

Primer parcial de Matemática Discreta II  
8 de mayo del 2007

Soluciones.

**Ejercicio 1.** Sea  $d = \text{mcd}(a, b)$ , tenemos que:

$$d = (b, 12) = (b, 3) = 1 \text{ ó } 3$$

donde la primera igualdad es porque  $a \equiv 12 \pmod{b}$  y la segunda igualdad porque  $b$  es impar.

Caso  $d = 1$ :  $ab = 12636 = 2^2 3^5 13$ .

Como  $b$  es impar entonces  $b|3^5 13$  y dado que  $d = \text{mcd}(b, 3) = 1$  entonces  $b|13$ .

Si  $b = 1$  entonces  $a = 12636$  y funciona.

Si  $b = 13$  entonces  $a = 972 \equiv 10 \pmod{13}$  así que no sirve.

Caso  $d = 3$ : Escribimos  $a = 3a'$  y  $b = 3b'$  con  $\text{mcd}(a', b') = 1$ .

Como  $ab = 12636 = 2^2 3^5 13$ , entonces  $a'b' = 2^2 3^3 13$  como  $b'$  es impar (pues  $b$  lo es) tenemos  $b'|3^3 13$ . Dado además que  $a'$  y  $b'$  son coprimos  $b' = 1, 3^3, 13$  ó  $3^3 13$  es decir  $b = 3, 3^4, 3 \cdot 13$  ó  $3^4 13$ .

Si  $b = 3$ ,  $a = 2^2 3^4 13$  verifica.

Si  $b = 3^4$ ,  $a = 2^2 \cdot 3 \cdot 13$  no verifica la primera.

Si  $b = 3 \cdot 13$ ,  $a = 2^2 3^4$  verifica.

Si  $b = 3^4 13$ ,  $a = 2^2 3$  verifica.

Las parejas  $(a, b)$  de soluciones son:  $(12636, 1)$ ,  $(4212, 3)$ ,  $(324, 39)$  y  $(12, 1053)$

**Ejercicio 2.** a) Si  $n = 3q$  entonces  $2^n = 2^{3q} \equiv 8^q \equiv 1^q \equiv 1 \pmod{7}$ .

Si  $n = 3q + 1$  entonces  $2^n = 2^{3q+1} \equiv 8^q \cdot 2 \equiv 1^q \cdot 2 \equiv 2 \pmod{7}$ .

Si  $n = 3q + 2$  entonces  $2^n = 2^{3q+2} \equiv 8^q \cdot 4 \equiv 1^q \cdot 4 \equiv 4 \pmod{7}$ .

Así que los únicos  $n$  que verifican son los múltiplos de 3.

b) Se tiene que  $a = 6$  y el sistema a resolver es:

$$\begin{cases} 7x \equiv 3 \pmod{17} \\ 6x \equiv 7 \pmod{11} \end{cases}$$

tenemos que  $7^{-1} \pmod{17} = 5$  y  $6^{-1} \pmod{11} = 2$  así que el sistema anterior es equivalente a:

$$\begin{cases} x \equiv 15 & (\text{mód } 17) \\ x \equiv 3 & (\text{mód } 11) \end{cases}$$

vemos que 168 es solución del sistema y por el Teorema del Resto Chino todas las soluciones son:

$$x = 168 + 187t, \quad \text{con } t \in \mathbb{Z}$$

- Ejercicio 3.** (a) Como  $p > 3$  es primo no puede ser múltiplo de 3, luego  $p \equiv \pm 1 \pmod{3} \Rightarrow p^4 \equiv 1 \pmod{3}$ , es decir  $p^4 - 1 = 3$ .
- (b)  $p = 2k+1$  por ser impar así que  $p^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k(k+1) = 8$ . Así que  $n = (p^2 - 1)(p^2 + 1) = 16$ , pues  $p^2 + 1 = 2$ .
- (c) Como  $p > 5$  es primo entonces  $p^4 \equiv 1 \pmod{p}$  por Fermat.
- (d) 1.  $c = at_1 = bt_2$  con  $t_1$  y  $t_2$  enteros, así que  $a|bt_2$  como  $\text{mcd}(a, b) = 1$  entonces  $a|t_2$  (Lema de Euclides). Si  $t_2 = ah$  entonces  $c = bah$ , luego  $ab|c$ .

$$2. \text{ iterando lo anterior, como } \left. \begin{array}{l} 5|p^4 - 1 \\ 16|p^4 - 1 \\ 3|p^4 - 1 \end{array} \right\} \Rightarrow 240|p^4 - 1$$

- (e) Por la parte a),  $p_i^4 \equiv 1 \pmod{3}$  para todo  $i = 1, 2, \dots, 9$ , luego  $p_1^4 + p_2^4 + \dots + p_9^4 \equiv 9 \equiv 0 \pmod{3}$ . Como además  $p_1^4 + p_2^4 + \dots + p_9^4 > 3$  no puede ser primo.

- Ejercicio 4.** (a) Ver apuntes teórico.
- (b) Ver apuntes teórico.
- (c) Utilizamos el método de Fermat:  
 $320347 + 1^2 = 320348$  no es cuadrado.  
 $320347 + 2^2 = 320351$  no es cuadrado.  
 $320347 + 3^2 = 566^2 \Rightarrow 320347 = 566^2 - 3^2 = 563 \cdot 569$  así que  $p = 563$  y  $q = 569$ .
- (d) Hay que hallar  $d$  tal que  $de \equiv 1 \pmod{\varphi(n)}$ . Tenemos que:

$$\varphi(n) = \varphi(pq) = (p-1)(q-1) = 562 \cdot 568 = 319216$$

Para resolver  $935d \equiv 1 \pmod{319216}$ , consideramos primero la ecuación diofántica  $935y + 319216q = 1$  y tenemos que  $319216q \equiv 1 \pmod{935}$ , como  $935 = 5 \cdot 11 \cdot 17$  esta congruencia equivale al sistema de congruencias:

$$\begin{cases} 7q \equiv 1 & (\text{mód } 11) \\ 7q \equiv 1 & (\text{mód } 17) \\ q \equiv 1 & (\text{mód } 5) \end{cases}$$

o equivalentemente:

$$\begin{cases} q \equiv 8 & (\text{mód } 11) \\ q \equiv 5 & (\text{mód } 17) \\ q \equiv 1 & (\text{mód } 5) \end{cases}$$

Usando el Teorema del Resto Chino tenemos que:  $q \equiv 481 \pmod{935}$ , luego  $y = (1 - 319216q)/935$ , tomando  $q = 481$  obtenemos  $y = -164217$ , luego  $d = y \pmod{319216} = 154999$ .

La función de descriptar viene dada por:

$$D : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, \quad D(y) = y^{154999} \pmod{320347}$$