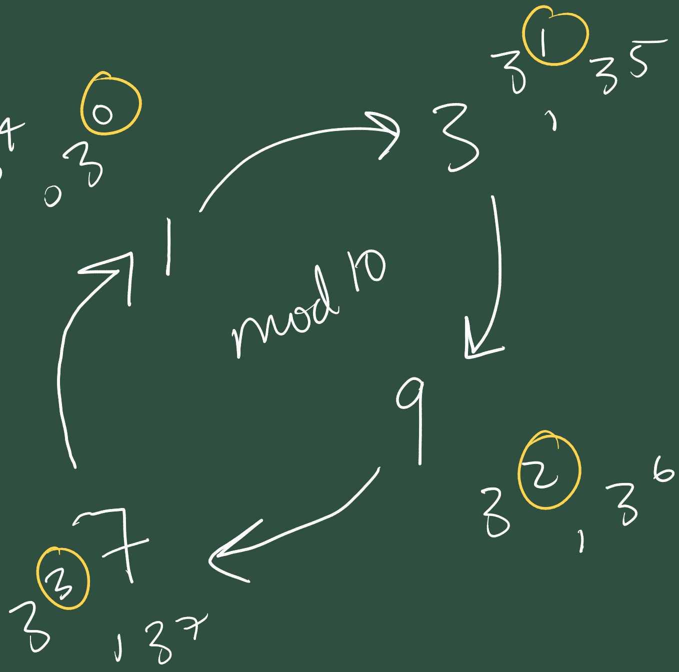
unit digit of x is x modulo $\underrightarrow{10}$.

$$3^{100} \equiv ? \mod 10$$

$$\phi(10) = \phi(2 \cdot 5) = 4$$

$$\Rightarrow 3^4 \equiv 1 \mod 10, \quad 3^4 = 81$$

$3^{100}, \ldots\ldots, 3^8, 3^4, 3^0$



well
$100 \equiv 0 \pmod 4$

So $3^{100} \equiv (3^4)^{25}$

$$\equiv 1^{25} \equiv 1 \pmod{10}$$

Chap 3 of AATA.

& Group, subgroups.

$a = a^{-1}$

$|||$

$a^2 = e$

Q31 Suppose G is a group where $a^2 = e$ for all $a \in G$.

Claim G is abelian.

i.e. for all $x, y \in G$ $xy = yx$

Proof Let $x, y \in G$

$xy = (xy)^{-1}$, because

$= y^{-1} x^{-1}$, true for all groups. and in the world generally

since $y = y^{-1}$, $x = x^{-1}$

$= yx$,

For instance. $U(8)$ this is true.

$U(8) = \{1, 3, 5, 7\}$

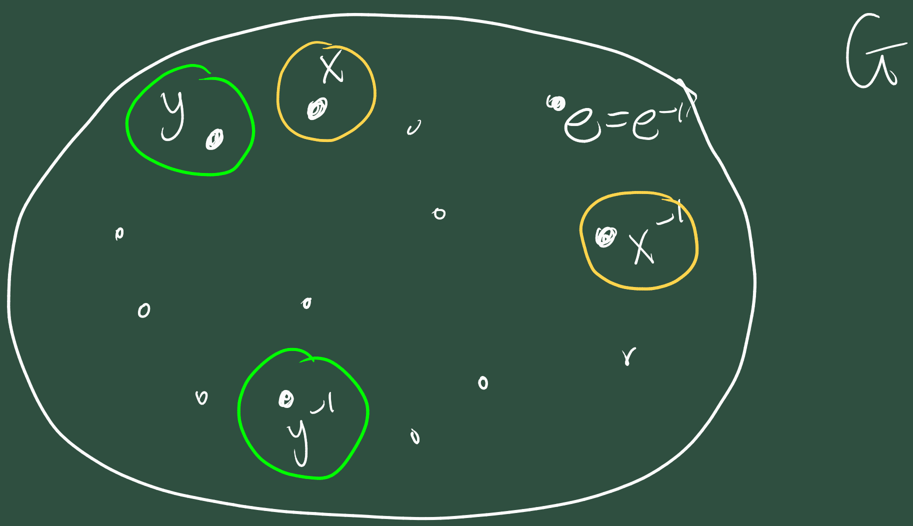
$1 = 1^2 = 3^2 = 5^2 = 7^2$, $3^{-1} = 3$, $5^{-1} = 5$

Q32 Assume G is a finite group of even order, i.e. even number of elements in G.

Claim there is some element a in G

$a \neq e$, $a^2 = e \Leftrightarrow a = a^{-1}$

Proof: "Think Noah's Ark" ie.
idea of ~~co~~ collecting things in pairs.



For $x \in G$, if $x \neq x^{-1}$, then we can identify the pair (x, x^{-1}) as two of the elements of G. We already have e as a self-inverse element. So since $|G|$ is even, we must have an odd number of $a \in G$ where $a \neq e$ and $a = a^{-1}$.

$\boxed{Q33}$ Suppose $(ab)^2 = a^2 b^2$ for all $a, b \in G$.

Claim: G is abelian

Let $x, y \in G$.

$xy =$

$= yx$

Sketching

$(xy)^2 = x^2y^2$, $(yx)^2 = y^2x^2$.

$(\cancel{xy})$ $(xy)^2 = \boxed{xyxy = x^2y^2.}$

$\Rightarrow x^{-1}xyxy = x^{-1}x^2y^2$

$\Rightarrow yxy = xy^2$

$\Rightarrow yxyy^{-1} = xy^2y^{-1}$

$\Rightarrow yx = xy$

So G is abelian.

$\boxed{Q45}$ Let H, K be subgroups of a group G.

Claim: $H \cap K$ is a subgroup of G

Proof: Use prop. 3.30

1. Claim: $e \in H \cap K$. ✓

Proof: $e \in H$, $e \in K$, since both are subgroups

2. Let $x, y \in H \cap K$ $\qquad xy \in G$.

$\Rightarrow x, y \in H$ and $x, y \in K$.

$\Rightarrow xy \in H$ and $xy \in K$, since H, K are both subgroups.

$\Rightarrow xy \in H \cap K$.

So $H \cap K$ is closed under the operation

3. Let $x \in H \cap K$.

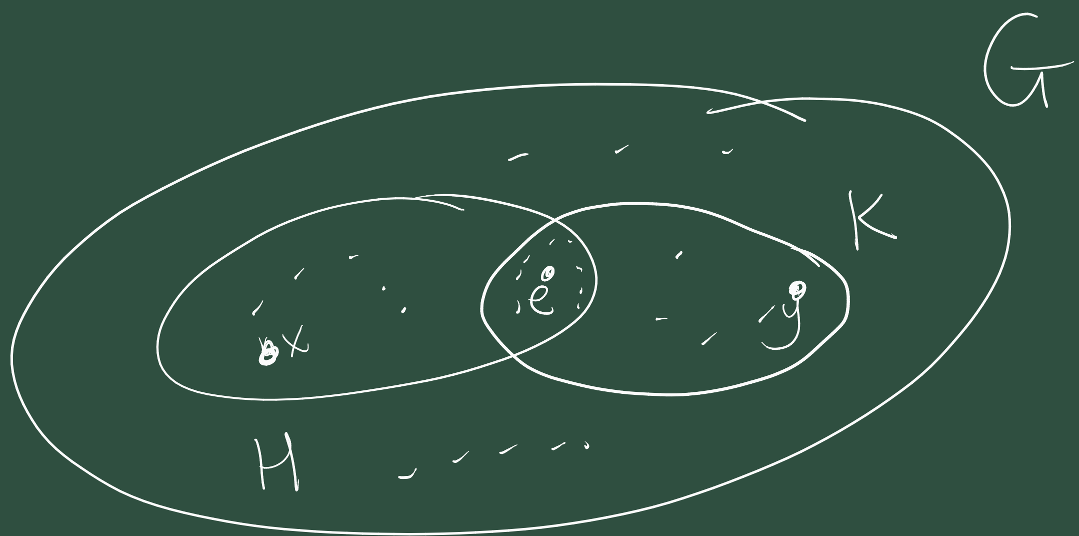
$\Rightarrow x \in H$ and $x \in K$

$\Rightarrow x^{-1} \in H$ and $x^{-1} \in K$, both subgroups.

$\Rightarrow x^{-1} \in H \cap K$

So all 1-3 are true for $H \cap K$

So by Prop 3.30 $H \cap K$ is a subgroup of G.



Q46 What about unions.

Consider: " If H and K are subgroups then $H \cup K$ is a subgroup "

Try and prove this with Prop 3.30

1. $e \in H \cup K$ because $e \in H$. ✓

3. If $x \in H \cup K$

$\Rightarrow x \in H$ or $x \in K$

$\Rightarrow x^{-1} \in H$ or $x^{-1} \in K$

$\Rightarrow x^{-1} \in H \cup K$ ✓

2. Let $x, y \in H \cup K$.

$\Rightarrow (x \in H$ or $x \in K)$ and $(y \in H$ or $y \in K)$.

FAILED

$xy \in G$

$\Rightarrow xy \in H$ or $xy \in K$.

$\Rightarrow xy \in H \cup K$.

We can't complete the derivation in the cases x, y are not in the same subgroup.

Can we exhibit a counter-example from our experience of groups.

Consider $U(8) = \{1, 3, 5, 7\}$

mult. mod 8.

$H = \{1, 3\}$ $\quad K = \{1, 5\}$

are subgroups,

but

$H \cup K = \{1, 3, 5\}$

is not a subgroup. as it is not

closed since $3 \cdot 5 = 7 \notin H \cup K$