

- Teoría de Números 2
 - Ejercicios
 - Problema 1
 - Solución
 - Problema 2
 - Solución
 - Problema_3
 - Solución
 - Problema 4
 - Solución
 - Solución (Leydis Laura)
 - Problema_5
 - Solución
 - Problema 6
 - Solución
 - Problema 7
 - Solución
 - Problema 8
 - Solución
 - Problema 9
 - 1. Solución
 - 2. Solución
 - 3. Solución
 - 4. Solución

Teoría de Números 2

Ejercicios

Problema 1

Sean a, b_1, b_2, \dots, b_n enteros con $a \neq 0$. Prueba que si $a \mid b_1 * b_2 * \dots * b_n$ y a es primo relativo con todos los b_i excepto b_n , entonces $a \mid b_n$

Solución

Procedamos por inducción:

- Caso base: para $n = 2$: Si $a \div b_1 b_2$ y $\text{mcd}(a, b_1) = 1 \Rightarrow a \div b_2$

Notese que si $\text{mcd}(a, b_1) = 1$ existen x, y tales que $\text{mcd}(x, y) = 1$ cumpliéndose que:

$$ax + b_1 y = 1$$

Luego, al multiplicar por b_2 queda que:

$$ab_2 x + b_1 b_2 y = b_2$$

Pero como $a \div ab_2$ y $a \div b_1 b_2$ por datos $\Rightarrow a \div b_2$

- Hipótesis de inducción: Supongamos que para $n = k$ se cumple que $a \div b_1 b_2 \cdots b_k$ y a es primo relativo con todos los b_i excepto b_k , entonces $a \div b_k$
- Entonces, para $n = k + 1$ se cumple que: como a es coprimo con $b_1, b_2 \Rightarrow a$ es coprimo con $b_1 b_2$. Demostremoslo.
 - Si $\text{mcd}(a, b_1) = 1 \Rightarrow$ existen x, y tal que

$$ax + b_1 y = 1 \Rightarrow ab_2 x + b_1 b_2 y = b_2$$

Como $\text{mcd}(b_2, a) = 1$ y $a \div ab_2 \Rightarrow a$ no divide a $b_1 b_2$.

Entonces sea $b_1 b_2 = t$, luego $b_1 b_2 \cdots b_{k+1} = tb_2 \cdots b_{k+1}$ y tendríamos k números de los cuales a es coprimo con los primeros $k - 1$, por lo que $a \div b_{k+1}$ por hipótesis de inducción

Problema 2

Prueba que $\text{mcd}(n, 6) = 1 \Rightarrow n^2 - 1$ es divisible por 24

Solución

Notemos que $n^2 - 1 = (n + 1)(n - 1)$ y como $\text{mcd}(n, 6) = 1 \Rightarrow n$ es impar, luego entre $n + 1$ y $n - 1$ uno de ellos será múltiplo de 2 y el otro múltiplo de 4 por ser dos

números pares consecutivos.

Para que sea divisible $n^2 - 1$ por 24, como ya probamos que es divisible entre 8 (por ser divisible por 2 y 4 simultáneamente) basta demostrar que entre $n - 1$ y $n + 1$ hay un factor 3. Observemos que de tres números consecutivos hay uno que es múltiplo de 3, luego, $(n - 1)n(n + 1)$ es múltiplo de 3, pero como $\text{mcd}(n, 6) = 1 \Rightarrow \text{mcd}(n, 3) = 1 \Rightarrow 3 \div (n - 1)(n + 1)$ que es lo que queríamos probar.

Problema_3

Sean a, b enteros con $b \neq 0$. Prueba que si $a = b * q + r$ para algun q, r entonces $\text{mcd}(a, b) = \text{mcd}(b, r)$

Solución

Supongamos que $\text{mcd}(a, b) = d_1 \geq \text{mcd}(b, r) = d_2$, como $d_1 \div a$ y $d_1 \div b \Rightarrow d_1 \div r \Rightarrow d_1 \div \text{mcd}(b, r)$ y como $d_1 \geq d_2 \Rightarrow d_1 = d_2$. Análogamente suponiendo que $d_2 \geq d_1$

Problema 4

Sean a_1, a_2, \dots, a_n enteros no todos ceros. Prueba que $\text{mcd}(a_1, a_2, \dots, a_n) = \text{mcd}(a_1, \text{mcd}(a_2, \dots, a_n))$

Solución

El problema podemos transformarlo en demostrar que todo divisor del miembro derecho divide al miembro izquierdo y todo divisor del miembro izquierdo divide al miembro derecho.

Supongamos que $d \div \text{mcd}(a_1, a_2, \dots, a_n) \Rightarrow d \div a_1, d \div a_2, \dots, d \div a_n$ entonces como $d \div a_1$ y d divide al resto entonces divide a su mcd y por tanto divide al $\text{mcd}(a_1, \text{mcd}(a_2, \dots, a_n))$

Supongamos que $d \div \text{mcd}(a_1, \text{mcd}(a_2, \dots, a_n)) \Rightarrow d \div a_1$ y $d \div \text{mcd}(a_2, \dots, a_n) \Rightarrow d \div a_1, d \div a_2, \dots, d \div a_n \Rightarrow d \div \text{mcd}(a_1, a_2, \dots, a_n)$

Solución (Leydis Laura)

Idea de la demostración: Agrupar los divisores comunes de a y b en un conjunto A ; agrupar los divisores comunes de b y R en un conjunto B . Demostrar que $A = B$.

Sea $d \in A$, $d \div a$ y $d \div b$. Luego $d \div a * x + b * y$, donde $x, y \in \mathbb{Z}^+$ (resultado del ejercicio 1 de la primera clase práctica).

Por dato $a = b * q + R$, entonces $R = a - b * q$.

$R = a * (1) + b * (-q)$, luego R es combinación lineal de a y b . Luego $d \div R$.

$$d \div b \text{ y } d \div R \implies d \in B$$

$$\forall d \in \mathbb{Z}, d \in A \implies d \in B$$

Luego $A \subseteq B$.

De forma análoga, podemos demostrar que $B \subseteq A$.

$$A \subseteq B \text{ y } B \subseteq A \implies A = B$$

Todo número tiene una cantidad finita de divisores. Luego A y B son conjuntos finitos. Como $A = B$, el mayor elemento de A , es el mayor elemento del conjunto B .

Sea d el mayor elemento de A y B . Entonces d es el mayor entero positivo que es divisor común de a y b (puesto que $d \in A$), por tanto $d = (a, b)$. Además, d es el mayor entero positivo que es divisor común de b y R (puesto que $d \in B$). Luego $d = (b, R)$. $(a, b) = (b, R)$

Problema_5

Sean a, b enteros no cero los dos y k entero. Prueba que $\text{mcd}(ka, kb) = k * \text{mcd}(a, b)$

Solución

Para demostrar este problema demostremos el siguiente lema:

- Si $\text{mcd}(a, b) = d$, $t \in \mathbb{Z}_+$ un número que divide a a, b, d y x, y números que cumplen que $ax + by = d$, entonces, al dividir entre t tenemos que esos mismos x, y generan la mínima combinación lineal de $\frac{a}{t} = a_1$ y $\frac{b}{t} = b_1$

Supongamos que es falso, o sea, que $\frac{d}{t}$ no es la mínima combinación lineal de a_1, b_1 , entonces sean x_1, y_1 números tal que $\text{mcd}(a_1, b_1) = d_1 < \frac{d}{t}$ y $a_1x_1 + b_1y_1 = d_1$, pero al multiplicar la ecuación por t se cumple que $ax_1 + by_1 = d_1t < d$, lo cual es falso porque $\text{mcd}(a, b) = d$

Sea $\text{mcd}(ka, kb) = d \Rightarrow$ existen x, y tal que $kax + kby = d \Rightarrow k(ax + by) = d$ y como x, y generan la menor combinación lineal de ka, kb entonces por el lema anteriormente demostrado $ax + by = \text{mcd}(a, b)$ y por tanto $k * \text{mcd}(a, b) = \text{mcd}(ka, kb)$

Problema 6

Halla el menor entero n compuesto que no es divisible por ninguno de los primeros k primos

Solución

Sea p_{k+1} el primo $k + 1$, entonces si n es compuesto $\Rightarrow n = ab$, como n no es divisible por ninguno de los primeros k primos entonces ni a ni b lo deben ser, por lo que, al menos deben ser divisibles por p_{k+1} , luego $n \geq (p_{k+1})^2 \Rightarrow$ el menor entero n que cumple es $n = (p_{k+1})^2$

Problema 7

Prueba que para todo n mayor que 2 se cumple que existe p primo tal que $n < p < n!$

Solución

Nótese que para $n > 2$ entre n y $n!$ existen números, luego como $n! = 1 * 2 * 3 * \dots * n \Rightarrow n! - 1$ es coprimo con cada número menor igual que n , por tanto, $n! - 1$ es primo o es divisible entre un primo mayor que n pero menor que $n!$

Problema 8

Sea p_n el n -ésimo primo. Prueba que $p_n \leq 2^{2^{n-1}}$

Solución

Demostremoslo por inducción fuerte:

- Caso base: para $n = 1$ tomemos 2 como el primer primo, entonces se cumple que $2 = 2 \Rightarrow p_1 \leq 2^{2^{1-1}}$
- Hipótesis de inducción: para todo i desde 1 hasta k se cumple que $p_i \leq 2^{2^{i-1}}$
- Demostremos que si multiplicamos todos los primos hasta el k -ésimo el resultado será un número mayor que el próximo primo, o sea, $p_1 p_2 \cdots p_k > p_{k+1}$
- - Nótese que si el número $p_1 p_2 \cdots p_k - 1$ es primo ya existe un primo mayor que p_k y menor que $p_1 p_2 \cdots p_k$, de lo contrario ese número se puede expresar como $a * b$ donde tanto a como b son coprimos con los primeros k primos, sin pérdida de generalidad sea $a > 1$, entonces si a cumple con el primo que estamos buscando, de lo contrario $a = a_1 * b_1$ y así se repite el proceso hasta que por el principio del buen orden, como estamos teniendo en cuenta solo los divisores positivos, llegaremos a algún a_m tal que sea primo y este cumplirá con la condición de ser mayor que p_k y menor que $p_1 p_2 \cdots p_k$
- Luego, utilizando que para todo $i \leq k$ se cumple que $p_i \leq 2^{2^{i-1}}$ y por tanto, teniendo en cuenta lo anteriormente demostrado $p_{k+1} < p_1 p_2 \cdots p_k \leq 2^{2^{n-1} + 2^{n-2} + \cdots + 2 + 1} = 2^{2^n - 1} < 2^{2^n} \Rightarrow p_{k+1} < 2^{2^n}$

Problema 9

Sean a, b enteros, $\text{mcd}(a, b) = 1$ y n entero positivo. Calcule:

1. $\text{mcd}(a + b, ab)$
2. $\text{mcd}(a + b, a - b)$
3. $\text{mcd}(a + b, a^2 + b^2)$
4. $\text{mcd}(n^2 + 1, (n + 1)^2 + 1)$

1. Solución

Lema: sean d, a, b enteros con $d > 1$ tal que $d \div ab$ entonces siempre existen d_1, d_2 tales que $d = d_1 d_2$ y $d_1 \div a, d_2 \div b$

- Demostración: sea $d_1 = \text{mcd}(a, d)$, como $d \div ab \Rightarrow \exists r \in \mathbb{Z}$ tal que:

$$dr = ab$$

Dividiendo entre d_1 tenemos que:

$$d_2 r = a_1 b$$

Pero como $d_1 = \text{mcd}(a, d) \Rightarrow \text{mcd}(d_2, a_1) = 1 \Rightarrow d_2 \div b$ que es lo que queríamos probar: $d = d_1 d_2$ con $d_1 \div a, d_2 \div b$

Supongamos que $\text{mcd}(a + b, ab) = d > 1$, entonces si $d = d_1 * d_2$ y utilizando el lema anteriormente demostrado, asumamos sin pérdida de generalidad que $d_1 > 1$ y $d_1 \div a$, y como $d_1 \div d \Rightarrow d_1 \div (a + b) \Rightarrow d_1 \div b$ contradicción porque $\text{mcd}(a, b) = 1$

2. Solución

Supongamos que $\text{mcd}(a + b, a - b) = d$ entonces $d \div (a + b)$ y $d \div (a - b)$ de donde, al sumar y restar ambas expresiones obtenemos que $d \div 2a$ y $d \div 2b$.

Por el lema demostrado en el ejercicio anterior $d = d_1 d_2$ tal que $d_1 \div 2$ y $d_2 \div a$ en la primera expresión, luego si $d_2 \div a$, como $d \div (a + b) \Rightarrow d_2 \div (a + b) \Rightarrow d_2 \div b \Rightarrow d_2 = 1$. Como $d_1 \div 2 \Rightarrow d_1 = 1$ o $d_1 = 2$ y por tanto, $d = 2$ cuando a, b son impares y $d = 1$ cuando uno es par y otro impar.

3. Solución

Supongamos que $\text{mcd}(a + b, a^2 + b^2) = d$ entonces $d \div (a + b)$ y $d \div (a^2 + b^2)$ de donde, en la primera expresión se cumple que $d \div (a + b)^2 \Rightarrow d \div (a^2 + b^2 + 2ab)$ y como $d \div (a^2 + b^2) \Rightarrow d \div 2ab$.

Análogamente a la demostración del último lema usado se puede demostrar que dado $d \div abc$ se cumple que existen d_1, d_2, d_3 tales que $d = d_1 d_2 d_3$ y $d_1 \div a, d_2 \div b, d_3 \div c$, por lo que, de vuelta al problema en el que estábamos, existen d_1, d_2, d_3 tales que $d = d_1 d_2 d_3$ y $d_1 \div 2, d_2 \div a, d_3 \div b$. De manera similar al inciso anterior se demuestra que $d_2, d_3 = 1$, por lo que $d = 1$ o $d = 2$

4. Solución

Supongamos que $\text{mcd}(n^2 + 1, (n + 1)^2 + 1) = d$ entonces:

1.
$$d \div (n^2 + 1)$$

2.
$$d \div ((n + 1)^2 + 1)$$

Restando ambas expresiones tenemos:

3.
$$d \div (2n + 1)$$

Luego, restando (1) con (3) resulta en:

4.
$$d \div n(n - 2)$$

Del lema utilizado en los incisos anteriores $d = d_1 d_2$ tal que $d_1 \div n$ y $d_2 \div (n - 2)$. Si $d_1 \div n$, teniendo en cuenta (1) llegamos a que $d_1 \div 1 \Rightarrow d_1 = 1 \Rightarrow$

5.
$$d \div (n - 2)$$

Restando (3) con (5) obtenemos que $d \div (n - 3)$ y restándole a este ultimo resultado la expresión (5) llegamos a la conclusión que $d \div 5$, de donde $d = 1$ o $d = 5$, caso que es posible cuando por ejemplo $n = 2$.