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

Matemáticas Discretas para la Computación - CC3101
Examen - Semestre Primavera 2014

1. *a*) (3pts) Asuma que la función $T : \mathbb{N}^+ \to \mathbb{R}$ se define como sigue: $T(1) = 1$ y $T(n) = T(n/2) + \log n$, para todo $n \geq 2$. Encuentre una función $f : \mathbb{N} \to \mathbb{N}$ tal que $T(n)$ es $\Theta(f(n))$. La función f no puede estar definida recursivamente. Justifique su respuesta.

   Solución: Asuma inicialmente que $n = 2^k$, para $k \geq 1$. Entonces es posible demostrar "desenrollando" la ecuación que $T(n) \leq T(n/2^k) + \sum_{i=0}^{k} \log(n/2^i)$. Pero $\log(n/2^i) = k - i$, por lo que $T(n) \leq T(1) + \sum_{i=0}^{k} i = T(1) + k(k+1)/2$. Por tanto, $T(n)$ en este caso es $O(\log^2 n)$. Considere ahora $2^k < n < 2^{k+1}$, para $k \geq 1$. Entonces dado que T es creciente se debe cumplir que $T(n) \leq T(2^{k+1}) \leq T(1) + (k+1)(k+2)/2$, lo que es $O(k^2)$. Claramente esto es $O(\log^2 n)$. (1,5pts).

   Para demostrar que $T(n)$ es $\Omega(\log^2 n)$ demostraremos por inducción que $T(n) \geq \frac{\log^2 n}{4}$, para todo $n \geq 1$. Claramente esto se cumple para $n = 1$. Consideremos ahora el caso inductivo $n \geq 2$. Entonces $T(n) = T(n/2) + \log n$. Por HI, $T(n) \geq \frac{\log^2(n/2)}{4} + \log n$. Basta demostrar entonces que $\frac{\log^2(n/2)}{4} + \log n \geq \frac{\log^2 n}{4}$. Claramente, $\log^2(n/2) = (\log n - 1)^2$, por lo que $\frac{\log^2(n/2)}{4} = \frac{1}{4} \cdot (\log^2 n - 2\log n + 1)$. Por tanto, basta demostrar que $1/4 - \frac{\log n}{2} + \log n \geq 0$. Esto es claramente cierto (1,5pts).

   b) (1,5pts) Considere una carrera en la que participan $n \geq 2$ competidores. Determine el número de resultados posibles de la carrera si es cada competidor puede salir solo primero, segundo o tercero. Es decir, permitimos empates entre los corredores y ningún corredor puede terminar más allá de tercero.

   Solución: Existen 3^n asignaciones de posiciones 1, 2 o 3 a los corredores, de las cuales no nos sirven las siguientes:

   - Aquellas que solo asignan valores en el conjunto $\{2, 3\}$. Hay 2^n de estas.
   - Aquellas que solo asignan valores en el conjunto $\{1, 3\}$ y que contienen al menos un valor 3. Hay $2^n - 1$ de estas.

   Por tanto, el valor total de asignaciones posibles es $3^n - 2^n - (2^n - 1) + 1$. El 1 que se suma al total corresponde a la asignación que le entrega el valor 3 a cada corredor y que fue restada dos veces.

   c) (1,5pts) Sean $C_1, \ldots, C_k$ conjuntos con r elementos cada uno, tal que $k \leq 2^{r-2}$. Los conjuntos no son necesariamente disjuntos entre si. Sea A el conjunto de elementos que aparecen en los C_i's. Coloree los elementos de A de la siguiente forma: Para cada elemento en A lance una moneda. Si sale cara el elemento se pinta azul y si sale sello se pinta rojo. Demuestre que la

probabilidad de que exista un C_i ($1 \leq i \leq k$) tal que todos los elementos de C_i tienen el mismo color es menor o igual a $1/2$.

Solución: Note que la probabilidad de que esto ocurra para un C_i particular es igual a la probabilidad de que todos los elementos en C_i sean rojos más la probabilidad de que todos los elementos en C_i sean azules. Esto es igual a $1/2^r + 1/2^r = 1/2^{r-1}$. Por tanto, la probabilidad de que exista algún C_i tal que todos sus elementos son del mismo color es $\leq k/2^{r-1}$, lo que es $\leq 1/2$.

2. Sea $G = (V, E)$ un grafo simple. Definimos $\chi(G)$ como el menor número de colores que se necesitan para colorear G y $\omega(G)$ como el tamaño del *clique* (grafo completo) más grande que está contenido en G. El subgrafo de G inducido por $V' \subseteq V$ se define como $G' = (V', E' = \{(u, v) \in E \mid u, v \in V'\})$. Un subgrafo *inducido* de G es un subgrafo de G inducido por algún $V' \subseteq V$ tal que $V' \neq \emptyset$.

   Un grafo simple G es *perfecto* si para todo subgrafo inducido G' de G se cumple que $\chi(G') = \omega(G')$.

   a) (1pto) Demuestre que existen grafos simples que no son perfectos.

   b) (1pto) Demuestre que todo grafo simple bipartito es perfecto.

   c) (4pts) Sea $G = (V, E)$ un grafo simple. Entonces $V' \subseteq V$ es *independiente* en G si para todo $u, v \in V'$ se cumple que $u = v$ o $(u, v) \notin E$.
   Demuestre que un grafo simple G es perfecto si y solo si en todo subgrafo inducido G' de G existe un conjunto independiente I de vértices tal que $\omega(G' - I) < \omega(G')$. Aquí, $G' - I$ representa el grafo que se obtiene desde G' al borrar todos los vértices en I (y, por supuesto, también los arcos que son incidentes a ellos).

   Hint: Para la dirección de derecha a izquierda ocupe inducción en el valor de $\omega(G)$.

Solución: Para la parte (a) tome un ciclo C de largo 5. Claramente, $\chi(C) = 3$ pero $\omega(C) = 2$. Por tanto, C no es perfecto. Para la parte (b) note que cualquier subgrafo inducido de un grafo bipartito es también bipartito. Por tanto, basta demostrar que para todo grafo bipartito G se cumple que $\chi(G) = \omega(G)$. Claramente $\chi(G) \leq 2$, si G es bipartito. Asuma primero que $\chi(G) = 1$. Entonces no existen arcos en G, y por tanto $\omega(G) = 1$. Asuma que $\chi(G) = 2$. Por tanto G contiene al menos un arco y $\omega(G) \geq 2$. Por otro lado, $\omega(G) \leq 2$ ya que los grafos bipartitos no contienen ciclos de largo tres.

Para la parte (c), asuma primero que G es perfecto y considere un subgrafo inducido G' cualquiera de G. Luego, $\chi(G') = \omega(G')$. Dado que el conjunto de vértices de G' no es vacío, debe existir al menos un nodo pintado de algún color, digamos rojo. Claramente el conjunto I de nodos pintados de rojo en G' es independiente. Además, $\omega(G' - I) \leq \chi(G' - I) = \chi(G') - 1 < \omega(G')$ (2pts). La otra dirección la demostraremos por inducción en el valor de $\omega(G)$. Si $\omega(G) = 1$ entonces el grafo no tiene arcos y, por tanto, es perfecto. Asuma entonces que $\omega(G) > 1$. Sea G' un subgrafo inducido cualquiera de G e I un conjunto independiente de sus vértices tal que $\omega(G' - I) < \omega(G')$. Claramente, $\omega(G' - I) < \omega(G)$, y además todo subgrafo inducido de $G' - I$ es también un subgrafo inducido de G por lo que satisface la condición. Por HI tenemos entonces que $\omega(G' - I) = \chi(G' - I)$. Por tanto, es posible colorear G' con $\omega(G' - I) + 1 \leq \omega(G')$ colores, de donde concluímos que $\chi(G') \leq \omega(G')$. La desigualdad $\chi(G') \geq \omega(G')$ se cumple por definición para todo G', por lo que concluímos que $\omega(G') = \chi(G')$. Dado que G' fue elegido arbitrariamente concluímos que G es perfecto. (2pts).

3. *a*) (1pto) Demuestre que si p es primo, entonces las únicas soluciones a la ecuación $x^2 \equiv 1 \pmod{p}$ son aquellos enteros x tal que $x \equiv 1 \pmod{p}$ o $x \equiv -1 \pmod{p}$.

   b) (3pts) Sea $p > 3$ un primo. Demuestre que los enteros en el intervalo $[2, p-2]$ pueden ser divididos en $(p-3)/2$ pares de enteros, de tal forma que los enteros en cada par son inversos uno del otro modulo p.

   c) (2pts) Desde la parte (b) concluya que si p es primo entonces $(p-1)! \equiv -1 \pmod{p}$.

Solución: Para la parte (a) note que $x^2 \equiv 1 \pmod{p}$ ssi $(x+1)(x-1) = kp$, para algún entero k. Dado que $(x+1)(x-1) \neq 0$, se debe cumplir que esto ocurre ssi p aparece en factorización prima de $(x+1)$ o en la de $(x-1)$. Es decir, esto ocurre ssi $x \equiv 1 \pmod{p}$ o $x \equiv -1 \pmod{p}$.

Para la parte (b) partimos por la observación de que un inverso a^- de a modulo p existe para todo $a \in [2, p-2]$. Esto ocurre ya que $gcd(a, p) = 1$. Podemos asumir además sin pérdida de generalidad que $a^- \in [2, p-2]$. De hecho, si a^- fuera 1, entonces $aa^- \equiv a \not\equiv 1 \pmod{p}$, lo que es una contradicción. De la misma forma, si $a^- = 0$, entonces $aa^- \equiv 0 \pmod{p}$, lo que es una contradicción. Finalmente, si $a^- = p-1$ entonces $aa^- \equiv -a \not\equiv 1 \pmod{p}$, lo que es una contradicción.

Por otro lado, para dos enteros distintos a_1, a_2 en este intervalo se tiene que $a_1^- \neq a_2^-$. De otra forma se obtendría que $a_1 \equiv a_2 \pmod{p}$, lo que es una contradicción. Además, $a^- \neq a$. Si no fuera así, tendríamos que $a^2 \equiv 1 \pmod{p}$, lo que por la parte (a) implicaría que $a^- = 1$ o $a^- = p-1$, lo que sabemos que no es posible. Por tanto, existe una función 1-1 f definida sobre $[2, p-1]$ tal que para todo $a \in [2, p-2]$ se cumple que $f(a) \neq a$ y $f(a)$ es un inverso de a modulo p. Esto demuestra lo que pedimos.

Finalmente consideramos la parte (c). Por definición, $(p-1)! = 1 \cdot (2 \cdot 3 \cdots (p-2)) \cdot (p-1)$. Pero por parte (b) se tiene que $2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$, y por tanto $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$.