

Solución del Examen de Matemática Discreta 2 del 13 de Diciembre de 2010

Ejercicio 1.

- (a) $\sigma = (1\ 2\ 3\ 4\ 5)$ es un 5-ciclo y por lo tanto tiene orden 5. Es fácil ver que elemento $\alpha = \sigma(6\ 7)$ tiene orden 10 (por ejemplo si k es impar se tiene que $\alpha^k = \sigma^k(6\ 7) \neq \text{id}$ y si k es par $\alpha^k = \sigma^k$ y por lo tanto el menor exponente tal que $\alpha^k = \text{id}$ es $k = 10$).
- (b) *Enunciado:* $o(\gamma\sigma) = \text{mcm}(k, l)$. *Dem:*
Como los ciclos son disjuntos entonces conmutan y por lo tanto $(\gamma\sigma)^n = \gamma^n\sigma^n$; entonces $(\gamma\sigma)^{\text{mcm}(k, l)} = \gamma^{\text{mcm}(k, l)}\sigma^{\text{mcm}(k, l)} = (\gamma^k)^{\frac{l}{\text{mcd}(k, l)}}(\sigma^l)^{\frac{k}{\text{mcd}(k, l)}} = \text{id}$.
Y si $(\gamma\sigma)^n = \text{id}$, entonces $\gamma^n\sigma^n = \text{id}$ y por lo tanto $\gamma^n = \sigma^{-n}$. Pero como γ y σ son ciclos disjuntos, sólo puede pasar si $\gamma^n = \text{id}$ y $\sigma^{-n} = \text{id}$. Entonces $k|n$ y $l|n$ y por lo tanto $\text{mcm}(k, l)|n$.
- (c) Si los ciclos no son disjuntos el enunciado no es cierto; por ejemplo tomando $\sigma = (1\ 2) = \gamma$ se tiene $\sigma\gamma = \text{id}$ y por lo tanto el orden de $\sigma\gamma$ es 1, mientras que $\text{mcm}(2, 2) = 2$.
- (d) Si existiera un elemento σ de orden 14, al escribirlo como producto de ciclos disjuntos $\sigma = \sigma_1 \cdots \sigma_r$, siendo σ_i un k_i -ciclo, por el resultado de la parte b) tenemos que $14 = \text{mcm}(k_1, \dots, k_r)$ y por lo tanto uno de los ciclos tiene largo 2 y otro largo 7. Pero entonces no serían disjuntos ya que son ciclos en S_7 .

Ejercicio 2. Sea n un entero, $n \geq 2$.

- (a) Ver teórico (Teo. de Korselt)
- (b) (i) Como n es compuesto, existen p y q primos que dividen a n . Como $p^2 \nmid n$, tenemos que $p \neq q$ y por lo tanto uno de los dos (digamos p) es impar y por lo tanto $p-1$ es par. Y como $p-1|n-1$ se tiene que $n-1$ es par y por lo tanto n es impar.
- (ii) Supongamos que $n = pq$ con p y q dos primos distintos. Como $p-1|n-1$ y $n-1 = pq-1 = q(p-1) + q-1$ tenemos que $p-1|q-1$. También $q-1|n-1$ y $n-1 = pq-1 = p(q-1) + p-1$ así que $q-1|p-1$. Por lo tanto se tiene que $p-1 = q-1$ y entonces $p = q$ lo cual es absurdo.

Ejercicio 3.

- (a) Ver Teórico.
- (b) Como por Fermat tenemos $7^{46} \equiv 1 \pmod{47}$ entonces $o(7)|46$ y por lo tanto las posibilidades para el orden de 7 son 1, 2, 23 y 46 (no puede ser 1 pues $7 \not\equiv 1 \pmod{47}$). $7^2 = 49 \equiv 2 \pmod{47}$ (en particular el orden de 7 no es 2). Ahora, $7^{23} = 7 \times 7^{22} \equiv 7 \times 2^{11} \pmod{47}$. Calculemos $2^{11} \pmod{47}$: $2, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 32, 2^6 = 64 \equiv 17 \pmod{47}, 2^7 \equiv 34 \pmod{47}, 2^8 \equiv 68 \pmod{47} \equiv 21 \pmod{47}, 2^9 \equiv 42 \pmod{47} \equiv -5 \pmod{47}, 2^{10} \equiv -10 \pmod{47}, 2^{11} \equiv -20 \pmod{47}$. Entonces $7^{23} \equiv 7 \times (-20) \pmod{47} \equiv -140 \pmod{47} \equiv 1 \pmod{47}$ y por lo tanto 7 no es raíz primitiva módulo 47.
- (c) La clave es c tal que $c \equiv 9^{44} \pmod{47}$. Nuevamente, por Fermat tenemos que $9^{46} \equiv 1 \pmod{47}$ y por lo tanto $9^2 c \equiv 1 \pmod{47}$; es decir que c es el inverso de 9^2 módulo 47. Ahora $9^2 = 81 \equiv 34 \pmod{47}$ y tenemos que hallar c tal que $34c \equiv 1 \pmod{47}$; es decir que $34c = 1 + 47k$ para algún $k \in \mathbb{Z}$. Entonces resolvemos la ecuación $34c - 47k = 1$. Utilizando el algoritmo de Euclides extendido obtenemos que $34(18) - 47(13) = 1$ y por lo tanto $c = 18$.