Discrete Mathematics: Midterm Exam

(Spring 2022, ShanghaiTech University)

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.

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 $0 \leq e < \phi(N)$ 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 $\frac{1}{2}\phi(N)$.

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 $a_i z \equiv b_i (\text{mod } n_i)$ 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 $\gcd(g, p) = 1$.

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**: $\gcd(g, p) = 1$)

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.

7. (**15 points**) Suppose that $n = p_1 p_2 p_3 p_4$ 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.

8. (**5 points**) Show that there exists a positive integer n such that
$$\left| \left\{ \{x_1, x_2, x_3, x_4\} : x_1, x_2, x_3, x_4 \in \mathbb{Z}^+, x_1 < x_2 < x_3 < x_4, x_1^3 + x_2^3 + x_3^3 + x_4^3 = n \right\} \right| \geq 2^{2022}.$$

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 $\{a_n\}_{n \geq 0}$.

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}.