UNAM, Facultad de Ciencias

# TAREA 1. Números enteros $\mathbb{Z}$ y Divisibilidad.

Daniela Terán

12 de marzo de 2024

Integrantes del equipo:
Flores Morán Julieta Melina

Resuelva los ejercicios que se enlistan a continuación, sea claro y formal en su proceder. El uso de símbolos lógicos queda prohibido.
Indique si las siguientes afirmaciones son verdaderas o falsas. En caso de ser ciertas de una demostración, en caso contrario un contra ejemplo.

1. (**0.25 puntos**) Considere $a, b, c \in \mathbb{Z}$ tres números enteros arbitrarios. Demuestre o brinde algún contraejemplo de lo siguiente:

   $1 \mid a$.

2. (**0.25 puntos**) Si $a \mid b$, entonces $a \mid -b$.
   Esta afirmación es cierta, por lo que daremos una demostración.
   Tenemos como hipótesis que $a \mid b$, por lo tanto, sabemos que $b = aq_1$ con $q_1 \in \mathbb{Z}$.
   Ya que $q_1 \in \mathbb{Z}$, entonces podemos saber que si $q_2 = q_1 \cdot -1 = -q_1$ y que entonces $q_2 \in \mathbb{Z}$.
   Ahora podemos ver que:

$$\begin{aligned} a \cdot q_2 &= a \cdot (q_1 \cdot -1) \\ &= (a \cdot q_1) \cdot -1 \\ &= b \cdot -1 \\ &= -b \end{aligned}$$

Por lo tanto, $-b = a \cdot q_2$ con $q_2 \in \mathbb{Z}$ y entonces $a \mid -b$

$\blacksquare$

3. (**0.25 puntos**) $a \mid 0$.

4. (**0.25 puntos**)

5. (**0.25 puntos**) Si $a \mid b$, entonces $a \leq b$.
   Esta afrimación es falsa, por lo que daremos un contraejemplo:
   Sea $a = 2$ y $b = -10$, $-10 = 2 \cdot -5$ por lo que $2 \mid -10$ pero $2 > -10$ entonces $a > b$ por lo que no se cumple que $a \leq b$.

6. (**0.25 puntos**) Si $a \leq b$, entonces $a \mid b$.

7. (**0.25 puntos**) Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.

8. (**0.25 puntos**) Si $a \nmid b$, entonces $b \nmid a$.
   Esta afirmación es falsa, por lo que daremos un contraejemplo:
   Sea $a = 25$ y $b = 5$. Podemos verificar que aplicando el algoritmo de la división en a y b, vemos que $5 = 25 \cdot 0 + 5 = a \cdot 0 + 5$. Por lo que $a \nmid b$ pero $25 = 5 * 5 + 0$ entonces $b \mid a$ y no se cumple que $b \nmid a$ .

9. (**0.25 puntos**) El $0_{\mathbb{Z}}$ no es par ni impar.

10. (**0.25 puntos**) El residuo es cero cuando un número entero par es divido por el 2.

11. (**0.25 puntos**) Si $a^2 = b^2$, entonces $a = b$.

12. (**0.25 puntos**) Si $a \mid (b + c)$, entonces $a \mid b$ y $a \mid c$.

13. (**0.25 puntos**) Si $a \mid bc$, entonces $a \mid b$ y $a \mid c$.

14. (**0.25 puntos**) Un entero positivo no primo es un número compuesto.

    Esta afirmación no es verdadera pues un entero positivo no primo es el 1, ya que la defínción de primo excluye explicitamente al 1. 1 sin embargo no es un número compuesto pues la definición de un número compuesto indica que es un número $n > 1$.Así que el contraejemplo es el 1.

15. (**0.25 puntos**) Un entero positivo no compuesto es un número primo.

16. (**0.25 puntos**) Todo número primo es impar.

17. (**0.25 puntos**) No hay primos mayores que un googolplex.
Esta afirmación no es verdadera, daremos por lo tanto un número primo mayor que un gogolplex. Tomemos el conjunto
$P = \{p$ |p es un número primo entre 0 y un googloplex$\}$. Ahora, tomemos $m = (\prod_{n \in P} n) + 1$, donde m es el el producto de todos los números en el conjunto P más uno. Aquí aseguramos que m es mayor que un googolplex ya que todos los primos p en P cumplen que p>1. También podemos notar que ninguno de los números primos en P dividen a m, ya que al aplicar el algoritmo de la división entre m y cualquier elemento de P el residuo que queda es igual a 1. Por el teorema fundamental de la aritmética hay dos opciones para mya que m es un entero y m>1:

    **Caso 1:**m es primo
    En este caso, m es un primo mayor que un googleplex por la definción de m, entonces ya encontramos el primo mayor que es m.
    **Caso 2:**m no es primo:
    En este caso, m debe ser un producto de números primos. Como m no tiene como factores a ningún primo que este entre el 2 hasta y el googleplex, debe tener otro factor primo que es mayor que un googleplex y por esto no esta en P. Entonces el número primo búscado es un factor primo de m que como no está en P, debe ser mayor que un googolple<.

    $\blacksquare$

18. (**0.25 puntos**) Si $p$ es un primo, entonces $p + 2$ es un primo.

19. (**0.25 puntos**) Si $p$ es un primo, entonces $p^2 + 1$ es un primo.

20. (**0.25 puntos**) Hay un número infinito de primos.
Esta afirmación es verdadera, por lo que lo demoestraremos por contradicción.
Supongamos, para buscar una contradicción, que el conjunto de números primos es finito y que consiste de exactamente los $k$ números primos $p_1, p_2, \ldots, p_k$. Consideremos el número: $m = p_1 \cdot p_2 \cdots p_k + 1$ El anterior número no es divisible por ninguno de los primos pues al aplicar el algoritmo de la división con m y cualquier número primo de $p_1$ a $p_k$, el residuo que queda es igual a 1. Ya que cada número primo $p_1, p_2, \ldots, p_k$ cumple con ser mayor que 1, podemos usar el teorema fundamental de la aritmética que dice que cualquier número entero mayor a 1 es primo o es producto de números primos, vemos que entonces m cumple uno de los dos casos:
**Caso 1:** m es primo: En este caso m es un número primo diferente de $p_1, \ldots, p_k$ ya que como vimos ninguno de estos divide a m, no pueden ser iguales.
**Caso 2:**m es un producto de primos: En este caso, m debe tener un divisor primo $p$ diferente de $p_1, p_2, \cdot, p_k$ ya que ninguno de estos divide a m.
Esto en ambos casos representa una contradicción, pues supusimos que sólo existían los primos $p_1, p_2, \ldots, p_k$. Como está contradicción viene de suponer que existen finitos números primos, entonces podemos concluir que no es así, y que hay un número de primos infinitos.

$\blacksquare$

21. (**0.25 puntos**) Hay un número infinito de números compuestos.

22. (**0.25 puntos**) Si $p$ es un primo tal que $p \mid ab$, entonces $p \mid a$ o $p \mid b$.

23. (**0.25 puntos**) Hay primos de la forma $n! + 1$.

    Demuestre que:

24. (**0.5 puntos**) El producto de cualesquiera dos enteros consecutivos es par.

25. (**0.5 puntos**) Cualquier entero impar es de la forma $4k + 1$ o $4k + 3$.

26. (**0.5 puntos**) $2^{4n} + 3n - 1$ es divisible por 9 con $n \in \mathbb{N}$
    Lo demostraremos por inducción sobre n.
    Veremos que con $n \in \mathbb{N}$, $9 \mid 2^{4n} + 3n - 1$. Lo que significa que, exite una $q \in \mathbb{Z}$ que cumple que $2^{4n} + 3n - 1 = 9 \cdot q$
    **Paso base:** n = 0

$$\begin{aligned}2^{4n} + 3n - 1 &= 2^{4\cdot 0} + 3 \cdot 0 - 1\\ &= 2^0 + 0 - 1\\ &= 1 - 1\\ &= 0\\ &= 0 \cdot 9\end{aligned}$$

    Ya que $0 \in \mathbb{Z}$ y $0 = 9 \cdot 0$, entonces $9 \mid 0$.
    **Hipótesis de inducción:**
    Para $n \in \mathbb{Z}$ , $2^{4n} + 3n - 1$ es divisible entre 9, es decir, existe $q \in \mathbb{Z}$ tal que $2^{4n} + 3n - 1 = 9 \cdot q$ por lo que $9 \mid 2^{4n} + 3n - 1$.
    **Paso inductivo:**
    Probaremos que existe una $q_2 \in \mathbb{Z}$ tal que $2^{4(n+1)} + 3(n + 1) - 1 = 9 \cdot q_2$.

$$\begin{aligned}2^{4(n+1)} + 3(n + 1) - 1 &= 2^{4n+4} + 3n + 21\\ &= 2^{4n} \cdot 2^4 + 3n + 2\\ &= 2^{4n} \cdot 16 + 3n + 2\\ &= 2^{4n} \cdot 16 + 48n - 48n + 3n - 16 + 16 + 2\\ &= 2^{4n} \cdot 16 + 3n \cdot 16 + 16 \cdot (-1) - 48n + 3n + 16 + 2\\ &= 16(2^{4n} + 3n - 1) - 48n + 3n + 16 + 2\\ &= 16(2^{4n} + 3n - 1) - 45n + 18\\ &= 16(9q) - 45n + 18\\ &= 9(16q) - (9)(5)n + (9)(2)\\ &= 9(16q - 5n + 2)\\ &= 9 \cdot q_2\end{aligned}$$

Vemos que $q_2 = 16q - 5n + 2 \in \mathbb{Z}$. Por lo que $9 \mid 2^{4n} + 3n - 1$.

Por lo tanto, para cualquier $n \in \mathbb{Z}$, $2^{4n} + 3n - 1$ es divisible por 9.

■

27. (**1 punto**) Encuentre los siguiente dos elementos de cada sucesión y de una descripción recursiva de la misma.

    *a*) $1, 3, 6, 10, 15, \ldots$

    *b*) $1, 4, 10, 20, 35, \ldots$

28. (**1 punto**) Encuentre los siguientes dos elementos de cada sucesión y obtenga una fórmula para la $n$-ésima posición. Demuestre que la fórmula es válida.

    *a*)
    $$\begin{aligned} 1 &= 1 \\ 1+4 &= 5 \\ 1+4+9 &= 14 \\ 1+4+9+16 &= 30 \end{aligned}$$

    *b*)
    $$\begin{aligned} 1+0\cdot 1 &= 1 \\ 1+1\cdot 3 &= 4 \\ 1+2\cdot 4 &= 9 \\ 1+3\cdot 5 &= 16 \end{aligned}$$

29. (**0.5 puntos**) Supongamos que $p$ y $q$ son números

    primos cuya diferencia es de tres unidades. Demuestre que $p = 5$.
    Ya que la diferencia entre p y q es de 3 unidades,$p - q = 3$, emtonces $q = p - 3$. Tenemos dos posibilidades para q.
    **Caso 1:**q es par
    Como q es primo y el único número primo par es 2, entonces q=2 y si $2 = p - 3$, entonces $p = 5$.
    **Caso 2:** q es impar:
    Que q sea impar significa que q es de la forma $q = 2k+1$ con $k \in \mathbb{Z}$. Así despejamos de $q = p - 3$

    $$\begin{aligned} 2k + 1 &= p - 3 \\ 2k + 4 &= p \\ 2(k + 2) &= p \end{aligned}$$

    Por lo tanto vemos que p es par, ya que $p = 1 \cdot (k + 2)$. Pero por hiótesis p debe ser primo y el único primo par es 2. Pero veamos que esto no es posible pues si p=2, entonces de despejar q=p-3 obtenemos $q = 2 - 3 = -1$ y ya que q es primo debe ser positivo. Así vemos que este caso no puede suceder.

    Así el único caso posible es el 1, y por lo tanto los únicos números primos cuya diferencia es de 3 unidades son 2 y 5, con p=5 y q=2.

■

30. (**0.5 puntos**) Si $n$ es un número compuesto, entonces $2^n - 1$ también es un número compuesto.

31. (**0.5 puntos**) Haciendo uso del algoritmo de Euclides encuentre el m.c.d. de los siguientes pares de números y luego escríbalo como una combinación lineal de ellos.

    *a*) $a = -121$ ; $b = 33$.

    *b*) $a = 543$ ; $b = -241$.

    *c*) $a = 78696$ ; $b = 19332$.

    *d*) $a = -216$ ; $b = 64110$.

    *e*) $a = 12$ ; $b = -36$.

32. (**0.5 puntos**) Demuestra que dados $a, b \in \mathbb{Z} - \{0\}$ se tiene que $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.
    Por lemas de clase sabemos que dados $a, b > 0$: $(a, b) \geq 1$, y también que $(a, b) = (-a, -b) = (-a, b) = (a, -b) = (|a|, |b|)$. Tambien consideremos que por propiedad del valor absoluto $|\frac{a}{b}| = \frac{|a|}{|b|}$.
    Por lo anterior, vemos que:

$$\begin{aligned}\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) &= \left(|\frac{a}{(a,b)}|, |\frac{b}{(a,b)}|\right) \\ &= \left(\frac{|a|}{|(a,b)|}, \frac{|b|}{|(a,b)|}\right) \\ &= \left(\frac{|a|}{(a,b)}, \frac{|b|}{(a,b)}\right) \\ &= \left(\frac{|a|}{(|a|,|b|)}, \frac{|b|}{(|a|,|b|)}\right)\end{aligned}$$

    Como $a, b \in \mathbb{Z} - \{0\}$, entonces $a \neq 0$ y $b \neq 0$ y $|a| \geq 1$ y $|b| \geq 1$. Con esto por el Teorema Fundamental del Algebra se le puede dar una descomposición canónica de $|a|$ y $|b|$ en factores primos, entonces veremos que podemos escribir:

$$\begin{aligned}|a| &= p_1^{\alpha_1} \cdots p_k^{\alpha_k} \\ |b| &= p_1^{\beta_1} \cdots p_k^{\beta_k}\end{aligned}$$

    Donde $p_1, \ldots, p_k$ son números primos y $\alpha_i, \beta_i \geq 0$.

    Existe un teorema que nos garantiza que $(|a|, |b|) = \prod_{i=1}^{k} p_i^{\gamma_i}$ donde $\gamma_i = \min\{\alpha_i, \beta_i\}$.
    Así, vemos que:

$$\begin{aligned}\frac{|a|}{(|a|,|b|)} &= \frac{p_1^{\alpha_1} \cdots p_k^{\alpha_k}}{p_1^{\gamma_1} \cdots p_k^{\gamma_k}} \\ &= p_1^{\alpha_1 - \gamma_1} \cdots p_k^{\alpha_1 - \gamma_1}\end{aligned}$$

$$\frac{|b|}{(|a|,|b|)} = \frac{p_1^{\beta_1}\cdots p_k^{\beta_k}}{p_1^{\gamma_1}\cdots p_k^{\gamma_k}}$$
$$= p_1^{\beta_1-\gamma_1}\cdots p_k^{\beta_1-\gamma_1}$$

.

Ya sabemos que $\left(\frac{|a|}{(|a|,|b|)}, \frac{|b|}{(|a|,|b|)}\right) = \prod_{i=1}^{k} p_i^{\phi_i}$ donde $\phi_i = \text{mín}\{\alpha_i - \gamma_i, \beta_i - \gamma_i\}$. Veremos que, por la definición de $\gamma_i$ debe pasar que $\alpha_i - \gamma_i = 0$ ó $\beta_i - \gamma_i = 0$. Hay 3 casos:

*a*) $\alpha_i = \beta_i$:
En este caso, $\gamma_i = \text{mín}\{\alpha_i, \beta_i\} = \alpha_i = \beta_i$. Por lo tanto, $\alpha_i - \gamma_i = 0$ y $\beta_i - \gamma_i = 0$. Con esto, ya que $\phi_i = \text{mín}\{\alpha_i - \gamma_i, \beta_i - \gamma_i\} = \text{mín}\ \{0, 0\} = 0$.

*b*) $\alpha_i < \beta_i$:
En este caso, $\gamma_i = \text{mín}\{\alpha_i, \beta_i\} = \alpha_i$. Por lo tanto, $\alpha_i - \gamma_i = 0$, además $\beta_i - \gamma_i > 0$. Con esto, ya que $\phi_i = \text{mín}\{\alpha_i - \gamma_i, \beta_i - \gamma_i\} = \text{mín}\ \{0, \beta_i - \gamma_i\} = 0$.

*c*) $\alpha_i > \beta_i$:
En este caso, $\gamma_i = \text{mín}\{\alpha_i, \beta_i\} = \beta_i$. Por lo tanto, $\beta_i - \gamma_i = 0$, además $\alpha_i - \gamma_i > 0$. Con esto, ya que $\phi_i = \text{mín}\{\alpha_i - \gamma_i, \beta_i - \gamma_i\} = \text{mín}\ \{\alpha_i - \gamma_i, 0\} = 0$.

Ya que demostramos que $\phi_i = 0$ para toda $1 \leq i \leq k$. Entonces: $\left(\frac{|a|}{(|a|,|b|)}, \frac{|b|}{(|a|,|b|)}\right) = \prod_{i=1}^{k} p_i^{\phi_i} = \prod_{i=1}^{k} p_i^{0} = p_1^0 \cdots p_k^0 = 1 \cdots 1 = 1$.

Así, queda demostrado que $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.

■

33. (**0.5 puntos**) Sean $a, b, c \in \mathbb{Z} - \{0\}$. Demuestre que $[ca, cb] = |c|\,[a, b]$.

34. (**0.5 puntos**) Sean $a, b \in \mathbb{Z} - \{0\}$ tales que $(a, b) = 1$. Demuestre que

$$[a, b] = |a| \cdot |b|.$$