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

Matemáticas Discretas para la Computación - CC3101
Examen - Semestre Primavera 2010

1. Un número n no primo que satisface la identidad $b^{n-1} \equiv 1 \pmod n$ para cada entero positivo $b < n$ tal que $gcd(b, n) = 1$ se denomina *número de Carmichael*.

   Sea $p_1 p_2 \cdots p_k$ la factorización prima de un entero positivo $n \geq 2$. Asuma que todos los p_j's son distintos y que $p_j - 1$ divide a $n - 1$ ($1 \leq j \leq k$). Demuestre que n es un número de Carmichael.

   Solución: Tome un b cualquiera tal que $gcd(n, b) = 1$. Para cualquier p_j, $1 \leq j \leq k$, se debe cumplir que $gcd(b, p_j) = 1$. (De otra forma, b y p_j tendrán factor primo en común, y por tanto, lo mismo ocurrirá con n y b). Por pequeño Teorema de Fermat: $b^{p_j - 1} \equiv 1 \pmod{p_j}$, para cada $1 \leq j \leq n$.

   Pero para cada $1 \leq j \leq n$ existe $k \geq 0$ tal que $b^{n-1} = b^{k(p_j - 1)}$ (porque $n - 1$ es divisible por $p_j - 1$). Luego $b^{n-1} \equiv 1 (\mathrm{mod}\, p_j)$, para cada $1 \leq j \leq n$. Pero como todos los p_j's son primos distintos, esto quiere decir que $b^{n-1} - 1$ es divisible por $p_1 p_2 \cdots p_n$. Concluimos que $b^{n-1} - 1$ es divisible por n.

2. Demuestre que si a y b son enteros positivos tal que $a > b$, entonces $(2^a - 1) \,\mathbf{mod} (2^b - 1) = 2^{a \,\mathbf{mod}\, b} - 1$.

   Solución: Asuma $a = kb + c$, donde $k \geq 1$ y $0 \leq c < a$. Entonces $2^a - 1 = 2^{kb+c} - 1$. Luego, $2^a - 1 \equiv 2^{kb+c} - 1 \pmod{2^b - 1}$. Note además que $2^{kb+c} - 1 \equiv 2^c - 1 \pmod{2^b - 1}$. Esto es porque $2^{kb+c} - 1 - (2^c - 1) = 2^c(2^{kb-1} - 1)$, y $2^{kb} - 1$ es divisible por $2^b - 1$ (suma geométrica). Concluimos que $(2^a - 1) \bmod (2^b - 1) = 2^{a \bmod b} - 1$, pues $a \bmod b = c$ y $2^b - 1 > 2^{a \bmod b} - 1$.

3. Sea $S(m, n)$ el número de funciones sobreyectivas que van desde un conjunto con m elementos hasta un conjunto con n elementos, $n \leq m$. Defina recursivamente a $S(m, n)$ en función de m, n, $C(n, k)$, para $k < n$, y $S(m, k)$, para $k < n$. Justifique su respuesta.

   Solución: $S(m, 1) = 1$ y $S(m, n) = n^m - \sum_{k=1}^{n-1} C(n, k) S(m, k)$.

4. Un *torneo* es un grafo simple y dirigido tal que si u y v son nodos distintos del grafo, entonces exactamente uno de los pares (u, v) y (v, u) es un arco del grafo.

   Demuestre que todo torneo tiene un camino Hamiltoniano; es decir, un camino simple que visita cada vértice exactamente una vez.

   Solución: Por inducción en el número n de vértices. Para $n = 1$ es trivial. Asuma que G tiene $n + 1$ vértices. Remueva un vértice v cualquiera de G. Entonces $G' = G\ v$ es un torneo, y, por hipótesis inductiva tiene camino hamiltoniano desde nodo u a u' . Si (v, u) o (u', v) son arcos en G entonces existirá camino hamiltoniano en G (desde v a u' o desde u a v). Asuma, por el contrario, que (u, v) y (v, u') son arcos en G. Entonces debe existir nodo u'' tal que (u'', v) y (u''', v) son arcos en G, donde u''' es el nodo que viene inmediatamente después que u'' en e el camino hamiltoniano de G'. Concluimos que G tiene como camino hamiltoniano el que empieza en u, sigue el camino hamiltoniano de G' hasta u'', visita v, vuelve a u''', y luego sigue el camino hamiltoniano de G hasta u'.