

Soluciones del examen de Matemática Discreta II
15 de diciembre de 2009

(Ejercicio 1) Sea $m \in \mathbb{Z}$, compuesto.

1. Definir pseudoprimo de Carmichael y redactar el Teorema de Korselt.
2. Probar que si p^2 divide a m , siendo p primo, entonces p divide a $\phi(m)$ (ϕ función de Euler).
3.
 - Probar que, si $\phi(m)$ divide a $m - 1$ entonces m es libre de cuadrados (o sea, no existe un primo p tal que p^2 divide a m).
 - Demostrar que si $\phi(m)$ divide a $m - 1$ entonces m es un pseudoprimo de Carmichael.

Solución al ejercicio 1:

1. Diremos que un entero positivo m , impar y compuesto es un pseudoprimo de Carmichael si: $b^n \equiv b \pmod{m}$, para todo $1 < b < m - 1$.
Teorema de Korselt: Un entero positivo impar compuesto m es un pseudoprimo de Carmichael si y solamente si cada factor primo p de m satisface las condiciones siguientes:
 - p^2 no divide a m ;
 - $p - 1$ divide a $m - 1$.
2. Si p^2 divide a m , entonces $m = p^\alpha \times q$, con $\alpha \geq 2$ y $\text{mcd}(p, q) = 1$. Luego $\phi(m) = p^{\alpha-1}(p-1) \times \phi(q)$. Como $\alpha \geq 2$ entonces $\alpha - 1 \geq 1$, y por lo tanto p divide a $\phi(m)$.
3.
 - Supongamos que p^2 divide a m , por lo tanto, por el ítem anterior, p divide a $\phi(m)$. Si $\phi(m)$ divide a $m - 1$, entonces p divide a $m - 1$, y por otro lado p divide a m , con lo cual p divide a 1, y esto es absurdo. Entonces m es libre de cuadrados.
 - Por el ítem anterior si $\phi(m)$ divide a $m - 1$, entonces m es libre de cuadrados. Según el teorema de Korselt, restaría por probar que $p - 1$ divide a $m - 1$, para todo factor primo p de m . Si p divide a m , entonces $m = p^\beta \times q$, con $\beta \geq 1$ y $\text{mcd}(p, q) = 1$. Entonces $\phi(m) = (p-1)p^{\beta-1} \times \phi(q)$. Luego $p - 1$ divide a $\phi(m)$, y éste, a su vez, divide a $m - 1$ según la hipótesis. Entonces $p - 1$ divide a $m - 1$, y hemos concluido.

(Ejercicio 2)

- i) Encontrar $x \in \mathbb{Z}$ que verifique: $20 \leq x \leq 90$, $x = 38^{44} \pmod{5}$ y $x = 6 \pmod{13}$. Mostrar que x es primo.
- ii) Hallar el orden de 5 en \mathbb{Z}_x^* y demostrar que el orden de 2 es $\frac{x-1}{2}$.
- iii) Dayenidamha y Li-Gnoy Kim arreglan una clave con el método Diffie-Helman con clave pública $(2, x)$. Li-Gnoy Kim elige $m = 17$ y recibe de Dayenidamha $2^m = 5 \pmod{x}$. Encontrar la clave común.

Solución al ejercicio 2:

- i) Primero observemos que $x \equiv 38^{44} \equiv (-2)^{44} \equiv 4^{44} \equiv 1^{44} \equiv 1 \pmod{5}$. Por otra parte como $x \equiv 6 \pmod{13}$ resulta que x es de la forma $x = 13y + 6$. Luego $x \equiv 1 \pmod{5}$ por lo que $13y + 6 \equiv 1 \pmod{5}$. Se deduce que $13y \equiv -5 \equiv 0 \pmod{5}$ con lo cual $y \equiv 0 \pmod{5} \Leftrightarrow 13y \equiv 0 \pmod{65} \Leftrightarrow x = 13y + 6 \equiv 6 \pmod{65}$. Por la condición $20 \leq x \leq 90$ la única posibilidad es $x = 65 + 6 = 71$.
- ii) Observemos que el orden de 5 módulo 71 debe ser divisor de $71 - 1 = 2 \cdot 5 \cdot 7$. Claramente ni $5^1 = 5$ ni $5^2 = 25$ son congruentes con 1 módulo 71. Como $5^5 = 3125 \equiv 1 \pmod{71}$ y por lo tanto 5 es el orden de 5 módulo 71.

Para ver que el orden de 2 módulo 71 es 35 podemos utilizar exponenciación binaria:

n	$2^{2^n} \bmod(71)$
0	2
1	4
2	16
3	$256 \equiv 43$
4	$1849 \equiv 3$
5	9

Así que $2^{35} = 2^{2^5} \cdot 2^{2^4} \cdot 2^{2^3} \cdot 2^{2^2} \cdot 2^{2^1} \cdot 2^{2^0} \equiv 9 \cdot 4 \cdot 2 = 72 \equiv 1 \pmod{71}$. Por lo tanto el orden de 2 es divisor de 35, ahora chequeamos que no es ni 5 ni 7:

$$2^5 = 32 \not\equiv 1 \pmod{71}; \quad 2^7 = 128 \equiv 57 \not\equiv 1 \pmod{71}.$$

Por lo tanto el orden de 2 módulo 71 es 35 como se quería probar.

- iii) Li-Gnoy Kim puede calcular la clave haciendo $5^{17} \pmod{71}$, como $17 \equiv 2 \pmod{5}$ donde 5 es el orden de 5 módulo 71 nos queda que $5^{17} \equiv 5^2 = 25 \pmod{71}$. Por lo tanto la clave acordada es $k = 25$.

(Ejercicio 3) Sea $G = \{\text{matrices reales } 3 \times 3 \text{ con determinante no nulo}\}$.

- Probar que G es un grupo con el producto habitual de matrices (se asume la asociatividad).
- Sea $H = \{M \in G / \det(M) = 1\}$. Mostrar que $H \triangleleft G$ y describir las clases del conjunto cociente usando el determinante.
- Demostrar que $G/H \cong \mathbb{R}^*$ (o sea $\mathbb{R} - \{0\}$ con el producto).
- Concluir que en G/H todos los elementos tienen orden infinito, salvo $[id]$ y $[-id]$.

Solución al ejercicio 3.

- El determinante de la matriz identidad vale uno, por lo que, la matriz identidad pertenece a G . Por otro lado, si una matriz tiene determinante no nulo, es invertible, y su inversa también tiene determinante no nulo. Es fácil ver que el producto de dos matrices de determinante no nulo es una nueva matriz de determinante no nulo (pues el determinante es multiplicativo). Luego en G , con el producto de matrices, tenemos la asociatividad que se asume, la matriz identidad, y cada matriz tiene inversa.
- Si $H = \{M \in G / \det(M) = 1\}$, entonces la matriz identidad pertenece a H . Por otro lado, el determinante del producto de dos matrices, es el producto de los determinantes de cada una de ellas. Luego, si dos matrices están en H , su producto también. Por último, el determinante de la matriz inversa, es el inverso del determinante de la matriz inicial. Entonces, si una matriz está en H , su inversa también está en H . Luego hemos probado que $H < G$ (subgrupo).

Para probar que H es normal a G , usamos que $\det(UMU^{-1}) = \det(U) \times \det(M) \times \det(U^{-1}) = \det(M) = 1$, si $M \in H$. Luego H es normal a G .

Sean A y B dos matrices, tal que $\det(A) = \det(B) = \nu \neq 0$. Entonces ambas son invertibles y $\det(AB^{-1}) = \det(A) \times \det^{-1}(B) = \nu \times \nu^{-1} = 1$. O sea, $AB^{-1} \in H$ y por lo tanto están en la misma clase del cociente. El razonamiento anterior es válido en orden inverso, o sea que si $AB^{-1} \in H$, entonces $\det(A) = \det(B) \neq 0$ (pues B es invertible).

Luego, concluimos que dos matrices están en la misma clase de equivalencia de G/H si tienen el mismo determinante (y este es no nulo).

- iii) Según lo demostrado en el ítem anterior si consideramos $\det: G/H \rightarrow \mathbb{R}^*$, la función está bien definida. Además sabemos que la función determinante es multiplicativa, o sea $\det(AB) = \det(A) \times \det(B)$. O sea que es un morfismo de grupos. La identidad de \mathbb{R}^* con el producto es el 1, y por lo tanto el $\ker(\det)$ (núcleo del morfismo) son las matrices que tienen determinante 1. O sea, la clase de H , o sea la identidad en el grupo cociente G/H . Por último es muy fácil de observar que la función \det es un epimorfismo, pues para todo $\lambda \in \mathbb{R}^*$ es fácil encontrar una matriz cuyo determinante valga λ . Entonces $G/H \cong \mathbb{R}^*$.
- iv) El orden de cada elemento en G/H coincide con el orden de su imagen a través de la función determinante, pues es un isomorfismo. Y en \mathbb{R}^* el orden de sus elementos es infinito excepto el elemento 1 (orden 1) y el elemento -1 (orden 2). Justamente, estos elementos corresponden, a través de la función determinante, a las matrices identidad y la matriz opuesta a la identidad (observar que el hecho que sean matrices 3×3 es importante en este momento).