Matemática Discreta

Licenciatura en Sistemas de Información

Docentes
Vaira, Stella - Fedonczuk, Miguel
Colliard, David - Cottonaro, Mariana - Froloff, Bárbara

FCyT - UADER

2025

Unidad 5: El sistema de los Enteros.

Principio del buen orden. Principio de inducción matemática. Definiciones recursivas. Algoritmo de la división. Números primos. Máximo común divisor. Algoritmo de Euclides. Teorema fundamental de la Aritmética. La función ϕ de Euler.

FCyT
Facultad de Ciencia y Tecnología

Retomemos una relación entre números presentada cuando se abordó Álbegras de Boole, solo que ahora se definirá para todo número entero de la siguiente manera:

Definición

Si $a, b \in \mathbb{Z}$ y $b \neq 0$, decimos que "b divide a a", y lo denotamos $b|a$, si existe un entero n tal que $a = bn$.

Cuando esto ocurre, decimos que b es un divisor de a, o que a es múltiplo de b.

Notar que si bien esta relación está ligada con la operación división dentro de $\mathbb{Z}$, no son lo mismo.

FCyT
Facultad de Ciencia y Tecnología

La relación de divisibilidad verifica las siguientes propiedades:

Para cualquier $a, b, c, x, y, z \in \mathbb{Z}$ (siempre que el divisor no sea 0)

1. $a|a$
2. $1|a$ (1 es divisor universal)
3. $a|0$
4. $(a|b \wedge b|a) \Rightarrow a = \pm b$
5. $(a|b \wedge b|c) \Rightarrow a|c$
6. $a|b \Rightarrow a|bx$
   Si a divide b, entonces a divide a cualquier múltiplo de b
7. Si $x = y + z$ y a divide a dos de x, y, z, entonces a divide al restante.
8. $(a|b \wedge a|c) \Rightarrow a|(bx + cy)$
   Si a divide a dos números, divide a cualquier combinación lineal de ellos
   Generalización: $a|c_i$ entonces $a|(c_1x_1 + c_2x_2 + ... + c_nx_n)$

FCyT
Facultad de Ciencia y Tecnología

Definición

Un número natural p mayor a 1 se dice **primo** si 1 y p son sus únicos divisores positivos. Si un número natural n mayor a 1 no es primo, diremos que es **compuesto**.

Extensión a $\mathbb{Z}$:

- $p \in \mathbb{Z}$ es **primo** si tiene exáctamente 4 divisores ($1, -1, p$ y $-p$).
- $n \in \mathbb{Z}$ con $|n| > 1$ es **compuesto** si no es primo.
- Los enteros 0, 1 y -1 quedan fuera de estas definiciones.

Si bien se extiende la definición a los enteros, salvo mención expresa, nos referiremos de aquí en más a primos positivos.

La sucesión de primos comienza con $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$ y se puede probar que es infinita.

Proposición

Si n es compuesto, entonces existe un primo p tal que $p|n$.

Actividad 1

a. Sea $a > 1$ y n un entero cualquiera, probar que si $a|(3n-1)$ y $a|(4n+9)$ entonces a es un número primo.

b. ¿Existen enteros x, y, z tales que $6x + 9y + 15z = 107$?

c. $\forall a, b \in \mathbb{Z}$, sea $2a+3b$ un múltiplo de 17, demuestre que $17|(9a+5b)$.

FCyT
Facultad de Ciencia y Tecnología

Sean $a, b \in \mathbb{Z}$, $b > 0$, entonces existen único $q, r \in \mathbb{Z}$ tales que

$$a = qb + r, \text{ con } 0 \leq r < b$$

Al entero b se lo llama *divisor*, a *es el dividendo*, q el cociente y r resto.

En el caso de que $r = 0$ diremos que la división es exacta, y que $a|b$.

Actividad 2
Hallar el cociente y el resto de dividir a a por b

- $a = 170$ y $b = 11$
- $a = 98$ y $b = 7$
- $a = -45$ y $b = 8$

FCyT
Facultad de Ciencia y Tecnología

Proposición

Si $n \in \mathbb{Z}^+$ y n es compuesto, entonces existe un primo p tal que $p|n$ y $p \leq \sqrt{n}$.

Esto constituye un criterio básico para evaluar si un número n es primo o no, ya que si n NO es divisible por algunos de los primos menores o iguales a su raíz cuadrada, entonces n NO es compuesto, es decir, es primo.

Actividad 3

Evaluar la primalidad de 3553 y de 7919.

FCyT
Facultad de Ciencia y Tecnología

Actividades propuestas

Para realizar las actividades prácticas correspondientes a este apartado te sugerimos realizar los siguientes ejercicios del capítulo 4, apartado 4.3 (Página 213) del libro *Matemática Discreta de Ralph Grimaldi* que se encuentra en el campus virtual: 2(a, b, c), 4, 5, 7, 8, 9, 10, 12, 13.

FCyT
Facultad de Ciencia y Tecnología

Definición

Sean $a, b \in \mathbb{Z}_0^+$, no ambos nulos simultáneamente. Entonces $d \in \mathbb{Z}^+$ es el *máximo común divisor* de a y b, y se denota $mcd(a,b)$ si:

- $d|a$, $d|b$
- para cualquier divisor c de a y b, entonces $c|d$

En otras palabras $mcd(a,b)$ es el mayor de sus divisores positivos comunes. Es decir,

$$mcd(a,b) = max\{D^+(a) \cap D^+(b)\}$$

Ejemplo 1

Hallamos $mcd(120,84)$ analizando los conjuntos $D^+(120)$ y $D^+(84)$:

$D^+(120) = \{1,2,3,4,5,6,8,10,12,15,20,24,30,40,60,120\}$

$D^+(84) = \{1,2,3,4,6,7,12,14,21,28,42,84\}$

$D^+(a) \cap D^+(b) = \{1,2,3,4,6,12\}$

$mcd(a,b) = max\{D^+(a) \cap D^+(b)\} = 12$

Observar que el método no es práctico.

FCyT Facultad de Ciencia y Tecnología

Proposición

El máximo común divisor entre dos números es único

Esta proposición nos asegura que utilizando cualquier método para hallar el máximo común divisor, arribaremos a un único resultado.

Definición

Se dice que a, b son *primos relativos (o coprimos)* si $mcd(a, b) = 1$.

Así

- 15 y 33 no son coprimos porque $mcd(15, 33) = 3$
- 15 y 22 son coprimos porque $mcd(15, 22) = 1$

Actividad 4

Para cualquier $n \in \mathbb{Z}^+$, demostrar que los enteros $8n + 3$ y $5n + 2$ son primos relativos.

FCyT
Facultad de Ciencia y Tecnología

Propiedades y extensión a todos los enteros:

- $mcd(0,0)$ no está definido
- $mcd(a,b) = mcd(b,a)$
- $mcd(a,1) = 1$
- $mcd(a,0) = |a|$
- $mcd(a,b) = mcd(|a|,|b|)$
- $mcd(a,b) = mcd(a-b,b)$

Esta última propiedad constituye un método para hallar el $mcd(a,b)$.

Actividad 5

a. Verificar, utilizando la propiedad anterior, que $mcd(120,84) = 12$
b. Probar que dos números enteros consecutivos son coprimos.

FCyT
Facultad de Ciencia y Tecnología

Proposición

Si $d = mcd(a,b)$, entonces existen enteros x e y tales que $d = ax + by$. Es decir, el $mcd(a,b)$ siempre se puede escribir como combinación lineal de a y b. Además, el $mcd(a,b)$ es la menor combinación lineal positiva de a y b.

Ejemplo 2

$mcd(14,25) = 1 = (9)\cdot 14 + (-5)\cdot 25 = (34)\cdot 14 + (-19)\cdot 25 = (59)\cdot 14 + (-33)\cdot 25$

$mcd(15,33) = 3 = (-2)\cdot 15 + 1\cdot 33 = (9)\cdot 15 + (-4)\cdot 33 = (20)\cdot 15 + (-9)\cdot 33$

Claramente, la combinación lineal no es única.

Al elegir una combinación lineal cualquiera entre 15 y 33, el resultado será el mcd o algún múltiplo de él, pero la menor combinación lineal positiva es el mcd.

- $(-1)\cdot 15 + (15)\cdot 33 = 480$
- $(-2)\cdot 15 + (14)\cdot 33 = 432$
- $(-3)\cdot 15 + (-4)\cdot 33 = -177$
- $(7)\cdot 15 + (73)\cdot 33 = 2514$
- $(2)\cdot 15 + (-1)\cdot 33 = -3$
- $(-33)\cdot 15 + (15)\cdot 33 = 0$

FCyT Facultad de Ciencia y Tecnología

Proposición

Sean a y b números enteros, $a \neq 0$ y sea r, el resto de dividir a a por b; entonces $mcd(a,b) = mcd(b,r)$.

Esta proposición es muy importante, ya que si el algoritmo se repite hasta obtener una división exacta ...

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1} + 0, \end{aligned}$$

entonces $mcd(a,b) = mcd(b,r_1) = mcd(r_1,r_2) = \cdots = mcd(r_n,0) = r_n$.

El máximo común divisor es el último resto no nulo de la sucesión de restos en este algoritmo.

FCyT Facultad de Ciencia y Tecnología

Actividad 6

a. Determinar el $mcd(259,111)$ y expresarlo como una combinación lineal de estos enteros.

b. Hallar una expresión general que permita encontrar todos los enteros x e y tales que $mcd(259,111) = 259x + 111y$

FCyT
Facultad de Ciencia y Tecnología

Definición

Una ecuación algebraica cuyos coeficientes son números enteros, y el conjunto solución es un subconjunto de $\mathbb{Z}$, recibe el nombre de *Ecuación diofántica* (*diofantina*).

Ejemplo 3

$$2x + 5y = 9 \qquad 7x - 8y^2 + z = 1 \qquad x^2 - 9y^2 = 6$$
$$2x - 5xy + y = 1 \qquad x + y + z + w = 1 \qquad x^3 + y^3 = z^3$$

En particular son de interés las *ecuaciones diofánticas lineales con dos incógnitas*. Son de la forma:

$$ax + by = c \quad \text{con } a, b, c \in \mathbb{Z}$$

FCyT Facultad de Ciencia y Tecnología

Actividad 7

Hallar el conjunto solución de las siguientes ecuaciones diofánticas

$7x + 9y = 102, \qquad 84x - 120y = 60, \qquad 25x + 30y = 42$

FCyT
Facultad de Ciencia y Tecnología

Actividad 8

En cada caso, plantear la ecuación diofántica que modela el problema, y resolver:

a. Juan depura un programa en Pascal en 6 minutos, pero en Python tarda 10 minutos. Si trabaja en forma continua durante 104 minutos y no le sobró tiempo, ¿cuántos programas depuró en cada lenguaje?

FCyT
Facultad de Ciencia y Tecnología

b. En una empresa de servicios de correo postal sólo se tienen sellos de 140 y 210 pesos. ¿De qué formas se pueden sellar un paquete mediano por importe de $ 7770?

FCyT
Facultad de Ciencia y Tecnología

- **c** Una ferretería arma combos de tornillos para clientes mayoristas. Hay dos tipos de cajas: Caja A con 37 tornillos, y Caja B con 102 tornillos. Un cliente pide exactamente 1017 tornillos. Determinar si es posible cumplir con el pedido.

FCyT
Facultad de Ciencia y Tecnología

Definición

El mínimo común múltiplo de dos número enteros positivos a y b, denotado $mcm(a,b)$, es el único número entero positivo m que satisface:

- m es múltiplo de a y de b.
- Todo múltiplo común de a y b es múltiplo m.

Ejemplo 4

Múltiplos positivos de 84: $84, 168, 252, 336, 420, 504, 588, 672, 840, \cdots$
Múltiplos positivos de 120: $120, 240, 360, 480, 600, 720, 840, \cdots$
$mcm(84,120) = 840$

Proposición

Para $a, b \in \mathbb{Z}^+$, $ab = mcm(a,b) \cdot mcd(a,b)$

Ejemplo 5

$$mcm(84,120) = \frac{84 \cdot 120}{12} = 840$$

FCyT Facultad de Ciencia y Tecnología

Actividades propuestas

Para realizar las actividades prácticas correspondientes a este apartado te sugerimos realizar los siguientes ejercicios del capítulo 4, apartado 4.4 (Página 225) del libro *Matemática Discreta de Ralph Grimaldi* que se encuentra en el campus virtual: 1(a, c, d), 2, 3, 5, 6, 11, 13, 14, 15, 16, 19, 20.

FCyT
Facultad de Ciencia y Tecnología

Proposición

Si $a, b \in \mathbb{Z}^+$, p es un primo y $p|ab$, entonces $p|a$ o $p|b$.

Y generalizando esta idea ...

Sea $a_i \in \mathbb{Z}^+$ para todo $1 \leq i \leq n$. Si p es primo y $p|a_1 a_2 ... a_n$, entonces $p|a_i$ para algún $1 \leq i \leq n$.

Teorema

Todo entero $n > 1$ se factoriza unívocamente de la forma

$$n = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$$

donde $p_1, p_2, \ldots, p_r$ son los divisores primos de n
y los exponentes $c_1, c_2, \ldots, c_r$ son números naturales.

Esta representación de n recibe el nombre de **representación canónica**.

Si bien, por ejemplo $440 = 44 \cdot 10 = 2 \cdot 22 \cdot 10$; su representación canónica, a la que llamaremos simplemente su "factorización" es $440 = 2^3 \cdot 5 \cdot 11$.

Aunque los resultados teóricos son claros, en la práctica no es tan fácil factorizar un número muy grande en tiempos computacionales razonables.

Actividad 9

a. Factorizar 980220.

b. ¿En cuántos ceros termina 80!?¿Cuál es la máxima potencia de 45 que lo divide?

FCyT
Facultad de Ciencia y Tecnología

Sean las factorizaciones de dos números enteros mayores a 1:

$$n = {p_1}^{e_1} {p_2}^{e_2} ... p_k^{e_k} \qquad m = {p_1}^{f_1} {p_2}^{f_2} ... p_k^{f_k}$$

Si $m|n$, entonces $0 \leq f_i \leq e_i$, para todo $1 \leq i \leq k$, por la regla del producto, el número de divisores positivos de n es

$$\#D^+(n) = (e_1 + 1)(e_2 + 1)...(e_k + 1)$$

Ejemplo 6

$n = 819896 = 2^3 \cdot 7^1 \cdot 11^4$, entonces sus divisores tendrán la forma:
$m = 2^{f_1} \cdot 7^{f_2} \cdot 11^{f_3}$, donde
f_1 puede tomar valores entre 0 y 3,
f_2 puede tomar valores entre 0 y 1, y
f_3 puede tomar valores entre 0 y 4. Por lo que

$$\#D^+(819896) = (3+1)(1+1)(4+1) = 40$$

FCyT
Facultad de Ciencia y Tecnología

Actividades propuestas

Para realizar las actividades prácticas correspondientes a este apartado te sugerimos realizar los siguientes ejercicios del capítulo 4, apartado 4.5 (Página 232) del libro *Matemática Discreta de Ralph Grimaldi* que se encuentra en el campus virtual: 1, 2, 4, 5, 12, 13, 15, 19.

FCyT
Facultad de Ciencia y Tecnología