Facultad de Ciencias Físicas y Matemáticas
Departamento de Ciencias de la Computación
Universidad de Chile
CC3101-01 Matemáticas de Discoteca para la Computación

Profesor: Pablo Barceló
Auxiliares: Tomás Martínez, Ignacio Riego

Auxiliar 11

Martes 20 de Junio, 2017

P1 Sean $a_1, ..., a_n$ números enteros positivos. Demuestre que existe una subsecuencia de ellos (es decir un subconjunto con índices consecutivos) que tiene suma divisible por n. Para esto considere $b_i = a_1 + ... + a_i$.

Solución: Consideremos $b_i \pmod n = b_j \pmod n$ para $i < j$ esto quiere decir que $a_{i+1} ... + a_j = k * n$ ya que sumar o restar esos números no cambia el módulo de la suma, por lo tanto encontramos nuestra subsecuencia divisible por n. En caso contrario $b_i \pmod n$ es siempre distinto para todo i, pero como hay n valores posibles, $b_i \pmod n$ debe tomarlos todos, en particular en alún momento debe tomar el valor 0, en otras palabras:

$\exists i, b_i \pmod n = 0$ por lo tanto $n|b_i$

P2 Demuestre que existen infinitos primos p tales que $p + 2$ no es primo.

Solución: Por contradicción, supongamos que son una cantidad finita de casos y sea p_f el último primo tal que $p_f + 2$ no es primo. Esto quiere decir que para todo primo p mayor a $p_f + 2$, $p+2$ es primo. Ahora consideremos uno de estos primos p, este número debe ser impar (ya que es mayor que 2) por lo tanto su último dígito puede ser $1, 3, 7, 9$, si termina en 3, $p + 2$ no puede ser primo yq que es divisible por 5, si termina en cualquier otro número puedo encontrar un k para que $p + 2k$ tenga como último dígito un 5 y por lo tanto no sea primo. Con esto nos quedan 2 posibilidades, o p_f es el último primo (lo que es imposible) o la propiedad es falsa. Con esta prueba por contradicción concluímos que hay infinitos primos que no cumplen esto.

Otra forma tal vez más simple es ver que si tomo todos los impares módulo 5 obtengo la siguiente secuencia:

1 3 0 2 4 1 3 0 ... y esta secuencia se repite. Como todos los primos mayores a 2 son impares todo primo debe encontrarse en alguna parte de esta secuencia. Ahora si tomo un primo cualquiera tal que $p + 2$ es primo y $p + 4$ es primo y así sucesivamente, esto nos permite ver que solo podemos hacer eso una cantidad limitada de veces hasta encontrar un contraejemplo, es decir que cada vez que encuentro un primo q puedo encontrar un primo p tal que $p + 2$ no es primo que será el último de la çadena"de primos que estoy formando, con lo que puedo concluir que los contraejemplos son infinitos.

P3 Considere la función $f(x) = (x \pmod 3, x \pmod 5)$. Note que $f(13) = (1, 3)$. Este hecho nos parece extremadamente curioso por lo tanto vamos a explorar el problema:

a) Compruebe que $(10u + 6v) \pmod 3 = u \pmod 3$ y $(10u + 6v) \pmod 5 = v \pmod 5$
solución: Es facil ver que $9u + 6v$ es divisible por 3, por lo tanto $10u + 6v = u + (9u + 6v)$ si aplico módulo obtengo $(u \pmod 3 + (9u + 6v) \pmod 3) \pmod 3 = u \pmod 3 \pmod 3 = u \pmod 3$. Para el caso con $\pmod 5$ es exactamente el mismo proceso.

b) Use lo anterior para encontrar todos los números de 2 díjitos $10a + b$ que cumplen $f(10a + b) = (a, b)$. Aproveche que $x(\text{mod n}) = [x(\text{mod nm})](\text{mod n})$
solución: Sabemos que los números de la forma $10u + 6v$ cumplen $f(10u + 6v) = (u, v)$ si $u < 3, v < 5$, pero nosotros queremos que el número sea de la forma $10u + v$, ese 6 nos está molestando.
Como vamos a aplicar $\pmod 5$ y $\pmod 3$, aplicar $\pmod{15}$ no va a cambiar el resultado final, en otras palabras $f(a \pmod{15}) = f(a)$. Entonces lo que queremos son números de la forma $10u + 6v$ tales que $10u + 6v \pmod{15} = 10u + v$ y obtendremos nuestras soluciones.
$10u + 6v \pmod{15} = 10u + v$ claramente esto solo es posible si u vale 1 o 0 ya que si no es imposible que se mantenga la igualdad. Luego para v, $6v \pmod{15} = v$ sol ose cumple para 0 y 3 (basta con probar los 5 valores distintos que puede tomar v para verificar). Con esto concluímos que nuestras posibilidades son $u = \{0, 1\}$ y $v = \{0, 3\}$. Y efectivamente $f(10) = (1, 0)$, $f(3) = (0, 3)$ y $f(0) = (0, 0)$

c) Para poder resolver este problema la parte a) fue fundamental pero no vimos claramente de donde salió, ahora para generalizar el problema veamos cómo encontrar ecuaciones de esta forma:

$$ku + lv \pmod{p_1} = u \pmod{p_1} \text{ y } ku + lv \pmod{p_2} = v \pmod{p_2},$$

Para p_1, p_2 primos distintos.

solución: Lo que buscamos es un par de números k, l tales que, para todo $u < p_1, v < p_2$ se cumpla:
$ku + lv \pmod{p_1} = u$ y $ku + lv \pmod{p_2} = v$.

Para que esto ocurra se debe cumplir $ku \pmod{p_1} = 1$ y $lv \pmod{p_1} = 0$ es decir que $p1|l$ y que $k \pmod{p_1} = 1$. Luego tenemos lo mismo para p_2, $p_2|k$ y $l \pmod{p_2} = 1$. Sin pérdida de generalidad vamos a asumir $p_1 < p_2$. Por lo tanto $l = sp_1$ ya que $p_1|l$, entonces $sp_1 \pmod{p_2} = 1$ se cumple cuando s es el inverso modular según p_2 de p_1, eso lo escribiremos así: $s = p_1^{-1} \pmod{p_2}$ y $l = sp_1$. Como p_2 es primo este s siempre va a existir. Ahora solo falta construir k, sabemos que $k = hp_2$ ya que p_2 lo divide, si agregamos la otra ecuación tenemos $hp_2 \pmod{p_1} = 1$.

Aquí se nos produce una pequeña dificultad ya que $p_2 > p1$ pero la solventaremos de la siguiente forma:
Impondremos $h \pmod{p_1} = h$, dado esto:
$hp_2 \pmod{p_1} = h * (p_2 \pmod{p_1}) \pmod{p_1} = 1$. Por lo tanto $h = (p_2 \pmod{p_1})^{-1} \pmod{p_1}$.
En conclusión, nuestros l, k serán:
$l = p_1 * (p_1^{-1} \pmod{p1})$ $k = p_2 * ((p_2 \pmod{p_1})^{-1} \pmod{p_1})$
Un ejemplo generado usando esto serían:
$p_1 = 7$
$p_2 = 13$
$7^{-1} \pmod{13} = 2$
$13 \pmod{7} = 6$ y $6^{-1} \pmod{7} = 6$
$k = 13 * 6 = 78$
$l = 7 * 2 = 14$

Ahora $78u + 14v \pmod{7} = u$ y $78u + 14v \pmod{13} = v$.

Si quisieramos encontrar los números a tales que $f_{7,13}(10a + b) = (a, b)$ haría falta encontrar aquellos que cumplen $78u + 14v \pmod{13 * 7} = 10u + v$. Pero esa parte es un poco matraquera así que dejamos nuestra exploración hasta acá.

P4 Grafos. Demuestre las siguientes propiedades:

a) $\chi(G) \geq \omega(G)$

b) $\chi(G) \cdot \alpha(G) \geq n$

C) Si $C = x_1, x_2, ..., x_n, x_1$ es ciclo de tamaño máximo, entonces para todo $v \notin C$, para $j \in \{1, ..., n-1\}$ se tiene que v no es vecino de x_j o de x_{j+1}.

d) Sea C como en la parte anterior. Si x_i y x_k son vecinos, entonces para cualquier $v \notin C$ se cumple que v no es vecino de x_{j+1} o no es vecino de x_{k+1}.

$\chi(G)$:= Tamaño del coloreo mínimo de G.
$\alpha(G)$:= Tamaño del independiente máximo de G.
$\omega(G)$:= Tamaño del clique máximo de G.
$\tau(G)$:= Tamaño mínimo de un vertex cover.