2. Teoría de números

En este capítulo se desglosan las principales definiciones y propiedades sobre los números naturales y enteros que se utilizan a lo largo de la asignatura.

Definición 2.1. *Definimos informalmente un **número natural** como cualquier número utilizado para contar los elementos de un conjunto. Representamos el conjunto de los números naturales como*

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$

*Sobre este conjunto se definen las operaciones usuales de suma y producto representadas por los símbolos + y ·. Como consecuencia directa de las propiedades de la suma, tiene sentido definir el opuesto o negativo de un número natural. Definimos así un **número entero** como cualquier número que es natural o bien el opuesto respecto de la suma de un número natural. Representamos el conjunto de los números enteros como*

$$\mathbb{Z} = \{\ldots - 3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Definimos también los conjuntos de números naturales o enteros mayores o iguales que un cierto número dado mediante las expresiones

$$\mathbb{N}_m = \{n \in \mathbb{N} \mid n \geq m\} = \{m, m+1, m+2, \ldots\}$$

y

$$\mathbb{Z}_m = \{n \in \mathbb{Z} \mid n \geq m\} = \{m, m+1, m+2, \ldots\}$$

Definición 2.2. *Sean $a, b \in \mathbb{Z}$, decimos que b **divide a** a, b **es divisor de** a, a **es dividido o es divisible por** b, o bien, a **es múltiplo de** b, si existe $k \in \mathbb{Z}$ que cumple $a = b \cdot k$. Lo denotamos por*

$$b|a \rightarrow a \geq b$$

*Si no existe $k \in \mathbb{Z}$ cumpliendo $a = b \cdot k$, decimos que b **no divide a** a y lo denotamos por*

$$b \nmid a$$

Definición 2.3. *Sean $a, b \in \mathbb{Z}$ siendo $a \neq 0$ o $b \neq 0$, definimos el **máximo común divisor** de a y b al número $d \in \mathbb{N}$ que cumple $d|a$ y $d|b$ (d es divisor común de a y b) y si $c \in \mathbb{N}$ cumple $c|a$ y $c|b$ entonces $c|d$ (d es el máximo de todos los divisores comunes de a y b respecto del orden de la divisibilidad). Lo denotamos por*

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

*Decimos que $m \in \mathbb{N} \backslash \{0\}$ es el **mínimo común múltiplo** de a y b si $a|m$ y $b|m$ (m es múltiplo común de a y b) y si $n \in \mathbb{N} \backslash \{0\}$ cumple $a|n$ y $b|n$ entonces $m|n$ (n es el mínimo de los divisores comunes de a y b respecto del orden de la divisibilidad). Lo denotamos por*

$$m = mcm(a, b)$$

! TIENE QUE CUMPLIR QUE:
- $a|m$ y $b|m$
- $m \in \mathbb{N} \backslash \{0\}$
- $a|n$ y $b|n$

Teorema 2.4 (Teorema de Bezout). *Sean $a, b \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$ y sea $d = mcd(a, b)$ entonces existen $m, n \in \mathbb{Z}$ tales que*

$$d = a \cdot m + b \cdot n$$

A esta igualdad se la denomina ***identidad de Bezout****.*

Teorema 2.5 (Teorema de Euclides). *Sean $a, b \in \mathbb{Z}$ y supongamos $|a| > |b|$, existen únicos $q, r \in \mathbb{Z}$ llamados* ***cociente*** *y* ***resto*** *respectivamente que cumplen la igualdad*

$$a = b \cdot q + r \qquad \begin{array}{c|c} a & b \\ \hline r & q \end{array}$$

siendo $0 \leq r < |b|$. Se cumplen además las siguientes propiedades:

1. *$b|a$ si y solo si $r = 0$* $\quad b|a \Leftrightarrow r=0$
2. *$mcd(a, b) = mcd(b, r)$*

Definición 2.6. *Decimos que $p \in \mathbb{Z}$ es un* ***número primo*** *si $p \geq 2$ y sus únicos divisores son ± 1 y $\pm p$.*

Teorema 2.7. *Sea $p \in \mathbb{N}$ un número primo y sean $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ tales que $p|(a_1 \cdot a_2 \cdots a_n)$ entonces $p|a_i$ para algún $i \in \{1, 2, \ldots, n\}$.*

Observación 2.8. *En el teorema anterior es muy importante tener en cuenta la hipótesis de que p es un número primo ya que si no se cumple dicha hipótesis podría no cumplirse la consecuencia del teorema. Por ejemplo, $6|(4 \cdot 3)$ pero $6 \nmid 4$ y $6 \nmid 3$*

Teorema 2.9 (Teorema de factorización única). *Sea $a \in \mathbb{N}$ con $a \geq 2$ entonces existen primos diferentes $p_1, p_2, \ldots, p_n$ únicos salvo el orden y existen $k_1, k_2, \ldots, k_n \in \mathbb{N}$ con $k_i \geq 1$ tales que*

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdots p_n^{k_n}$$

Ejercicios

Ejercicio 2.1 (Parcial febrero 2011). *Sean $a, b, c \in \mathbb{N}$ tales que $a|(b + c)$ entonces:*

- ☒ *Si $a|b$ entonces $a|c$* : $b = ak \rightarrow c = ak'$ $\quad a|(b+c) \equiv b+c = ka$
- ☐ $a|(b \cdot c)$ $\longrightarrow bc = ak$
- ☐ $a|mcd(b, c)$ $\longrightarrow a \,|\, sb+tc \rightarrow sb+tc = ak$

$ak + ak' = ah$
$a(k+k') = ah$
$ak'' = ah$ ✓

Ejercicio 2.2 (Parcial febrero 2014). *Sean $a, b \in \mathbb{N}$ tales que $mcd(a, 4) = mcd(b, 4) = 2$. Indica la respuesta correcta:*

$at + bs$
$at + 4s = by + 4z = 2$

- ☐ $mcd(a + b, 4) = 2.$ $\rightarrow (a+b)t + 4s = 2$
- ☐ $mcd(a + b, 4) = 4.$ $\rightarrow (a+b)t + 4s = 4$
- ☐ $mcd(a + b, 4) = 1.$ $\rightarrow (a+b)t + 4s = 1$
- ☐ *Ninguna de las anteriores.*

$at + 4s = 2$
$by + 4z = 2$
$at + 4s = by + 4z$

$\rightarrow at + 4s = 2$
$\rightarrow b + 4$

EMAIL: rafamathsinformatica@gmail.com

$\mathbb{N}$

Ejercicio 2.3 (Parcial febrero 2014). *Sean a, b y c tres números naturales tales que a y b son primos y $a|(b \cdot c)$. Indica la respuesta correcta:*

- ☐ *Siempre se da que $a|c$.* $c = ak$ NO
- ☐ *Si a y b son distintos, entonces $a|c$.* $a \neq b \Rightarrow \times$
- ☐ *Si c es primo entonces $a|c$.*
- ☐ *Ninguna de las anteriores.*

Ejercicio 2.4 (Parcial febrero 2015). *Sean $a, b, c, d \in \mathbb{N}$ tales que $a|b$ y $c|d$. Considera los asertos:*

$b = k_2 a$
$d = k_3 c$

✓ 1. *Se cumple $(a + c)|(b + d)$.* $\equiv$ $b+d = k_1(a+c)$; $k_2 a + k_3 c = k_1(a+c)$; $k_4(a+c) = k_1(a+c)$

✓ 2. *Se cumple $(a \cdot c)|(b \cdot d)$* $\equiv$ $bd = ack_1$; $k_2 a \cdot k_3 c = ack_1 \rightarrow k_2 \cdot k_3 \cdot ac = ack_1$; $k_4 \cdot ac = ack_1$

Determina el enunciado correcto:

- ☐ *El primer aserto siempre se cumple, pero el segundo algunas veces no se cumple.*
- ☐ *El segundo aserto siempre se cumple, pero el primero algunas veces no se cumple.*
- ☐ *Existen situaciones en que ninguno de los dos se cumple.*
- ☒ *Los dos asertos siempre se cumplen.*

Ejercicio 2.5 (Final junio 2015). *Sean $p \in \mathbb{N}_1$ y $j \in \{1, 2, \ldots, p-1\}$, marca la respuesta correcta*

- ☐ *Si p es primo entonces p es divisor de $\binom{p}{j}$*
- ☐ *p es siempre divisor de $\binom{p}{j}$*
- ☐ *p nunca es divisor de $\binom{p}{j}$*
- ☐ *Si p es compuesto entonces p es divisor de $\binom{p}{j}$*

Ejercicio 2.6 (Final septiembre 2015). *Si $a, b, c \in \mathbb{N}$ son tales que $a|(b + c)$ entonces*

$b + c = ak'$
$ak + c = ak' \rightarrow c = ak' - ak$
$c = a(k' - k)$

- ☒ *Si $a|b$ entonces $a|c$* $b = ak \rightarrow c = ak$
- ☐ $a|(b \cdot c)$ $bc = ak$ No
- ☐ $a|mcd(b, c)$ $(bt + cs) = ak \rightarrow$
- ☐ *Ninguna de las anteriores*

Ejercicio 2.7 (Parcial febrero 2016). *Dados $a, b, c \in \mathbb{Z}$ tales que $a|c$, $b|c$ y $mcd(a, b) = 1$ entonces* $\to as + bt = 1$

$c = ak_1$
$c = bk_2$ $\Big\}$ $ak_1 = bk_2$

- ☐ $(a \cdot b)|c$
- ☐ $(a \cdot b)|c$ *sólo si a y b son primos.*
- ☐ $(a \cdot b)|c$ *sólo si $a + b$ es primo.*
- ☐ $(a \cdot b) \nmid c$

$b = kp$

Ejercicio 2.8 (Parcial febrero 2017). *Sean $a, b \in \mathbb{Z}$ y sea p un número primo, si $p|a$ y $p|(a^2 + b^2)$ demuestra que $p|b$.*

$a = pk_1$ $\quad a^2 + b^2 = pk_2$

$a^2 + b^2 = pk_2 \to b^2 = pk_2 - a^2$
$b^2 = pk_2 - (pk_1)^2 =$
$pk_2 - (pk_1)^2 - b^2$
$-(pk_1)^2 + pk_2 - b^2$
$(pk_1)^2 + pk_2 - b^2$
$k_2 = 2a \to$ (

Ejercicio 2.9 (Final junio 2017). *Sean $a, b \in \mathbb{N}$ tales que $mcd(2, a) = mcd(2, b) = 1$, entonces siempre sucede que*

- ☐ $2|(a + b)$
- ☐ $2 \nmid (a + b)$
- ☐ $2|(a + b + 1)$
- ☐ $2|(a \cdot b)$

Ejercicio 2.10 (Parcial febrero 2018). *Dadas las dos siguientes afirmaciones, donde $a \in \mathbb{Z}$:*

$6 \nmid a^2$

1. $6|a^2 \implies 6|a$ ✓
   $6|6^2$ $\quad 6|36$ ✓

NO

2. ~~$4|a^2 \implies 4|a$~~
   $4|6^2$ ✓ $\to$ $4|6$ ✗
   $4|4^2$ ✓ $\to$ $4|4$

Determina el enunciado correcto:

$a^2 = 6k \implies a = 6k$ $\qquad a^2 = 4k \implies a = 4k$

- ☐ *Ambas son ciertas.*
- ☐ *Ambas son falsas.*
- ☒ *Solamente es cierta la primera.*
- ☐ *Solamente es cierta la segunda.*

Ejercicio 2.11 (Parcial febrero 2018). *Sea p un número primo y sean $a, b \in \mathbb{Z}$ siendo $a, b \geq 2$. Demuestra que si $p|a^2$ y $p|b^3$, entonces $p|(a + b)$.*

Ejercicio 2.12 (Final junio 2018). *Sean a, b, d números enteros mayores que 0, si $mcd(a, b) = 1$, indica la respuesta correcta:*

- ☐ *Si $d|b$ entonces siempre $mcd(a, d) = 1$*
- ☐ *Si $d|b$ entonces siempre $mcd(a, d) = d$*
- ☐ *Si $d|(a \cdot b)$ entonces siempre $mcd(a, d) = d$*
- ☐ *Si $d|a$ entonces siempre $mcd(a, d) = 1$*

Ejercicio 2.13 (Final septiembre 2018). *Sean* $a, b, c \in \mathbb{Z}$ *tales que* $a|(b+c)$ *entonces siempre:*

- ☐ *Si* $a|b$ *entonces* $a|c$
- ☐ $a|(b \cdot c)$
- ☐ $a|mcd(b, c)$
- ☐ $a|c$ *y* $a|b$

Ejercicio 2.14 (Parcial enero 2019). *Si* a *y* b *son enteros positivos tales que* $3a - 5b = 27$ *entonces*

- ☐ *el* $mcd(a, b)$ *no puede ser* 27
- ☐ *el* $mcd(a, b)$ *no puede ser* 13
- ☐ *el* $mcd(a, b)$ *puede ser* 14
- ☐ *Ninguna de las afirmaciones anteriores es cierta*

Ejercicio 2.15 (Parcial enero 2019). *Sean* $a, b, c \in \mathbb{N}_1$. *Demuestra que*

$$c|a \ \wedge \ c|b \Longleftrightarrow c|mcd(a, b)$$

(Idea: en uno de los sentidos conviene usar el teorema de Bezout)

Ejercicio 2.16 (Final junio 2019). *Dado un número* a

- ☐ *Para cualquier número natural positivo* n *se cumple* $(a-1)|(a^n - 1)$
- ☐ $(a-1)|(a^n - 1)$ *sólo si* n *es primo*
- ☐ $(a+1) \nmid (a^2 - 1)$
- ☐ $(a-1)|(a^n - 1)$ *sólo si* $n = 2$