

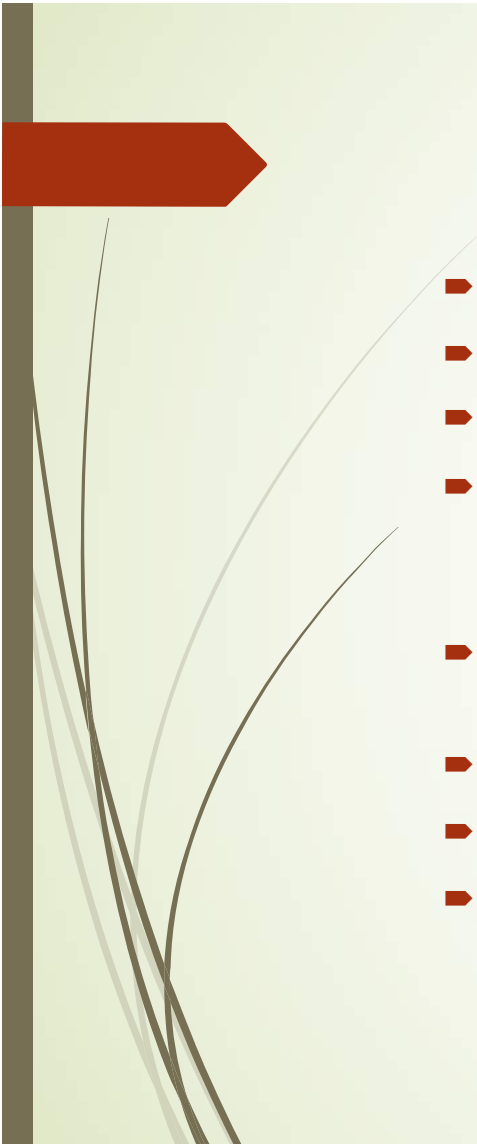


→ Clase 3

- 
- Nos dirigimos hacia el Teorema Fundamental de la Aritmética, el cual nos habla de cómo descomponer los enteros no nulos en producto de números primos. Para llegar hasta allí hace falta relacionar el concepto de Máximo Común Divisor con el algoritmo de la división entera. Esto nos da el siguiente resultado:


- **Algoritmo de Euclides (para el máximo común divisor):** Dados dos enteros a y b no ambos nulos, el siguiente algoritmo acaba y da como resultado $d = \text{mcd}(a,b)$:

- 1. (Suponer $a > b > 0$): como $\text{mcd}(a,b) = \text{mcd}(b,a) = \text{mcd}(|a|, |b|)$ podemos suponer $a \geq b > 0$ (el caso $b = 0$ es trivial pues $\text{mcd}(a, 0) = |a|$).
- Si $a = b$ el resultado es $\text{mcd}(a,b) = a$. Por lo tanto, supongamos que se tiene $a > b > 0$.
- 2. (División entera) Calcular q, r_1 enteros con: $a = bq + r_1$, $0 \leq r_1 < b$.

- 
- 3. (¿Acaba?) Si $r_1 = 0$ entonces $b \mid a$, luego $\text{mcd}(a,b) = b$.
 - 4. Si $r_1 \neq 0$: Calcular q_2 y r_2 tales que:
 - $b = r_1 q_2 + r_2$, con $0 \leq r_2 < r_1$. Si $r_2 = 0$, entonces $\text{mcd}(a,b) = r_1$. Si no:
 - Calcular q_3 y r_3 tales que: $r_1 = r_2 q_3 + r_3$ con $0 \leq r_3 < r_2$, y así sucesivamente, es decir, dados r_{j-1} y r_{j-2} (con $j > 2$) si son ambos no nulos calculamos q_j y r_j tales que: $r_{j-2} = r_{j-1} q_j + r_j$ con $0 \leq r_j < r_{j-1}$.
 - Llamemos ahora i al último índice tal que el resto r_i es no nulo (¿¿Existe siempre un tal índice?? Ya veremos que sí).
 - Por lo tanto, se tiene que $r_i \neq 0$ y $r_{i+1} = 0$. Luego, existe q_{i+1} tal que:
 - $r_{i-1} = r_i q_{i+1} + 0$. Afirmamos que para este índice i se tiene que:
 - $\text{mcd}(a,b) = r_i$




Euclides



Pero...¿Porqué este algoritmo calcula lo que queremos que calcule?

- Tenemos que probar que el algoritmo “funciona”: en primer lugar, debemos explicar porqué es cierto que acaba, o sea, que existe un índice i tal que tras iterar el algoritmo de la división entera se acaba con un resto $r_{i+1} = 0$. Luego, debemos ver que si $i+1$ es el primer índice donde esto ocurre se tiene que $r_i = \text{mcd}(a,b)$.
- El algoritmo acaba tras un número finito de iteraciones: Esto se sigue del hecho de que los sucesivos restos, mientras que no son 0, forman una sucesión decreciente de enteros positivos:
- $b > r_1 > r_2 > \dots > r_j > 0$. Pero no se puede descender con enteros positivos indefinidamente (por ejemplo tras $j = b$ pasos ya saldríamos del conjunto de los enteros positivos), por lo tanto tiene que existir un índice i tal que $r_{i+1} = 0$.

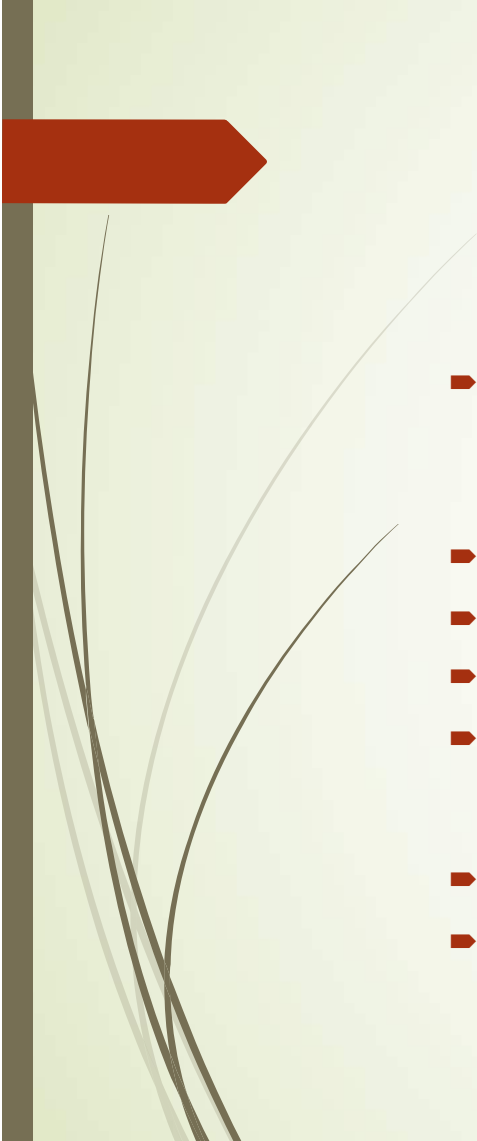
- 
- Si $r_i \neq 0$ y $r_{i+1} = 0$, entonces $r_i = \text{mcd}(a,b)$:
 - Apliquemos en cada paso el Lema 2:
 - $\text{mcd}(a,b) = \text{mcd}(b,a) = \text{mcd}(b, a - b q) = \text{mcd}(b, r_1)$
 - Análogamente: $\text{mcd}(b, r_1) = \text{mcd}(r_1, b) = \text{mcd}(r_1, b - r_1 q_2) = \text{mcd}(r_1, r_2)$.
 - Iterando este argumento deducimos que:
 - $\text{mcd}(a,b) = \text{mcd}(b, r_1) = \text{mcd}(r_1, r_2) = \dots = \text{mcd}(r_{i-1}, r_i) = \text{mcd}(r_i, r_{i+1}) =$
 - $\text{mcd}(r_i, 0) = r_i$.

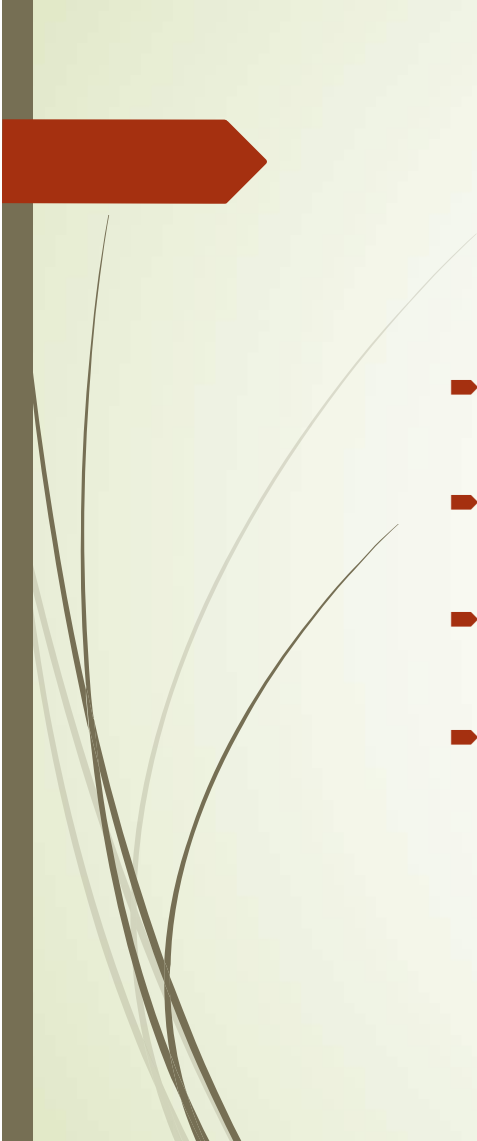
➤ Q.E.D.

- 
- **Lema 3 (Identidad de Bézout):** Sean a, b dos enteros no ambos nulos y $d = \text{mcd}(a, b)$. Entonces existen enteros x e y tales que:

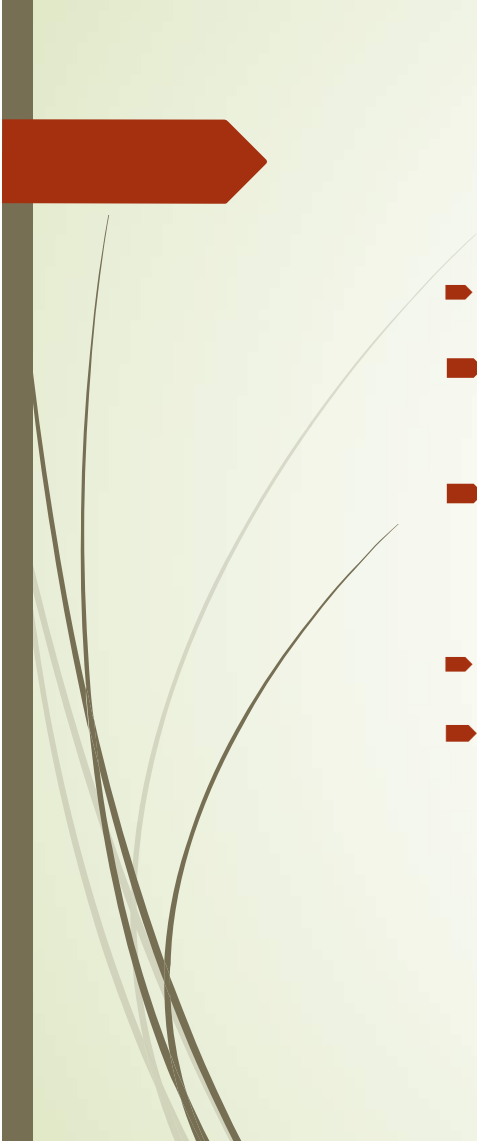
$$\text{➤ } d = ax + by$$


- **Observación:** En esta situación se dice que d es combinación \mathbb{Z} -lineal de a y b .
- **Demostración:** Aplicando el Algoritmo de Euclides consideremos la sucesión de restos r_1, r_2, \dots, r_i con $r_{i+1} = 0$ y $r_i = d = \text{mcd}(a, b)$.
- Probaremos con un razonamiento recursivo (que equivale a aplicar el principio de inducción sobre el conjunto de índices) que todos los restos r_j son combinación \mathbb{Z} -lineal de a y b , y en particular por lo tanto esto vale para d .

- 
- Comenzamos por mencionar el caso trivial en que $\text{mcd}(a,b) = a$ o $\text{mcd}(a,b) = b$, en cuyo caso ya tenemos la identidad de Bézout trivialmente satisfecha. Veamos ahora que r_1 y r_2 son combinaciones \mathbb{Z} -lineales de a y b . Recordemos que:
 - $r_1 = a - b q_1$, y los coeficientes 1 y $-q_1$ son enteros.
 - $r_2 = b - r_1 q_2 = b - (a - b q_1) q_2 = -a q_2 + b (1 + q_1 q_2)$, y los coeficientes $-q_2$ y $1 + q_1 q_2$ son enteros.
 - Razonando recursivamente, supongamos que para un índice j arbitrario se tiene que r_{j-2} y r_{j-1} son ambas combinaciones \mathbb{Z} -lineales de a y b , es decir, que existen enteros α , β , γ y δ tales que:
 - $r_{j-2} = \alpha a + \beta b$, y
 - $r_{j-1} = \gamma a + \delta b$

- 
- Y veamos que lo mismo ocurre para r_j : Como $r_j = r_{j-2} - r_{j-1} q_j$, reemplazando obtenemos:
 - $r_j = (\alpha a + \beta b) - (\gamma a + \delta b)q_j = a(\alpha - \gamma q_j) + b(\beta - \delta q_j)$, que es una combinación \mathbb{Z} -lineal de a y b .
 - Concluimos que todos los restos r_j que aparecen en el Algoritmo de Euclides son combinación \mathbb{Z} -lineal de a y b . En particular esto se aplica a
 - $r_i = d = \text{mcd}(a, b)$.

➤ Q.E.D.

- 
- Aplicando esta identidad, probemos la siguiente:
 - **Proposición:** Si a y b son dos enteros no ambos nulos y n un entero con: $n \mid a$ y $n \mid b$, entonces $n \mid d = \text{mcd}(a, b)$.
 - **Demostración:** Sabemos por la identidad de Bézout que existen enteros x, y con: $d = ax + by$. Como $n \mid a$ y $n \mid b$, aplicamos la propiedad básica de "linealidad" de la divisibilidad y concluimos que:
 - $n \mid ax + by = d$. **Q.E.D.**
 - **Observación:** Se tiene por lo tanto que el máximo común divisor no sólo es el mayor de los divisores comunes si no que también es múltiplo de cualquier divisor común.

- 
- **Lema Fundamental de la Aritmética:** Si p es un número primo y a, b son enteros tales que $p \mid a \cdot b$, entonces $p \mid a$ o $p \mid b$.
 - **Demostración:** Supongamos que p no divide a b . Como p es primo, está claro que se tiene: $\text{mcd}(p, b) = 1$ (no puede ser p pues p no divide a b , y no hay otros divisores de p a parte del 1).
 - Aplicando la Identidad de Bézout, se deduce que existen enteros x e y con:
 - $1 = b x + p y$. Multiplicando por a ambos miembros obtenemos:
 - $a = a b x + a p y$ (😊) .
 - Como por hipótesis $p \mid a b$, se tiene (transitividad de la divisibilidad) que $p \mid a b x$. Por otro lado es evidente que $p \mid a p y$. Luego de (😊) deducimos que $p \mid a$.
 -

Q.E.D.





→ Clase 4




Stefano Bézout

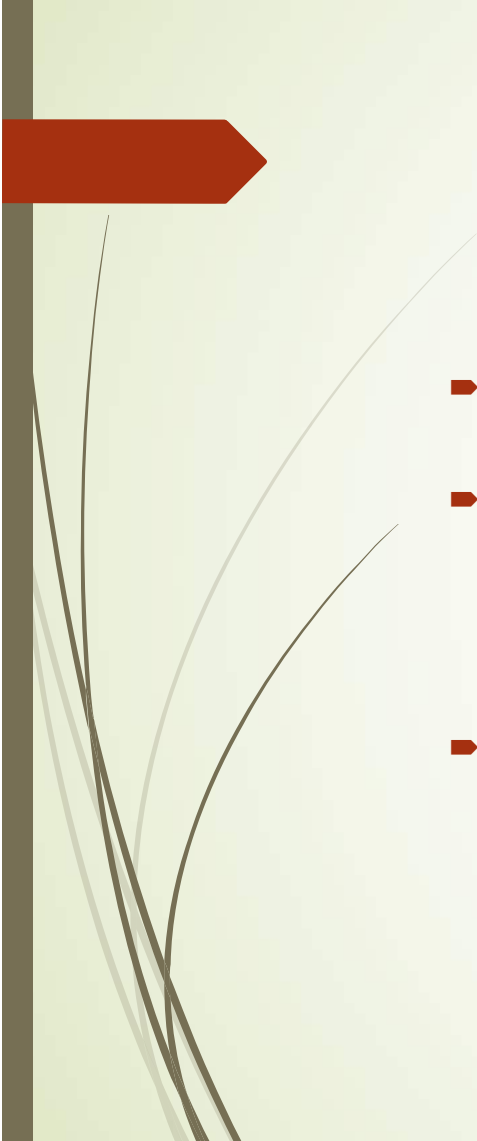
Bézout


- 
- Con el mismo argumento se prueba el:
 - **Lema de Euclides:** Si a, b, c son enteros tales que $b \mid a \cdot c$ y $\text{mcd}(a,b) = 1$, entonces $b \mid c$.
 - **Demostración:** Como $\text{mcd}(a,b) = 1$, la identidad de Bézout nos dice que existen enteros x, y tales que: $1 = a x + b y$.
 - Multiplicando por c obtenemos: $c = c a x + c b y$, y como por hipótesis se tiene que $b \mid a c$, también vale $b \mid c a x$, y como claramente $b \mid c b y$, concluimos que $b \mid c$.
 - El lema Fundamental también tiene el siguiente:


- 
- **Corolario:** Si p es un número primo y a_1, a_2, \dots, a_r enteros tales que
 - $p \mid a_1 a_2 \dots a_r$, entonces $p \mid a_i$ para algún $i \in \{1, 2, \dots, r\}$.
 - Demostración: Aplicamos inducción en el número r de factores. Para $r=2$ esto es el Lema Fundamental ya probado. Si $r > 2$, Supongamos que la proposición es cierta para el caso de $r-1$ factores. Entonces, partiendo de:
 - $p \mid a_1 a_2 \dots a_r = a_1 (a_2 a_3 \dots a_r)$, aplicando el Lema Fundamental se tiene que: $p \mid a_1$ o $p \mid a_2 a_3 \dots a_r$. En el primer caso ya tenemos lo que queríamos. En el segundo caso aplicamos la hipótesis de inducción (es decir, la presunción de que para el caso de $r-1$ factores la propiedad es cierta), y concluimos que $p \mid a_i$ para algún $i \in \{2, 3, \dots, r\}$, lo cual también acaba la demostración.

➤ Q.E.D.

- 
- **Teorema Fundamental de la Aritmética:** Todo entero positivo n puede escribirse como producto de números primos, y tal descomposición es única excepto por el orden en que se escriban los factores.
 - **Demostración:** Para $n=1$, el enunciado es cierto si interpretamos que cogemos como conjunto de primos el conjunto vacío y que el producto de elementos del conjunto vacío es 1 por convención. Alternativamente, podemos decir que el teorema solo es válido para los enteros $n > 1$.
 - Consideremos entonces los números $n > 1$ y veamos por inducción que se pueden escribir como producto de primos. El caso $n=2$ es cierto pues 2 es primo. Dado $n > 2$, supongamos pues que el teorema es cierto para todo entero positivo menor que n . Separamos la prueba en dos casos, según si n es primo o es compuesto.

- 
- Si n es primo, escribiendo $n = n$ esto prueba el teorema (entendemos en este caso que se está haciendo un “producto” de un único factor).
 - Si n es compuesto, sabemos que existen $1 < a, b < n$ tales que: $n = a b$. Por hipótesis de inducción, a y b pueden ambos escribirse como producto de primos, por lo tanto está claro que $n = a b$ también puede escribirse como producto de primos (no hay más que multiplicar los primos que “aparecen” en a por los que “aparecen” en b).
 - Aquí acaba la demostración por inducción de que todo n (mayor que 1 si se quiere) puede escribirse como producto de primos. Ahora tenemos que ver la unicidad de este tipo de factorización, y es aquí donde usaremos la **ARTILLERÍA PESADA** que hemos venido desarrollando (el lema fundamental y su variante para r factores).

- 
- Unicidad: Sea $n > 1$ y supongamos que lo podemos escribir como producto de primos:
 - $n = p_1 p_2 \dots p_d$, donde los p_i son primos. Supongamos que también tenemos que:
 - $n = q_1 q_2 \dots q_m$, donde los q_j son primos. Queremos ver que ambas descomposiciones en primos son iguales (excepto quizás por el orden).
 - Como $p_1 \mid n = q_1 q_2 \dots q_m$, por el corolario al lema fundamental concluimos que para algún $j \in \{1, 2, \dots, m\}$ se tiene que $p_1 \mid q_j$. Como estos dos números son primos, claramente esto implica que $p_1 = q_j$.
 - Cambiando si fuera preciso el orden en que estaban los factores, podemos suponer que en la igualdad anterior se tiene $p_1 = q_1$.

- 
- Luego, en la igualdad:
 - $n = p_1 p_2 \dots p_d = q_1 q_2 \dots q_m$ podemos cancelar este factor común y si llamamos $n' = n/p_1$ se tiene:
 - $n' = p_2 p_3 \dots p_d = q_2 q_3 \dots q_m$
 - Aquí iteramos el mismo razonamiento, para concluir que $p_2 = q_2$, y luego de simplificar este factor común se deduce análogamente que $p_3 = q_3$, y así sucesivamente cada p_i es igual a un q_j , lo cual prueba la unicidad de la descomposición.
 - Esto concluye la demostración excepto por el hecho de que aparentemente necesitamos suponer que $d = m$. Pero es fácil ver que esto tiene forzosamente que ser cierto, pues de no ser así, si fuera por ejemplo $d < m$, tras iterar d veces el proceso de “cancelar un primo en común” acabaríamos con:
 - $1 = q_{d+1} q_{d+2} \dots q_m$
 - Que es claramente imposible pues ningún primo divide a 1.

■ Q.E.D.



➤ **Teorema (Euclides):** Existen infinitos números primos.

➤ **Demostración:** Lo hacemos por reducción al absurdo. Supongamos que hay sólo una cantidad finita de números primos, que son:

p_1, p_2, \dots, p_r , para algún $r > 0$. Consideremos el número:

➤ $n = 1 + p_1 \cdot p_2 \cdot \dots \cdot p_r$

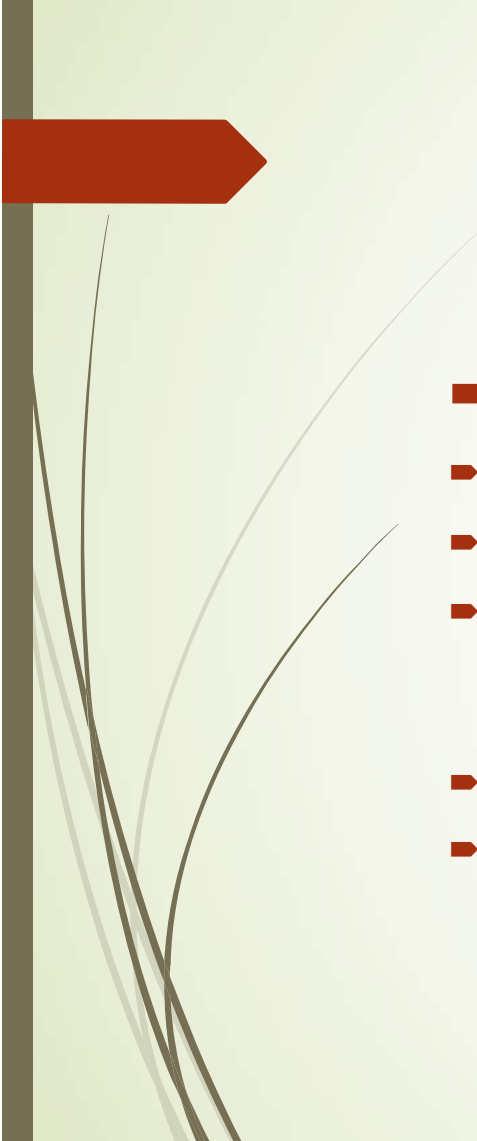
➤ Para cada i entre 1 y r tenemos que: $p_i \mid n - 1$, y por lo tanto que p_i no divide a n . Como $n > 1$, por el Teorema Fundamental de la Aritmética sabemos que existe al menos un primo p que divide a n . Pero acabamos de decir que n no es divisible por ninguno de los p_i con lo cual $p \neq p_i$, para todo $i = 1, 2, \dots, r$. Esto es una contradicción pues habíamos supuesto que no existían más primos que los p_i , por lo tanto concluimos que la hipótesis que hicimos es falsa, es decir, que existen infinitos primos.

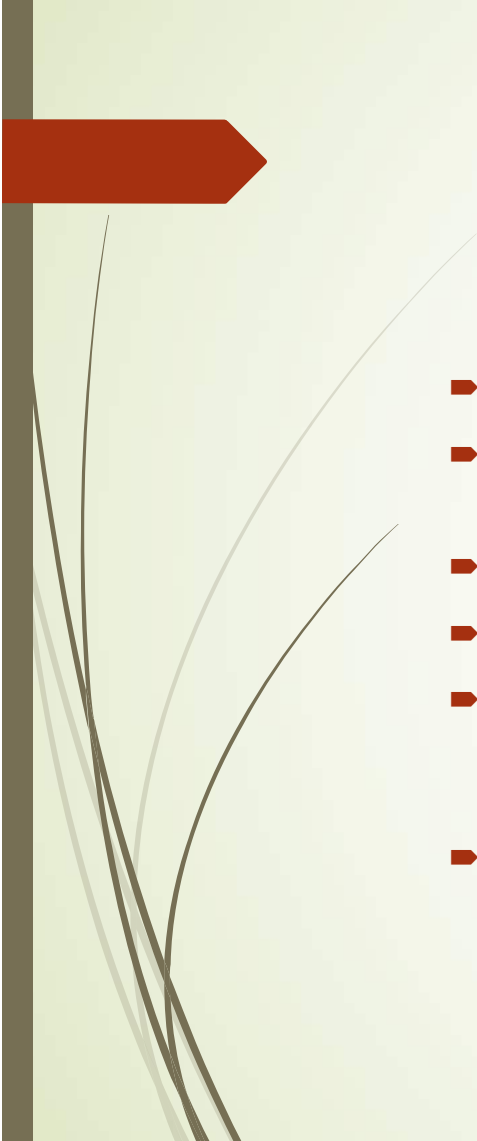
Ecuaciones Diofánticas Lineales

- **Definición:** Una ecuación en varias variables:
- $f(x_1, x_2, \dots, x_n) = 0$ donde f es un polinomio a coeficientes enteros y de la cual se buscan las soluciones enteras se llama Ecuación Diofántica.
- Ejemplo: La ecuación: $x^3 + y^3 = z^3$ en enteros, para la cual Euler probó que sólo posee como soluciones las "triviales" que se dan cuando alguno de los tres enteros vale 0.
- **Teorema (Diofántica Lineal, 2 variables):** La ecuación $ax + by = n$ tiene solución en enteros (x_0, y_0) sí y sólo sí $d = \text{mcd}(a, b)$ divide a n . En el caso en que exista una solución (x_0, y_0) , hay infinitas soluciones (x, y) y éstas se expresan en función de (x_0, y_0) y un parámetro $t \in \mathbb{Z}$ mediante la fórmula:
$$x = x_0 + \frac{b}{d} t, \quad y = y_0 - \frac{a}{d} t.$$

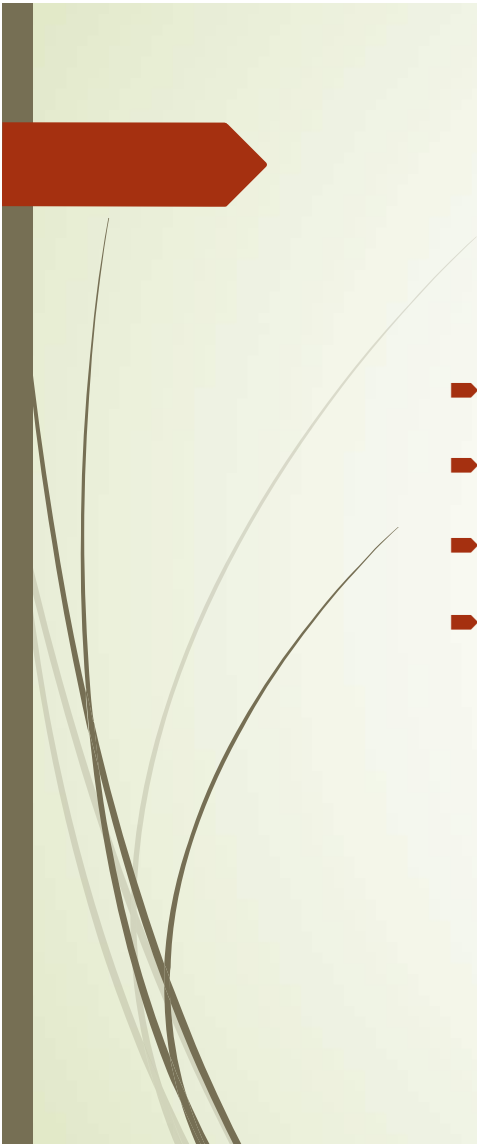


Diofanto

- 
- **Demostración:** Llamemos $\frac{b}{d} = B$ y $\frac{a}{d} = A$.
 - Para la primera afirmación, si existe solución (x_0, y_0) en enteros se cumple:
 - $a x_0 + b y_0 = n$, de donde como $d \mid a$ y $d \mid b$ concluimos que $d \mid n$.
 - Recíprocamente, si $d \mid n$, llamemos $\frac{n}{d} = N$. Sabemos por Bézout que existen enteros x', y' tales que: $d = a x' + b y'$. Si multiplicamos por N ambos lados de esta igualdad obtenemos: $n = a (x' N) + b (y' N)$, luego vemos que
 - $(x' N, y' N)$ es solución de $a x + b y = n$.
 - Observación: Sabemos que aplicando el algoritmo de Euclides podemos calcular una solución (x', y') de la identidad de Bézout. De aquí, multiplicando por $N = \frac{n}{d}$ obtenemos una solución de $a x + b y = n$.

- 
- Segunda afirmación: Sea (x_0, y_0) una solución de $ax + by = n$.
 - Como $a = dA$ y $b = dB$ con $d = \text{mcd}(a, b)$ se tiene: $\text{mcd}(A, B) = 1$. Supongamos que se tiene otra solución (x_1, y_1) de la misma ecuación.
 - Tenemos que $ax_0 + by_0 = n = ax_1 + by_1$, de donde, restando:
 - $a(x_0 - x_1) = b(y_1 - y_0)$. Dividiendo por d ambos miembros obtenemos:
 - $A(x_0 - x_1) = B(y_1 - y_0)$. Por lo tanto tenemos que A divide al producto $B(y_1 - y_0)$, y como A es coprimo con B se tiene (Lema de Euclides) que A divide a $y_1 - y_0$. Por lo tanto: $y_1 - y_0 = wA$, para un entero w .
 - Análogamente, como el lado izquierdo es divisible por B y B es coprimo con A se tiene que B divide a $x_0 - x_1$. Luego: $x_0 - x_1 = zB$, para un entero z .

- Reemplazando en la fórmula previa obtenemos:
- $A \cdot z \cdot B = B \cdot w \cdot A$, de donde: $z = w$. Por lo tanto tenemos que:
- $x_1 = x_0 - z B$, $y_1 = y_0 + z A$. Tomando $t = -z$ y recordando la definición de A y B obtenemos:
- $x_1 = x_0 + t \frac{b}{d}$, $y_1 = y_0 - t \frac{a}{d}$ (🤖)
- Hemos probado que toda solución (x_1, y_1) de la ecuación será de la forma
- (🤖) para algún entero t , pero falta ver que para todo entero t los enteros x_1 e y_1 dados por las expresiones (🤖) son siempre solución de la ecuación. Esto es fácil de comprobar, basta sustituir las variables por las expresiones en (🤖) en la ecuación $ax + by = n$ y verificar que se tiene igualdad:



➤ (sin olvidar, por supuesto, que (x_0, y_0) es solución por hipótesis):

➤ $ax_1 + by_1 = a(x_0 + t\frac{b}{d}) + b(y_0 - t\frac{a}{d}) = ax_0 + by_0 + t(\frac{ab}{d} - \frac{ba}{d}) =$

➤ $ax_0 + by_0 = n.$

➤

Q.E.D.