Universidad de la República
Facultad de Ingeniería.

Solución Examen de Matemática Discreta II
17 de febrero de 2014

1. *a*) Sean a, b, n enteros positivos tales que $d = \text{mcd}(a, n)$, con $d \neq 1$ y $d \mid b$
   Hallar todas las soluciones de $ax \equiv b$ mód (n). ¿Cuántas soluciones hay entre 1 y n?

   b) Resolver la ecuación diofántica $2x \equiv 14$ mód(80).

   c) Sea n el mayor natural mayor que 1 y menor que 80 que es solución de la ecuación de la parte anterior. Determinar cuántas raíces primitivas tiene $U(n)$, y hallar la menor de todas.

   Resolución:

   a) Como d =mcd(a, n), entonces, consideramos, $a' = \frac{a}{d}$ y $n' = \frac{n}{d}$. Recordemos que $\text{mcd}(a', n') = 1$. Definimos también $b_0 = \frac{b}{d} \in \mathbb{Z}$, pues $d \mid b$. Tenemos que $ax \equiv b$ mód $(n) \Leftrightarrow$ existe $t \in \mathbb{Z}$ tal que $ax - b = tn$. Esto se cumple si y solo si existe $t \in \mathbb{Z}$ tal que $a'x - b_0 = tn'$ o sea si y solo si $a'x \equiv b_0$ mód(n'). Como $\text{mcd}(a', n') = 1$, existe el inverso de a' en U(n'), y por lo tanto la ecuación anterior es equivalente a: $x \equiv (a')^{-1} b_0$ mód(n'). O sea las soluciones de la ecuación inicial son de la forma: $x = (a')^{-1} b_0 + un'$, con $u \in \mathbb{Z}$.

   El número de soluciones entre 1 y n las calculamos planteando: $1 \leq \alpha + un' \leq n = dn'$, siendo $\alpha = (a')^{-1} b_0$. La doble inecuación anterior es equivalente a: $\frac{1}{n'} - \frac{\alpha}{n'} \leq u \leq d - \frac{\alpha}{n'}$ con $u \in \mathbb{Z}$. Como $d - \frac{\alpha}{n'} - (\frac{1}{n'} - \frac{\alpha}{n'}) = d - \frac{1}{n'}$, en ese rango siempre encontramos d soluciones.

   b) Por lo visto arriba las soluciones son $x = 7 + 40t$ con $t \in \mathbb{Z}$.

   c) Entre 1 y 80 tenemos las soluciones 7 y 47. Entonces $n = 47$. Luego, $U(47)$ tiene, por lo visto en teórico, $\phi(\phi(47))$ raíces primitivas, siendo ϕ la función de Euler. Entonces $\phi(\phi(47)) = \phi(46) = \phi(2 \times 23) = \phi(23) = 22$. La menor raíz primitiva de 47 es 5, pues $2^{23} \equiv 1$ mód(47) y también $3^{23} \equiv 1$ mód(47) (por lo tanto 2 y 3 no son raíces primitivas) y por su parte $5^{23} \not\equiv 1$ mód(47) y $5^2 = 25 \not\equiv 1$ mód(47).

2. *a*) Sea $\sigma \in S_n$ y $\sigma = c_1 \dots c_n$ producto de ciclos disjuntos.
      1) Escribir $o(\sigma)$ en función de $o(c_1), \dots, o(c_n)$
      2) Probar el resultado enunciado en 1).

   b) Considerar $\mathbb{Z}_{30}$. Exhibir elementos $a, b \in \mathbb{Z}_{30}$ tales que $o(a + b) < \text{mcm}(o(a), o(b))$.

   c) Dado $(G, \cdot)$ grupo finito y $x, y \in G$ con $xy = yx$ entonces, si $a = o(x)$, $b = o(y)$, m =mcm(a, b) y d =mcd(a, b), demostrar que $\frac{m}{d} | o(xy)$ y que $o(xy) | m$.

   Resolución:

   a) 1) Se tiene que $o(\sigma) = \text{mcm}(o(c_1), \dots, o(c_n))$. O sea el orden de la permutación σ es el menor entero positivo que es múltiplo de todos los órdenes de los ciclos $c_1, c_2, ..., c_n$.

      2) Para demostrar la afirmación anterior llamemos $\beta = \text{mcm}(o(c_1), \dots, o(c_n))$. Tenemos que existen enteros positivos ν_i tal que $\beta = \nu_i \times o(c_i)$, para todo $i = 1, 2, ..., n$. Entonces $\sigma^\beta = (c_1 \dots c_n)^\beta = c_1^\beta . c_2^\beta . \cdots . c_n^\beta$, porque, al ser ciclos disjuntos, conmutan entre sí. Luego, cada $c_i^\beta = c_i^{\nu_i \times o(c_i)} = (c_i^{o(c_i)})^{\nu_i} = (id)^{\nu_i} = \text{id}$, para todo $i = 1, 2, ..., n$. Por lo tanto $\sigma^\beta = \text{id}$ y esto implica que o$(\sigma) \mid \beta$.

Por el otro lado, como $\sigma = c_1 \ldots c_n$, se tiene que $(c_1 \ldots c_n)^{o(\sigma)}$ =id. Como son ciclos disjuntos, conmutan entre sí, por lo que se obtiene: $c_i^{o(\sigma)} = c_1^{o(\sigma)}.c_2^{o(\sigma)}.\cdots.c_{i-1}^{o(\sigma)}.c_{i+1}^{o(\sigma)}.\cdots.c_n^{o(\sigma)}$. La igualdad anterior es posible si y solo si para todo $i = 1, ..., n$, $c_i^{o(\sigma)} = \mathrm{id} = c_1^{o(\sigma)}.c_2^{o(\sigma)}.\cdots.c_{i-1}^{o(\sigma)}.c_{i+1}^{o(\sigma)}.\cdots.c_n^{o(\sigma)}$ pues todos los ciclos son disjuntos. O sea que $\mathrm{o}(c_i) \mid \mathrm{o}(\sigma)$, para todo $i = 1, 2, ..., n$, por lo tanto $\beta = \mathrm{mcm}(o(c_1), \ldots, o(c_n)) \mid \mathrm{o}(\sigma)$.

O sea, hemos probado que $\mathrm{o}(\sigma) = \beta$.

b) Es posible considerar muchas parejas que ejemplifiquen lo que se pide. Una pareja posible es: $a = 10$ y $b = 5$, pues $\mathrm{o}(10) = 3$, $\mathrm{o}(5) = 6$, mientras que $\mathrm{o}(10 + 5) = 2$.

c) Sean $a' = \frac{a}{d}$ y $b' = \frac{b}{d}$. Sabemos que m=mcm$(a, b) = ab' = a'b$. Consideramos $(xy)^m = x^m y^m$, pues x e y conmutan. Luego $(xy)^m = x^m y^m = (x^a)^{b'}(y^b)^{a'} = (id)^{b'}(id)^{a'} = id$. Por lo tanto $\mathrm{o}(xy) \mid m$.

Para abreviar llamemos t =o(xy). Entonces $\mathrm{id} = (xy)^t = x^t y^t$, con lo que tenemos que $x^t = y^{-t}$. Luego $x^{ta} = (x^t)^a = (x^a)^t = \mathrm{id}$. Pero también: $x^{tb} = (x^t)^b = (y^{-t})^b = (y^b)^{-t} = \mathrm{id}$. Como $d = \mathrm{mcd}(a, b)$, por el Lema de Bezout, existen α y β enteros tales que $d = \alpha a + \beta b$. Entonces $x^{td} = x^{t(\alpha a + \beta b)} = (x^{ta})^\alpha (x^{tb})^\beta = \mathrm{id}$. O sea: $x^{td} = \mathrm{id}$. Por lo tanto $a = \mathrm{o}(x) \mid td$, o sea $a' \mid t$.

Análogamente se puede probar que $y^{td} = \mathrm{id}$ con lo cual se concluye que $b = \mathrm{o}(y) \mid td$, o sea $b' \mid t$. Pero, recordemos que $\mathrm{mcd}(a', b') = 1$, por lo que $a'b' \mid t$. Conculyendo: $\frac{m}{d} = a'b' \mid \mathrm{o}(xy)$.

3. *a*) Calcular:
   - 41^{-1} mód(71);
   - 71^{-1} mód(41).

   b) Calcular 236^3 mód(2911) y 317^3 mód(2911).

   Sugerencia: usar el Teorema Chino del Resto.

   c) Sean $p = 41$, $q = 71$ y $n = p.q$.
   - ¿El par $(2911, 3)$ sirve como clave pública para *RSA*? Justifique.
   - Se usa *Cifrado en Bloques* para encriptar un texto. ¿Cuántos dígitos ha de tener cada bloque de entrada? ¿Cuántos dígitos ha de tener cada bloque de salida del texto encriptado?

   d)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

   En base a la tabla, encripte, usando *RSA* y *Cifrado en Bloques* el texto: CHIMBOLI.

Resolución:

a) Para buscar 41^{-1} mód(71) necesitamos hallar $1 \leq x \leq 70$ tal que $41x \equiv 1$ mód(71). Como $41 \equiv -30$ mód(71), debemos resolver $30x \equiv -1$ mód(71) $\Leftrightarrow 2 \times 3 \times 5 \times x \equiv -1$ mód(71) $\Leftrightarrow 3 \times 5 \times x \equiv -36$ mód(71) $\Leftrightarrow 3 \times 5 \times x \equiv 35$ mód(71) $\Leftrightarrow 5 \times x \equiv 24 \times 35$ mód(71) $\Leftrightarrow 5 \times x \equiv 59$ mód(71) $\Leftrightarrow x \equiv 57 \times 59$ mód(71), pues 36 es el inverso de 2, 24 es el inverso de 3 y 57 es el inverso de 5 en U(71). Como 57×59 mód(71) $\equiv 19 \times 3 \times 59$ mód(71) $\equiv 19 \times 35$ mód(71) $\equiv 19 \times 5 \times 7$ mód(71) $\equiv 24 \times 7$ mód(71) $\equiv 2 \times 12 \times 7$ mód(71) $\equiv 2 \times 13$ mód(71) $\equiv 26$ mód(71). Por lo tanto 26 es el inverso de 41 módulo 71. O sea existe $t \in \mathbb{Z}$, tal que $26 \times 41 - 1 = 71 \times t$. Como $26 \times 41 = 1066$, diviendo entre 71 se obtiene t: $26 \times 41 = 15 \times 71 + 1$, por lo tanto $26 \times 41 + (-15) \times 71 = 1$. Luego tenemos los coeficientes de Bezout y los inversos que buscamos: -15=26 es el inverso de 71 módulo 41 y 26 es el inverso de 41 módulo 71.

b) Para calcular 236^3 mód(2911) y 317^3 mód(2911), observemos que $2911 = 41 \times 71$. Por lo tanto comenzamos resolviendo 236^3 mód(41) y 236^3 mód(71).

Tenemos que 236^3 mód$(41) \equiv 31^3$ mód$(41) \equiv (-10)^3$ mód$(41) \equiv (-10) \times 18$ mód$(41) \equiv (-2) \times 5 \times 18$ mód$(41) \equiv (-2) \times 8$ mód$(41) \equiv 25$ mód(41).

Por su lado 236^3 mód$(71) \equiv 23^3$ mód$(71) \equiv (48)^2 \times 23$ mód$(71) \equiv 48 \times 2 \times 24 \times 23$ mód$(71) \equiv 25 \times 24 \times 23$ mód$(71) \equiv 25 \times 3 \times 8 \times 23$ mód$(71) \equiv 4 \times 8 \times 23$ mód$(71) \equiv 21 \times 8$ mód$(71) \equiv 13 \times 2$ mód$(71) \equiv 26$ mód(41).

Luego, con lo obtenido hasta ahora, y lo calculado en el item anterior, por el teorema chino del resto, podemos concluir que: $236^3 = 25 \times 71 \times 26 + 26 \times 41 \times 26$ mód(2911). O sea, $236^3 \equiv 73866$ mód$(2911) \equiv 1091$ mód(2911).

Con el mismo tipo de técnicas y apoyándonos nuevamente en el item anterior se puede calcular que $317^3 \equiv 2851$ mód(2911).

c)
- El par $(2911, 3)$ sirve como clave pública para RSA pues 2911$= 41 \times 71$ siendo 41 y 71 números primos, y además el $\text{mcd}(3, \phi(2911)) = 1$, pues $\phi(2911) = 40 \times 70 = 2^4 \times 5^2 \times 7$ (donde ϕ es la función de Euler).
- Como son 28 dígitos, buscamos $k \in I\!N$ tal que $28^k < n < 28^{k+1}$. Entonces $k = 2$. Por lo tanto los bloques de entrada tendrán 2 dígitos y los de salida tendrán 3.

d) El texto encriptado es: DJIBK BEÑCUL.