USO DE ÁLGEBRAS MODERNAS PARA SEGURIDAD Y CRIPTOGRAFÍA
TAREA I

Resuelve los siguientes problemas. La tarea deberá ser entregada en hojas blancas (digitalizadas en un solo archivo pdf). No se aceptarán tareas en hojas de libreta o de algún otro tipo de cuaderno. Trabajen con limpieza y hagan procedimientos legibles y claros, argumentando cada paso en su solución. No entreguen la tarea con portada, pero especifiquen bien sus nombres, matrícula, número de equipo, y el número de la tarea que están entregando; escriban estos datos en la parte superior de la primera hoja. Si desean entregar un documento en formato pdf generado con Latex, esto también está permitido.

FECHA DE ENTREGA: domingo 24 de abril de 2022.

1. Sea $d = \text{mcd}(a, b)$. Si $a = dx$ y $b = dy$, prueba que $\text{mcd}(x, y) = 1$.
2. Muestra que $5n + 3$ y $7n + 4$ son primos relativos para todo $n \in \mathbb{N}$.
3. En la canción "As" de Stevie Wonder, él menciona que $8 \times 8 \times 8 = 4$. Encuentra todos los enteros para los cuales esto es cierto módulo n.
4. Encuentra los inversos de los siguientes elementos:
   (a) $13 \in \mathbb{Z}_{20}$.
   (b) $13 \in U(14)$.
   (c) $n - 1 \in U(n)$.
5. Muestra que la ecuación $5x \equiv 3 \mod 20$ no tiene solución, pero que la ecuación $3x \equiv 5 \mod 20$ sí la tiene. ¿A qué es igual x?
6. Muestra que el conjunto $G = \{5, 15, 25, 35\}$ es un grupo bajo la multiplicación módulo 40. ¿Cuál es la identidad de este grupo? ¿Encuentras una relación entre este grupo y $U(8)$?
7. Prueba que un grupo G es Abeliano si y solo si $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.
8. Prueba que un grupo G con la propiedad de que $\forall g \in G$, $g^2 = e$, entonces G es Abeliano.
9. Sea $G = \{e, a, a^2, b, ab, a^2b\}$. Si $|a| = 3$ y $|b| = 2$, determina cuál de los seis elementos de G es igual a aba^2 y cual es equivalente a a^2bab.
10. Sea G un grupo y sea n un entero impar positivo tal que $g^n = e$ para todo $g \in G$. Si $a, b \in G$ y $a^2 = b^2$, prueba que $a = b$.
11. Para cualquier grupo G, prueba que para todo $a, b \in G$ se tiene que $|ab| = |ba|$. Explica por qué esto prueba que $|abab| = |baba|$. Además, ¿es verdad que $|aba| = |bab|$?
12. Asume que H es un subgrupo propio de $\mathbb{Z}$ bajo la adición y que $18, 30, 40 \in H$. Determina H.
13. Si H y K son subgrupos de G, demuestra que $H \cap K$ también es un subgrupo de G.
14. Encuentra un grupo que no sea cíclico, pero cuyos subgrupos sí lo sean.
15. Sea G un grupo cíclico y sea $a \in G$. Prueba que $\langle a \rangle = \langle a^{-1} \rangle$.
16. Prueba que $U(2^n)$ no es cíclico si $n \geq 3$.
17. ¿Cuál es el orden de el producto de un par de ciclos disyuntos de longitud 4 y 6? Si ahora se tienen tres ciclos disyuntos con longitudes iguales a 6, 8 y 10, ¿cuál es el orden del producto de estos ciclos?
18. ¿Cuál es el entero positivo n más pequeño para el cual S_n tiene un elemento de orden igual a 30?

19. Sea $\alpha = (123)(145)$. Obtén la versión de ciclos disyuntos de α y calcula α^{99}.

20. Para cualquier grupo G y cualquier automorfismo $\phi : G \to G$, demuestra que para todo $a \in G$, $|a| = |\phi(a)|$.

21. Asume que $\phi : \mathbb{Z}_{20} \to \mathbb{Z}_{20}$ es un automorfismo y $\phi(5) = 5$. ¿A qué puede ser igual $\phi(x)$? ¿Son estas posibilidades isomórficas a algún subgrupo de $U(20)$? Si es así, ¿cuál sería ese subgrupo?

22. Sean α y β isomorfismos que van de un grupo G a este mismo. Prueba que $H = \{g \in G : \alpha(g) = \beta(g)\}$ es un subgrupo de G.