1. (a) p is an odd prime. $(p-1)$ is even.

Since p is prime. and Z_n^*'s definition: $Z_n^* = \{[a]_n \in Z_n, \gcd(a,n)=1\}$

$\Rightarrow Z_p^* = \{1, 2, \cdots p-1\}$.

$$\sum_{\alpha \in Z_p^*} = 1+2+\cdots p-1 \quad , p-1 \text{ is even}$$

$$= [1+(p-1)] + [2+(p-2)] + \cdots + \left[\tfrac{p-1}{2} + (p-\tfrac{p-1}{2})\right]$$

$$= \frac{(p-1)p}{2}$$

$p \mid \frac{(p-1)p}{2} \Rightarrow \sum_{\alpha \in Z_p^*} = [0]_p$.

(b) p is odd prime. $(p-1)$ is even

$$\sum_{i=1}^{p-1} \frac{1}{i} = 1 + \frac{1}{2} + \cdots \frac{1}{p-1}$$

$$= \left(1+\frac{1}{p-1}\right) + \left(\frac{1}{2}+\frac{1}{p-2}\right) + \cdots + \left(\frac{1}{\frac{p-1}{2}} + \frac{1}{p-\frac{p-1}{2}}\right)$$

$$= \frac{p}{p-1} + \frac{p}{2(p-2)} + \cdots \frac{p}{\left(\frac{p-1}{2}\right)\left(p-\frac{p-1}{2}\right)}$$

let's take $m = (p-1)\cdot 2(p-2) \cdots \frac{p-1}{2} \cdot \left(p-\frac{p-1}{2}\right)$

product of all denominator $= 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right) \cdots (p-2)\cdot(p-1)$

$= (p-1)!$

$$\Rightarrow \sum_{i=1}^{p-1} \frac{1}{i} = \frac{p\left[\frac{(p-1)!}{p-1} + \cdots + \frac{(p-1)!}{\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)}\right]}{(p-1)!} \quad (1)$$

$\Rightarrow$ from wilson's $(p-1)! \equiv -1 \pmod p$

$\Rightarrow p \nmid$ denominator,

and $p \mid$ numerator

$\Rightarrow$ in all, $p \mid$ numerator of $\sum_{i=1}^{p-1} \frac{1}{i}$

2. p, q are prime, $N = pq$

$\phi(N) = pq - p - q + 1 = (p-1)(q-1)$

p, q are odd, let: $p = 2m+1$, $q = 2n+1$

$\phi(N) = 2m \cdot 2n = 4mn$.

$0 < e < \phi(N)$, $\gcd(e, \phi(N)) = 1$, $\phi(N)$ even $\rightarrow$ ~~gcd~~ e odd.

$\Rightarrow$ def choice number of e: $|\{e\}|$

$$|\{e\}| \leqslant \text{number of all odd in } [\phi(N)] = \frac{\phi(N)}{2}.$$

specific N: $p=3$, $q=5$, $N = pq = 15$.

$\phi(N) = (p-1)(q-1) = 8$.

$\gcd(e, \phi(N)) = 1$, e odd. both: 1, 3, 5, 7 are possible since they all coprime with $8 = \phi(N)$

possible e number $= 4 = \frac{\phi(N)}{2}$

3. "$\Rightarrow$":

if $a_i z \equiv b_i \pmod{n_i}$ has a solution ($i \in \{1,2,3\}$)

$\exists t$, $a_i z - b_i = n_i t$, $t \in \mathbb{Z}$

$a_i z + n_i t = b_i$

$d_i = \gcd(a_i, n_i)$ $d_i \mid a_i$, $d_i \mid n_i$

$d_i \mid a_i z$, $d_i \mid n_i t$, $d_i \mid a_i z + n_i t = b_i$

"$\Leftarrow$": $d_i = \gcd(a_i, n_i)$, $d_i \mid b_i$

$\exists m_i \in \mathbb{Z}$: $b_i = m_i d_i$

$\exists p_i\, q_i \in \mathbb{Z}$: $a_i p_i + n_i q_i = d_i$

$\Rightarrow (m_i p_i) a_i + (m_i q_i) n_i = d_i m_i = b_i$

$\Rightarrow a_i (m_i p_i) \equiv b_i \pmod{n_i}$

$\exists$, $z_i = m_i q_i$, satisfy it.

from CRT, for $i = 1, 2, 3$.

from Chinese Remainder Theorem.

for system $\begin{cases} x \equiv b_1 \bmod n_1 \\ x \equiv b_2 \bmod n_2 \\ x \equiv b_3 \bmod n_3 \end{cases}$

$n_1 n_2 n_3$ relative prime.

exists only 1 solution $\rightarrow$ exist the only 1 z

inthat, There exists a z satisfy

$\begin{cases} z_1 \equiv e_1 \pmod{n_1} \\ z_2 \equiv e_2 \pmod{n_2} \\ z_3 \equiv e_3 \pmod{n_3} \end{cases}$ ther linear congruence system.

$e_1, e_2, e_3 \in \mathbb{Z}$.

4. "$\Rightarrow$": $[g]_p$ is a generator of $\mathbb{Z}_p$

$\mathbb{Z}_p = \{[0]_p \cdots [p-1]_p\}$

$\exists n \in \mathbb{Z}$

$\rightarrow ng \equiv r \pmod{p}$, $r \in \{1, \cdots p-1\}$. for any r.

$\exists n, m \in \mathbb{Z}$ $ng + mp = r$

take $r = 1$. $\exists n, m$: $ng + mp = 1 \Rightarrow \gcd(g, p) = 1$

"$\Leftarrow$": $\gcd(g, p) = 1$

$\exists n, m \in \mathbb{Z}$: $ng + mp = 1$

for any $r \in \{1, \cdots p-1\}$: $r = rng + rmp \Rightarrow rng \equiv r \pmod{p}$.

$\Rightarrow [g]_p$ generate $\mathbb{Z}_p$

5. for Alice $[A]_p = \underbrace{[g]_p + \cdots + [g]_p}_{a} = \sum_a [g]_p \Rightarrow A = ag + np,\ n \in \mathbb{Z}$

Bob $[B]_p = \sum_b [g]_p \cdot a \Rightarrow B = bg + mp,\ m \in \mathbb{Z}$.

$\gcd(g,p) = 1$

$\Rightarrow \exists s, t \in \mathbb{Z}:\ gs + pt = 1. \Rightarrow (As)g + (At)p = A.$

$\xrightarrow{A = ag+np} (As - a)g + (At - n)p = 0.$

$\Rightarrow As = a,\ At = n.$ since $\gcd(g,p) = 1$.

when we now g, p. s,t can be find with Extended Euclidean Algorithm). ($\gcd(g,p)=1$)

with knowing A. $a = As$ can be found.

6. let $A = \{(x,y,z): x^2+y^2+z^2 = 1,\ (x,y,z) \in \mathbb{R}^3\}$. $B = [0,1) \times [0,1)$.

① define $f := (\sin\pi m \sin 2\pi n,\ \sin\pi m \cos 2\pi n,\ \cos\pi m)$, $n \in [0,1)$, $m \in [0,1)$.

$(\sin\pi m \sin 2\pi n)^2 + (\sin\pi m \cos 2\pi n)^2 + \cos^2\pi m$

$= \sin^2\pi m(\sin^2 2\pi n + \cos^2 2\pi n) + \cos^2\pi m$

$= \sin^2\pi m \cdot 1 + \cos^2\pi m$

$= 1$

f is a bijection from B to A, $|A| = |B|$

② for $B = [0,1) \times [0,1)$ $C = (0,1) \times (0,1)$.

$f:\ f(0) = 2^{-1}.\ f(2^{-n}) = 2^{-n-1}$ $n = 1, 2, 3 \cdots$

$f(x) = x$ for other x. for both B's dimension

bijection, $|B| = |C|$.

③ $D = \mathbb{R}^2$

$f = \tan(\pi(x - \frac{1}{2}))$ for both C's dimension.

f_2 is a bijection. $|C| = |D|$

$\Rightarrow |A| = |B| = |C| = |D|$

④. $\mathbb{R}^2$, $\mathbb{R}$

$|\mathbb{R}| = 2^{\aleph_0}$;

$|\mathbb{R} \times \mathbb{R}| = |\mathbb{R}|^2 = (2^{\aleph_0})^2 = 2^{\aleph_0} = |\mathbb{R}|$

$\Rightarrow |A| = |B| = |C| = |D| = |\mathbb{R}^2| = |\mathbb{R}|$.

扫描全能王 创建

7. p_1, p_2, p_3, p_4 relative prime, distinct

without loss of generality:

def $p_1 < p_2 < p_3 < p_4$

$n = p_1 p_2 p_3 p_4$.

in $[n]$: $A_1 = [0]_{p_2p_3p_4} = \{k p_2p_3p_4 \mid 1 \le k \le p_1\}$. $|A_1| = p_1$

def: $A_2 = [0]_{p_1p_3p_4} = \{k p_1p_3p_4 \mid 1 \le k \le p_2\}$ $|A_2| = p_2$

$A_3 = [0]_{p_1p_2p_4} = \{k p_1p_2p_4 \mid 1 \le k \le p_3\}$. $|A_3| = p_3$

$A_4 = [0]_{p_1p_2p_3} = \{k p_1p_2p_3 \mid 1 \le k \le p_4\}$. $|A_4| = p_4$

for a_1 in A_1, a_2 in A_2:

if $a_1 = a_2$:

$k_1 p_2p_3p_4 = p_1 k_2 p_3 p_4$. $\in [1, p_1]$

$k_1 p_2 = k_2 p_1$, $k_1, k_2 \in [1, p_2]$.

$p_1 \mid k_2 p_1 \Rightarrow p_1 \mid k_1 p_2$, $\gcd(p_1, p_2) = 1 \Rightarrow p_1 \nmid p_2 \Rightarrow p_1 \mid k_1$

$k_1 \in [1, p_1]$, $k_1 = p_1$, $k_2 = p_2$

$\Rightarrow$ only one $k_1 = p_1$, $k_2 = p_2$, $k_1 p_2p_3p_4 = k_2 p_1 p_3 p_4$

$\Rightarrow$ A_1 and A_2 have only 1 same element: $(p_1p_2p_3p_4)$

Same for (A_2, A_3), (A_3, A_4). (A_4, A_1)

$\Rightarrow$ Number of all integers in $[n]$ satisfy:

number $= |A_1| + |A_2| + |A_3| + |A_4| - 4 + 1$.

$= p_1 + p_2 + p_3 + p_4 - 3$.

8. $A: \{(x_1, x_2, x_3, x_4) \mid x_1, x_2, x_3, x_4 \in \mathbb{Z}^+,\ x_1 < x_2 < x_3 < x_4 \le n\}$

(Since $x_1, x_2, x_3, x_4 > 0$, $x_1^3, x_2^3, x_3^3, x_4^3 > 0$)

$A: \{(1,2,3,4), (1,3,4,5), (2,3,4,5) \cdots\cdots (n-3, n-2, n-1, n)\}$.

$B: \{\{x_1, x_2, x_3, x_4\}: x_1, x_2, x_3, x_4 \in \mathbb{Z}^+,\ x_1 < x_2 < x_3 < x_4,\ x_1^3 + x_2^3 + x_3^3 + x_4^3 = n\}$.

$B \subseteq A$.

Since $x_1 < x_2 < x_3 < x_4$, $0 < x_1^3 < x_2^3 < x_3^3 < x_4^3 < n$

let's take B_i: $\{(x_1, x_2, x_3, x_4\}: x_1, x_2, x_3, x_4 \in \mathbb{Z}^+,\ x_1 < x_2 < x_3 < x_4.\ x_1^3 + x_2^3 + x_3^3 + x_4^3 = i\}$.

for elements in A. $(x_1^3 + x_2^3 + x_3^3 + x_4^3) \in [1^3 + 2^3 + 3^3 + 4^3,\ n^3 + (n-1)^3 + (n-2)^3 + (n-3)^3]$

$= [100,\ 4n^3 - 18n^2 + 42n - 36]$, $(x_1^3 + x_2^3 + x_3^3 + x_4^3) \in \mathbb{Z}^+$

$\Rightarrow \{B_{100}, \ldots B_{4n^3 - 18n^2 + 42n - 36}\}$ is a cover of A. ($B_i \subseteq A$).

from pigeon-hole:

A has $\binom{n}{4} = \dfrac{n(n-1)(n-2)(n-3)}{24}$ elements.

$n' = 4n^3 - 18n^2 + 4n - 36 - 100 + 1 = 4n^3 - 18n^2 + 4n - 135$ elements in cover

$\Rightarrow \exists B_k$ in cover: $|B_k| \ge \left|\dfrac{\binom{n}{4}}{n'}\right| = \dfrac{n(n-1)(n-2)(n-3)}{24(4n^3 - 18n^2 + 4n - 135)}$

let $|B_k| \ge 2^{2022}$ $\dfrac{n(n-1)(n-2)(n-3)}{24(4n^3 - 18n^2 + 42n - 135)} \ge 2^{2022}$ ①

compute ①:

$\dfrac{n(n-1)(n-2)(n-3)}{24(4n^3 - 18n^2 + 42n - 135)} = \dfrac{n^4 - 6n^3 + 11n^2 - 6n}{24(4n^3 - 18n^2 + 42n - 135)}$

$> \dfrac{n^4 - 6n^3}{24 \cdot 4n^3}$ ② (when $n > 100$).

let ② $> 2^{2022}$.

$n - 6 > 3 \cdot 2^{2027}$

$n > 3 \cdot 2^{2027} + 6$.

$\Rightarrow$ exist integer n satisfies.

9. for $\{a_n\}_{n\geq 0}$ RR: $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$.

Generating function:

let $A(x) = \sum_{n=0}^{\infty} a_n x^n$

$a_0 = a_1 = 0,\ a_2 = 1$

$= 0 + 0 + x^2 + \sum_{n=3}^{\infty} (6a_{n-1} - 11a_{n-2} + 6a_{n-3}) x^n$

$= x^2 + \sum_{n=3}^{\infty} 6a_{n-1}x^n - \sum_{n=3}^{\infty} 11a_{n-2}x^n + \sum_{n=3}^{\infty} 6a_{n-3}x^n.$

$= x^2 + 6x(a_0 + a_1x + \sum_{n=2}^{\infty} a_nx^n - a_0 - a_1x) - 11x^2(a_0 + \sum_{n=1}^{\infty} a_nx^n - a_0) + 6x^3 \sum_{n=0}^{\infty} a_nx^n$

$a_0 = a_1 = 0,\ a_2 = 1$

$= x^2 + 6x\sum_{n=0}^{\infty} a_nx^n - 11x^2\sum_{n=0}^{\infty} a_nx^n + 6x^3\sum_{n=0}^{\infty} a_nx^n.$

$= x^2 + (6x - 11x^2 + 6x^3)\sum_{n=0}^{\infty} a_nx^n$

$\sum_{n=0}^{\infty} a_nx^n = x^2 + (6x - 11x^2 + 6x^3)\sum_{n=0}^{\infty} a_nx^n.$

Generating function:

$$A(x) = \sum_{n=0}^{\infty} a_nx^n = \frac{x^2}{1 - 6x + 11x^2 - 6x^3} = \frac{x^2}{(-2x+1)(3x-1)(x-1)}$$

10. let $a_r = \{ s \in \{1,2,3,4\}^r,$ s has odd "1"s, even "2"s, a least 2 "3"s $\}$.

$R_1 = \{1, 3, 5 \cdots\}$

$R_2 = \{0, 2, 4 \cdots\}.$

$R_3 = \{2, 3, 4 \cdots\}.$

$R_4 = \{0, 1, 2, 3 \cdots\}.$

$1 + \frac{x}{1!} - 1 - \frac{x}{1!}$

$\sum_{r=0}^{\infty} \frac{a_r}{r!}x^r = (\frac{x}{1!} + \frac{x^3}{3!} + \cdots)(1 + \frac{x^2}{2!} + \cdots)(\frac{x^2}{2!} + \frac{x^3}{3!} \cdots)(1 + \frac{x}{1!} + \frac{x^2}{2!} \cdots)$

$= \frac{e^x - e^{-x}}{2} \cdot \frac{e^x + e^{-x}}{2} \cdot (e^x - 1 - x) \cdot e^x$

$\Rightarrow a_r = \frac{1}{4}\left[4^r - 3^r + (-1)^r + [-3^{r-1} + (-1)^{r-1}] \cdot r\right]$

$= \frac{e^{3x} - e^{-x}}{4} \cdot (e^x - x - 1)$

$a_{100} = \frac{4^{100} - 99 - 103 \cdot 3^{99}}{4}$

$= \frac{1}{4}(e^{4x} - 1 - xe^{3x} + xe^{-x} - e^{3x} + e^{-x})$

$= \frac{1}{4}\sum_{r=0}^{\infty}\left(\frac{(4x)^r}{r!} - \frac{x(3x)^r}{r!} + \frac{x(-x)^r}{r!} - \frac{(3x)^r}{r!} + \frac{(-x)^r}{r!}\right) - \frac{1}{4}.$

$= \frac{1}{4}\sum_{r=0}^{\infty}\left(\frac{4^r - 3^r + (-1)^r}{r!}\right)x^r + \frac{1}{4}x\sum_{r=0}^{\infty}\left(\frac{-3^r + (-1)^r}{r!}\right)x^r - \frac{1}{4}$

$= \frac{1}{4}\sum_{r=0}^{\infty}\left(\frac{4^r - 3^r + (-1)^r}{r!}\right)x^r + \frac{1}{4}\sum_{r=1}^{\infty}\left(\frac{-3^{r-1} + (-1)^{r-1}}{(r-1)!}\right)x^r - \frac{1}{4}$

Since $= \frac{1}{4} \cdot \frac{1-1+1}{1} + \frac{1}{4}\sum_{r=1}^{\infty}\left[\frac{4^r - 3^r + (-1)^r}{r!} + \frac{-3^{r-1} + (-1)^{r-1}}{(r-1)!}\right]x^r - \frac{1}{4}$

$a_0 = 0$

$\sum_{r=0}^{\infty}\frac{a_r}{r!}x^r = \sum_{r=1}^{\infty}\frac{a_rx^r}{r!} = \frac{1}{4}\sum_{r=1}^{\infty}\left[\frac{4^r - 3^r + (-1)^r}{r!} + \frac{-3^{r-1} + (-1)^{r-1}}{(r-1)!}\right]x^r$