RESUMEN ALGEBRA 1

FINAL

NUMEROS ENTEROS (PARTE 1)

Capítulo 4

Enteros – Primera parte.

4.2 Divisibilidad.

Definición 4.2.1. (Divisibilidad.)

Sean $a, d \in \mathbb{Z}$ con $d \neq 0$. Se dice que d *divide* a a, y se nota $d \mid a$, si existe un elemento $k \in \mathbb{Z}$ tal que $a = k \cdot d$ (o sea si el cociente $\frac{a}{d}$ es un

$$d \mid a \iff \exists k \in \mathbb{Z} : a = k \cdot d.$$

El conjunto de los divisores positivos y negativos de un entero a se notará por $\operatorname{Div}(a)$ y el de los divisores positivos por $\operatorname{Div}_+(a)$.

Propiedades 4.2.2. (De la divisibilidad.)

Se concluye que $d \mid a \Leftrightarrow |d| \mid |a|$

- Ahora podemos probar fácilmente que los únicos números enteros que son inversibles son 1 y -1. Es claro que tanto 1 como -1 son

- $d \mid a$ y $a \mid d \Leftrightarrow a = \pm d$

Definición 4.2.3. (Números primos y compuestos.)

- Se dice que $a \in \mathbb{Z}$ es un número *primo* si $a \neq 0, \pm 1$ y tiene únicamente 4 divisores (o 2 divisores positivos). Por ejemplo $\pm 2, \pm 3, \pm 5, \pm 7, \pm 11$.

- Se dice que a es un número *compuesto* si $a \neq 0, \pm 1$ y tiene más que 4 divisores (o más que 2 divisores positivos). Por ejemplo $\pm 4, \pm 6, \pm 8, \pm 9$.

Propiedades 4.2.4. (De la divisibilidad.)

Sean $a, b, d \in \mathbb{Z}$, $d \neq 0$.

- $d \mid a$ y $d \mid b \Rightarrow d \mid a + b$.

- $d \mid a$ y $d \mid b \Rightarrow d \mid a - b$.
- $d \mid a + b$ no implica que $d \mid a$ y $d \mid b$:

- Sin embargo si $d \mid a + b$ y *se sabe que* $d \mid a$, entonces $d \mid b$.
  (Pues $d \mid (a + b) - a$.)
- $d \mid a \Rightarrow d \mid c \cdot a$, $\forall c \in \mathbb{Z}$.
- $d \mid a \Rightarrow d^2 \mid a^2$ y $d^n \mid a^n$, $\forall n \in \mathbb{N}$.
  (Pues si $a = k \cdot d$, entonces $a^2 = k^2 \cdot d^2$ y $a^n = k^n \cdot d^n$.)

- $d \mid a \cdot b$ no implica $d \mid a$ o $d \mid b$: Por ejemplo, $6 \mid 3 \cdot 4$ pero $6 \nmid 3$ y $6 \nmid 4$.

4.2.1 Congruencia.

Definición 4.2.5. (Congruencia.)

Sea $d \in \mathbb{Z}$, $d \neq 0$. Dados $a, b \in \mathbb{Z}$, se dice que a *es congruente a* b *módulo* d si $d \mid a - b$.

$$a \equiv b \pmod{d} \iff d \mid a - b.$$

Proposición 4.2.6. (La congruencia es una relación de equivalencia.)

Sea $d \in \mathbb{Z}$, $d \neq 0$. Sea $\mathcal{R}$ la relación en $\mathbb{Z}$ dada por

$$a \,\mathcal{R}\, b \iff a \equiv b \pmod{d}, \quad \forall\, a, b \in \mathbb{Z}.$$

Entonces $\mathcal{R}$ es una relación de equivalencia.

Demostración.

- *Reflexividad* : Para todo $a \in \mathbb{Z}$, $a \equiv a \pmod{d}$ pues $d \mid a - a$.
- *Simetría* : Hay que probar que para todo $a, b \in \mathbb{Z}$ tales que $a \equiv b \pmod{d}$, entonces $b \equiv a \pmod{d}$. Pero $a \equiv b \pmod{d}$ significa que $d \mid a - b$, y por lo tanto $d \mid -(a - b) = b - a$, luego $b \equiv a \pmod{d}$.
- *Transitividad* : Hay que probar que para todo $a, b, c \in \mathbb{Z}$ tales que $a \equiv b \pmod{d}$ y $b \equiv c \pmod{d}$ entonces $a \equiv c \pmod{d}$. Pero $a \equiv b \pmod{d}$ significa que $d \mid a - b$, y $b \equiv c \pmod{d}$ significa que $d \mid b - c$. Por lo tanto $d \mid (a - b) + (b - c) = a - c$, es decir $a \equiv c \pmod{d}$.

Proposición 4.2.7. (Propiedades de la congruencia.)

Sea $d \in \mathbb{Z}$, $d \neq 0$. Entonces :

2. *Para todo* $n \in \mathbb{N}$, $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{Z}$,

$$\left\{ \begin{array}{lcl} a_1 & \equiv & b_1 \pmod{d} \\ & \vdots & \\ a_n & \equiv & b_n \pmod{d} \end{array} \right. \implies a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n \pmod{d}.$$

3. $\forall\, a, b, c \in \mathbb{Z}$,

$$a \equiv b \pmod{d} \implies c\,a \equiv c\,b \pmod{d}.$$

5. *Para todo* $n \in \mathbb{N}$, $a_1, \dots, a_n, b_1, \dots, b_n \in \mathbb{Z}$,

$$\begin{cases} a_1 \equiv b_1 \pmod{d} \\ \quad \vdots \\ a_n \equiv b_n \pmod{d} \end{cases} \implies a_1 \cdots a_n \equiv b_1 \cdots b_n \pmod{d}.$$

6. $\forall\, a, b \in \mathbb{Z}$, $n \in \mathbb{N}$,

$$a \equiv b \pmod{d} \;\Rightarrow\; a^n \equiv b^n \pmod{d}.$$

4.3 Algoritmo de división.

Teorema 4.3.1. **(Algoritmo de división.)**

Dados $a,\, d \in \mathbb{Z}$ *con* $d \neq 0$, *existen* $k,\, r \in \mathbb{Z}$ *que satisfacen*

$$a = k \cdot d + r \quad \text{con} \quad 0 \leq r < |d|.$$

Además, k *y* r *son únicos en tales condiciones.*

Se dice que k es el *cociente* y r es el *resto* de la división de a por d (a es el *dividendo* y d el *divisor*). Al resto r lo notaremos $r_d(a)$ para especificar que es el "resto de a al dividir por d".

Observación 4.3.3. **(Divisibilidad y resto.)**

Sean $a,\, d \in \mathbb{Z}$, $d \neq 0$. Entonces

$$r_d(a) = 0 \iff d \mid a \iff a \equiv 0 \pmod{d}.$$

Esto observación se extiende inmediatamente:

Proposición 4.3.4. **(Congruencia y resto.)**

Sea $d \in \mathbb{Z}$, $d \neq 0$. *Entonces*

1. $a \equiv r_d(a) \pmod{d}$, $\forall\, a \in \mathbb{Z}$.
2. $a \equiv r \pmod{d}$ *con* $0 \leq r < |d| \;\Rightarrow\; r = r_d(a)$.
3. $r_1 \equiv r_2 \pmod{d}$ *con* $0 \leq r_1, r_2 < |d| \;\Rightarrow\; r_1 = r_2$.
4. $a \equiv b \pmod{d} \iff r_d(a) = r_d(b)$.

Corolario 4.3.5. **(Tablas de Restos.)**

Sean $a, b, d \in \mathbb{Z}$, $d \neq 0$. *Entonces*

- $r_d(a+b) = r_d\big(r_d(a) + r_d(b)\big)$.
- $r_d(a \cdot b) = r_d\big(r_d(a) \cdot r_d(b)\big)$.
- $r_d(a^n) = r_d\big(r_d(a)^n\big)$, $\forall\, n \in \mathbb{N}$.

Ejemplo: Probar que $\forall\, a \in \mathbb{Z}$ tal que $7 \nmid a$, $r_7(a^3) = 1$ o 6. Aplicando las tablas de restos, $r_7(a^3) = r_7\big(r_7(a)^3\big)$ y como $7 \nmid a \Leftrightarrow r_7(a) \neq 0$, alcanza con analizar la tabla

a	1	2	3	4	5	6
a^2	1	4	2	2	4	1
a^3	1	1	6	1	6	6

,

donde la primer fila indica los posibles restos de a módulo 7, la segunda fila los restos correspondientes de a^2 módulo 7 y la tercera fila los restos correspondientes de a^3 módulo 7. O sea por ejemplo si $a \equiv 3 \pmod{7}$, entonces $a^3 \equiv 6 \pmod{7}$, es decir si $r_7(a) = 3$, entonces $r_7(a^3) = 6$.

4.4 Sistemas de numeración.

Teorema 4.4.1. **(Desarrollo en base d.)**
Sea $d \in \mathbb{N}$ con $d \geq 2$. Todo número $a \in \mathbb{N}_0$ admite *un desarrollo en base d de la forma*

$$a = r_n \cdot d^n + r_{n-1} \cdot d^{n-1} + \cdots + r_1 \cdot d + r_0,$$

con $0 \leq r_i < d$ para $0 \leq i \leq n$ y $r_n \neq 0$ si $a \neq 0$.

Además dicho desarrollo, con las exigencias $0 \leq r_i < d$ impuestas para los símbolos, es único.

Se nota $a = (r_n \ldots r_0)_d$.

4.4.1 Criterios de divisibilidad.

Sea $a = \pm r_n r_{n-1} \cdots r_1 r_0$ el desarrollo decimal de a.

- Probemos el conocido criterio de divisibilidad por 3:

$$3 \mid a \iff 3 \mid r_n + r_{n-1} + \cdots + r_1 + r_0.$$

- Criterio de divisibilidad por 11:

$$11 \mid a \iff 11 \mid (-1)^n r_n + (-1)^{n-1} r_{n-1} + \cdots - r_1 + r_0.$$

4.5 Máximo común divisor.

Definición 4.5.1. (**Máximo común divisor**.)
Sean $a, b \in \mathbb{Z}$, no ambos nulos. El *máximo común divisor* entre a y b, que se nota $(a : b)$, es el mayor de los divisores comunes de a y b. Es decir:

$$(a:b) \mid a, \ (a:b) \mid b \ \text{ y si } \ d \mid a \text{ y } d \mid b, \text{ entonces } \ d \leq (a:b).$$

4.5.1 Algoritmo de Euclides.

En particular, para todo $k \in \mathbb{Z}$, $\quad (a:b) = (b : a - k \cdot b),$
y dados $a, b, c \in \mathbb{Z}$ con $b \neq 0$,

$$a \equiv c \pmod{b} \implies (a:b) = (b:c).$$

Aplicando esto a $a \equiv r_b(a) \pmod{b}$, se obtiene que $(a:b) = (b : r_b(a))$.

Teorema 4.5.3. **(Algoritmo de Euclides.)**
Sean $a, b \in \mathbb{Z}$ no nulos. Existe $\ell \in \mathbb{N}_0$ tal que en una sucesión finita de $\ell + 1$ divisiones se llega por primera vez al resto nulo $r_{\ell+1} = 0$. Entonces $(a:b) = r_\ell$, el último resto no nulo.

<u>Una aplicación no trivial del Algoritmo de Euclides:</u>

Sean $a \in \mathbb{N}$, $a \neq 1$, y $m, n \in \mathbb{N}$. Entonces

$$(a^m - 1 : a^n - 1) = a^{(m:n)} - 1.$$

Teorema 4.5.5. **(Mcd y combinación entera.)**

Sean $a, b \in \mathbb{Z}$, *no ambos nulos. Entonces existen* $s, t \in \mathbb{Z}$ *tales que*

$$(a : b) = s \cdot a + t \cdot b.$$

Observación 4.5.6. **(Combinaciones enteras de a y b.)**

Sean $a, b \in \mathbb{Z}$ no ambos nulos, y $c \in \mathbb{Z}$.

$$c = s' \cdot a + t' \cdot b \ \text{ para } \ s', t' \in \mathbb{Z} \quad \Longleftrightarrow \quad (a : b) \mid c.$$

Proposición 4.5.7. **(Mcd y divisores comunes.)**

Sean $a, b \in \mathbb{Z}$, *no ambos nulos y sea* $d \in \mathbb{Z}$, *con* $d \neq 0$. *Entonces*

$$d \mid a \ \text{ y } \ d \mid b \iff d \mid (a : b).$$

Proposición 4.5.8. **(Mcd de múltiplo común de dos números.)**

Sean $a, b \in \mathbb{Z}$, *no ambos nulos, y sea* $k \in \mathbb{Z}$ *con* $k \neq 0$. *Entonces*

$$(k\,a : k\,b) = |k| \cdot (a : b).$$

4.5.2 Números coprimos.

Definición 4.5.10. **(Números coprimos.)**

Se dice que $a, b \in \mathbb{Z}$ no ambos nulos son *coprimos* si y solo si $(a : b) = 1$, es decir si y solo si los únicos divisores comunes de a y b son ± 1.

$$a \perp b \iff (a : b) = 1$$

Observación 4.5.11. **(Coprimos y combinación entera.)**

Sean $a, b \in \mathbb{Z}$ no ambos nulos. Entonces

$$a \perp b \iff \exists\, s, t \in \mathbb{Z} \ : \ 1 = s\,a + t\,b.$$

Proposición 4.5.12. **(Propiedades esenciales de divisibilidad con coprimalidad.)**

Sean $a, b, c, d \in \mathbb{Z}$ *con* $c \neq 0$ *y* $d \neq 0$. *Entonces*

1. Sea $c \perp d$. Entonces $c \mid a,\ d \mid a \Leftrightarrow c\,d \mid a.$

2. Sea $d \perp a$. Entonces $d \mid a\,b \Leftrightarrow d \mid b.$

Proposición 4.5.13. **("Coprimizando")**

Sean $a, b \in \mathbb{Z}$, *no ambos nulos. Entonces*

$$\frac{a}{(a : b)} \perp \frac{b}{(a : b)}.$$

Por lo tanto

$$a = (a : b)\,a' \ \text{ y } \ b = (a : b)\,b'$$

donde los números enteros $a' = \dfrac{a}{(a : b)}$ *y* $b' = \dfrac{b}{(a : b)}$ *son coprimos.*

4.6 Primos y factorización.

Proposición 4.6.1. (Todo número entero $\neq 0, \pm 1$ es divisible por algún primo.)

Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$. *Entonces existe un número primo (positivo)* p *tal que* $p \mid a$.

4.6.1 La propiedad fundamental de los números primos.

Teorema 4.6.3. (Propiedad fundamental de los números primos.)

Sea p *un primo y sean* $a, b \in \mathbb{Z}$. *Entonces*

$$p \mid a \cdot b \implies p \mid a \quad o \quad p \mid b.$$

p es primo si y solo si cada vez que p divide a un producto divide a alguno de los factores.

Proposición 4.6.4. *Sea* p *un número primo y sean* $a_1, \dots, a_n \in \mathbb{Z}$, *con* $n \geq 2$. *Entonces*

$$p \mid a_1 \cdots a_n \implies p \mid a_i \text{ para algún } i,\ 1 \leq i \leq n.$$

En particular, dado $a \in \mathbb{Z}$, *si* $p \mid a^n$ *entonces* $p \mid a$.

4.6.2 El Teorema fundamental de la aritmética.

Teorema 4.6.5. (Teorema fundamental de la aritmética.)

Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$. *Entonces* a se escribe en forma única como producto de primos (positivos), *(o se factoriza en forma única como producto de primos (positivos),) es decir:*

- $\forall\, a \in \mathbb{Z}$, $a \neq 0, \pm 1$, *existe* $r \in \mathbb{N}$ *y* existen *primos positivos* $p_1, \dots, p_r$ *distintos y* $m_1, \dots, m_r \in \mathbb{N}$ *tales que*

$$a = \pm\, p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}.$$

- *Esta escritura es única salvo permutación de los primos.*

Proposición 4.6.7. (Divisores de un número y cantidad.)

Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$, *y sea* $a = \pm p_1^{m_1} \cdots p_r^{m_r}$ *la factorización en primos de* a. *Entonces*

1. $d \mid a \iff d = \pm p_1^{n_1} \cdots p_r^{n_r}$ *con* $0 \leq n_1 \leq m_1, \dots, 0 \leq n_r \leq m_r$.
2. $\#\mathrm{Div}_+(a) = (m_1+1)\cdots(m_r+1)$ *y* $\#\mathrm{Div}(a) = 2(m_1+1)\cdots(m_r+1)$.

Proposición 4.6.8. (Divisores y potencias.)

Sean $a, d \in \mathbb{Z}$ *con* $d \neq 0$, *y sea* $n \in \mathbb{N}$. *Entonces*

$$d \mid a \iff d^n \mid a^n.$$

Proposición 4.6.9. **(Máximo común divisor y factorización.)**
Sean $a, b \in \mathbb{Z}$ *no nulos de la forma*

$$a = \pm p_1^{m_1} \cdots p_r^{m_r} \quad con \quad m_1, \dots, m_r \in \mathbb{N}_0,$$
$$b = \pm p_1^{n_1} \cdots p_r^{n_r} \quad con \quad n_1, \dots, n_r \in \mathbb{N}_0.$$

Entonces

$$(a : b) = p_1^{\min\{m_1,n_1\}} \cdots p_r^{\min\{m_r,n_r\}}.$$

Corolario 4.6.10. **(Mcd de potencias.)**
Sean $a, b \in \mathbb{Z}$ *no nulos.*

1. *Sean* $a, b \neq 0, \pm 1$ *con factorización en primos* $a = \pm p_1^{m_1} \cdots p_r^{m_r}$, $m_1, \dots, m_r \in \mathbb{N}$, *y* $b = \pm q_1^{n_1} \cdots q_s^{n_s}$, $n_1, \dots, n_s \in \mathbb{N}$. *Entonces*

$$(a : b) = 1 \iff p_i \neq q_j, \ \forall\, i, j.$$

2. $(a : b) = 1$ *y* $(a : c) = 1 \iff (a : bc) = 1$.

3. $(a : b) = 1 \iff (a^m : b^n) = 1, \ \forall\, m, n \in \mathbb{N}$.

4. $(a^n : b^n) = (a : b)^n, \ \forall\, n \in \mathbb{N}$.

4.6.3 Mínimo común múltiplo.

Definición 4.6.11. **(Mínimo común múltiplo.)**
Sean $a, b \in \mathbb{Z}$, no nulos. El *mínimo común múltiplo* entre a y b, que se nota $[a : b]$, es el menor número natural que es un múltiplo común de a y b.

Proposición 4.6.12. **(Mínimo común múltiplo y factorización.)**
Sean $a, b \in \mathbb{Z}$ *no nulos de la forma*

$$a = \pm p_1^{m_1} \cdots p_r^{m_r} \quad con \quad m_1, \dots, m_r \in \mathbb{N}_0,$$
$$b = \pm p_1^{n_1} \cdots p_r^{n_r} \quad con \quad n_1, \dots, n_r \in \mathbb{N}_0.$$

Entonces

$$[a : b] = p_1^{\max\{m_1,n_1\}} \cdots p_r^{\max\{m_r,n_r\}}.$$

Corolario 4.6.13. **(Mcm y múltiplos comunes.)**
Sean $a, b \in \mathbb{Z}$, *no ambos nulos y sea* $m \in \mathbb{Z}$, *con* $m \neq 0$. *Entonces*

$$a \mid m \ \ y \ \ b \mid m \iff [a : b] \mid m.$$

Proposición 4.6.14. **(Producto mcd y mcm.)**
Sean $a, b \in \mathbb{Z}$, *no nulos, entonces* $|a \cdot b| = (a : b) \cdot [a : b]$.
En particular, si $a \perp b$, *entonces* $[a : b] = |a \cdot b|$.

EJERCICIOS DE FINAL:

27/7/22

1. Probar que para todo $n \in \mathbb{N}$,

$$(7.3^n - 5^{n+1} : 3^{n+1} + 7.5^n)$$

es igual a 2 o 4.