Tutorial 4 : Discussion / Hints

2.1

First focus on sharing s s.t. (any two dogs) and (any two cats) can recover s.

This problem is an example of 2-level secret sharing.

Hint 1 : How to share a secret s among t 'groups' such that they recover it only if all t are present?

Combine Hint-1 with (2-out-of-4)-SS and (3-out-of-5)-SS

2.2

1. $\gcd(m, n) = 1$. $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Solution: In the last tutorial, you showed the Chinese Remainder Thm:

Bijection between $\mathbb{Z}_{m \cdot n}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$.

$$\mathbb{Z}_{mn} \xrightarrow{(x \bmod m,\ x \bmod n)} \mathbb{Z}_m \times \mathbb{Z}_n$$

The same mapping is also a bijection

$$\mathbb{Z}^*_{mn} \xrightarrow{(x \bmod m,\ x \bmod n)} \mathbb{Z}^*_m \times \mathbb{Z}^*_n$$

To show this, we only need to show that the mapping $f(x) = (x \bmod m,\ x \bmod n)$ maps every $\mathbb{Z}^*_{mn}$ element to $\mathbb{Z}^*_m \times \mathbb{Z}^*_n$, and maps no element in $\mathbb{Z}_{mn} \setminus \mathbb{Z}^*_{mn}$ to $\mathbb{Z}^*_m \times \mathbb{Z}^*_n$.

Show this to conclude $|\mathbb{Z}^*_{mn}| = |\mathbb{Z}^*_m| \cdot |\mathbb{Z}^*_n|$.

2. $\varphi(p^k)$: Let $n = p^k$

$$\mathbb{Z}_n^* = \{ m : \gcd(m, p^k) = 1 \}$$

Observation : If $\gcd(m, p^k) \neq 1$, then p divides m.

Follows from the definition of gcd, and the fact that the only divisors of n are powers of p.

There are p^{k-1} multiples of p in $\mathbb{Z}_n$.

Therefore, $|\mathbb{Z}_n^*| = p^{k-1}(p-1)$

3. Use (1) and (2), together with Fundamental Theorem of Arithmetic.

2.3 If $x \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$, then x is either 0, or multiple of p, or mult. of q.

Case 1: $x = 0$. Result holds.

Case 2: $x = kp$ for some $1 \leq k < q$.

$x \bmod p = 0$. Let $x \bmod q = y$

Let $z = \exp_n(\exp_n(x, e), d) \in \mathbb{Z}_n$.

Consider $(\underbrace{z \bmod p}_{\alpha}, \underbrace{z \bmod q}_{\beta})$

$z \bmod p = 0$.

What can we say about $z \bmod q$?

Use Chinese Remainder Theorem.

2.4 Predicate is false, show a counterexample.

2.5 $\exp_p(x, 2) = 1$ is a deg. 2 polynomial, therefore it has at most 2 distinct roots. Check that 1 and $(p-1)$ are two roots of this equation.

Every element 'a' other than 1 and $(p-1)$ has a mult. inverse 'b' s.t. $a \neq b$. (using the fact that $\exp_p(a, 2) \neq 1$)

Pair the elements in the set

$\{2, 3, \ldots, p-2\}$ appropriately.

Conclude that the product of all elements in $\mathbb{Z}_p \setminus \{0\}$ is $(p-1)$.

2.6 For $n = 4$, $1 \times_4 2 \times_4 3 = 2$

$n = 6$, $1 \times_6 2 \times_6 3 \times_6 \cdots \times_6 5 = 0$

$n = 8$, $1 \times_8 2 \times_8 3 \times_8 \cdots \times_8 7 = 0$.

You can observe that for $n \geq 6$, n always divides $1 \times_n 2 \times_n \cdots \times_n (n-1)$.

Prove this formally. One approach is via the fundamental Thm of Arithmetic [maybe break into two cases: $n = p^k$, $n \neq p^k$]

2.7

Suppose $(x-1) \times_n (x-2) \times_n (x-3) = 0.$ $\quad (*)$

Then $(x-1) \times_p (x-2) \times_p (x-3) = 0$ ... (i)

and $(x-1) \times_q (x-2) \times_q (x-3) = 0$ ... (ii)

How many elements in $\mathbb{Z}_p$ satisfy (i)?

How many elements in $\mathbb{Z}_q$ satisfy (ii)?

Given a solution $\alpha \in \mathbb{Z}_p$ that satisfies (i),
and a sol^n $\beta \in \mathbb{Z}_q$ " " (ii),
how to construct a sol^n in $\mathbb{Z}_n$ that satisfies $(*)$?

Use this to give a bound on the number of roots of $(*)$ in $\mathbb{Z}_n$.

2.8

It suffices to show that 2, 3 and 7 divide $n^7 - n$ for all $n \in \mathbb{N}$.

a) 2 divides $n^7 - n$:

n is either odd or even, in both cases 2 divides $n^7 - n$.

b) 3 divides $n^7 - n$:

Take any $n \in \mathbb{N}$.

$$n^7 - n \pmod 3$$

$$= \left((n \bmod 3)^7 - (n \bmod 3)\right) \bmod 3$$

$$= \left[\left((n \bmod 3)^6 \bmod 3\right) \cdot (n \bmod 3) - (n \bmod 3)\right] \bmod 3$$

using Fermat's Little Thm, $(n \bmod 3)^2 \bmod 3 = 1$

$$= \left[1 \cdot (n \bmod 3) - (n \bmod 3)\right] \bmod 3$$

c) 7 divides $n^7 - n$

Same argument as (b).

2.9 Look up Euler's criterion online.