

TP3 – Números

Agustina Sol Rojas

Ejercicio 1.

Probar que no hay enteros simultáneamente pares e impares

1. Sea $a \in \mathbb{Z}$, a es múltiplo de $b \in \mathbb{Z}$ si $\exists c \in \mathbb{Z} : a = b * c$
2. Un numero $x \in \mathbb{Z}$ es par si es múltiplo de 2 ($\exists c \in \mathbb{Z} : x = 2 * c$). Caso contrario es impar ($\nexists c \in \mathbb{Z} : x = 2 * c$).

$\exists n \in \mathbb{Z} : n$ es par e impar

Planteos auxiliares:

n es par $\rightarrow \exists c \in \mathbb{Z} : n = 2 * c$

n es impar $\rightarrow \nexists c \in \mathbb{Z} : n = 2 * c$

$\therefore \exists c \in \mathbb{Z} : n = 2 * c$ y $\nexists c \in \mathbb{Z} : n = 2 * c \rightarrow absurdo.$

$\therefore \nexists n \in \mathbb{Z} : n$ es par e impar

Ejercicio 2.

Analizar si las siguientes afirmaciones son verdaderas o falsas:

- a) Si $a|1$ entonces $a = 1$ o $a = -1$

Planteos auxiliares:

$a|1$ si $\exists c \in \mathbb{Z} : 1 = a * c$

Si $a = -1 \rightarrow -1|1$

$\exists d \in \mathbb{Z} : 1 = -1 * d$

$$\begin{aligned} \text{Si } a = 1 &\rightarrow 1|1 \\ \exists e \in Z : 1 &= 1 * e \end{aligned}$$

Como $\exists c \in Z : 1 = a * c$
 entonces $-1|1$ o $1|1$
 entonces $\exists d \in Z : 1 = -1 * d$ o $\exists e \in Z : 1 = 1 * e$

Demostración

$$1 = -1 * d$$

$$\frac{1}{-1} = d$$

$$-1 = d$$

$$1 = 1 * e$$

$$\frac{1}{1} = e$$

$$1 = e$$

$$\therefore \exists d = -1 \in Z : 1 = -1 * (-1) \text{ y } \exists e = 1 \in Z : 1 = 1 * 1$$

$$\therefore \text{Si } a|1 \text{ entonces } a = 1 \text{ o } a = -1$$

b) $a|b$ y $b|c$ entonces $a|c$

Planteos auxiliares:

$$a|b \text{ si } \exists d \in Z : b = a * d$$

$$b|c \text{ si } \exists e \in Z : c = b * e$$

$$a|c \text{ si } \exists f \in Z : c = a * f$$

$$¿\exists f \in Z : c = a * f?$$

$$\text{Como } \exists d \in Z : b = a * d \text{ y } \exists e \in Z : c = b * e$$

$$\text{entonces } \exists f \in Z : c = a * f$$

Demostración

$$b = a * d$$

$$c = b * e$$

$$c = b * e = (a * d) * e = a * (d * e) = a * f$$

$$f = d * e \in Z$$

$$\therefore \exists f \in Z : c = a * f \rightarrow a|c$$

c) $a(a - 1)$ es par

Para poder demostrar que $a(a-1)$ es par se demostrara primero que la multiplicación de un numero par con cualquier otro entero da un numero par:

Asumiendo que x es par, entonces $\exists y \in Z : x = 2 * y$

Sea z un entero cualquiera (sea par o no)

$x * z$ es par si $\exists f \in Z : x * z = 2 * f$

$$x = 2 * y$$

$$x * z = (2 * y) * z = 2 * (y * z) = 2 * f$$

$$f = (y * z) \in Z$$

$$\therefore \exists f \in Z : x * z = 2 * f$$

Ahora se demostrará que $a(a-1)$ es par considerando dos casos:

1. a es par:

Si a es par, entonces $\exists c \in Z : a = 2 * c$

$$a = 2c$$

$$a(a - 1) = (2c) * (2c - 1)$$

Como $2c$ es par, $(2c) * (2c - 1)$ es par y por lo tanto $a(a - 1)$ es par

2. a es impar:

Si a es impar, entonces $\nexists c \in Z : a = 2 * c$

Como no existe entero que haga valer la igualdad se tratara de aproximar de la mejor manera posible a a por un multiplo de 2, haciendo uso de la diferencia entre a y dicho número, lo que se llama resto, siendo aquel en este caso 1. Reescribiendo quedaría:

Si a es impar, entonces $\exists c \in Z : a = 2 * c + 1$

$$a = 2c + 1$$

$$a(a - 1) = (2c + 1) * (2c + 1 - 1) = (2c + 1) * (2c)$$

Como $2c$ es par (por 1.), $(2c + 1) * (2c)$ es par y por lo tanto $a(a - 1)$ es par

d) $x|y$ y $y|z$ entonces $x|yz$

Planteos auxiliares

$$x|y \text{ si } \exists t \in Z : y = x * t$$

$$y|z \text{ si } \exists w \in Z : z = y * w$$

$$x|yz \text{ si } \exists j \in Z : yz = x * j$$

Como $\exists t \in Z : y = x * t$ y $\exists w \in Z : z = y * w$
 entonces $\exists j \in Z : yz = x * j$

Demostración

$$y = x * t$$

$$z = y * w$$

$$yz = (x * t) * (y * w) = x * (t * y * w) = x * j$$

$$j = (t * y * w) \in Z$$

$$\therefore \exists j \in Z : yz = x * j \rightarrow x|yz$$

Ejercicio 3.

Si a un número se lo divide por 5, el resto es 3 y si se lo divide por 7, el resto es 4. ¿Cuál es el resto si se lo divide por 35 ?

- a. $N = 5q_1 + 3$
- b. $N = 7q_2 + 4$

$N = 35q + r$ ¿Cuál es el r si se divide al número por 35?

1. Se multiplican las ecuaciones (ambos lados de la igualdad) de tal forma que el primer término a la derecha de la igualdad tenga el valor de $35 * q_i$:

Se hace uso de la propiedad distributiva.

- a. $7N = 7 * 5q_1 + 3 * 7 = 35q_1 + 21$
- b. $5N = 5 * 7q_2 + 4 * 5 = 35q_2 + 20$

2. Luego se multiplicarán ambas ecuaciones de tal forma que la resta entre ambas nos deje un solo N:

$$a. \quad 3 * (7N) = 3 * 35 * q_1 + 21 * 3 \rightarrow 21N = 35 * (3q_1) + 63$$

$$b. \quad 4 * 5N = 4 * 35 * q_2 + 20 * 4 \rightarrow 20N = 35 * (4q_2) + 80$$

Se reordena un poco la ecuación haciendo uso de la propiedad asociativa de la multiplicación.

3. Se restan ambas ecuaciones:

$$\begin{array}{r} 21N = 35 * (3q_1) + 63 \\ - 20N = 35 * (4q_2) + 80 \\ \hline \end{array}$$

$$N = 35(3q_1 - 4q_2) + (63 - 80)$$

Teniendo en cuenta que $q_3 = (3q_1 - 4q_2) \in \mathbb{Z}$ nos queda:

$$N = 35q_3 + (-17)$$

4. Esto nos deja con un resto negativo, lo cual no es válido (el resto debe tomar valores $0 \leq r < |35|$), para tener un ecuación con resto valido se la debe reescribir, para ello se sumará y se restara a la ecuación el numero 35 (es como sumar 0, el elemento neutro de la suma):

$$N = 35q_3 + (-17) + 35 - 35$$

Reescribiendo la ecuacion quedaría:

$$N = 35q_3 - 35 + 18$$

Sacamos factor común de $35q_3 - 35$

$$N = 35(q_3 - 1) + 18$$

Teniendo en cuenta que $q = (q_3 - 1) \in \mathbb{Z}$ nos queda:

$$N = 35q + 18$$

\therefore Si se divide a N por 35 el resto es 18

Ejercicio 4.

Sean a y b dos números enteros que tienen restos 4 y 7 respectivamente en la división por

11. Hallar los restos de la división por 11 de $(a + b^2)$

a. $a = 11 * q_1 + 4$

b. $b = 11 * q_2 + 7$

$$(a + b^2) = 11 * q + r \text{ ¿Cuál es el } r \text{ si se divide } (a + b^2) \text{ por } 11?$$

1. Se reemplaza en $(a + b^2)$ a a y b por sus respectivas formulas y se aplican propiedades de la suma, la multiplicación y la regla del binomio:

$$\begin{aligned}(a + b^2) &= (11q_1 + 4) + (11q_2 + 7)^2 = 11q_1 + 4 + 11q_2 * 11q_2 + 2 * 11q_2 * 7 + 49 \\&= (11q_1 + 11q_2 * 11q_2 + 2 * 11q_2 * 7) + 53 \\&= 11 * (q_1 + (q_2)^2 + 14q_2) + 53\end{aligned}$$

2. Teniendo en cuenta que $q_3 = (q_1 + (q_2)^2 + 14q_2) \in \mathbb{Z}$ nos queda:

$$(a + b^2) = 11 * q_3 + 53$$

3. Esto nos deja con un resto mayor a $|11|$, lo cual no es válido (el resto debe tomar valores $0 \leq r < |11|$), para tener un ecuación con resto valido se la debe reescribir, para ello escribirá a 49 como $11 + 11 + 11 + 11 + 9$:

$$(a + b^2) = 11 * q_3 + 11 + 11 + 11 + 11 + 9$$

Sacamos factor común de $11 * q_3 + 11 + 11 + 11 + 11$

$$(a + b^2) = 11 * (q_3 + 4) + 9$$

Teniendo en cuenta que $q = (q_3 + 4) \in \mathbb{Z}$ nos queda:

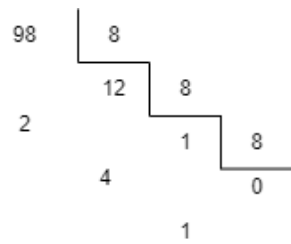
$$(a + b^2) = 11 * q + 9$$

\therefore Si se divide $a(a + b^2)$ por 11 el resto es 9

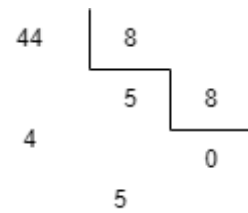
Ejercicio 5.

Convertir los siguientes números de base 10 a base 8:

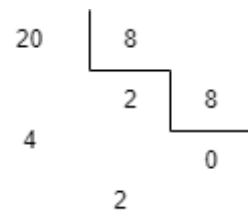
a) 98



b) 44



c) 20



Ejercicio 6.

Calcular el máximo común divisor entre

i) (16, 24)

Se descompone cada entero en producto de primos y se buscan los factores en común.

$$16 = 2 * 2 * 2 * 2$$

$$24 = 2 * 2 * 2 * 3$$

$2 * 2 * 2 = 2^3 = 8$ es el mayor factor en común y por lo tanto es el mcd.

ii) (70, 50)

Se descompone cada entero en producto de primos y se buscan los factores en común.

$$70 = 2 * 5 * 7$$

$$50 = 2 * 5 * 5$$

$2 * 5 = 10$ es el mayor factor en común y por lo tanto es el mcd.

iii) (121, 88)

Se descompone cada entero en producto de primos y se buscan los factores en común.

$$121 = 11 * 11$$

$$88 = 2 * 2 * 2 * 11$$

11 es el mayor factor en común y por lo tanto es el mcd.

iv) (-90, 90)

Como el 90 es un divisor de -90 (y de el mismo) el mcd es 90.

v) (980, 224)

Se descompone cada entero en producto de primos y se buscan los factores en común.

$$980 = 2 * 2 * 5 * 7 * 7$$

$$224 = 2 * 2 * 2 * 2 * 2 * 7$$

$2 * 2 * 7 = 28$ es el mayor factor en común y por lo tanto es el mcd.

Ejercicio 7.

Probar que si a y b son enteros:

- a) $a + b$ es coprimo con a (tener en cuenta $(a, b) = 1$)

Se quiere probar $(a + b, a) = 1$

1. Dado $(a + b, a) = d$, por definicion de mcd se cumple:

- $d | a + b$, es decir, $\exists m_1 \in \mathbb{Z} : a + b = d * m_1$
- $d | a$, es decir, $\exists m_2 \in \mathbb{Z} : a = d * m_2$

2. Teniendo en cuenta que $a + b = d * m_1$ despejando b quedaría:

$$b = d * m_1 - a = d * m_1 - d * m_2 = d(m_1 - m_2)$$

3. Teniendo en cuenta que $c = m_1 - m_2 \in \mathbb{Z}$:

$$b = d * c$$

4. Esto implica que $d | b$

5. Por lo tanto si $d | a + b$ y $d | a$, entonces $d | b$ y $d | a$ entonces $d | (a, b)$ pero por enunciado se sabe que $(a, b) = 1$, por lo tanto no queda otra opción que $d = 1$, entonces $(a + b, a) = 1$, es decir, $a + b$ es coprimo con a .

- b) sí a es no nulo, $(a, 0) = |a|$

1. Dados $a, 0 \in \mathbb{Z}$ si a no es nulo, entonces d es el mcd de a y 0 si $d > 0$ y:
 - $d|a$ y $d|0$.
 - Si existe otro numero D tal que $D|a$ y $D|0$, entonces necesariamente $D|d$.
2. Como $d|0$ siempre se cumple, ya que 0 es divisible por todos los enteros, se debe buscar un d entero mayor a 0 tal que $d|a$ cumpliéndose que exista otro número D tal que $D|a$ y $D|0$, entonces $D|d$.
3. Para que $d|a$ debe existir un $c \in \mathbb{Z} : a = d * c$
 - a. Si $a > 0, d = |a|$ y $c = 1$ se cumple $a = |a| * 1$
 - b. Si $a < 0, d = |a|$ y $c = -1$ se cumple $a = |a| * -1$
4. En ambos casos el valor de d es $|a|$, ya que para cualquier otra combinación de valores de d y c no se cumpliría la igualdad $a = d * c$ a la vez que se cumple la definición de mcd.
5. Entonces necesariamente $d = |a|$, por lo tanto si a es no nulo $(a, 0) = |a|$.

c) $(a, b) = 1$ entonces $ma + nb = k$, con m, n y k enteros.

1. Dado que $(a, b) = 1$, por la Identidad de Bézout existen enteros m_1 y n_1 tal que:

$$m_1 a + n_1 b = 1$$
2. Multiplicando a ambos lados de la ecuación por k quedaría:

$$k * m_1 a + k * n_1 b = 1k \rightarrow (km_1)a + (kn_1)b = k$$
3. Teniendo en cuenta que $m = km_1 \in \mathbb{Z}$ y $n = kn_1 \in \mathbb{Z}$ nos queda:

$$ma + nb = k$$
4. Por lo tanto queda demostrado que si $(a, b) = 1$ entonces $ma + nb = k$, con m, n y k enteros.

Ejercicio 8.

Hallar $\text{mcd}(5k + 3, 3k + 2)$, para cualquier k entero

1. Dado $(5k + 3, 3k + 2)$ se desea encontrar un entero $d > 0$ tal que para todo k se cumpla:

- $d|5k + 3$, es decir, $\exists m_1 \in \mathbb{Z} : 5k + 3 = d * m_1$
- $d|3k + 2$, es decir, $\exists m_2 \in \mathbb{Z} : 3k + 2 = d * m_2$
- Existe otro numero D tal que $D|5k + 3$ y $D|3k + 2$, entonces necesariamente $D|d$.

2. Para ello se multiplicarán ambas ecuaciones de tal forma que los coeficientes de k en ambas tengan el mismo valor para poder eliminar el término con k al restarlas.

- $3 * 5k + 3 * 3 = 3 * d * m_1 \rightarrow 15k + 9 = 3 * d * m_1$
- $5 * 3k + 5 * 2 = 5 * d * m_2 \rightarrow 15k + 10 = 5 * d * m_2$

3. Luego se restan ambas ecuaciones:

$$\begin{array}{r} 15k + 9 = 3 * d * m_1 \\ - 15k + 10 = 5 * d * m_2 \\ \hline -1 = (3 * d * m_1 - 5 * d * m_2) \end{array}$$

4. Teniendo en cuenta que $c = (3m_1 - 5m_2) \in \mathbb{Z}$ nos queda:

$$-1 = d(3m_1 - 5m_2) = d * c$$

5. Para que la igualdad se satisfaga $d = 1$ y $c = -1$ o $d = -1$ y $c = 1$, con cualquier otra combinación de valores de d y c no se cumple la igualdad.

6. Siguiendo la definición de mcd , d debe ser un valor positivo, por lo que necesariamente $d = 1$.

7. Por lo tanto $(5k + 3, 3k + 2) = 1$ para todo k .

8. Por lo tanto $5k + 3$ y $3k + 2$ son coprimos para todo k .

Ejercicio 9.

Sean $a, b \in \mathbb{Z}$ y sea p primo. Demostrar que si $p|ab$ entonces $p|a$ o $p|b$.

Mostrar que esto no se cumple si p no es primo.

1. Suponiendo que $p|ab$ por definicion de divisibilidad se cumple:

- $\exists c \in \mathbb{Z} : a * b = p * c$

2. Si $p|a$ o $p|b$ se cumple que:

- $\exists x \in \mathbb{Z} a = p * x$ o $\exists w \in \mathbb{Z} b = p * w$

3. Siguiendo el Teorema Fundamental de la Aritmética siendo a y b enteros (distintos a 0, 1, -1) estos son productos finito de números primos y esa factorización es única salvo el orden:

- $a = \prod_{i=1}^n p_i^{\alpha_i}$
- $b = \prod_{j=1}^n q_j^{\alpha_j}$

4. Si p no es uno de los factores primos en la factorización de a entonces $(a, p) = 1$.

5. Siguiendo la Identidad de Bézout existen enteros m y n tales que:

$$1 = a * m + p * n$$

6. Multiplicamos ambos lados de la ecuación por b y la reescribimos un poco siguiendo las propiedades de la suma y la multiplicación para obtener:

$$b = a * b * m + p * n * b$$

7. Se sabe por hipótesis que $a * b = p * c$, por lo tanto se puede reemplazar $a * b$ en la ecuación:

$$b = p * c * m + p * n * b$$

8. Usando algunas propiedades de la multiplicación y la suma, la ecuación se puede reescribir como:

$$b = p * (c * m + n * b)$$

9. Teniendo en cuenta que $w = (c * m + n * b) \in \mathbb{Z}$:

$$b = p * w$$

10. Por lo tanto se cumple que $p|b$
11. Como se demostró que si $p|ab$ y p no divide a a , entonces p necesariamente debe dividir a b , lo cual se termina demostrando. Por lo tanto la afirmación es verdadera.
12. Se puede demostrar de forma análoga si $p|ab$ y p no divide a b , entonces p necesariamente debe dividir a a .

Si p no es primo, esto no se cumple:

Contraejemplo:

1. Sean:
 - $p = 6$
 - $a = 2$
 - $b = 3$
2. $a * b = 2 * 3 = 6$, claramente $6|6$, ya que $\exists c \in \mathbb{Z} : 6 = 6 * c$, con $c = 1$.
3. No se cumple que $6|2$ puesto que $\nexists c \in \mathbb{Z} : 2 = 6 * c$
4. No se cumple que $6|3$ puesto que $\nexists d \in \mathbb{Z} : 3 = 6 * d$
5. Esto demuestra que si p no es primo, puede dividir a $a * b$ sin dividir a ninguno de los factores individuales.

Ejercicio 10.

Hallar, si existe, un número entero q tal que $7290q$ es el cubo de un entero

1. Se debe hallar un $q \in \mathbb{Z}$ tal que $7290 * q = x^3$
2. Se reescribirá a 7290 como su descomposición en factores primos:

$$7290 = 2^1 \cdot 3^6 \cdot 5^1$$

3. Para que $7290 * q = x^3$ todos los exponentes deben ser múltiplos de 3:
 - 2^1 necesita ser elevado a la 2^3 por lo tanto se necesita 2^2 .
 - 3^6 ya es múltiplo de 3.
 - 5^1 necesita ser elevado a la 5^3 por lo tanto se necesita 5^2
4. Como 7290 está siendo multiplicado por q , se puede establecer el valor de ese q como lo que “necesita” cada factores primo para tener un exponente múltiplo de 3, eso nos dejaría:

$$q = 2^2 * 5^2 = 100$$

5. Por lo tanto q debe ser 100 para que $7290 * q = x^3$

6. Verificación:

$$7290 * 100 = x^3$$

$$\sqrt[3]{7290 * 100} = \sqrt[3]{x^3}$$

$$\sqrt[3]{2^3 * 3^6 * 5^3} = \sqrt[3]{x^3}$$

$$2 * 3^2 * 5 = x$$

$$x = 90$$

$$x^3 = 90^3 = 729000$$

Ejercicio 11.