339 Review

1. $d = \gcd(a,b)$

So $d = as + bt$ for some s,t. (d minimal)

$= a'ds + b'dt$

or $1 = a's + b't$

so $\gcd(a',b') \leq 1$ but must then be 1

2. $(23 \cdot 27) \bmod 20 = 3 \cdot 7 \bmod 20 = 1$

3. Say $a \sim b$ if a beats b

Then its worse if $a \sim b$ if a beats or ties b

Then not transitive

4. if $a \sim b \iff (a-4) \bmod n = 0$

then $a \sim 3 \iff (a-3) \bmod n = 0$

or $a - 3 = nq$

or $a = 3 + nq$ q any integer

5. $r f r^2 f r^3 f r^4 f r^{-4}$

$= r f r^2 f r^3 r^{-4} f f r^{-4}$

$= r f r^2 f r^{-1} r^{-4}$

$= r f r^3 r^2 f r^{-5}$

$= r f r^7 f = r^{-6} f^2 = r^{-6}$.

6. $U(n) = \{a : \gcd(a,n)=1,\ 0 \le a < n\}$.

Under $*$! - forgot to mention this

1) identity $e=1$ as $1 \cdot a = a \cdot 1 = a$ for any integer, in particular these

2) inverse. by commutivity of multiplication modulo n we only need to show for each a in $U(n)$ there exists b w/ $ab \bmod n = 1$.

but $\gcd(a,n)=1$ implies there exists s,t w/

$1 = as + tn$

so $sa \bmod n = 1$. take $b = s \bmod n$.

3. associativity comes for free.

so $\overline{T}_{ab} \circ \overline{T}_{a'b'} = \overline{T}_{a+a', b+b'}$ so the operation is closed.

Also the operation is commutative as $+$ is, and the operation (composition) is associative.

what's left? an inverse and identity.

we verify $\overline{T}_{0,0} = e$ as

$\overline{T}_{a,b} \circ \overline{T}_{0,0} = \overline{T}_{a+0, b+0} = \overline{T}_{a,b}$

Also $T_{-a,-b}$ is an inverse to $T_{a,b}$ as

$$T_{a,b} \circ T_{-a,-b} = T_{a-a,b-b} = T_{0,0}$$

8. Suppose e, e' both think they are an inverse

Then $e = ee'$ as e' is a right inverse

and $ee' = e'$ as e is a left inverse

so $e = ee' = e'$ and we've shown there's only one.

9. ~~$G \subseteq \mathbb{Z}$~~ Notice $G \subseteq \mathbb{R} \setminus \{0\}$, $*$ [Reals without 0 under multiplication is a group] so we only need to show closure and inverses

if $a = 3^m 6^n$, $b = 3^{m'} 6^{n'}$

then $ab = 3^m 6^n \cdot 3^{m'} 6^{n'}$

$= 3^{m+m'} 6^{n+n'}$ ⊛ is in G

as well, $\tilde{a} = 3^{-m} 6^{-n}$ is in G and

$$a\tilde{a} = 3^m 6^n \cdot 3^{-m} 6^{-n} = 3^{m-m} 6^{n-n} = 1 \cdot 1 = 1$$

Similarly, by commutivity $\tilde{a}a = ⊛$ so $\tilde{a}$ is the inverse of a.

in Z_7 we $a \equiv b$ if $a \bmod 7 = b \bmod 7$ (1)

$1 \cdot 5 = 5$

$2 \cdot 5 = 10 \equiv 3$

$3 \cdot 5 \equiv 3+5 = 1$

$4 \cdot 5 = 6$

$5 \cdot 5 = 5+6 = 11 \equiv 4$

$6 \cdot 5 = 9 \equiv 2$

$7 \cdot 5 = 7 \equiv 0$ pone $|5| = 7$

in $U(19)$ $5 = 5$

$5^2 \equiv 25 \equiv 6$

$5^3 = 30 \equiv 11$

$5^4 = 55 \equiv$ ~~-15~~ $\equiv -2$

$5^5 \equiv 9$

$5^6 \equiv 45 \equiv 7$

$5^7 \equiv 35 \equiv -3$

$5^8 \equiv -15 \equiv 4$

$5^9 \equiv 20 \equiv 1$. $|5| = 9$.

in $\mathbb{Z}$ $\langle 5 \rangle = \{ \ldots, -10, -5, 0, 5, 10, 15, \ldots \}$

= infinite.

11 D_3 (noncommutative) $\mathbb{Z}_6$ (cyclic) -5

12. H = center of G !

13. We need closure to make a subgroup as G is finite

so we need e, r^4, f, r^4f and that's it

as $fr^4 = r^{-4}f = r^4f$

and $r^4f\,r^4f = r^4r^{-4}ff = e$.

14. Recall if $\mathbb{Z}_n$ $|a| = \frac{lcm(a,n)}{a} = \frac{an}{gcd(a,n)}$

So $|3| = \frac{30}{gcd(3,30)} = \frac{30}{3} = 10$ $\quad |6| = \frac{30}{gcd(6,30)} = \frac{30}{6} = 5$

$|4| = \frac{30}{gcd(4,30)} = \frac{30}{2} = 15$ $\quad |7| = \frac{30}{gcd(7,30)} = \frac{30}{1} = 30$

$|5| = \frac{30}{gcd(5,30)} = \frac{30}{5} = 6$

15. In $\mathbb{Z}_{30}$ we can count the following

3, 27, 9, 21

we need $\frac{30}{gcd(i,30)} = 10$ so $gcd(i,30) = 3$

so $i = 3 \cdot j$ when 2, 5 do not divide j.