Office Hours Final:

Thurs Dec 11 4:00-6:00

Fri Dec 12 1:00-2:00 *

Fri Dec 12 7:00-MIDNIGHT? (Twitch)

Sat Dec 13 2:30-4:30.

3.a. List all elements $[x] \in \mathbb{Z}_{13}$ s.t. $[5][x]^2 = [6]$.

Approach: Find $[5]^{-1}$

Multiply both sides by $[8]$:

$$[x]^2 = [48] = [9].$$

$\therefore [x] = [\pm 3] = [3]$ or $[10]$.

These are the only ones since the polynomial $x^2 - 9$ over $\mathbb{Z}_{13}$ has at most 2 roots since $\mathbb{Z}_{13}$ is a field.

3.b. Solve the pair of congruences

$x \equiv 5 \bmod 9$ & $10x \equiv 6 \bmod 28$

$x = 5 + 9k$ for some $k \in \mathbb{Z}$.

$10(5+9k) \equiv 6 \bmod 28$

$50 + 90k \equiv 6 \bmod 28$

$6k \equiv -44 \bmod 28$

$6k \equiv 12 \bmod 28$

$6k + 28y = 12$

$3k + 14y = 6$

LDE 2 $k = 2 + 14n$. $\forall n \in \mathbb{Z}$. (General solution)

$y = 0 - 3n$

$\therefore k \equiv 2 \bmod 14$

ie $k = 2 + 14\ell$ for some $\ell \in \mathbb{Z}$.

$\therefore x = 5 + 9k = 5 + 9(2 + 14\ell)$

$= 23 + 126\ell$

$\therefore x \equiv 23 \bmod 126$.

6.a. Determine the number of positive integers a s.t. $a \mid 9!$ & $\gcd(a, 3600) = 180$.

$3600 = 36 \cdot 100 = 6^2 \cdot 10^2 = 2^4 \cdot 3^2 \cdot 5^2$

$180 = 18 \cdot 10 = 2^2 \cdot 3^2 \cdot 5$

$9! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 = 2^7 \cdot 3^4 \cdot 5 \cdot 7$

B: $180 \mid a$ ie $a = 2^2 \cdot 3^2 \cdot 5 \cdot N$ for some $N \in \mathbb{Z}$

Note $2 \nmid N$ & $5 \nmid N$ (GCDPF)

Since $N \mid 9!$, $3 \mid N$ and/or $7 \mid N$.

Combining: $N \mid 3^2 \cdot 7$

DFPF $\Rightarrow$ # of divisors of $3^2 \cdot 7$ is

$(2+1)(1+1) = 6$.

6.b. Prove that

$$\gcd(5^{98}+3,\ 5^{99}+1) = 14.$$

$5^{99}+1 = 5(5^{98}+3) - 14$ So by GCDUR:

$\gcd(5^{98}+3,\ 5^{99}+1) = \gcd(5^{98}+3,\ -14)$

WANT = 14

Note $215^{98}+3$. WANT $7 \mid 5^{98}+3$

ie WANT $5^{98}+3 \equiv 0 \mod 7$

$5^{98}+3 \equiv (5^6)^{16}\cdot 5^2 + 3 \mod 7$ $\because \gcd(5,7)=1$.

$\equiv 1^{16}\cdot 25 + 3 \mod 7$ (FLT)

$\equiv 0 \mod 7$. ✓

4.b.

Determine the private key (n, d) which corresponds to the public key $(n, e) = (253, 29)$