

Examen de Matemática Discreta II
13 de julio de 2009

Solución al ejercicio 1:

1) Aplicamos el Algoritmo de Euclides con 66 y 35:

$$66 = 2 \cdot 35 - 4, \quad 35 = 9 \cdot 4 - 1$$

Así que $1 = -35 + 9 \cdot 4 = -35 + 9(2 \cdot 35 - 66) = -35 + 18 \cdot 35 - 9 \cdot 66 = 17 \cdot 35 - 9 \cdot 66$ así que $h = 17$ verifica.

2) Volvemos a aplicar el Algoritmo de Euclides con 101 y 85:

$$101 = 1 \cdot 85 + 16, \quad 85 = 5 \cdot 16 + 5, \quad 16 = 3 \cdot 5 + 1$$

Así que $1 = 16 - 3 \cdot 5 = 16 - 3(85 - 5 \cdot 16) = 16 - 3 \cdot 85 + 15 \cdot 16 = 16 \cdot 16 - 3 \cdot 85 = 16(101 - 85) - 3 \cdot 85 = 16 \cdot 101 - 16 \cdot 85 - 3 \cdot 85 = 16 \cdot 101 - 19 \cdot 85$.

En resumen $16 \cdot 101 - 19 \cdot 85 = 1$, tomando congruencia módulo 101 resulta que $-19 \cdot 85 \equiv 1 \pmod{101} \Rightarrow 85^{-1} \equiv -19 \equiv 82 \pmod{101}$ (es decir, 85 es invertible módulo 101 y su inverso es 82).

3) Tenemos que $a \equiv a^{101} \equiv a^{35} \cdot a^{66} \equiv 44 \cdot (-16) = -704 \equiv 3 \pmod{101}$ (donde en la primer congruencia hemos aplicado Fermat).

Solución al ejercicio 2.

a) Para todo $x, y \in U(p)$ se tiene que $\psi(xy) = (xy)^2 = x^2 y^2 = \psi(x)\psi(y)$ (donde en la segunda igualdad se ha usado que $U(p)$ es abeliano).

b) $x \in N(\psi) \Leftrightarrow x^2 \equiv 1 \pmod{p} \Leftrightarrow x^2 - 1 = (x-1)(x+1) \equiv 0 \pmod{p}$ y como p es primo esto equivale a que $x-1 \equiv 0 \pmod{p}$ ó $x+1 \equiv 0 \pmod{p}$ por lo tanto $x \equiv \pm 1 \pmod{p}$.

c) La función ψ es un morfismo con kernel $\{1, -1\}$ así que el resultado es directo usando el Primer Teorema de Isomorfismos. Tomando cardinales tenemos que:

$$|Im(\psi)| = \frac{|U(p)|}{|\{1, -1\}|} = \frac{p-1}{2}$$

d) Sea $x \in Im(\psi)$ un resto cuadrático, entonces $\langle x \rangle < Im(\psi)$, por lo tanto el orden de x es $o(x) = |\langle x \rangle| \leq |Im(\psi)| = (p-1)/2 < p-1$, por lo tanto x no es una raíz primitiva.

e) El número de raíces primitivas es $\varphi(\varphi(p)) = \varphi(2^{2^h}) = 2^{2^h-1} = p-1/2$.

f) Por la parte d) los restos cuadráticos no pueden ser raíces primitivas, pero existen exactamente $p-1-(p-1/2) = p-1/2$ elementos que no son restos cuadráticos que es la misma cantidad de raíces primitivas (por parte e)), por lo tanto esos conjuntos coinciden, es decir, los no restos cuadráticos son las raíces primitivas.

Solución al ejercicio 3.

a) Ver Teórico, libro de Coutinho ó apuntes en pdf en la página web.

b) De acuerdo al protocolo Diffie-Hellman, Pedro puede calcular la clave como $34^{41} \pmod{89}$. Con la idea de hacer exponenciación rápida calculemos $34^2, 34^4, 34^8, \dots$

$34^2 = 1156 \equiv 88 \equiv -1 \pmod{89}$, $34^4 = (34^2)^2 \equiv (-1)^2 \equiv 1$. En el camino, nos hemos topado con el orden de 34, entonces tenemos una forma mucho mas corta de resolverlo (usando el algoritmo de división):

$$34^{41} = (34^4)^{10} \cdot 34^1 \equiv 34 \pmod{89}$$

Por lo tanto la clave secreta acordada es $k = 34$.

c) Como $34 = 3 \cdot 11 + 1$, la palabra clave para ser usada en Vigenere (con la correspondencia dada en el cuadrito) es HC, teniendo la clave es sencillo descriptar el mensaje (colocando la clave repetida varias veces debajo del texto encriptado y restando), nos queda en este caso: NO COPIEN.