1. (**15 points**) Let p be an odd prime. Wilson's theorem says that $(p-1)! \equiv -1 (\text{mod } p)$.

(a) Show that $\sum_{\alpha \in \mathbb{Z}_p^*} = [0]_p$.

(b) Show that the numerator of the fraction $\sum_{i=1}^{p-1} \frac{1}{i}$ is a multiple of p.

(a) $[0]_p = 0 + pZ = \{np : n \in Z\} = \{0, \pm p, \pm 2p, \cdots\}$

since p is an odd prime

then $Z_p^* = \{1, 2, 3, \cdots, p-1\}$

So $\sum_{\alpha \in Z_p^*} = 1 + 2 + \cdots + (p-1) = \frac{(1+p-1)(p-1)}{2} = \frac{p(p-1)}{2}$

since p is an odd prime

then $\frac{p-1}{2} \in Z$

So $\sum_{\alpha \in Z_p^*} = [0]_p$

1. **(15 points)** Let p be an odd prime. Wilson's theorem says that $(p-1)! \equiv -1 (\mathrm{mod}\ p)$.

(a) Show that $\sum_{\alpha \in \mathbb{Z}_p^*} = [0]_p$.

(b) Show that the numerator of the fraction $\sum_{i=1}^{p-1} \frac{1}{i}$ is a multiple of p.

(b) $\sum_{i=1}^{p-1} \frac{1}{i} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$

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

$= \frac{p}{p-1} + \frac{p}{2(p-2)} + \cdots + \frac{p}{\frac{(p-1)(p+1)}{4}}$

$= p \times \left[\frac{1}{p-1} + \frac{1}{2(p-2)} + \cdots \frac{1}{\frac{(p-1)(p+1)}{4}} \right]$

$= p \times \frac{a}{b}$ ($\frac{a}{b}$ is a fraction in lowest term)

b is the result of dividing the common denominator of $\frac{1}{p-1} + \frac{1}{2(p-2)} + \cdots + \frac{1}{\frac{(p-1)(p+1)}{4}}$

so b is a divisor of $1 \times 2 \times 3 \times \cdots \times (p-1) = (p-1)!$

Since $(p-1)! \equiv -1 (\mathrm{mod}\ p)$ and p is an odd prime

then $b \nmid p$

so pa must be a multiple of p

thus, the numerator of the fraction $\sum_{i=1}^{p-1} \frac{1}{i}$ is a multiple of p

2. (**10 points**) In the RSA public key cryptosystem, if $N = pq$ is the product of two odd primes, we always choose the public encryption exponent e such that $0 \le e < \phi(N)$ and $\gcd(e, \phi(N)) = 1$. Show that the number of all possible choices of e is at most $\frac{1}{2}\phi(N)$. Find a specific N such that this number is exactly equal to $\frac{1}{2}\phi(N)$.

since $p \neq q$, then $\phi(N) = (p-1)(q-1)$ is even

since $0 \le e < \phi(N)$ and $\gcd(e, \phi(N)) = 1$

then e is odd in $\{1, 2, 3, \cdots, (p-1)(q-1)\}$

so $n \le \frac{(p-1)(q-1)}{2} = \frac{1}{2}\phi(N)$

Thus, the number of all possible choices of e is at most $\frac{1}{2}\phi(N)$

a specific $N = 15 = 3 \times 5$

$\phi(N) = 8$

$e = 1, 3, 5, 7$

$n = 4 = \frac{1}{2}\phi(N)$

3. (**10 points**) Let n_1, n_2, n_3 be three positive integers such that $\gcd(n_1, n_2) = \gcd(n_1, n_3) = \gcd(n_2, n_3) = 1$. Let a_1, a_2, a_3 and b_1, b_2, b_3 be integers. Let $d_i = \gcd(a_i, n_i)$ for $i = 1, 2, 3$. Show that there is an integer z such that $a_i z \equiv b_i (\bmod\ n_i)$ for all $i \in \{1, 2, 3\}$ if and only if $d_i | b_i$ for all $i \in \{1, 2, 3\}$.

① $\Leftarrow$ for all $i \in \{1,2,3\}$

since $d_i | b_i$, then d_i is a divisor of b_i

since $d_i = \gcd(a_i, n_i)$. then d_i is a divisor of a_i, n_i

so d_i is a common divisor of a_i, b_i, n_i

let $a_i = l d_i$, $b_i = m d_i$, $n_i = n d_i$ $(l, m, n \neq 0)$

then $(a_i z - b_i) = k n_i$ is $(l d_i z - m d_i) = k n d_i$ $(k \neq 0)$

the equation always has a solution $\begin{cases} z = 1 \\ k = 1 \end{cases}$

so there is an integer z such that $a_i z \equiv b_i (\bmod\ n_i)$

for all $i \in \{1,2,3\}$

② $\Rightarrow$ we know there is an integer z such that $a_i z \equiv b_i (\bmod\ n_i)$

then there is an integer k such that $a_i z - b_i = k n_i$ $(k \neq 0)$

Since $d_i = \gcd(a_i, n_i)$ for $i = 1, 2, 3$

then there are two integers k_1 and k_2 such that

$a_i = k_1 d_i$, $n_i = k_2 d_i$ $(k_1, k_2 \neq 0)$

So $z k_1 d_i - b_i = k k_2 d_i$

that is $b_i = (z k_1 - k k_2) d_i$

since $z k_1 - k k_2$ must be an integer

then $d_i | b_i$ for all $i \in \{1,2,3\}$

Conclusion: there is an integer z such that $a_i z \equiv b_i (\bmod\ n_i)$

for all $i \in \{1,2,3\}$ if and only if $d_i | b_i$ for all $i \in \{1,2,3\}$

4. (**10 points**) For any prime p, $\mathbb{Z}_p$ is a cyclic group with respect to the addition of residue classes modulo p. For example, $[1]_p$ is a generator of $\mathbb{Z}_p$ because $\mathbb{Z}_p = \langle [1]_p \rangle$: any $[k]_p \in \mathbb{Z}_p$ can be expressed as the addition of k copies of $[1]_p$, i.e.,

$$[k]_p = \underbrace{[1]_p + \cdots + [1]_p}_{k}.$$

Show that an element $[g]_p \in \mathbb{Z}_p$ is a generator of $\mathbb{Z}_p$ if and only if $\gcd(g, p) = 1$.

① $\Rightarrow$ we know $[g]_p \in Z_p$ is a generator of Z_p.
so any $[k]_p \in Z_p$ can be expressed as the addition of a copies of $[g]_p = \{g + pn ; n \in Z\}$
if $\gcd(g,p) \neq 1$
then there is no $n \in Z$ such that $g + pn = 1$
this is a contradiction.
so $\gcd(g,p) = 1$

② $\Leftarrow$ we know $\gcd(g,p) = 1$
then there are two integers such that $sg + tp = 1$
so any $[k]_p \in Z_p$ can be expressed as follows:

$$[k]_p = \underbrace{[1]_p + \cdots + [1]_p}_{k} = \underbrace{[sg+tp]_p + \cdots + [sg+tp]_p}_{k}$$

$$= \underbrace{s[g]_p + \cdots + s[g]_p}_{k} + \underbrace{t[p]_p + \cdots + t[p]_p}_{k}$$

$$= \underbrace{[g]_p + \cdots + [g]_p}_{k} + \underbrace{[0]_p + \cdots + [0]_p}_{k}$$

$$= \underbrace{[g]_p + \cdots + [g]_p}_{k}$$ so $[g]_p \in Z_p$ is a generator of Z_p

Conclusion: an element $[g]_p \in Z_p$ is a generator of Z_p if and only if $\gcd(g,p) = 1$

5. (**5 points**) Let p be a large odd prime and let $[g]_p$ be a generator of the additive group $G = \mathbb{Z}_p$, where $0 \leq g < p$. We modify the Diffie-Hellman key exchange protocol as follows:

- Alice: choose $a \in \{0, 1, \ldots, p-1\}$ uniformly at random; compute $[A]_p = \underbrace{[g]_p + \cdots + [g]_p}_{a}$, where $0 \leq A < p$; send (p, G, g, A) to Bob;
- Bob: choose $b \in \{0, 1, \ldots, p-1\}$ uniformly at random; compute $[B]_p = \underbrace{[g]_p + \cdots + [g]_p}_{b}$, where $0 \leq B < p$; send B to Alice; output the integer K $(0 \leq K < p)$ such that $[K]_p = \underbrace{[A]_p + \cdots + [A]_p}_{b}$.
- Alice: output the integer K $(0 \leq K < p)$ such that $[K]_p = \underbrace{[B]_p + \cdots + [B]_p}_{a}$.

Show that it's easy to compute a from (p, G, g, A) and so this modified protocol is not secure. (**Hint**: $\gcd(g, p) = 1$)

Since $[g]_p$ is a generator of the additive group $G = \mathbb{Z}_p$

we can know $\gcd(g, p) = 1$

$[g]_p = \{g + np, n \in \mathbb{Z}\}$ $\quad [A]_p = \{A + np, n \in \mathbb{Z}\}$.

So from $[A]_p = \underbrace{[g]_p + \cdots + [g]_p}_{a}$

$A + n_1 p = ag + an_2 p$

since $0 \leq A < p$, $0 \leq g < p$. then $A = ag$

It's easy to compute $a = \frac{A}{g}$ or 0 because we have known (p, G, g, A)

Conclusion: it's easy to compute a from (p, G, g, A) and so this modified protocol is not secure.

6. (**5 points**) Determine whether the set $\{(x, y, z) : (x, y, z) \in \mathbb{R}^3, x^2 + y^2 + z^2 = 1\}$ and the set $\mathbb{R}$ of real numbers have the same cardinality. Show your answer.

Denote $A = \{(x,y,z) \in R^3 : x^2+y^2+z^2=1$

Define $f: [0,1) \mapsto A$

$s,t \to (\sin(2\pi s)\cos(2\pi t), \sin(2\pi s)\sin(2\pi t), \cos(2\pi s))$

$\forall P \in A$, denote $\theta = \angle POz \in [0,\pi]$ φ is azimuth angle $\in [0,2\pi)$

$\sin\theta\cos\varphi = X$, $\sin\theta\sin\varphi = y$, $\cos\theta = Z$

$(X_1, y_1, Z_1) = (X_2, y_2, Z_2) \Rightarrow \sin\theta_1\cos\varphi_1 = \sin\theta_2\cos\varphi_2$,

$\sin\theta_1\sin\varphi_1 = \sin\theta_2\sin\varphi_2$, $\cos\theta_1 = \cos\theta_2$

for $2\pi s, 2\pi t \in [0, 2\pi)$. $\theta_1 = \theta_2$, $\varphi_1 = \varphi_2 \Rightarrow s_1 = s_2$, $t_1 = t_2$

So $f([0,1)) = A$ that is f is both injective

and surjective, so f is bijective

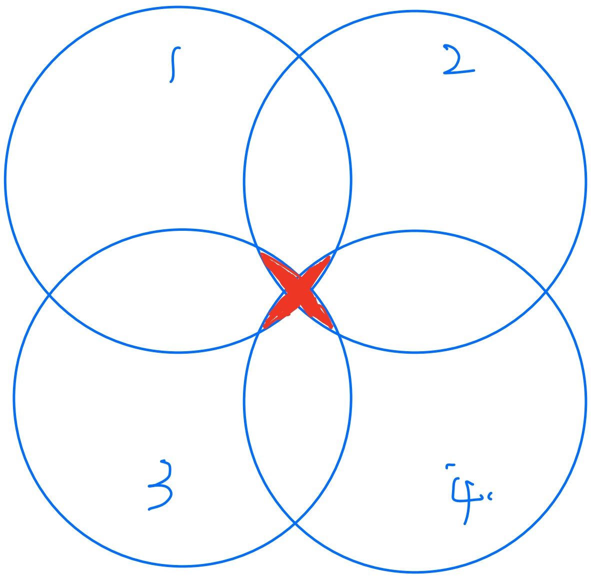
So $|A| = |[0,1)|$ and $|[0,1)| = |R|$

so $|\{(x,y,z) : (x,y,z) \in R^3, x^2+y^2+z^2=1\}| = |R|$

7. (**15 points**) Suppose that $n = p_1p_2p_3p_4$ is the product of four distinct primes p_1, p_2, p_3 and p_4. Determine the number of integers in $[n] = \{1, 2, \ldots, n\}$ that are divisible by at least three of the primes p_1, p_2, p_3 and p_4.

the number of integers that are divisible by P_1, P_2, P_3 / P_1, P_2, P_4 / P_1, P_3, P_4 / P_2, P_3, P_4 are P_4, P_3, P_2, P_1 respectively

the number of integers that are divisible by P_1, P_2, P_3, P_4 is 1.



so the total number is $(P_4 - 1) + (P_3 - 1) + (P_2 - 1) + (P_1 - 1) + 1$

$= P_1 + P_2 + P_3 + P_4 - 3$

8. (**5 points**) Show that there exists a positive integer n such that

$$\left|\left\{\{x_1, x_2, x_3, x_4\} : x_1, x_2, x_3, x_4 \in \mathbb{Z}^+, x_1 < x_2 < x_3 < x_4, x_1^3 + x_2^3 + x_3^3 + x_4^3 = n\right\}\right| \geq 2^{2022}.$$

Consider $A = \{\{x_1, x_2, x_3, x_4\}; x_1, x_2, x_3, x_4 \in Z^+, x_1 < x_2 < x_3 < x_4 \leq N\}$.

It's easy to calculate $|A| = \binom{N}{4}$

and $B_n = \{\{x_1, x_2, x_3, x_4\}: x_1, x_2, x_3, x_4 \in Z^+, x_1 < x_2 < x_3 < x_4 \leq N$

$x_1^3 + x_2^3 + x_3^3 + x_4^3 = n\}$ and $n_{max} = N^3 + (N-1)^3 + (N-2)^3 + (N-3)^3$

Hence, $\{B_1, B_2, B_3, \cdots, B_{n_{max}}\}$ covers A. We can tell that $|A_n| \geq \frac{|A|}{n_{max}}$

then we just consider a solution of N that $\frac{|A|}{n_{max}} \geq 2^{2022}$

$$\frac{N(N-1)(N-2)(N-3)}{5 \times 4 N^3} \sim \frac{N(N-1)(N-2)(N-3)}{(N^3 + (N-1)^3 + (N-2)^3 + (N-3)^3)} \geq 2^{2022}$$

$$\frac{(N-1)(N-2)(N-3)}{N^2} \sim N \geq 20 \times 2^{2022}$$

It's obvious to show that N exists.

So n_{max} exists, then must have a $n \leq n_{max}$ satisfied the statement.

9. (**15 points**) Suppose that $\{a_n\}_{n\geq 0}$ is a sequence such that $a_0 = a_1 = 0, a_2 = 1$ and $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$ for every $n \geq 3$. Find the generating function of $\{a_n\}_{n\geq 0}$.

$$G(x) = \sum_{k=0}^{\infty} a_k x^k$$

$$xG(x) = \sum_{k=0}^{\infty} a_k x^{k+1} = \sum_{k=1}^{\infty} a_{k-1} x^k$$

$$x^2 G(x) = \sum_{k=0}^{\infty} a_k x^{k+2} = \sum_{k=2}^{\infty} a_{k-2} x^k$$

$$x^3 G(x) = \sum_{k=0}^{\infty} a_k x^{k+3} = \sum_{k=2}^{\infty} a_{k-3} x^k$$

$$G(x) - 6xG(x) + 11x^2 G(x) - 6x^3 G(x)$$

$$= (a_0 + a_0 + a_1 + a_0 + a_1 + a_2) + \sum_{k=3}^{\infty} (a_k - 6a_{k-1} + 11a_{k-2} - 6a_{k-3})x^k$$

$$= 1$$

$$(1 - 6x + 11x^2 - 6x^3)\, G(x) = 1$$

$$G(x) = \frac{1}{1 - 6x + 11x^2 - 6x^3}$$

$$= \sum_{n=3}^{\infty} \frac{1}{2} x^{n-3} (1 - 2^{n+1} + 3^n) \quad (n \geq 3)$$

Since $a_0 = a_1 = 0$, $a_2 = 1$ also fits

Hence the generating function of $\{a_n\}_{n\geq 0}$

is $G(x) = \sum_{n=0}^{\infty} \frac{1}{2} (1 - 2^{n+1} + 3^n) x^n$

10. (**10 points**) For every integer $r \geq 1$, let a_r be the number of ways of distributing r labeled balls into four labeled boxes such that the first box receives an odd number of balls, the second box receives an even number of balls, the third box receives at least 2 balls. Determine a_{100}.

$R_1 = \{1, 3, 5, \cdots\}$ $R_2 = \{0, 2, 4, \cdots\}$ $R_3 = \{2, 3, 4, \cdots\}$ $R_4 = \{0, 1, 2, \cdots\}$

$$\sum_{r=0}^{\infty} \frac{a_r}{r!} x^r = \left(x + \frac{x^3}{3!} + \frac{x^5}{5!} + \cdots\right)\left(1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \cdots\right)\left(\frac{x^2}{2!} + \frac{x^3}{3!} + \cdots\right)\left(1 + x + \frac{x^2}{2!} + \cdots\right)$$

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

$$= \frac{e^{3x} - e^{-x}}{4} \left[e^x - (x+1)\right]$$

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

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

$$\therefore a_{100} = 100! \times \frac{1}{4} \times \left[\frac{4^{100}}{100!} - \frac{3^{100} - 1}{100!} - \frac{3^{99} + 1}{99!} \right]$$

$$= \frac{1}{4} \left[4^{100} - 3^{100} + 1 - 100 \cdot 3^{99} - 100 \right]$$

$$= \frac{1}{4} \left(4^{100} - 3^{100} - 100 \cdot 3^{99} - 99 \right)$$