Universidad de la República - Facultad de Ingeniería - IMERL.
Matemática Discreta 2

Examen - 8 de febrero de 2018.

Ejercicio 1.

a. Sean $0 \neq a,\, b \in \mathbb{Z}$, probar que

$$\operatorname{mcd}(a,b) = \text{mín}\{s > 0 \,:\, s = ax + by \text{ con } x, y \in \mathbb{Z}\}.$$

Solución: Ver Proposición 1.2.6 de las notas teóricas.

b. Sean $a, b \in \mathbb{Z}$, probar que la ecuación diofántica $ax + by = c$ tiene solución si y solo si $\operatorname{mcd}(a,b)|c$.

Solución: Ver la parte 1 del teorema 1.5.3 de las notas teóricas

c. Hallar todas las soluciones módulo 62 de la ecuación

$$26x \equiv 262 \pmod{62}.$$

Solución: Como $262 \equiv 14 \pmod{62}$, debemos resolver $26x \equiv 14 \pmod{62}$. Por definición de congruencia, es equivalentema resolver la diofántica

$$26x + 62y = 14$$

y dividiendo todo entre 2, obtenemos la diofántica equivalente

$$13x + 31y = 7.$$

Aplicando el algoritmo extendido de Euclides obtenemos que $13(12) + 31(-5) = 1$ y por lo tanto (multiplicando por 7) obtenemos que $13(12 \cdot 7) + 31(-5 \cdot 7) = 7$. Entonces la diofántica $13x + 31y = 7$ tiene solución particular $(x_0,\, y_0) = (84, -35)$ y todas sus soluciones son de la forma $(x,\, y) = (84 + 31k,\, -35 - 13k)$ para k entero. Por lo tanto

$$x = 84 + 31k \equiv 22 + 31k \pmod{62},\; k \in \mathbb{Z},$$

y tomando $k = 0, 1$ obtenemos todas las posibles soluciones módulo 62, que son 22 y $22 + 31 = 53$.

Ejercicio 2.

a. Resolver los siguientes sistemas de congruencias:

i) $\begin{cases} x \equiv 0 \pmod{11} \\ x \equiv 8 \pmod{17} \end{cases}$ ii) $\begin{cases} x \equiv 33 \pmod{44} \\ x \equiv 25 \pmod{34} \end{cases}$

Solución:

i) Si escribimos $x = 17t+8$, $t \in \mathbb{Z}$, y lo sustituímos en la primer congruencia, obtenemos $17t + 8 \equiv 0 \pmod{11}$. Por lo tanto $6t \equiv 3 \pmod{11}$ y como 3 es coprimo con 11 podemos cancelarlo y obtenemos $2t \equiv 1 \pmod{11}$, por lo tanto $t = 6$ y $x \equiv 17 \cdot 6 + 8 \pmod{11 \cdot 17} \equiv 110 \pmod{11 \cdot 17}$.

ii) Si escribimos $44 = 4 \cdot 11$ y $34 = 2 \cdot 17$ podemos aplicar el TCR a ambas congruencias para obtener el siguiente sistema equivalente al planteado

$$\begin{cases} x \equiv 33 \pmod{4} & \equiv 1 \pmod{4} \\ x \equiv 33 \pmod{11} & \equiv 0 \pmod{11} \\ x \equiv 25 \pmod{2} & \equiv 1 \pmod{2} \\ x \equiv 25 \pmod{17} & \equiv 8 \pmod{17} \end{cases}$$

Como la primer congruencia de este sistema implica la tercera, podemos eliminar la tercera. Además, usando la parte anterior, el sistema nos queda equivalente

$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 110 \pmod{11 \cdot 17} \end{cases}$$

que tiene solución 297.

b. Sean p y q dos primos distintos. Describir el criptosistema RSA usando p y q (especificar cuáles datos son públicos y cuáles privados y definir las funciones E y D de cifrado y descifrado respectivamente).
Solución: Ver notas teóricas.

c. Probar que en el criptosistema RSA, la función de descifrado D es la función inversa de la función de cifrado E.
Solución: Ver Proposición 5.3.1 de las notas teóricas.

d. Mostrar con un ejemplo por qué, en el sistema RSA, es necesario que los primos p y q sean distintos.
Solución: Si tomamos $x = p$ y $e > 1$, cuando aplicamos la función E obtenemos $E(p) = p^e \pmod{p^2} = 0$; entonces al aplicar la función de descifrado al 0 deberíamos obtener p. Pero $D(0) = 0^d = 0 \neq p \pmod{p^2}$ y entonces $D(E(p)) \neq p$.

e. Con los primos 11 y 17 utilizar el criptosistema RSA con $e = 171$ para cifrar el número $x = 121$.
Solución: Tenemos que calcular $x = 121^{171} \pmod{11{\cdot}17}$. Como $\operatorname{mcd}(121, 11{\cdot}17) = 11 \neq 1$, no podemos aplicar Euler en esta congruencia. Como $\operatorname{mcd}(11, 17) = 1$, por el TCR, la congruencia es equivalente al sistema

$$\begin{cases} x \equiv 121^{171} \pmod{11} & \equiv 11^{2\cdot 171} \pmod{11} & \equiv 0 \pmod{11} \\ x \equiv 121^{171} \pmod{17} & \equiv 11^{2\cdot 171} \pmod{17} \end{cases}$$

Para la segunda congruencia podemos aplicar Euler y como $\varphi(17) = 16$ y $2 \cdot 171 \equiv 6 \pmod{16}$, tenemos que $x \equiv 11^6 \pmod{17} \equiv (-6)^6 \equiv (36)^3 \equiv 2^3 \pmod{17} \equiv 8 \pmod{17}$. Por lo tanto tenemos que resolver el sistema

$$\begin{cases} x \equiv 0 \pmod{11} \\ x \equiv 8 \pmod{17} \end{cases},$$

que por la primer parte del ejercicio sabemos que es 110, por lo tanto $E(121) = 110$.

Otro camino para reducir la 2da. ecuación poría haber sidp, a partir de $x \equiv (121)^{171} \pmod{17} \equiv 2^{171} \pmod{17}$, aplicando Euler obtenemos $x \equiv 2^{11} \equiv 2^{2^4+2^1+2^0} \pmod{17}$. Utilizamos el método de exponenciación rápida para obtener las potencias $2^{2^k} \pmod{17}$, $k = 0, 1, 2, 3, 4$. Primero $2^{2^0} = 2$, luego $2^{2^1} = 2^2 = 4$, $2^{2^2} = 16 \equiv -1 \pmod{17}$, $2^{2^3} \equiv 2^{2^4} \pmod{17} \equiv 1 \pmod{17}$. Por lo tanto $2^{11} \equiv 2 \cdot 4 \cdot 1 \pmod{17} \equiv 8 \pmod{17}$.

Ejercicio 3.

a. Definir grupo.
Solución: Ver notas teóricas.

b. Sea $(G, \times)$ un grupo, probar que el neutro es único.
Solución: Ver notas teóricas.

c. Sea $(G, \times)$ un grupo y $g \in G$, probar que el inverso de g es único.
Solución: Ver notas teóricas.

d. Sean G y K dos grupos y $f : G \to K$ un homomorfismo. Probar que si $g \in G$ es un elemento de orden finito entonces

$$\mathrm{o}(f(g)) \mid \mathrm{o}(g).$$

Solución: Ver notas teóricas.

e. Hallar todos los homomorfismos $f : U(13) \to \mathbb{Z}_9$ (sugerencia: hallar una raíz primitiva módulo 13).
Solución: Veamos primero que 2 es raiz primitiva módulo 13. Sabemos que $\varphi(13) = 12 = 2^2 3$. Hay que probar que $2^4, 2^6 \not\equiv 1 \pmod{13}$. Veamos eso, $2^4 = 16 \equiv 3 \pmod{13}$ y $2^6 \equiv 3 \cdot 4 \pmod{13} \equiv -1 \pmod{13}$.
Como $U(13)$ es cíclico, todos los homomorfismos son $f\left(2^k\right) = k \cdot n$, con $\mathrm{o}(n)|\mathrm{o}(2) = 12$, $n \in \mathbb{Z}_9$. Estos elementos son $0, 3, 6$ cuyos ordenes son $1, 3, 3$. Por lo tanto tenemos 3 homomorfismos.