TEMA 4: NÚMEROS ENTEROS. DIVISIBILIDAD. NÚMEROS PRIMOS

TIEMPO: 98 — 101

Esquema

1) Introducción
2) Enteros
   - 2.1) Definición + dibujo
   - 2.2) Suma
     - 2.2.1) Propiedades
   - 2.3) Producto
     - 2.3.1) Propiedades
   - 2.4) Orden
     - 2.4.1) Propiedades
     - 2.4.2) Valor absoluto + Propiedades
3) Ideales
   - 3.1) Definición
   - 3.2) $(a) \in \mathbb{Z}$
   - 3.3) $\mathbb{Z}$ anillo principal
   - 3.4) Definiciones
     - 3.4.1) Subideal
     - 3.4.2) Suma
     - 3.4.3) Intersección
4) Divisibilidad
   - 4.1) Definición 1 + asociados
   - 4.2) Propiedades
   - 4.3) Definición 2
   - 4.4) m.c.d.
     - 4.4.1) Definición
     - 4.4.2) Teorema de Bezout
     - 4.4.3) Teorema de Euclides
   - 4.5) m.c.m
     - 4.5.1) Definición
     - 4.5.2) Algoritmo de Euclides
5) Primos
   - 5.1) Definición

5.2) I maximal $\longleftrightarrow$ I primo en $\mathbb{Z}$

5.3) Propiedades

5.4) Criba de Eratóstenes

5.5) Teorema Fundamental de la Aritmética

6) Congruencias

6.1) Definición 1 + Definición 2

6.2) Propiedades

6.3) Teorema

6.4) Teorema (congruencia de Fermat)

6.5) Restos potenciales

6.5.1) Criterios de divisibilidad

1) Introducción:

▷ Hablar un poco sobre los Naturales.

▷ Con los números naturales, ecuaciones del tipo $a + x = b$ no tienen solución salvo que $b \geq a$, como consecuencia de que ningún elemento, salvo el cero, es simetrizable para la operación "suma". Se trata de buscar otro conjunto donde podamos ampliar el número de soluciones de la clase de ecuación propuesta, de forma que $\mathbb{N}$ sea una parte estable del nuevo conjunto con la suma inducida y donde la estructura algebraica goce de la propiedad de simetría.

2) Enteros:

▷ En $\mathbb{N} \times \mathbb{N}$ definimos la relación binaria: $(a,b)R(c,d) \longleftrightarrow a+d=b+c$ que es, trivialmente, una relación de equivalencia (reflexiva, simétrica, y transitiva).

▷ **Definición**: llamamos conjunto de los Números Enteros ($\mathbb{Z}$) al conjunto $\frac{\mathbb{N} \times \mathbb{N}}{R}$

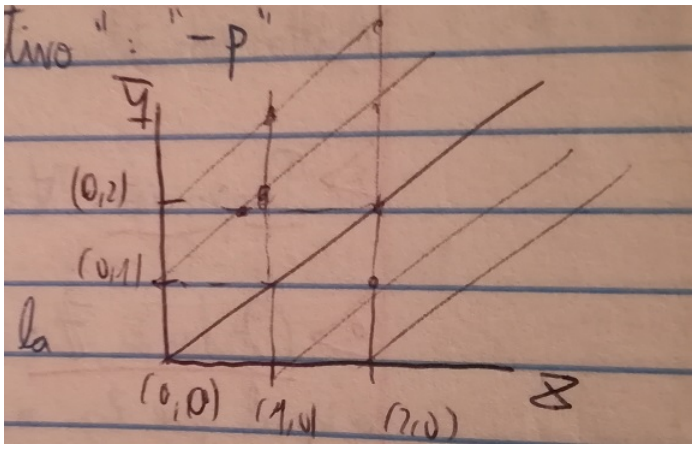
▷ Vamos a elegir los representantes canónicos de cada clase. Sea (a, b), tendremos:

a) $a > b \longrightarrow$ tomamos como representante (n,0) donde $a = n + b$ y lo llamaremos "positivo": $+n$

b) $a = b \longrightarrow$ tomamos como representante el (0,0) y lo llamaremos "cero": 0

c) $a < b \longrightarrow \exists p \in \mathbb{N}$ tal que $a + p = b \longrightarrow$ (0,p) y lo llamaremos "negativo": $-p$

Si consideramos la semirrecta diagonal del primer cuadrante cada clase de equivalencia estará formada por las parejas naturales que están sobre la misma semirrecta paralela a la citada. Los representantes canónicos son los puntos de origen de la semirrecta. Giramos el eje $\overline{OY}$ hasta prolongar el $\overline{OX}$ para obtener la representación usual como una recta.



▷ Suma o adición: $\forall x, y \in \mathbb{Z}$ siendo (a, b), (c, d) elementos de sus clases respectivas, definimos la suma de x e y como:

$$x + y = (a + c, b + d)$$

▷ Propiedades:

1) Asociativa: $\forall x, y, z \in \mathbb{Z}$, $(x + y) + z = x + (y + z)$

2) Elemento neutro: $\forall z \in \mathbb{Z}$, $\exists! e =$ "0"$\in \mathbb{Z} : e + z = z + e = z$

3) Elemento simétrico: $\forall z \in \mathbb{Z}$, $\exists! \hat{z}$ tq $z + \hat{z} = \hat{z} + z = 0$. Si $z = (a, b) \longleftrightarrow \hat{z} = (b, a)$

4) Conmutativa: $\forall x, y \in \mathbb{Z}$, $x + y = y + x$

▷ **Proposición**: $\forall x, y, z \in \mathbb{Z}$ si $x + z = y + z \Longrightarrow x = y$

▷ **Proposición**: la ecuación $a + x = b$, $\forall a,\, b \in \mathbb{Z}$, tiene solución en $\mathbb{Z}$

▷ Producto: $\forall x,\, y \in \mathbb{Z}$ siendo $(a,\, b)$ y $(c,\, d)$ elementos de sus clases respectivas, definimos el producto como:

$$x \cdot y = (a \cdot c + b \cdot d, a \cdot d + b \cdot c)$$

▷ Propiedades:

1) Asociativa: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
2) Elemento neutro: $\exists! e \in \mathbb{Z},\, e = \mathbf{1}$ tal que $\mathbf{1} \cdot z = z \cdot \mathbf{1} = z$, $\forall z \in \mathbb{Z}$
3) Conmutativa: $\forall x, y \in \mathbb{Z},\, x \cdot y = y \cdot x$
4) Distributiva: $\forall x,\, y,\, z \in \mathbb{Z}$: $x \cdot (y + z) = x \cdot y + x \cdot z$

▷ Por lo tanto, $(\mathbb{Z},\, +,\, \cdot)$ es un anillo conmutativo con unidad.

▷ **Proposición**: $\forall z \in \mathbb{Z},\, z \cdot 0 = 0 \cdot z = 0$

▷ **Proposición**: $(\mathbb{Z},\, +,\, \cdot)$ no tiene divisores de cero, luego es un Dominio de Integridad (= anillo conmutativo sin divisores de cero y con unidad).

▷ **Proposición**: $\forall x,\, y,\, z \in \mathbb{Z}^*$, si $x \cdot y = x \cdot z \longleftrightarrow x = y$

▷ Orden en $\mathbb{Z}$: $\forall x,\, y \in \mathbb{Z}$ siendo $(a,\, b)$, $(c,\, d)$ elementos de sus clases respectivas, decimos que x es menor o igual a y si:

$$x \leq y \text{ si } a + d \leq b + c \quad (\text{o } x \leq y \longleftrightarrow y - x \in \mathbb{Z}^+ \cup \{0\})$$

▷ **Proposición**: la relación "$\leq$" es una relación de orden y es de orden total.

▷ **Proposición**: el orden propuesto es compatible con la suma y el producto de enteros positivos.
Si $x \leq y$ y $z \leq w \longrightarrow x + z \leq y + w$
Si $k \in \mathbb{Z} \cup \{0\}$, $x \cdot k \leq y \cdot k$

▷ **Proposición**: $(\mathbb{Z},\, +,\, \cdot,\, \leq)$ no está bien ordenado. $(\mathbb{Z}^+,\, \leq)$ sí lo está pero $(\mathbb{Z}^-,\, \leq)$ no.

▷ Valor absoluto: llamamos valor absoluto de un número a la aplicación
$f : \mathbb{Z} \longmapsto \mathbb{N},\, z \longmapsto |z| = \{z \text{ si } z > 0,\, -z \text{ si } z < 0,\, 0 \text{ si } z = 0$

▷ Propiedades:

1) $|z| \geq 0$

2) $|z| = 0 \longleftrightarrow z = 0$

3) $z \leq |z|$

4) $-|z| \leq z$

5) $|z| \leq a \longleftrightarrow -a \leq z \leq a$

6) $\forall x,\, y \in \mathbb{Z},\, ||x| - |y|| \leq |x + y| \leq |x| + |y|$

7) $\forall x,\, y \in \mathbb{Z},\, |x \cdot y| = |x| \cdot |y|$

3) Ideales:

▷ **Definición**: sea A anillo conmutativo e $I \subset A$ subconjunto. Decimos que I es un ideal de A si:

a) I es un subgrupo del grupo aditivo de A

b) $\forall a \in A, \forall x \in I, a \cdot x \in I$

▷ El elemento neutro de la suma es un ideal de A llamado ideal cero. El anillo A es otro ideal. Si A posee unidad el ideal 1 es el propio A. Los ideales (0) y (A) se llaman impropios. Cualquier otro ideal se llama propio.

▷ **Definición**: $\forall a \in \mathbb{Z}$, llamamos conjunto de múltiplos de "a", al conjunto: $(a) = \{z \in \mathbb{Z} \text{ tq } z = a \cdot h, \text{ con } h \in \mathbb{Z}\}$

▷ **Proposición**: el conjunto (a) es un ideal de $\mathbb{Z}$

Proof. $\forall x, y \in (a)$, ¿$x - y \in (a)$?: $x = a \cdot h$, $y = a \cdot k \longrightarrow x - y = a(h - k) = a \cdot m \in (a)$
¿$\forall z \in \mathbb{Z}$, $\alpha \cdot x \in (a)$ con $x = a \cdot h$?: $\alpha \cdot x = a(h \cdot h) = a \cdot k \in (a)$

□

▷ **Definición**: al conjunto de ideales de $\mathbb{Z}$ lo llamaremos $\mathbb{I}(\mathbb{Z})$.

▷ **Definición**: diremos que un ideal es ideal principal si está generado por un solo elemento.

▷ **Definición**: un anillo se llamará principal si es conmutativo y todo ideal de A es principal.

▷ **Teorema**: $\mathbb{Z}$ es un anillo principal.

Proof. Sea $I \subset \mathbb{Z}$ ideal. Sean I^+ e I^- el conjunto de los números positivos y negativos de I. El conjunto I^+ tiene primer elemento por estar bien ordenado.
Sea $x = \text{mín}\{I^+\}$, $\forall \alpha \in I^+$, $\alpha > x \longrightarrow \alpha = x \cdot q + r$ con $r < x \Rightarrow r = \alpha - x \cdot q$, con $r \geq 0$.
Pero si $r > 0$ por ser $r < x$ y $r \in I^+$ tendríamos una contradicción con que x es el elemento mínimo $\longrightarrow r = 0 \longrightarrow \forall \alpha \in I^+$, $\alpha = q \cdot x \longrightarrow$ tomando $-\alpha = (-q) \cdot x$ tenemos que $I =< x >= (x)$. Por tanto, $I(\mathbb{Z}) = (x)$, $\forall x \in \mathbb{Z}$

□

▷ **Definición**: decimos que (a) es un subideal de (b), o que (b) es un superideal de (a), cuando (a) es un subconjunto de (b).

▷ La relación "ser subideal de" es una relación de orden en $I(\mathbb{Z})$. Es decir, $(I(\mathbb{Z}), \subset)$ es un conjunto ordenado donde si (a) es subideal de (b), $(a) \subset (b)$ como conjunto. Por ejemplo, (8) es un subideal de (4)

▷ **Definición**: $\forall (a), (b) \in I(\mathbb{Z})$ llamamos suma de (a) y (b) al siguiente ideal:
$(a) + (b) = \{z \in \mathbb{Z} \text{ tq } z = x + y \text{ con } x \in (a),\ y \in (b)\}$

▷ Propiedades:

1) Idempotencia: $(a) + (a) = (a)$

2) Asociativa: $[(a) + (b)] + (c) = (a) + [(b) + (c)]$

3) Conmutativa: $(a) + (b) = (b) + (a)$

▷ **Definición**: llamamos intersección de (a) y (b) al siguiente ideal:
$(a) \cap (b) = \{z \in \mathbb{Z} \text{ tq } z \in (a) \text{ y } z \in (b)\}$

▷ Propiedades: las mismas que la suma.

▷ *Nota*: $(a) + (b) = (d) \in I(\mathbb{Z})$, $(a) \cap (b) = (m) \in I(\mathbb{Z})$

▷ **Teorema**: $\forall (a), (b) \in I(\mathbb{Z})$ tenemos que: Sup$((a), (b))$=$(a)+(b) = (d)$, Ínf$((a),(b))$=$(a) \cap (b) = (m)$

Proof. $(a) = \{z \in \mathbb{Z} \text{ tq } z = x + 0 \text{ tq } x \in (a),\ 0 \in (b)\}$ y $(b) = \{z \in \mathbb{Z} \text{ tq } z = 0 + y \text{ tq } 0 \in (a),\ y \in (b)\}$, luego (a) y (b) son subideales de (d).
Supongamos $(\hat{d})$ tal que $(a), (b) \subset (\hat{d}) \longrightarrow (a), (b) \subset (\hat{d})$ y, por lo tanto, $(a)+(b) = (d) \subset (\hat{d}) \longrightarrow (d)$ es el menor que los contiene.
Se demuestra análogamente para la intersección.

□

▷ **Corolario**: vimos que el par $(I(\mathbb{Z}), \subset)$ era un conjunto ordenado y a cada par de ideales les hemos asociado un extremos superior y un extremo inferior. Por tanto, $(I(\mathbb{Z}), \subset)$ es un retículo.

4) Divisibilidad:

▷ **Definición**: $\forall a,\, b \in \mathbb{Z}$ decimos que "a" divide a "b" cuando $\exists c \in \mathbb{Z}$ tq $a \cdot c = b$. Lo notamos por $a|b$.

▷ Esta relación de divisibilidad es de preorden, pues cumple reflexiva y transitiva pero no antisimétrica. Para que cumpla esta última tendremos que tomar números asociados.

▷ **Definición**: sea $U = \{-1,\, +1\}$. Decimos que $a,\, b \in \mathbb{Z}$ son asociados si $a = u \cdot b$ para cierta $u \in U$

▷ **Definición**: la relación "$\hat{a}$" divide a "$\hat{b}$" cuando hablamos con números asociados es de orden y la notamos por: $\hat{a}|\hat{b} \longleftrightarrow \exists c \in \mathbb{Z}$ tq $\hat{a} \cdot c = \hat{b}$ donde $\in \mathbb{Z}/$asociados.

▷ *Nota*: a partir de ahora se sobreentiende la relación de divisibilidad y por ello escribimos $a|b$ nada más.

▷ Propiedades:

1) Si $a|b$ y $a|c \longrightarrow a|(b+c)$ y $a|(b-c)$
2) Si $a|b \longrightarrow a|(b \cdot k)$, $\forall k \in \mathbb{Z}$
3) Si $a|b \longrightarrow a|b^n$, $\forall n \in \mathbb{N}^*$
4) Si $a|b \longrightarrow a|\ |b|$
5) Si $a|b \longrightarrow |a|\ |\ |b|$
6) Si $a|b \longrightarrow b = 0$ o $|a| \leq |b|$
7) $\forall a \in \mathbb{Z}$, $a|0$
8) Si $u \in U$, $u|b$, $\forall b \in \mathbb{Z}$

▷ **Definición**: $\forall a,\, b \in \mathbb{Z}$ decimos que "a" divide a "b" cuando $(b) \subset (a)$.

▷ **Proposición**: ambas definiciones son equivalentes.

Proof. Si $a|b \longrightarrow \exists c \in \mathbb{Z}$ tq $a \cdot c = b \longrightarrow (b) \subset (a)$ por ser $\mathbb{Z}$ anillo principal.
Si $a|b \longrightarrow (b) \subset (a)$, luego $b \in (a)$ y como $\mathbb{Z}$ es anillo principal, $\exists c \in \mathbb{Z}$ tq $a \cdot c = b$

□

▷ Con la definición a través de ideales todas las propiedades anteriores son demostradas automáticamente sin esfuerzo, algo que no es obvio si usamos asociados. Para hablar del m.c.d. y del m.c.m. usaremos ideales pues nos dan demostraciones más elegantes que si usamos la otra definición.

▷ **Definición**: llamaremos ideal m.c.d. de "a" y "b" al ideal suma: $(d) = (a) + (b)$.

▷ **Definición**: llamaremos m.c.d. de "a" y "b" (y lo notamos por m.c.d.(a, b)) a la base positiva de: $(d) = (a) + (b)$.

▷ **Proposición**: sea d =m.c.d.(a, b). Entonces todo divisor de "a" y de "b" es divisor de "d".

Proof. $\hat{d}|a \longleftrightarrow (a) \subset (\hat{d})$, $\hat{d}|b \longleftrightarrow (b) \subset (\hat{d}) \longrightarrow (a) + (b) = (d) \subset (\hat{d}) \longleftrightarrow \hat{d}|d$

□

▷ **Corolario**:"d" es el mayor de divisores comunes de "a" y "b". Además, si $a|b \leftrightarrow$ m.c.d.$(a, b)= a$

▷ **Teorema de Bezout**: si d =m.c.d.$(a, b) \longrightarrow \exists \lambda, \mu \in \mathbb{Z}$ tq $d = \lambda \cdot a + \mu \cdot b$

Proof. $\forall x \in (a) \longleftrightarrow \exists \lambda \in \mathbb{Z}$ tq $\lambda \cdot a = x$
$\forall y \in (b) \longleftrightarrow \exists \mu \in \mathbb{Z}$ tq $\mu \cdot b = y$
Si d =m.c.d.$(a, b) \longrightarrow (a)+(b) = (d) \longrightarrow x+y = d$ para ciertos $x \in (a)$ e $y \in (b)$. Luego, $d = \lambda \cdot a + \mu \cdot b$

□

▷ **Definición**: decimos que dos números son primos entre sí si m.c.d.(a, b)=1

▷ Propiedades:

1) Si m.c.d.$(a, b)= d \longrightarrow$ m.c.d.$(a/d, b/d)$=1, es decir, a/d y b/d son primos entre sí.
2) Si m.c.d.(a, b)=1,$\exists \lambda, \mu \in \mathbb{Z}$ tq $\lambda \cdot a + \mu \cdot b = 1$
3) Si m.c.d.$(a, b)= d \longrightarrow$ m.c.d.$(a \cdot c, b \cdot c)= d \cdot c$
4) Si m.c.d.$(a, b)= d$ y además $c|a$ y $c|d \longrightarrow$ m.c.d.$(a/c, b/c)= d/c$

▷ **Teorema de Euclides**: si $a|b \cdot c$ y m.c.d.("a", "b")=1$\longrightarrow a|c$

Proof. Por el Teorema de Bezout, $\exists \lambda, \mu \in \mathbb{Z}$ tq $\lambda \cdot a + \mu \cdot b = 1 \longrightarrow \lambda c \cdot a + \mu c \cdot b = c$.
Como $a|\lambda ca$ y $a|\mu bc$ por hipótesis $\longrightarrow a|(\lambda a + \mu b) \cdot c \longrightarrow a|c$

□

▷ **Definición**: llamamos ideal mínimo común múltiplo de "a" y "b" al ideal intersección: $(m) = (a) \cap (b)$

▷ **Definición**: llamamos mínimo común múltiplo de "a" y "b" (y lo notamos por m.c.m.(a, b)) a al base positiva de: $(m) = (a) \cap (b)$.

▷ **Proposición**: sea $\hat{m}$ otro múltiplo de "a" y "b". Entonces $m|\hat{m}$.

Proof. Como $a|\hat{m}$, $b|\hat{m} \longrightarrow (\hat{m}) \subset (a)$, $(b) \longrightarrow (a) \cap (b) = (m) \supset (\hat{m}) \longleftrightarrow m|\hat{m}$

□

▷ **Corolario**: El número m=m.c.m.(a, b) es el menor múltiplo de "a" y "b".
Además, si $a|b \longleftrightarrow$ m.c.m.$(a, b)= b$

▷ **Definición**: dados $a, b \in \mathbb{Z}$ decimos que son primos entre sí cuando m.c.m.$(a, b)= a \cdot b$

▷ Algoritmo de Euclides: este algoritmo nos permite hallar el m.c.d. de dos números a partir de divisiones sucesivas. El teorema nos dice que si al considerar la división entera de dos números enteros $a > b$ nos da resto "r", entonces: m.c.d.(a, b)=m.c.d.(b, r).

Proof. $a = b \cdot q + r \longrightarrow r = a - b \cdot q \longrightarrow$ si $d|a \longrightarrow d|r \longrightarrow$ m.c.d.(a, b)=m.c.d.(b, r)

□

▷ Al proceso de divisiones sucesivas lo llamamos Algoritmo de Euclides.
m.c.d.(a, b)=m.c.d.(b, r_1)=m.c.d.$(r_1, r_2)= \ldots =$m.c.d.$(r_n, 0)=r_n$

▷ **Teorema**: sean $a, b \in \mathbb{Z}$. Entonces $a \cdot b =$m.c.d.$(a, b) \cdot$ m.c.m.$(a, b)=d \cdot m$

▷ **Corolario**: m.c.m.$(a, b)= m \longrightarrow$ m.c.d.$(m/a, m/b)$=1.
Además, m.c.d.$(a, b)= 1 \longleftrightarrow$ m.c.m.$(a, b)= a \cdot b$.
Lo anterior nos prueba que las dos definiciones de primos entre sí son equivalentes.

5) Primos:

▷ **Definición**: sin considerar los números 0, 1 y -1, decimos que $p \in \mathbb{Z}$ es primo si es divisible sólo por las unidades, él y su opuesto. Es decir, $Div(p) = \{1, -1, p, -p\}$.

▷ **Definición**: un número $z \in \mathbb{Z}$ es compuesto cuando, siendo distinto de 0, 1 y -1, no es primo.

▷ **Definición**: un ideal $I \in I(\mathbb{Z})$ es maximal cuando $\nexists J \in I(\mathbb{Z})$ con $I \subsetneq J \subsetneq \mathbb{Z}$

▷ **Teorema**: en $\mathbb{Z}^*$ un ideal I es primo $\longleftrightarrow$ es maximal.

Proof. $\Longrightarrow$: sea $I \in I(\mathbb{Z})$. Si $\mathbb{I}$ no es maximal $\longrightarrow \exists J$ tal que $I \subsetneq J \subsetneq \mathbb{Z}$.
Como $I =< p >$ y $J =< a >$ entonces $< p > \subset < a > \longleftrightarrow a|p \Longrightarrow p$ no es primo.
$\Longleftarrow$: Si $< p >= I$ no es primo, $\exists b \in \mathbb{Z}$ tq $b|p \longrightarrow < p > \subsetneq < b >= J \in I(\mathbb{Z}) \Longrightarrow I$ no es maximal.

□

▷ *Nota*: si no consideramos el ideal $< 0 >$, tenemos una biyección entre (P) ideal primo y (M) ideal maximal.

▷ Propiedades:

1) Si p es primo y $p \nmid a \longrightarrow$ m.c.d.$(p, a) = 1 \longleftrightarrow$ "a" y "p" son primos entre sí.
2) Si $p, q\mathbb{Z}$ son primos y $p|q \longrightarrow p$ y q son asociados.
3) Si $p|a \cdot b \longrightarrow p|a$ o $p|b$
4) El conjunto de los primos es infinito.

   Proof. $p_1, \ldots, p_n \longleftarrow A = p_1 \cdot \ldots p_n + 1 \longrightarrow p_j \nmid A$, $\forall j \longrightarrow A$ es primo y no estaba en la lista.

□

▷ Criba de Eratóstenes: sea $n \in \mathbb{N}$, escribimos $\{2, 3, \ldots, n-1\}$. Tachamos los múltiplos de 2, después los de 3,... y así hasta obtener todos los primos menores que ese número.

▷ **Definición**: sea $p \in \mathbb{Z}$. Llamaremos números primarios a las potencias de p, p^n (con $n \in \mathbb{N}^*$). Estos números serán la base de los ideales primarios de $\mathbb{Z}$.

▷ Se trata de ver que todo número compuesto admite una descomposición en factores primos únicos salvo el signo. En ideales significará que todo ideal propio de $\mathbb{Z}$ admite una descomposición primaria como intersección finita de ideales primarios. Por ejemplo:
Si $24 = 2^3 \cdot 3 \longrightarrow < 24 >= < 2^3 > \cap < 3 >$

▷ **Teorema**: el menor divisor (salvo unidades) de un número compuesto es un número primo.

Proof. Sea $a \in \mathbb{Z}$ y p su menor divisor. Si p no es primo, $\exists q < p$ tq $q|p \longrightarrow q|a \longrightarrow$ contradicción.

□

▷ **Teorema Fundamental de la Aritmética**:

a) Todo número compuesto se puede descomponer como producto de números primos.

b) La descomposición es única salvo el signo de los factores (única si consideramos asociados).

Proof. Existencia:
Sea $a \in \mathbb{Z}$ compuesto $\longrightarrow$ su menor divisor es un número primo $\longrightarrow a = p_1 \cdot x_1$.
Si x_1 es primo ya hemos terminado. Si no, $\exists p_2|x_1$ primo $\longrightarrow a = p_1 \cdot p_2 \cdot x_2$
Repetimos el proceso y como $a < \infty$ terminamos en algún momento: $a = p_1 \cdot p_2 \cdots p_n$ con p_j primo.
Unicidad:
Sean $a = p_1 \cdots p_n$ y $a = q_1 \cdots q_m$ dos descomposiciones distintas.
Tenemos que $p_1|a$ y $p_1|q_j$ para cierto índice j. Reordenamos para obtener que $q_j = q_1$ y tenemos que: $p_1(p_2 \cdots p_n) = q_1(q_2 \cdots q_m)$. Entonces se ha de tener que $p_1 = u_1 \cdot q_1$ con $u_1 \in \{1, -1\} \longrightarrow p_2 \cdots p_n = u_1 \cdot q_2 \cdots q_m$
Repetimos el proceso hasta obtener (supongamos $n < m$): $1 = u_1 \cdots u_n \cdot q_{n+1} \cdots q_m \longrightarrow q_{n+1} \cdots q_m$ es una unidad $\longrightarrow n = m$ y, además, $p_j = u_j \cdot q_j$

□

▷ *Nota*: si consideramos asociados, el teorema nos muestra la unicidad de la descomposición pues $p_j = u_j \cdot q_j$. Es por ello que se habla de primos y factores en $\mathbb{N}$.

1) Pueden aparecer primos repetidos: $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, $\alpha_j \geq 1$

2) Todo número compuesto tiene descomposición única como producto de números primarios.

3) Todo ideal propio de $\mathbb{Z}$ se puede expresar como intersección finita de ideales primarios: $< a >=< p_1^{\alpha_1} > \cap \ldots \cap < p_n^{\alpha_n} >$

4) $a|b \longleftrightarrow$ "b" tiene todos los factores primos de "a" con exponentes iguales o mayores.

5) Sea $a \in \mathbb{N}$, $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$. Entonces, cualquier divisor de "a" es de la forma $d = p_1^{k_1} \cdots p_n^{k_n}$ con $0 \leq k_j \leq \alpha_j$

6) Sea $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, entonces la suma de sus divisores es: $S = \dfrac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \dfrac{p_n^{\alpha_n+1} - 1}{p_n - 1}$

7) El número de divisores es: $|Div(a)| = (\alpha_1 + 1) \cdots (\alpha_n + 1)$

8) El producto de sus divisores, $\{d_1, \ldots, d_k\}$, es: $P = \sqrt{a^k}$

6) Congruencias:

▷ **Definición**: dados $a, b \in \mathbb{Z}$, diremos que son congruentes módulo "m" si $m \in \mathbb{Z} - \{0\}$ y $m|(a-b)$. Lo notaremos por $x \equiv_m y$ o $x \equiv y \bmod m$ o $x \equiv y\ (m)$.

▷ **Definición**: dados $x, y \in \mathbb{Z}$ diremos que $x \equiv_m y$ si $m \in \mathbb{Z} - \{0\}$ y al dividir "x" e "y" entre m nos da el mismo resto.

▷ **Proposición**: ambas definiciones son equivalentes.

Proof. 1) $\to$ 2): Si $m|(x-y) \longrightarrow \exists q \in \mathbb{Z}$ tal que $m \cdot q = x - y$. Sea $y = m \cdot \alpha + r$ con $0 \leq r < m$, entonces:
$x = m \cdot q + y = m \cdot q + m \cdot \alpha + r = m(q + \alpha) + r \longrightarrow$ Ambos tienen el mismo resto $\longleftrightarrow x \equiv_m y$
2) $\to$ 1): $x = m \cdot q + r$; $y = m \cdot p + r \longrightarrow x - y = m(q-p) \longrightarrow m|(x-y) \longleftrightarrow x \equiv_m y$

□

▷ **Proposición**: la relación de congruencia módulo "m" es una relación de equivalencia.

▷ Dos enteros pertenecerán a la misma clase si al dividirlas por "m" nos da igual resto. Las llamaremos "clases congruentes módulo "m"" y las notaremos por $\overline{x} = x + (m)$ y el conjunto cociente será $\mathbb{Z}/(m) = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$. Es decir, tendremos tantas clases como restos distintos se pueden obtener al dividir entre "m". Por ello también se llaman "conjunto de las clases de resto módulo "m"".

▷ Propiedades:

1) Si $x \equiv_m y$ y $\hat{x} \equiv_m \hat{y} \longrightarrow x + \hat{x} \equiv_m y + \hat{y}$
2) Si $x \equiv_m y$ y $\hat{x} \equiv_m \hat{y} \longrightarrow x \cdot \hat{x} \equiv_m y \cdot \hat{y}$
3) $\overline{x} + \overline{y} = \overline{x + y}$
4) $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$

▷ **Teorema**: Sean $2 \leq m \in \mathbb{N}$. Entonces equivalen:

a) $\mathbb{Z}/(m)$ es un Dominio de Integridad
b) $\mathbb{Z}/(m)$ es un cuerpo
c) m es primo.

▷ Propiedades:

1) Si $a + b \equiv_m \hat{a} + b \longrightarrow a \equiv_m \hat{a}$
2) Si $a \cdot b \equiv_m \hat{a} \cdot b \not\Rightarrow a \equiv_m \hat{a}$. Sólo si m.c.d.$(m,b)$=1
3) $c \cdot x \equiv_m c \cdot y \longleftrightarrow x \equiv y\ (m/\text{m.c.d.}(m,c))$
4) Si $x \equiv y\ (m_1, \ldots, m_k) \longleftrightarrow x \equiv y\ (\text{m.c.m.}(m_1, \ldots, m_k))$

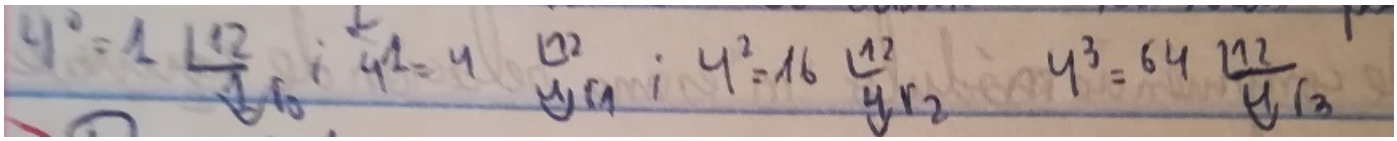
▷ **Definición**: dados $a_1, \ldots, a_m \in \mathbb{Z}$, decimos que forman un sistema completo de números congruentes módulo "m" si los restos al dividirlos por "m" son todos distintos.

▷ **Definición**: dados $a_1, \ldots, a_k \in \mathbb{Z}$ y $k < m \in \mathbb{Z}$, decimos que forman un sistema de números incongruentes módulo "m" si los restos al dividirlos entre "m" son todos distintos.

▷ **Teorema (congruencia de Fermat)**: sea $p \in \mathbb{Z}$ primo y sea $n \in \mathbb{Z}$ con m.c.d.(n,p)=1. Entonces, se verifica:

$$n^{p-1} \equiv 1 \bmod p$$

▷ **Definición**: sea $a \in \mathbb{N} - \{0\}$. Llamamos restos potenciales de "a" módulo "m" a los diferentes restos que obtenemos al dividir sucesivas potencias de "a" por "m".



▷ Propiedades:

1) $r_0 = 1$
2) Sea r_k el resto potencial de a^k entre "m", $a^k \equiv r_k \longrightarrow a^{k+1} \equiv_m a \cdot r_k$, con lo que tenemos la regla: multiplicamos el resto anterior a uno dado por "a" y dividimos por "m" para obtener el siguiente resto potencial.
3) El número de restos potenciales es finito ($\leq m$).
4) Si algún resto potencial es cero, lo son todos los siguientes.
5) A partir del primer resto que se repita, los siguientes se reproducen en el mismo orden.
6) Si $a = m + b$ con $b < a$, los restos potenciales de $a(m)$ son los mismos que los de $b(m)$

▷ Criterios de divisibilidad: sean "b" una base numérica, $A = \alpha_0 + \alpha_1 \cdot b^1 + \ldots + \alpha_n \cdot b^n$. Sean $a_1, \ldots, a_n$ los restos potenciales de "b" módulo "m":

$$A = \alpha_0 + \alpha_1 \cdot a_1 + \ldots + \alpha_n \cdot a_n \bmod m$$

De donde obtenemos que la condición necesaria y suficiente para que un número A sea divisible por "m" es que lo sea el número: $\alpha_0 + \alpha_1 \cdot a_1 + \ldots + \alpha_n \cdot a_n$

▷ Sea $b = 10$, entonces:

1) A es divisible por $2 \longleftrightarrow \alpha_0$ lo es.

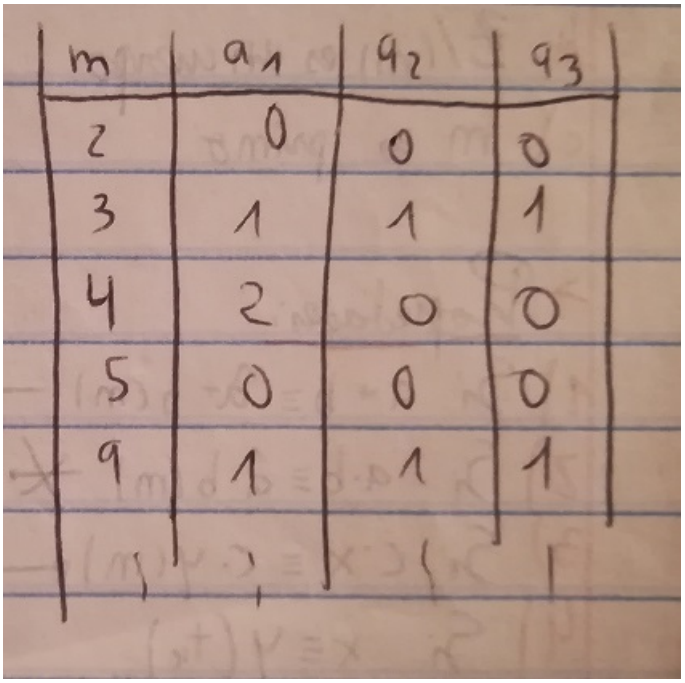
2) A es divisible por $3 \longleftrightarrow \alpha_0 + \ldots \alpha_n$ lo es.

3) A es divisible por $4 \longleftrightarrow \alpha_0 + 2\alpha_1$ lo es.

4) A es divisible por $5 \longleftrightarrow \alpha_0$ lo es.

5) A es divisible por $9 \longleftrightarrow \alpha_0 + \ldots + \alpha_n$ lo es.

6) Etcétera



m	a_1	a_2	a_3
2	0	0	0
3	1	1	1
4	2	0	0
5	0	0	0
9	1	1	1