UNIVERSIDAD DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

Matemáticas Discretas para la Computación - CC3101
Examen - Semestre Otoño 2013

1. *a*) (2pts) Demuestre que la congruencia lineal $mx \equiv c \pmod{n}$ tiene solución si y solo si c es divisible por $\gcd(m, n)$.

   b) (2pts) Demuestre que si $c \equiv d \pmod{\gcd(n_1, n_2)}$ entonces el sistema de congruencias lineales $x \equiv c \pmod{n_1}$ y $x \equiv d \pmod{n_2}$ tiene solución.

   c) (2pts) Demuestre que existe un número infinito de primos de la forma $(6n + 5)$.

   Solución:

   a) Por definición, $mx \equiv c \pmod{n}$ ssi existe $y \in \mathbb{Z}$ tal que $mx+ny = c$. Basta demostrar entonces que $mx + ny = c$ tiene solución ssi c es divisible por $\gcd(m, n)$. Como demostramos en clases, existen $x', y' \in \mathbb{Z}$ tal que $mx' + ny' = \gcd(m, n)$. Dado que c es divisible por $\gcd(m, n)$ concluímos que existen $x, y \in \mathbb{Z}$ tal que $mx + ny = c$. Por otro lado, si $mx + ny = c$ entonces claramente c es divisible por $\gcd(m, n)$.

   b) Las soluciones a la ecuación $x \equiv c \pmod{n_1}$ son de la forma $k_1n_1 + c$. Poniendo junto a la segunda ecuación tenemos que existe solución al sistema de congruencias si es que existen $k_1, k_2 \in \mathbb{Z}$ tal que $k_1n_1 + k_2n_2 = d - c$. Por solución anterior esto ocurre ssi $d - c$ es divisible por $\gcd(n_1, n_2)$. Pero lo anterior se cumple por hipótesis.

   c) Asuma por contradicción que conjunto de números primos de la forma $(6n + 5)$ es finito y que estos son $p_1 < p_2 < \ldots < p_k$. Considere el número $r = 6p_1p_2 \ldots p_k - 1$. Este número es de la forma $(6n + 5)$ para $n = p_1p_2 \ldots p_k - 1$. Considere factorización prima $q_1q_2 \ldots q_m$ de r. Entonces $q_i > p_k$ para cada $1 \leq i \leq m$ (porque de otra forma q_i dividiría a 1). Además, algún q_i debe ser de la forma $(6n + 5)$ (porque el producto de primos de la forma $(6n + 1)$ o $(6n + 3)$ es de la forma $(6n + 1)$ o $(6n + 3)$). Esto es una contradicción.

2. Sea $p \geq 2$ primo.

   a) (1,5pto) Demuestre que todo a con $1 \leq a \leq p - 2$ tiene inverso módulo p. Además, no existen $2 \leq a_1 < a_2 \leq p - 2$ que tengan el mismo inverso módulo p.

   b) (3,5pts) Utilizando lo anterior demuestre que $(p - 2)! \equiv 1 \pmod{p}$.

   c) (1pto) Concluya que $(p - 1)! \equiv -1 \pmod{p}$.

   Solución:

   a) La primera parte se sigue de que a y p son primos relativos para todo $1 \leq a \leq p-1$. La segunda parte es directa.

   b) Ningún número a entre 2 y $p - 2$ es su auto inverso. Por parte (a), $(p - 2)!$ consiste del producto de 1 con pares de inversos modúlo p. Concluímos que $(p - 2)! \equiv 1 \pmod{p}$.

c) Directo de la parte (b) y del hecho que $(p-1) \equiv -1 \pmod{p}$.

3. Sean n, m enteros positivos tal que $m \geq n$. Determine el número de funciones sobreyectivas que existen desde un conjunto con m elementos a un conjunto con n elementos.

   Solución: Teorema 1 del Capítulo 6.7 del libro.

4. Un *clique maximal* de un grafo simple G es un subgrafo G' de G que es un clique (esto es, todo par de nodos en G' está conectado por un arco), y no existe subgrafo G'' de G que contiene a G' y también es un clique.

   Sea $\mathcal{I}$ un conjunto finito de intervalos cerrados sobre los reales. El grafo simple $G(\mathcal{I})$ tiene un nodo v_i por cada intervalo $i \in \mathcal{I}$, de tal forma que los nodos v_i y $v_{i'}$ son adyacentes en $G(\mathcal{I})$ si y solo si $i \neq i'$ y $i \cap i' \neq \emptyset$.

   Demuestre que los cliques maximales de $G(\mathcal{I})$ pueden ser ordenados como $M_1, M_2, \ldots, M_p$, de tal forma que si un nodo v_i pertenece a M_j y M_k, para $1 \leq j < k \leq p$, entonces $v_i \in M_l$ para todo $j \leq l \leq k$.

   Solución: Los cliques maximales de $G(\mathcal{I})$ son precisamente los nodos asociados con aquellos subconjuntos maximales S de $\mathcal{I}$ tal que $i_1 \cap i_2 \neq \emptyset$, para cada $i_1, i_2 \in S$. Ordenaremos estos conjuntos en orden creciente con respecto al menor real $inf(S)$ que pertenece a un intervalo de S. Si para dos de estos conjuntos S_1 y S_2 se tiene que $inf(S_1) = inf(S_2)$, entonces S_1 aparece antes que S_2 en el ordenamiento si el mayor real $sup(S_1)$ que aparece en un intervalo de S_1 es menor que el mayor real $sup(S_2)$ que aparece en un intervalo de S_2. Si $inf(S_1) = inf(S_2)$ y $sup(S_1) = sup(S_2)$, entonces ordenamos a S_1 y S_2 arbitrariamente.

   Sea $S_1, S_2, \ldots, S_p$ nuestro ordenamiento y asuma que el intervalo i pertenece a S_j y S_k, para $1 \leq j < k \leq p$. Considere $j \leq l \leq k$. Entonces $inf(S_j) \leq inf(S_l) \leq inf(S_k)$. Asuma por contradicción que $i \notin S_l$, esto es, $inf(i) > sup(S_l)$ o $sup(i) < inf(S_l)$. El segundo caso es imposible porque entonces S_k aparecería antes que S_l en el ordenamiento. Consideremos el segundo caso. Se debe tener entonces que $sup(S_l) < inf(S_i)$. Pero entonces $S_i = S_l$, lo que es una contradicción.