Facultad de Informática y Estadística

I.T.I. de Sistemas y Gestión

INTRODUCCIÓN A LA MATEMÁTICA DISCRETA

11 de septiembre de 2002

Entreguen cada ejercicio en folios separados, sin doblar las esquinas.
Escriban en cada folio "1er APELLIDO 2° APELLIDO, NOMBRE" (En **MAYÚSCULAS**).

Ejercicio 1

Responder a los siguientes apartados independientes:

1. Para cada entero no negativo n, se considera el valor $P(n)$

$$P(n) = \frac{n^7}{7} + \frac{n^3}{3} + \frac{11n}{21}$$

   (a) Demostrar usando el teorema de Fermat que en $\mathbf{Z}_3$ y en $\mathbf{Z}_7$ se verifica:

$$3n^7 + 7n^3 + 11n = 0$$

   (b) Demostrar que $P(n)$ es un entero.

2. Sea A un conjunto de 101 enteros elegidos sin repetición de $S = \{1, 2, \ldots, 200\}$

   (a) Para cada elemento $a \in A$ se considera $a = 2^k b$ con b impar y $k \geq 0$. Demostrar mediante el principio de distribución que hay dos elementos a que dan el mismo b.

   (b) Deducir que en A hay dos elementos tales que uno de ellos divide al otro.

Solución:

1. (a) **En $\mathbf{Z}_3$:**
si $3 \mid n$ entonces $3 \mid n(3n^6 + 7n^2 + 11)$ con lo que $3n^7 + 7n^3 + 11n = 0$.
Si $3 \nmid n$ entonces por el teorema de Fermat, $n^2 = 1$ con lo que
$n^3 = n^2 \cdot n = n$ y $n^7 = (n^2)^3 \cdot n = n$. Así $3n^7 + 7n^3 + 11n = 3n + 7n + 11n = 21n = 0$.
En $\mathbf{Z}_7$, se razona de forma análoga:
si $7 \mid n$ entonces $7 \mid n(3n^6 + 7n^2 + 11)$ con lo que $3n^7 + 7n^3 + 11n = 0$.
Si $7 \nmid n$ entonces por el teorema de Fermat, $n^6 = 1$ con lo que $n^7 = n$ y $7n^3 = 0$.
Así $3n^7 + 7n^3 + 11n = 3n + 11n = 14n = 0$.

   (b) Sea $P(n) = \dfrac{n^7}{7} + \dfrac{n^3}{3} + \dfrac{11n}{21} = \dfrac{3n^7 + 7n^3 + 11n}{21}$
Según el apartado anterior, $3n^7 + 7n^3 + 11n = 0$ en $\mathbf{Z}_3$ y en $\mathbf{Z}_7$, por lo que $3n^7 + 7n^3 + 11n$ es simultáneamente múltiplo de 3 y de 7, siendo en consecuencia múltiplo de 21.
Queda así demostrado que $P(n)$ es un entero.

2. (a) A es un conjunto con 101 elementos, sin repetir y elegidos entre los del conjunto $S = \{1, 2, \ldots, 200\}$; al ser cada elemento $a \in A$, de la forma $a = 2^k b$, siendo b impar y $k \geq 0$, resulta que los valores b deben pertenecer al conjunto $\{1, 3, \ldots, 199\}$, el cual tiene sólo 100 elementos. Los 101 elementos del conjunto A dan lugar a 101 elementos b que sólo pueden tomar valores en un conjunto con 100 elementos, aplicando el principio de distribución, al menos dos elementos b se deben repetir, es decir, existen dos elementos $a_1, a_2 \in A$ tales que, $a_1 = 2^k \cdot b, \quad a_2 = 2^r \cdot b \quad$ con el mismo valor de b.

   (b) Según el apartado anterior, $a_1 = 2^k \cdot b, \quad a_2 = 2^r \cdot b \quad$ con $k \geq 0$, $r \geq 0$ y $k \neq r$. Como los enteros están ordenados se tiene que cumplir que $k > r$ o bien $r > k$. Vamos a suponer que $k > r$, por lo que $k = r + s$ para algún valor de $s > 0$. Sustituyendo: $a_1 = 2^k \cdot b = 2^r \cdot 2^s \cdot b = 2^s \cdot (2^r \cdot b) = 2^s \cdot a_2 \quad$, resultando que a_2 divide a a_1.

Ejercicio 2

El código de barras de cualquier producto consta de 13 dígitos decimales $\{0, 1, 2, \ldots, 9\}$. Los 7 primeros $a_0, \ldots, a_6$ se refieren a los datos del fabricante; los 5 siguientes dan información acerca del producto y el último, a_{12}, es un dígito de control que es capaz de detectar errores de lectura. La fórmula que se debe verificar para que los datos sean correctos es:

$$3(a_1 + a_3 + a_5 + a_7 + a_9 + a_{11}) + a_0 + a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12} \equiv 0 \ (mod\ 10)$$

Se pide:

1. Demostrar que si hay exactamente un error de lectura, el sistema siempre lo detecta.
2. Si el escáner no lee un dígito (y sabe cuál es su posición), demostrar que el sistema es capaz de calcularlo.
3. Demostrar que si se intercambian dos dígitos consecutivos (por ejemplo, a_0, a_1) entonces el sistema detecta el error siempre que la diferencia entre ellos no sea 5.

Solución:

1. Sean $a = (a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12})$ el código y $b = (b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7, b_8, b_9, b_{10}, b_{11}, b_{12})$ la lectura.
   Por ser el código a correcto, debe verificar la fórmula dada, es decir:

   $$3(a_1 + a_3 + a_5 + a_7 + a_9 + a_{11}) + a_0 + a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12} \equiv 0 \ (mod\ 10)$$

   Si b fuera correcto cumpliría

   $$3(b_1 + b_3 + b_5 + b_7 + b_9 + b_{11}) + b_0 + b_2 + b_4 + b_6 + b_8 + b_{10} + b_{12} \equiv 0 \ (mod\ 10)$$

   La diferencia de dos valores múltiplos de 10 es múltiplo de 10, por lo que si restamos ambas expresiones debe cumplir:

   $$3(a_1 + a_3 + a_5 + a_7 + a_9 + a_{11} - b_1 - b_3 - b_5 - b_7 - b_9 - b_{11})$$

$$+a_0 + a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12} - b_0 - b_2 - b_4 - b_6 - b_8 - b_{10} - b_{12} \equiv 0 \ (mod\ 10)$$

Hay dos situaciones a considerar:

Si el error de lectura está en una posición de subíndice impar, por ejemplo a_1, la expresión anterior resulta $3(a_1 - b_1) \equiv 0 \ (mod\ 10)$, y puesto que $a_1 \neq b_1$ se llega a una congruencia imposible, detectándose que hay un error.

Si el error de lectura está en una posición de subíndice par, por ejemplo a_2, la expresión anterior resulta $a_2 - b_2 \equiv 0 \ (mod\ 10)$ y puesto que $a_2 \neq b_2$, igualmente se detecta que hay un error.

2. Si suponemos que el dígito que no lee tiene una posición de subíndice impar, por ejemplo a_1, como sabemos que los datos del código verifican la fórmula dada, resulta que

$$A = 3(a_3+a_5+a_7+a_9+a_{11})+a_0+a_2+a_4+a_6+a_8+a_{10}+a_{12} \equiv -3a_1 \ (mod\ 10) \equiv 7a_1 \ (mod\ 10)$$

Como 7 es primo con 10, es invertible, siendo el inverso de 7 el 3.
$3 \cdot 7 = 21 \equiv 1 \ (mod\ 10)$. Por lo tanto el sistema es capaz de calcular el valor del dígito no leído $\quad a_1 = 3A \ (mod\ 10)$.

Si suponemos que el dígito que no lee tiene una posición de subíndice par, por ejemplo a_2, se obtendría

$$B = 3(a_1 + a_3 + a_5 + a_7 + a_9 + a_{11}) + a_0 + a_4 + a_6 + a_8 + a_{10} + a_{12} \equiv -a_2 \ (mod\ 10)$$

resultando $B = 9a_2 \ (mod 10)$, y como $9 = 9^{-1} \ (mod\ 10)$ el valor del dígito no leído en este caso es $\quad a_2 = 9B \ (mod\ 10)$

3. Con la lectura correcta la fórmula es:

$$3(a_1 + a_3 + a_5 + a_7 + a_9 + a_{11}) + a_0 + a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12} \equiv 0 \ (mod 10)$$

Al intercambiar los dígitos a_0, a_1 consecutivos la fórmula dada resulta:

$$3(a_0 + a_3 + a_5 + a_7 + a_9 + a_{11}) + a_1 + a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12} \equiv K \ (mod 10)$$

Si restamos se obtiene: $3(a_0 - a_1) + a_1 - a_0 \equiv K \ (mod 10)$
$2a_0 - 2a_1 = 2(a_0 - a_1) \equiv K \ (mod\ 10)$, y por tanto el sistema detectará el error siempre que $K \neq 0 \ (mod\ 10)$. Esto ocurre sólo para $a_0 - a_1 \equiv 5 \ (mod\ 10)$.

Ejercicio 3

Responder a los siguientes apartados independientes:

1. Sean p_1, p_2, p_3 tres números primos diferentes y $x = p_1^\alpha \cdot p_2^\beta \cdot p_3^\gamma$. Sabiendo que :

   a) $\phi(x) = 480$
   b) $25 \mid x$, $8 \mid x$
   c) $125 \nmid x$, $64 \nmid x$

   Hallar **todos** los posibles valores para x.

2. Si $F_0 = 0,\ F_1 = 1, \quad F_{n+1} = F_n + F_{n-1}$ para $n \geq 1$

   Demostrar por inducción que :

$$\forall n \geq 1 \qquad F_{n+1} \cdot F_{n-1} - F_n^2 = (-1)^n$$

Solución:

1. Si se conoce la descomposición en factores primos de x, $x = p_1^\alpha \cdot p_2^\beta \cdot p_3^\gamma$,
   también conocemos su función ϕ de Euler, que será:
   $\phi(x) = p_1^{\alpha-1} \cdot p_2^{\beta-1} \cdot p_3^{\gamma-1} \cdot (p_1 - 1) \cdot (p_2 - 1) \cdot (p_3 - 1)$
   Como $8 \mid x$ pero $64 \nmid x$, para $p_1 = 2$, α debe verificar $3 \leq \alpha \leq 5$.
   Como $25 \mid x$ pero $125 \nmid x$, si $p_2 = 5$, $\beta = 2$
   Sabemos que $\phi(x) = \phi(2^\alpha) \cdot \phi(5^2) \cdot \phi(p_3^\gamma) = 480$
   $\phi(5^2) = 20$; $\phi(2^\alpha) = 2^{\alpha-1} \cdot (2-1)$ y $\phi(p_3^\gamma) = p_3^{\gamma-1} \cdot (p_3 - 1)$

   Como $3 \leq \alpha \leq 5$, los casos posibles son:

   (a) $\alpha = 3$. Sustituyendo en lo anterior resulta:
   $\phi(x) = 480 = 4 \cdot 20 \cdot \phi(p_3^\gamma)$, de donde se deduce que $\phi(p_3^\gamma) = 6$ y por tanto:
   o bien $p_3^\gamma = 7^1$ siendo $x = 2^3 \cdot 5^2 \cdot 7 = 1400$,
   o bien $p_3^\gamma = 3^2$ y $x = 2^3 \cdot 5^2 \cdot 3^2 = 1800$.

   (b) $\alpha = 4$. Sustituyendo en lo anterior resulta:
   $\phi(x) = 480 = 8 \cdot 20 \cdot \phi(p_3^\gamma)$, de donde se deduce que $\phi(p_3^\gamma) = 3$. Esta situación es imposible ya que la función ϕ nunca toma el valor 3, ya que $\phi(\quad)$ devuelve siempre valores pares.

   (c) $\alpha = 5$. Resulta:
   $\phi(x) = 480 = 16 \cdot 20 \cdot \phi(p_3^\gamma)$. De aquí se deduce que $\phi(p_3^\gamma) = \dfrac{3}{2}$. Esta situación es imposible ya que la función ϕ siempre toma valores enteros.

   Como conclusión, los únicos valores que cumplen las condiciones anteriores son 1400 y 1800.

2. Para actuar por inducción primero consideramos un caso inicial $n = 1$.
   Como $F_0 = 0,\ F_1 = 1,$ se verifica la expresión.

$$F_2 \cdot F_0 - F_1^2 = 1 \cdot 0 - 1^2 = -1 = (-1)^1$$

   Supongamos que es cierta para $k = 1, 2, \ldots, n$ y lo probaremos para $k = n + 1$

$$F_{n+2} \cdot F_n - (F_{n+1})^2 = (F_n + F_{n+1})F_n - F_{n+1}^2 =$$
$$F_{n+1} \cdot F_n + F_n^2 - F_{n+1}^2 = F_{n+1}(F_n - F_{n+1}) + F_n^2 = -F_{n+1}F_{n-1} + F_n^2 =$$
$$-(F_{n+1}F_{n-1} - F_n^2) = -(-1)^n = (-1)^{n+1}$$

   quedando demostrada la igualdad para todo $n \geq 1$.