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

Matemática Discreta 2
Curso segundo semestre 2024

EXAMEN - 18 DICIEMBRE 2024.

Cédula de identidad	APELLIDO, Nombre	Número de lista

Ejercicio 1.

1) Enuncie y demuestre el teorema que caracteriza la existencia y forma de las soluciones de una ecuación diofántica.

2) Debo transferir 510 pesos a una empresa utilizando un cajero automático que únicamente dispone de billetes de 20 y 50. ¿Es posible pagar exactamente este monto?. Justifique su respuesta. En caso afirmativo, describa todas las combinaciones posibles de billetes que permitan cubrir exactamente esa cantidad, junto con la justificación correspondiente.

Solución:

1) Teorema 1.5.3. Notas de P. Q. R. página 18.

2) Detrás del problema está la resolución de la diofántica: $20x + 50y = 510$. Tengo que analizar si tiene solución. Como $\mathrm{mcd}(20, 50) = 10 \,|\, 510$ existen soluciones. Una solución particular es $20x + 50y = \mathrm{mcd}(20, 50)$ es $(x_0, y_0) = (-2, 1)$ (Euclides). Por lo que una solución particular de $20x + 50y = 510$ seria $(x_1, y_1) = (-2 \cdot 51, 1 \cdot 51) = (-102, 51)$. El conjunto de todas las soluciones es $\{(x_1 + 50/10 \cdot k, y_1 - 20/10 \cdot k) : k \in \mathbb{Z}\}$ como queremos soluciones positivas tenemos que $-102 + 5k \geq 0$ and $51 - 2k \geq 0$ es decir, $25,5 = 51/2 \geq k$ y $k \geq 102/5 = 20,4$, esto es $k = 21$ o 22 o 23 o 24 o 25. Si sustituyo obtengo las posibles soluciones $(x, y) = (-102 + 5 \cdot 21, 51 - 2 \cdot 21) = (3, 9)$, o $(x, y) = (8, 7)$, $(x, y) = (13, 5)$, $(x, y) = (18, 3)$, o $(x, y) = (23, 1)$.

Ejercicio 2.

1) Defina subgrupo normal. Sea H un subgrupo de un grupo G. Pruebe que H es normal sii $gHg^{-1} \subseteq H$, para todo $g \in G$.

2) Sea $f : G \to G'$ un homomorfismo, pruebe que $\mathrm{Ker}(f)$ es un subgrupo normal de G.

3) Dado un subgrupo normal H de G hallar un homomorfismo cuyo kernel sea exactamente H.

4) Sea $(G, \cdot, e)$ un grupo. Denotemos con $\sim$ una relación de equivalencia definida en G. Sea $H = \{g \in G : g \sim e\}$. Recordemos que una relación de equivalencia se dice de congruencia si satisface: $a_1 \sim a_2$ y $b_1 \sim b_2$ implica $a_1 b_1 \sim a_2 b_2$ para todo $a_1, a_2, b_1, b_2 \in G$. Probar que si la relación es de congruencia entonces H es un subgrupo normal de G.

Solución:

1) Definición 3, página 8 notas Teo. isomorfismos y Proposición 1 página 10.

2) Por la parte 1) basta ver que $gHg^{-1} \subseteq H$, para todo $g \in G$ con $H = \mathrm{Ker}(f)$: si $b \in \mathrm{Ker}(f)$ entonces $f(gbg^{-1}) = f(g)f(b)f(g^{-1}) = f(g)f(b)f(g)^{-1} = e$.

3) Consideremos el mapa $\pi : G \to G/H$ dado por la proyección a las clases de equivalencia. Este mapa es un homomorfismo cuyo kernel es H. Ver notas.

4) H es un subgrupo: la propiedad idéntica $e \sim e$ de la relación de equivalencia implica $e \in H$. Si $a \in H$ y $b \in H$ entonces $a \sim e$ y $b \sim e$ por lo que por ser de congruencia $ab \sim e$, es decir $ab \in H$. Si Si $a \in H$, esto es, $a \sim e$ entonces como $a^{-1} \sim a^{-1}$ se cumple que $aa^{-1} \sim ea^{-1}$ por ser una congruencia. Es decir, $e \sim a^{-1}$ por lo que $a^{-1} \sim e$ por simetria, esto es $a^{-1} \in H$.

   H es normal: quiero probar que $aha^{-1} \in H$ para todo $h \in H$. Si $h \in H$ entonces $h \sim e$ entonces se cumple $aha^{-1} \sim aea^{-1}$ por ser una congruencia. esto es, $aha^{-1} \sim e$, por lo que $aha^{-1} \in H$.

Ejercicio 3.

1) Dado $n \in \mathbb{Z}^+$, definir raíz primitiva módulo n.

2) Demostrar que si p es un primo impar y r es una raíz primitiva módulo p entonces

$$r^a \equiv r^b \pmod{p} \Leftrightarrow a \equiv b \pmod{p-1}$$

3) Probar que 5 es raíz primitiva módulo 23.

4) Hallar $\log_5(16) \in \mathbb{Z}_{22}$

5) Resolver $x^3 \equiv 16 \pmod{23}$

Solución:

1) Notas de P. Q. R. página 62, Definición 4.1.1.

2) Como r es raíz primitiva módulo p, tenemos que $o(\bar{r}) = \varphi(p) = p-1$ en $U(p)$. Luego,

$$\begin{aligned} r^a \equiv r^b \pmod{p} &\Leftrightarrow r^a r^{-b} \equiv r^b r^{-b} \pmod{p} \\ &\Leftrightarrow r^{a-b} \equiv 1 \pmod{p} \\ &\Leftrightarrow \bar{r}^{a-b} = \bar{1} \text{ en } U(p) \\ &\Leftrightarrow o(\bar{r}) | a-b \\ &\Leftrightarrow p-1 | a-b \\ &\Leftrightarrow a \equiv b \pmod{p-1} \end{aligned}$$

3) Los divisores primos de $\varphi(23) = 22$ son 2 y 11 por lo que, para ver que 5 es raíz primitiva modulo 23, alcanza con ver que $5^2 \not\equiv 1 \pmod{23}$ y que $5^{11} \not\equiv 1 \pmod{23}$.

   Luego como, $5^2 \equiv 2 \pmod{23}$ y $5^{11} \equiv 5^{2^3} 5^{2^1} 5^{2^0} \equiv 16 \cdot 2 \cdot 5 \equiv 22 \pmod{23}$ concluímos que 5 es raíz primitiva modulo 5.

4) Dado que $5^8 \equiv 16 \pmod{23}$, tenemos que $\log_5(16) \equiv 8 \pmod{22}$.

5) Dado que 5 es raíz primitiva modulo 23, podemos escribir $x \equiv 5^k \pmod{23}$ para algún $k \in \mathbb{Z}$. Luego,

$$\begin{aligned} x^3 \equiv 16 \pmod{23} &\Leftrightarrow (5^k)^3 \equiv 5^8 \pmod{23} \\ &\Leftrightarrow 3k \equiv 8 \pmod{22} \\ &\Leftrightarrow 15 \cdot 3k \equiv 15 \cdot 8 \pmod{22} \\ &\Leftrightarrow k \equiv 10 \pmod{22} \end{aligned}$$

   Concluímos que $x^3 \equiv 16 \pmod{23} \Leftrightarrow x \equiv 5^{10} \equiv 9 \pmod{23}$.