DIVISION ENTERA. DIVISIBILIDAD

- Def.
  Sean $a, b \in \mathbb{Z}$. Decimos b divide a, b es un factor de a o a es un múltiplo de b si existe un entero c tal que $a = b \cdot c$. Escribimos $b \mid a$

  Si $b \neq 0$ y c existe, es único y decimos que es el cociente de a dividido por b.

- División entera.

  Teorema Sean $a, b \in \mathbb{Z}$, $b > 0$. Existen c, r unívocamente determinados tal que $a = bc + r$ y $0 \leq |r| < b$.

  $a \equiv$ dividendo. $c \equiv$ cociente.

  $b \equiv$ divisor. $r \equiv$ resto.

  Dem.

  - $a \geq 0 \quad 0 \leq r < b$
    1. Unicidad de cociente y resto.
       Sea $a = bc_1 + r_1 \quad 0 \leq r_1 < b$
       $a = bc_2 + r_2 \quad 0 \leq r_2 < b$
       Supongamos $c_2 < c_1 \implies c_1 - c_2 \geq 1$. Luego

       $$r_2 = a - bc_2 = bc_1 + r_1 - bc_2 = b(c_1 - c_2) + r_1 \underset{(c_1 - c_2 \geq 1)}{\underset{\uparrow}{\geq}} b + r_1 \underset{(0 \leq r_1)}{\underset{\uparrow}{\geq}} b$$

       Por tanto $r_2 \geq b$ que contradice $r_2 < b$.
       Análogamente si $c_2 > c_1$
       Luego $c_1 = c_2$ y $r_1 = a - bc_1 = a - bc_2 = r_2$
    2. Existencia de cociente y resto.
       Lo demostramos por inducción completa sobre el valor de a.
       Dado $b \in \mathbb{Z} \quad b > 0$
       Base $a \in \mathbb{Z} \quad a \leq b$ (como b es un número natural sólo hay un número finito de $a \leq b$)
       Caso 1: $a < b \quad a = 0 \cdot b + a$
       Caso 2: $a = b \quad a = 1 \cdot b + 0$
       Paso Inductivo
       $a > b$
       Hipótesis Inducción
       $\forall 0 \leq k < a$ existen c', r' únicos tales que $k = b \cdot c' + r'$ con $r' < b$

       Lo demostramos para a:

       $$\left.\begin{array}{l} a > b \\ b > 0 \end{array}\right\} \implies a > a - b \geq 0$$

$$\text{Luego} \quad a - b = b \cdot c' + r' \quad 0 \le r' < b$$

$$a = b \cdot c' + b + r' = b(c' + 1) + r'$$

- $a < 0$
  En este caso consideramos $a' = -a$ y aplicamos el resultado anterior:
  $-a = b \cdot c' + r' \quad 0 \le r' < b \implies a = -(b \cdot c' + r') \implies a = b(-c') + (-r')$
  Luego $c = -c' \quad r = -r' \implies |r| = |-r'| = r'$ ya que $0 \le r' < b \implies 0 \le |r| < b$

Ej.
$-17 = 5 \cdot (-3) + (-2) \quad 0 \le |-2| = 2 < 5$

También podemos escribir $-17 = 5 \cdot (-4) + 3 \quad 3 < 5$. En este caso el resto es positivo. $r > 0$. Esto da lugar al corolario siguiente:

- Corolario
  Sean $a, b \in \mathbb{Z},\ b > 0$. Existen c, r unívocamente determinados tal que $a = bc + r$ y $0 \le r < b$.

  Dem.

  - $a \ge 0$ (Primera parte del teorema)
  - $a < 0$
    Por el segundo caso del teorema $a = bc' + r' \qquad c' < 0 \quad r' \le 0$
    Si $r' = 0$ ya está.
    Si $r' < 0$ como también $|r'| < b \implies 0 \le b + r' < b$
    Luego $a + b = bc' + r' + b \implies a = b(c' - 1) + (r' + b)$ como queríamos demostrar.

  También utilizaremos la siguiente notación:

  $c = a \ div \ b$

  $r = a \ mod \ b$

- Máximo Común Divisor
  Def.
  Si a y $b \in \mathbb{Z},\ b \ne 0$ decimos que $d > 0$ es el máximo común divisor de a y b sii:

  1. $d \mid a \quad d \mid b$
  2. si $c \mid a$ y $c \mid b \implies c \mid d$

Vamos a demostrar que si existe el mcd de dos números, es único.

Si $d = mcd(a,b)$ y $d' = mcd(a,b)$ ambos verifican estas condiciones 1) y 2).

Tomamos d como el $mcd(a,b)$. Como $d' \mid a$ y $d' \mid b$ porque también verifica 1) $Longrightarrow$ $d' \mid d$ por 2).

Tomamos d' como el $mcd(a,b)$. Como $d \mid a$ y $d \mid b$ porque también verifica 1) $Longrightarrow$ $d \mid d'$ por 2).

Se verifica $d \mid d'$ y $d' \mid d$ pero como tienen que ser positivos $d = d'$. Por tanto, si existe un $d > 0$ que cumpla 1) y 2), es único.

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

Nota.
$mcd(0,b) = mcd(b,0) = |b|$

$mcd(0,0)$ no tiene sentido ya que todo natural positivo divide al 0.

- Algoritmo de Euclides.

  Es un método para calcular el mcd de dos enteros a, b.

  Podemos suponer $a \geq b > 0$ pues $mcd(a,b) = mcd(|a|,|b|)$.

- Lema

  Dados $a \geq b > 0$, $a = bc + r$ $0 \leq r < b$, entonces $mcd(a,b) = mcd(b,r)$.

  Dem.
  Sea $d = mcd(a,b)$ y $d' = mcd(b,r)$ como $d' \mid b$ y $d' \mid r \implies$
  $b = d' \cdot t_1 \quad r = d' \cdot t_2$
  $a = b \cdot c + r \implies a = (d' \cdot t_1) \cdot c + d' \cdot t_2 = d'(t_1 \cdot c + t_2) \implies d' \mid a$

  Se tiene $d' \mid a \quad d' \mid b \implies d' \mid d$

  Como $d = mcd(a,b)$, se tiene $d \mid a \quad d \mid b \implies$
  $a = d \cdot t'_1 \quad b = d \cdot t'_2$
  $a = b \cdot c + r \implies d \cdot t'_1 = (d \cdot t'_2) \cdot c + r \implies r = d(t'_1 - t'_2 \cdot c) \implies d \mid r$
  $d \mid r$ junto con $d \mid b \implies d \mid d'$

  Luego $d \mid d' \quad d' \mid d \implies d = d'$

- Teorema

  Dados enteros $a > b \geq 0$, existe el $mcd(a,b)$.

  Dem.
  Por inducción sobre b.

  Base $b = 0$ $mcd(a,b) = mcd(a,0) = a$.

  Paso Inductivo

(HI) $\equiv$ Si $b > 0$, para todo a', b' tal que $a' > b' \geq 0$ y $b' < b$ existe el $mcd(a', b')$.

Por el Lema, si $a = bc + r \quad 0 \leq r < b \quad mcd(a,b) = mcd(b,r)$ y como $r < b$ entonces $mcd(b,r)$ existe.

- Ej.
Calcula el $mcd(2406, 654)$

  $2406 = 654 \cdot 3 + 444 \implies mcd(2406, 654) = mcd(654, 444)$
  $654 = 444 \cdot 1 + 210 \implies mcd(654, 444) = mcd(444, 210)$
  $444 = 210 \cdot 2 + 24 \implies mcd(444, 210) = mcd(210, 24)$
  $210 = 24 \cdot 8 + 18 \implies mcd(210, 24) = mcd(24, 18)$
  $24 = 18 \cdot 1 + 6 \implies mcd(24, 18) = mcd(18, 6)$
  $18 = 6 \cdot 3 + 0 \implies mcd(18, 6) = mcd(6, 0) = 6$

  En general, para calcular el $mcd(a,b)$ $(a, b \geq 0)$ definimos q_i y r_i recursivamente mediante las ecuaciones

  $a = bq_1 + r_1 \quad 0 \leq r_1 < b$

  $b = r_1 q_2 + r_2 \quad 0 \leq r_2 < r_1$

  $r_1 = r_2 q_3 + r_3 \quad 0 \leq r_3 < r_2$

  $\vdots$

  $r_{k-4} = r_{k-3} q_{k-2} + r_{k-3} \quad 0 \leq r_{k-2} < r_{k-3}$

  $r_{k-3} = r_{k-2} q_{k-1} + r_{k-1} \quad 0 \leq r_{k-1} < r_{k-2}$

  $r_{k-2} = r_{k-1} q_k$

  El proceso termina cuando $r_k = 0$. Esto siempre ocurre ya que $b > r_1 > r_2 > \ldots > r_k$ y r_k tiene que ser cero para algún $k \in \mathbb{N}$ ya que no hay ninguna sucesión infinita descendiente en $\mathbb{N}$

- Teorema de Bezout
Sean $a, b \in \mathbb{Z}$. Si $d = mcd(a,b)$ existen $m, n \in \mathbb{Z}$ tal que $d = m \cdot a + n \cdot b$.

  Dem
  Si suponemos que el teorema es cierto cuando $a, b \geq 0$, como $d = mcd(a,b) = mcd(|a|, |b|)$ $\quad d = k \cdot |a| + l \cdot |b| = m \cdot a + n \cdot b$ Donde m y n se obtienen de k y l cambiando el signo, si fuese necesario.

  Por tanto, podemos limitarnos a estudiar el caso $a, b \geq 0 \quad d = mcd(a,b)$

  Según los cálculos desarrollados más arriba $d = r_{k-1}$ y por la penúltima ecuación se verifica

  $r_{k-1} = r_{k-3} - r_{k-2} q_{k-1}$

Luego d podemos escribirlo en la forma $m'r_{k-2} + n'r_{k-3}$ donde $m' = -q_{k-1}$ y $n' = 1$. Sustituyendo r_{k-2} en términos de r_{k-3} y r_{k-4} obtenemos

$d = m'(r_{k-4} - r_{k-3}q_{k-2}) + n'r_{k-3}$ que puede escribirse como $m''r_{k-3} + n''r_{k-4}$ con $m'' = n' - m'q_{k-2}$ y $n'' = m'$. Continuando así, finalmente obtenemos una expresión para d en la forma pedida.

- Ej. Calcula el $mcd(2406, 654)$

$2406 = 654 \cdot 3 + 444$
$654 = 444 \cdot 1 + 210$
$444 = 210 \cdot 2 + 24$
$210 = 24 \cdot 8 + 18$
$24 = 18 \cdot 1 + 6$
$18 = 6 \cdot 3 + 0 \implies mcd(18, 6) = mcd(6, 0) = 6$

$6 = 24 - 18 = 24 - (210 - 24 \cdot 8) = -210 + 24(1 + 8) = -210 + 9 \cdot 24 = -210 + 9(444 - 210 \cdot 2) = 444 \cdot 9 + 210(-1 - 18) = 444 \cdot 9 + 210(-19) = 444 \cdot 9 + (-19)(654 - 444 \cdot 1) = (-19) \cdot 654 + 444(9 + 19) = (-19) \cdot 654 + 444(28) = (-19) \cdot 654 + 28(2406 - 654 \cdot 3) = 28 \cdot 2406 + 654(-19 - 84) = 28 \cdot 2406 + 654(-103)$

$6 = 28 \cdot 2406 + 654(-103)$

$mcd(a, b) = 1 \iff$ a y b son **primos entre sí** $\iff \quad 1 = m \cdot a + n \cdot b$.

- <u>NUMEROS PRIMOS.</u>
- <u>Def.</u>
  Un entero p se dice que es primo si $p \geq 2$ y los únicos divisores de p son p y 1.
- <u>Teorema</u>
  Si p es primo y $p \mid x_1 \dots x_n$ con $x_1 \dots x_n \in \mathbb{Z}$ entonces $p \mid x_i$ para algún i, $1 \leq i \leq n$

  <u>Dem.</u>
  La demostración es por inducción sobre $n \geq 1$

  Base $n = 1$ Trivial.

  Paso Inductivo Lo suponemos cierto para $n = k$ y lo demostramos para $n = k + 1$.

  Suponemos $p \mid x_1 \dots x_k x_{k+1}$. Consideramos dos casos:

  1. $x = x_1 \dots x_k$ y $p \mid x \underset{\text{H.I.}}{\overset{\uparrow}{\Longrightarrow}} p \mid x_i$ para algún i, $1 \leq i \leq k$
  2. $x = x_1 \dots x_k$ y $p \not| \, x \Longrightarrow mcd(p, x) = 1$ ya que p es primo.
     Por el teorema de Bezout $1 = r \cdot p + s \cdot x$ luego $x_{k+1} = r \cdot p \cdot x_{k+1} + s \cdot x \cdot x_{k+1}$ ya que $p \mid x \cdot x_{k+1} \Longrightarrow x \cdot x_{k+1} = p \cdot t \Longrightarrow x_{k+1} = p \cdot r \cdot x_{k+1} + s \cdot p \cdot t = p(r \cdot x_{k+1} + s \cdot t) \Longrightarrow p \mid x_{k+1}$

- <u>Nota</u>
  Si p no es primo, el resultado es falso. Por ejemplo, $6 \mid 3 \cdot 8$ pero $6 \not| \, 3$ y $6 \not| \, 8$.
- <u>Teorema</u>(Teorema Fundamental de la Aritmética)
  Todo entero $n \geq 1$ se descompone unívocamente en producto de primos.

  Dem.
  Ya hemos demostrado que si $n \geq 2$, $n \in \mathbb{Z}$ puede escribirse como producto de primos. Falta, por tanto, demostrar que este producto es único, es decir si $x = p_1 \dots p_k = p'_1 \dots p'_l \Longrightarrow k = l$ (algunos primos pueden estar repetidos) las descomposiciones sólo difieren en el orden de los factores.

  Base $n = 1 \longrightarrow k = l = 0$

  Paso Inductivo $n > 1$ $n = p'_1 \dots p'_l$ y por el teorema $p_1 \mid p'_j$ para algún $1 \leq j \leq l$ Reordenando los primos podemos suponer $j = 1$, por tanto $p_1 \mid p'_1$ y al ser p_1 y p'_1 primos $p_1 = p'_1$.

  Distinguimos dos casos:

  - $k = 1$ $p_1 \mid p'_1 \dots p'_l$ $n = p_1 = p'_1 \dots p'_l \Longrightarrow l = 1$ (si no p_1 no sería primo.)

- $k > 1 \implies n > p_1 \implies l > 1$. Como $p_1 = p'_1 \quad p_2 \dots p_k = p'_2 \dots p'_l = m$ y $m < n$ podemos aplicar la hipótesis de inducción luego
  $k - 1 = l - 1 \quad p_2 = p'_2 \ \dots \ p_k = p'_l$ Esto, junto con $p_1 = p'_1$ nos da el resultado buscado.

- Ej.
  $7000 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 5 \cdot 7 = 2^3 \cdot 5^3 \cdot 7$

- Teorema
  El conjunto de números primos S is infinito.

  Dem.
  Supongamos que S es finito. S $= \{p_1, \dots, p_n\}$ y S $\neq \emptyset$ ya que 2 es primo.

  Consideramos $m = p_1 \dots p_n + 1$ Por el teorema anterior m puede descomponerse de manera unívoca en producto de primos y vamos a ver que ningún p_i divide a m. Supongamos que lo divide: $m = p_i \cdot t = p_1 \dots p_n + 1 \implies p_i(t - p_1 \dots p_{i-1}p_{i+1} \dots p_n) = 1$ luego p_i divide a 1. Contradicción.

- Ej.
  $\sqrt{2}$ es irracional.

  Supongamos que es racional y vamos a ver que llegamos a contradicción.

  $\sqrt{2} = \dfrac{m}{n} \quad m, n \in \mathbb{Z} \implies 2 = \dfrac{m^2}{n^2} \implies 2n^2 = m^2$ Escribimos $m = 2^k u$ y $n = 2^l v$ tal que $2 \nmid u \quad 2 \nmid v \implies \begin{array}{l} m^2 = (2^k u)^2 = 2^{2k} u^2 \\ 2n^2 = 2(2^l v)^2 = 2^{2l+1} v^2 \end{array}$
  Como $2n^2 = m^2 \longrightarrow 2^{2l+1}v^2 = 2^{2k}u^2$ Por tanto, el exponente de 2 es $2k$ que es par pero también es $2l+1$ que es impar. Sabemos que la decomposición de un número en primos es única, luego no es posible.

- Ej.
  Si n es un entero compuesto, entonces n tiene un divisor primo $p \leq \sqrt{n}$

  Sea $n = t \cdot q \quad \begin{array}{l} 1 < t < n \\ 1 < q < n \end{array}$ si $t > \sqrt{n}$ y $q > \sqrt{n} \implies n = t \cdot q > \sqrt{n} \cdot \sqrt{n}$
  Si t o q no son primos, tienen un divisor primo $p' < \sqrt{n}$.

  Aplicamos este resultado para demostrar que 101 es primo.
  Los únicos primos $< \sqrt{101}$ son 2,3,5,7. Como no dividen a 101 $\implies$ 101 es primo.

- **PROPIEDADES DIVISIBILIDAD** (Algunas resueltas en problemas.)

1. Sean $a, b, c, d \in \mathbb{Z}^+$
   (a) Si $a \mid b$ y $b \mid c \implies a \mid c$
   (b) Si $a \mid b$ y $c \mid d \implies ac \mid bd$
   (c) Si $a \mid b \implies ac \mid bc$
   (d) Si $ac \mid bc \implies a \mid b$
   (e) Si $a \mid b$ y $a \mid c \implies a \mid bx + cy \ \forall x, y \in \mathbb{Z}$
2. Si dos enteros a, b verifican $ab = 1$, entonces o bien $a = b = 1$ o bien $a = b = -1$. Si m, n son enteros tales que $m \mid n$ y $n \mid m$, entonces $m = n$ ó $m = -n$.
3. Si existen enteros x, y tales que $ax + by = 1$ entonces $mcd(a, b) = 1$.
4. Sean $a, b, d \in \mathbb{Z}$ con $d > 0$. Si d es un divisor de a y de b y existen enteros x, y tales que $ax + by = d$ entonces $mcd(a, b) = d$.
5. (Lema de Euclides) Sean $a, b, c \in \mathbb{Z}$ con $a \neq 0$ o $b \neq 0$. Si $a \mid bc$ y $mcd(a, b) = 1$ entonces $a \mid c$.
6. Sean $a, b \in \mathbb{Z}$ $\forall k \geq 1$ demuestra que $mcd(ka, kb) = k \cdot mcd(a, b)$.
7. Sean $a, b \in \mathbb{Z}$, si $mcd(a, b) = d$, entonces $mcd(a/d, b/d) = 1$.
8. $mcd(a, b) * mcm(a, b) = a * b$