Universidad de la República
Facultad de Ingeniería
Instituto de Matemática y Estadística

Matemática Discreta 2

EXAMEN- 9 FEBRERO 2024.

Ejercicios de respuesta verdadero (V) o falso (F):

Afirmación 1. Si p y q son primos entonces existen infinitos $x \in \mathbb{Z}$ tales que $\frac{x-p}{q} \in \mathbb{Z}$ y $\frac{x-q}{p} \in \mathbb{Z}$.

Verdadero: basta considerar $x = kpq + p + q$ con $k \in \mathbb{Z}^+$. Otra justificación sería observando que por el Teorema Chino del resto el sistema de congruencias $x \equiv p \pmod{q}$, $x \equiv q \pmod{p}$ tiene infinitas soluciones pues los módulos son coprimos cuando $p \neq q$ y cuando $p = q$ puedo tomar cualquier $x = \dot{p}$.

Afirmación 2. Existe $x \in \mathbb{Z}$ que verifica simultaneamente: $x \equiv 1 \pmod{1527}$ y $x \equiv 2 \pmod{7251}$.

Falso: observar que 3 divide a 1527 y a 7251 luego la primer congruencia implicaría $x \equiv 1 \pmod{3}$ y la segunda $x \equiv 2 \pmod{3}$ lo cuál es absurdo.

Afirmación 3. La ecuación diofántica $2^{10}x + 3^{10}y = 5^{10}$ tiene tres soluciones que verifican $1 \leq x \leq 3^{11}$.

Verdadero: Como $\mathrm{mcd}(2^{10}, 3^{10}) = 1$ entonces toda solución es de la forma $x = x_0 + 3^{10}t$, $y = y_0 - 2^{10}t$ donde (x_0, y_0) es una solución particular. Existen exactamente $3^{11}/3^{10} = 3$ valores enteros de t tales que $1 \leq x \leq 3^{11}$ y consecuentemente tres soluciones de la ecuación diofántica.

Afirmación 4. Si G un grupo finito de orden par entonces existe $g \neq e$ tal $g = g^{-1}$.

Verdadero: Recordemos que $(g^{-1})^{-1} = g$. Si no fuera cierta la tesis entonces podría describir a G como conjunto de la siguiente manera: $G = \{e, g_1, g_1^{-1}, \ldots, g_m, g_m^{-1}\}$ (es decir un conjunto y no una lista) dado que un elemento y su inverso formaría una pareja, excepto la identidad que es su propio inverso. Pero esto nos lleva a una contradición porque entonces el cardinal sería impar lo que por hipótesis excluimos.

Ejercicios de respuesta múltiple opción:

Ejercicio 1.

Determinar exactamente cuáles de los siguientes enteros $\{40, 53, 49, 50, 55, 343\}$ son solución a la ecuación $2^{43} \equiv 2^x \pmod{7}$.

(A) $\{40, 49, 55, 343\}$.

(B) $\{40, 53, 49, 50, 55, 343\}$.

(C) $\{49, 50, 343\}$.

(D) $\{40, 343\}$.

Solución:

Recordando que si $o(g) < \infty$ entonces $g^m = g^k$ sii $m \equiv k \pmod{o(g)}$. Como $o(\bar{2}) = 3$ en $U(7)$ resulta que $2^{43} \equiv 2^x \pmod{7}$ sii $x \equiv 43 \equiv 1 \pmod{3}$. Los elementos de la lista congruentes con 1 módulo 3 son exactamente $40, 49, 55$ y 343 por lo tanto la opción correcta es la (A).

Ejercicio 2.

Paul y Ringo dos musicos de una Banda musical famosa tienen acordado cual sera el ritmo de su próximo éxito musical. Sin embargo, Paul quedó a cargo de enviarle a Ringo la melodía para terminar la composición. Para evitar que piratas les robe la idea acuerdan emplear un método de cifrado utilizando un sistema afín con clave de parámetros (a, k). Teniendo en cuenta que son doce las notas musicales ordenadas en el sentido usual, cuantos posibles sistema pueden considerar para esta tarea.

(A) 48 (C) 100

(B) 24 (D) 28

Solución: Recordar que las posibles funciones de encriptado son de la forma $E : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$, $E(x) = ax+k \pmod{12}$ donde $\mathrm{mcd}(a, 12) = 1$. Tenemos $\varphi(12) = 4$ posibilidades para a y 12 posibilidades para k. Luego tenemos $4 \cdot 12 = 48$ posibles funciones de encriptado (una correspondiente con cada clave posible). La opción correcta en este caso es la (A).

Preguntas de respuesta por desarrollo escrito:

Pregunta 1:

a) Definición de máximo comun divisor.

b) Sean $a, b \in \mathbb{Z}$, con $a, b \neq 0$, entonces demuestre que $\mathrm{mcd}(a, b) = \min\{s > 0 : s = ax + by,\ x, y \in \mathbb{Z}\}$.

Solución:

a) Ver notas Definición 1.2.4. página 7.

b) Ver notas Teorema 1.2.8 página 10.

Pregunta 2A: (opcional con la pregunta 2B).

a) Sea G un grupo, H un subgrupo normal de G y la aplicación al cociente $\pi : G \to G/H$. Entonces demostrar que para todo morfismo de grupos $f : G \to G'$ tal que $H \subseteq Ker(f)$, existe un único morfismo de grupos $\hat{f} : G/H \to G'$ tal que $\hat{f} \circ \pi = f$.

b) Demostrar que $6\mathbb{Z}/30\mathbb{Z} \cong \mathbb{Z}_5$, siendo en general $m\mathbb{Z}$ el subgrupo aditivo de los enteros múltiplos de m y $\mathbb{Z}_n$ el grupo aditivo de los enteros módulo n.

Solución:

a) Definimos la función $\hat{f} : G/H \to G'$ mediante $\hat{f}(gH) = f(g)$. Veamos que está "bien definida"sobre las clases: si $gH = g'H$ entonces $g'^{-1}g \in H \subseteq ker(f)$ por lo que $f(g'^{-1}g) = 1$ de donde $f(g')^{-1}f(g) = 1$, esto es $f(g') = f(g)$ lo cual significa que $\hat{f}(g'H) = \hat{f}(gH)$. Es fácil ver que $\hat{f}$ es un homomorfismo: $\hat{f}(g_1Hg_2H) = \hat{f}(g_1g_2H) = f(g_1g_2) = f(g_1)f(g_2) = \hat{f}(g_1H)\hat{f}(g_2H)$. Por definición tenemos que $\hat{f}(\pi(g)) = \hat{f}(gH) = f(g)$, es decir, $\hat{f} \circ \pi = f$. Finalmente la unicidad: supongamos otra solución $\bar{f}$ que cumpla $\bar{f} \circ \pi = f$. Entonces vale $\bar{f}(gH) = \bar{f} \circ \pi(g) = f(g) = \hat{f} \circ \pi(g) = \hat{f}(gH)$, esto es $\bar{f} = \hat{f}$.

b) Si consideramos $f : 6\mathbb{Z} \to \mathbb{Z}_5$ definida por $f(x) = \overline{m} \pmod 5$ siendo $x = 6m$ con $m \in \mathbb{Z}$ entonces vemos que f es un homomorfismo de grupos sobreyectivo: si $x = 6m$ y $y = 6m'$ entonces $f(x+y) = \overline{m + m'} = \overline{m}+\overline{m'} \pmod 5$. Si $\overline{y} \in \mathbb{Z}_5$ entonces $f(6y) = \overline{y}$. Por la parte a), dado que todo subgrupo de $\mathbb{Z}$ es normal por ser un grupo abeliano entonces existe $\hat{f} : 6\mathbb{Z}/30\mathbb{Z} \to \mathbb{Z}_5$ homomorfismo sobreyectivo. Veamos que además es inyectivo: si $\hat{f}(6m + 30\mathbb{Z}) = \hat{f}(6m' + 30\mathbb{Z})$ entonces $\overline{m} = \overline{m'} \pmod 5$ por lo que $5|m - m'$ es decir, $6 \cdot 5|6 \cdot (m - m')$ esto es, $6m + 30\mathbb{Z} = 6m' + 30\mathbb{Z}$.

Pregunta 2B: En este ejercicio p es un número primo y $U(p)$ denota el grupo multiplicativo de invertibles módulo p.

a) Sean $x, y \in U(p)$ cuyos ordenes $o(x) = a$ y $o(y) = b$ son coprimos. Probar que $o(xy) = o(x)o(y)$.

b) Suponga que para cada divisor positivo $d|p - 1$ la ecuación $x^d \equiv 1 \pmod p$ tiene exactamente d raíces distintas en $U(p)$. Probar que existen raices primitivas módulo p.

Ver notas Lema 4.1.7 y Teorema 4.1.10 (observe que la hipótesis que se da en la letra es exactamente el enunciado del Lema 4.1.9)