Entrenamiento Especial de Teoría de Números

Jesús Liceaga
jose.liceaga@cimat.mx

5 de marzo de 2021

En esta sesión, repasaremos y profundizaremos en el concepto del máximo común divisor, además de discutir el algoritmo de Euclides y sus aplicaciones.

-Liceaga

1. Teoría: Parte 1

Proposición 1. Sean a y b enteros con $b \neq 0$. Si $b|a$, entonces $|b| \leq |a|$.

Observación. Dados dos enteros a y b, estos tienen al menos un divisor en común: 1.

Definición 1. Sean a y b enteros, alguno de ellos distinto de 0. Definimos el *máximo común divisor* de a y b, denotado como $mcd(a, b)$ o (a, b), como el máximo de los divisores comunes de a y b. Es decir,

$$mcd(a, b) = \text{máx}\{d \in \mathbb{Z} : d|a \text{ y } d|b\}.$$

Proposición 2. Sean a y b enteros, con $a \neq 0$. Entonces

a) $mcd(a, b) = mcd(b, a)$.

b) $mcd(a, b) = mcd(\pm a, \pm b) = mcd(|a|, |b|)$.

c) $mcd(a, 0) = a$.

Proposición 3. Sean a y b enteros, alguno de ellos distinto de 0. Entonces

$$mcd(a, b) = mcd(a, b - a) = mcd(b, a - b) = mcd(a, a + b).$$

Corolario. Sean a y b enteros, alguno de ellos distinto de 0, y sea n otro entero cualquiera. Entonces $mcd(a, b) = mcd(a, b - an)$.

Definición 2. Decimos que a y b son *primos relativos* si $mcd(a, b) = 1$.

2. Problemas: Parte 1

Problema 1. Calcula el máximo común divisor de 2540 y 1651.

Problema 2. Nuria tiene dos barras de chocolate gigantes, una de 120 cm de largo y la otra de 96 cm. Si desea cortarlas de tal manera que todos los trozos resultantes tengan la misma longitud, que debe de ser entera, y quiere que esta sea la más grande posible, ¿cuántos trozos de chocolate obtendrá al cortar?

Problema 3. Decimos que una fracción $\frac{a}{b}$ es irreducible si a y b son primos relativos. Demuestra que la fracción $\frac{15n+4}{10n+3}$ es irreducible para todo entero n.

Problema 4. ¿Cuál es el mayor valor posible de $mcd(5n + 6, 8n + 7)$?

3. Teoría: Parte 2

Teorema 1. (Algoritmo de Euclides) Dados los enteros positivos a y b , mediante la aplicación repetida del algoritmo de la división podemos obtener una sucesión de cocientes y residuos

$$\begin{aligned}
a &= bq_0 + r_0 && 0 \leq r_0 < b && (0)\\
b &= r_0q_1 + r_1 && 0 \leq r_1 < r_0 && (1)\\
r_0 &= r_1q_2 + r_2 && 0 \leq r_2 < r_1 && (2)\\
&\vdots\\
r_{n-2} &= r_{n-1}q_n + r_n && 0 \leq r_n < r_{n-1} && (n)\\
r_{n-1} &= r_nq_{n+1}, && && (n+1)
\end{aligned}$$

donde r_n es el último residuo distinto de 0. Entonces, se tiene que r_n es el máximo común divisor de a y b.

Teorema 2. (Identidad de Bézout) Si a y b son enteros, alguno de ellos distinto de 0, entonces existen enteros x y y tales que

$$ax + by = mcd(a, b).$$

Definición 3. Una expresión de la forma $ax + by$ se llama *combinación lineal* de a y b.

Teorema 3. Si a, b son enteros, alguno de ellos distinto de 0, y $d = ax + by$ es su combinación lineal positiva mínima, entonces $d = mcd(a, b)$.

Corolario. Sean a y b enteros para los cuales existen enteros x y y tales que $ax + by = 1$. Entonces $mcd(a, b) = 1$.

Proposición 4. Sean a y b enteros, alguno de ellos distinto de 0 y $c \neq 0$ un entero. Si $c|ab$ y $mcd(a, c) = 1$ entonces $c|b$.

Teorema 4. Sean a, b enteros, alguno de ellos distinto de 0, y sea $d > 0$ otro entero. Entonces las siguientes afirmaciones son equivalentes (si se cumple una se cumplen todas):

a) d = mcd(a, b).

b) d es la combinación lineal positiva mínima de a y b.

c) $d|a$, $d|b$ y para todo entero c tal que $c|a$ y $c|b$ se tiene que $c|d$.

d) $d|a$, $d|b$ y d es combinación lineal de a y b.

4. Problemas: Parte 2

Problema 5. Expresa al máximo común divisor de 21 y 56 como combinación lineal de éstos dos.

Problema 6. Sean a y b enteros, alguno de ellos distinto de 0, y sea $d = mcd(a, b)$. Prueba que $mcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Problema 7. Sean a y b enteros tales que $mcd(a, b) = 1$. Prueba que $mcd(a^2, b^2) = 1$.

Problema 8. Sean a y b enteros tales que $mcd(a, b) = 1$ y r, s enteros positivos. Prueba que $mcd(a^r, b^s) = 1$.

Problema 9. Sean a, b y n enteros positivos. Prueba que $mcd(na, nb) = n \cdot mcd(a, b)$.

Problema 10. Sean a y b enteros tales que $mcd(a, b) = 1$. Prueba que $mcd(a + b, a - b) = 1$ o 2.

Problema 11. Sean a y b enteros tales que $mcd(a, b) = 1$. Prueba que $mcd(a + b, a^2 - ab + b^2) = 1$ o 3.

Problema 12. Sean $\overline{ab}$ y $\overline{ba}$ números de dos dígitos, donde a y b son primos relativos. Si $mcd\left(\overline{ab}, \overline{ba}\right) = \frac{a+b}{2}$, encuentra el valor de $a + b$.

Problema 13. Sea n un entero positivo par y sean a y b enteros positivos primos relativos tales que $a + b | a^n + b^n$. Encuentra a y b.

Problema 14. Sean $a > 1$ un entro y b, c enteros, alguno de ellos distinto de 0. Demuestra que $mcd(a^b - 1, a^c - 1) = a^{mcd(b,c)} - 1$

Problema 15. Sean m y n enteros positivos con m impar. Demuestra que $2^m - 1$ y $2^n + 1$ son primos relativos.

Problema 16. Los números de la sucesión $101, 104, 109, 116, \ldots$ son de la forma $a_n = 100 + n^2$, donde n es un entero positivo. Sea $d_n = mcd(a_n, a_{n+1}$. ¿Cuál es el mayor valor que puede tomar d_n?

Problema 17. Sean a y b enteros positivos y sea d su máximo común divisor. Si $\frac{a+1}{b} + \frac{b+1}{a}$ es un entero, demuestra que $d \leq \sqrt{a + b}$.

Problema 18. Determina todas las parejas (a, b) de enteros positivos tales que el número

$$\frac{a^2(b - a)}{b + a}$$

es el cuadrado de un número primo.