CSC3001 Discrete Mathematics

Final Examination

December 22, 2022: 1:30pm - 4:00pm

Name: _____ Student ID: _____

Answer ALL questions in the Answer Book.

Question	Points	Score
1	20	
2	20	
3	16	
4	12	
5	12	
6	20	
Total:	100	

1. (20 points) A graph is k-regular if and only if all of its vertices are of degree k.

   Let $k, n \in \mathbb{Z}^+$, $k \geq 1$, $n \geq 2$. Let G be a k-regular graph with n vertices.

   (a) (10 points) Show that the sum of degrees of all vertices in G is kn.

   (b) (10 points) Show that at least one of k and n is even.

Solution:

Part (a) Because all vertices are of the same degree, the sum of degrees is the product of the number of vertices and the degree of each vertex, which is kn.

Part (b) By the handshaking lemma the sum of degrees must be even. Therefore kn must be even and subsequently at least one of k, n must be even.

2. (20 points) Let $A = \{n \mid 1 \leq n \leq 1000, 3|n\}$, $B = \{n \mid 1 \leq n \leq 1000, 7|n\}$, $C = \{n \mid 1 \leq n \leq 1000, \text{there is at least one digit 3 in the decimal representation of } n\}$. Find $|A \cup B|$ and $|A \cup C|$. Please justify your answer.

Solution:

$|A \cup B| = |A| + |B| - |A \cap B| = \lfloor \frac{1000}{3} \rfloor + \lfloor \frac{1000}{7} \rfloor - \lfloor \frac{1000}{21} \rfloor = 428$.

To compute $|C|$, because 0 and 1000 do not have digit 3, we instead consider $0 \leq n \leq 999$. $|C|$ is then $1000 - 9^3 = 271$.

Let A_i, $i = 1, 2, 3$, denote the set of multiples of 3 such that the i-th digit is 3. Then each A_i is of size 34, each $A_i \cap A_j$, $i \neq j$ is of size 4, and the size of $A_1 \cap A_2 \cap A_3$ is 1. Therefore $|A \cap C| = |A_1 \cup A_2 \cup A_3| = 91$.

Then, $|A \cup C| = |A| + |C| - |A \cap C| = 513$.

3. (16 points) Recall that the binomial coefficient for nonnegative integers a, b is

$$\binom{a}{b} = \begin{cases} a!/(b!(a-b)!) & \text{if } 0 \leq b \leq a\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

   Let r, s, n be nonnegative integers such that $n \leq r + s$. Show that

$$\sum_{k=0}^{n} \binom{r}{k}\binom{s}{n-k} = \binom{r+s}{n}\,.$$

Solution:

We prove the claim by double counting. Suppose a committee is formed by r teachers and s students. The number of ways to form a subcommittee of n members is $\binom{r+s}{n}$. At the same time, this number can also be counted by summing over the number of ways to form a subcommittee of k teachers and $n-k$ students for all $k = 0, 1, \ldots, n$, i.e,

$$\sum_{k=0}^{n} \binom{r}{k}\binom{s}{n-k}.$$

4. (12 points) Let $a_1 = 1, a_2 = \sqrt{2}$, and for $n \geq 3$, $a_n = |a_{n-1} - a_{n-2}|$. Show that for all $n \in \mathbb{Z}^+$, a_n is nonzero.

Solution:

We prove the claim by contradiction. Suppose that $a_{n-1} \neq 0, a_n = 0$ for some $n \geq 3$, then both $\frac{a_{n-1}}{a_{n-1}}$ and $\frac{a_{n-2}}{a_{n-1}}$ are rational. By strong induction over $k = n-1, n-2, \ldots$ we have that $\frac{a_k}{a_{n-1}}$ is rational for all $1 \leq k \leq n-1$. This indicates that $\sqrt{2} = \frac{a_2}{a_1} = \frac{a_2}{a_{n-1}} / \frac{a_1}{a_{n-1}}$ is rational. Contradiction.

5. (12 points) Let k, n be positive integers and let $A = \{1, 2, \ldots, kn\}$.

Suppose $\{B_1, B_2 \ldots, B_n\}$ and $\{C_1, C_2, \ldots, C_n\}$ are both partitions of A into n sets of size k. Show that there exists a set T of size n such that for all $i = 1, \ldots, n$, it holds that

$$|T \cap B_i| = |T \cap C_i| = 1\,.$$

Solution:

Construct a bipartite graph $G = (V, W; E)$ as follows. The set V is formed by n vertices corresponding to $B_1, \ldots, B_n$, and the set W is formed by n vertices corresponding to $C_1, \ldots, C_n$. To construct the set E, we note that for each $j \in A$, there exist unique $s, t \in \{1, \ldots, n\}$ such that $j \in B_s$ and $j \in C_t$. Put the edge corresponding to B_s, C_t in the set E, and the label edge by j.

Observe that any perfect matching in G results in a set T satisfying the required property. Indeed, we can simply take T to be the set of the labels of the edges in a perfect matching. So it suffices to show there exists a perfect matching in G.

Note that G is k-regular bipartite graph as $|B_i| = |C_i| = k$ for all $i = 1, \ldots, n$. Since every k-regular bipartite graph has a perfect matching, there is a perfect matching in G. (Alternatively, you may use Hall's theorem to show there exists a perfect matching in G.)

6. (20 points) For any integer $N > 1$, define the set

$$\mathbb{Z}_N^* = \{b \in \{1, \ldots, N-1\} \mid \gcd(b, N) = 1\}\,.$$

Let $\phi(N) = |\mathbb{Z}_N^*|$.

(a) (8 points) Let p, q be distinct primes and $N = pq$. Show that

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

(b) (8 points) Let N be a positive integer and $N > 1$. Show that for any $a \in \mathbb{Z}_N^*$,

$$a^{\phi(N)} \equiv 1 \pmod{N}\,.$$

(c) (4 points) Let N be a positive integer and $N > 1$. Let $e > 0$ be an integer such that $\gcd(e, \phi(N)) = 1$ and define a function f_e for all $x \in \mathbb{Z}_N^*$ by $f_e(x) = x^e \bmod N$. Show that f_e is a bijection from $\mathbb{Z}_N^*$ to $\mathbb{Z}_N^*$.

Solution:

Part (a) If $a \in \{1, \ldots, N-1\}$ but $a \notin \mathbb{Z}_N^*$, then either $p|a$ or $q|a$. Let $A_p = \{a \in \{1, \ldots, N-1\} \mid p \text{ divides } a\}$ and $A_q = \{a \in \{1, \ldots, N-1\} \mid q \text{ divides } a\}$. Note that $A_p \cap A_q = \emptyset$ since any integer in $\{1, \ldots, N-1\}$ cannot be divisible by both p and q. Therefore,

$$|\mathbb{Z}_N^*| = N - 1 - |A_p| - |A_q| = pq - 1 - (q-1) - (p-1) = (p-1)(q-1)\,.$$

Part (b) Let us write $\mathbb{Z}_N^* = \{b_1, b_2, \ldots, b_{\phi(N)}\}$. Then $ab_1, \ldots, ab_{\phi(N)}$ are all distinct since $ab_i \equiv ab_j \pmod{N}$ if and only if $b_i \equiv b_j \pmod{N}$. Moreover, $ab_i \equiv b_k \pmod{N}$ for some $k \in \{1, \ldots, \phi(N)\}$. Thus,

$$\prod_{i=1}^{\phi(N)} (ab_i) \equiv \prod_{k=1}^{\phi(N)} b_k \pmod{N}\,.$$

Since $\gcd(b_k, N) = 1$ for all $k = 1, \ldots, \phi(N)$, canceling $b_1, \ldots, b_{\phi(N)}$ from both sides of the above equation, we obtain

$$a^{\phi(N)} \equiv 1 \pmod{N}\,.$$

Part (c) It suffices to show that f_e is invertible. Since $\gcd(e, \phi(N)) = 1$, there exists an integer d such that $1 \equiv ed \pmod{\phi(N)}$, i.e., $ed = 1 + k\phi(N)$ for some integer k. Define $f_d(x) = x^d \bmod N$. We desire that f_d is the inverse of f_e. Indeed, for any $x \in \mathbb{Z}_N^*$ we have

$$\begin{aligned} f_d(f_e(x)) &= (x^e)^d \bmod N \\ &= x^{1+k\phi(N)} \bmod N \\ &= x\,, \end{aligned}$$

where the last equality follows by **Part (b)**.

Remark:

One could alternatively prove Part (a) by pointing out $\phi(pq) = \phi(p)\phi(q)$ because of the Chinese remainder theorem.

Part (b) is known as Euler's theorem, which is an extension of Fermat's little theorem. Part (c) applies Euler's theorem and is used in the RSA encryption system. When N is pq for some large primes p, q, $\phi(N)$ is hard to compute (because N is hard to factor) and d is used as the private key of the encryption.