ARITMÉTICA ENTERA

Gregorio Hernández

UPM

Matemática Discreta I

NÚMEROS ENTEROS Z

$\mathbf{Z} = \{...., -3, -2, -1, 0, 1, 2, 3,....\}$
$\mathbf{N} = \{1, 2, 3,....\}$
$\mathbf{N_0} = \{0, 1, 2, 3,....\}$

Operaciones en **Z**, suma y producto
Relación de **orden** total en **Z**, $a \leq b$
- reflexiva $a \leq a$
- antisimétrica $a \leq b, b \leq a \Rightarrow a=b$
- transitiva $a \leq b, b \leq c \Rightarrow a \leq c$

compatible con las operaciones:
$a \leq b \Rightarrow a + c \leq b + c \quad \forall\, c \in \mathbf{Z}$
$ac \leq bc \quad \forall\, c \geq 0$

b es **cota inferior** de $X \subset \mathbf{Z}$ es si $b \leq x \quad \forall\, x \in \mathbf{X}$

Axioma de buena ordenación (en **Z**)
"Si **X** es un subconjunto no vacío de **Z** y acotado inferiormente, entonces **X** tiene mínimo".

Axioma de buena ordenación (en **N**)
"Si **X** es un subconjunto no vacío de **N** o $\mathbf{N_0}$, entonces **X** tiene mínimo".

En **Q,** con el orden usual, el axioma no se verifica.

El conjunto {1, 1/2, 1/3, 1/4, …} está acotado inferiormente por 0 pero no posee un elemento mínimo

Q es un conjunto bien ordenado, es decir, existe un orden en **Q** para el que se verifica el axioma de buena ordenación

Expresiones recursivas

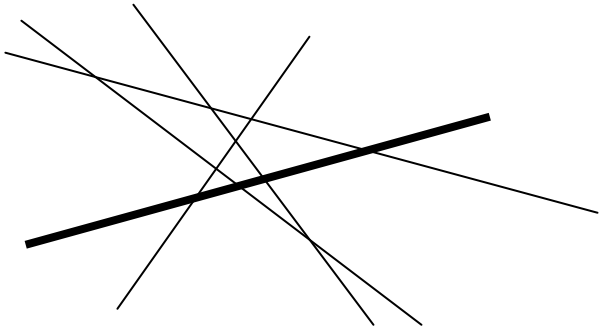
¿Cuántas rectas se pueden definir con n puntos del plano?
¿Cuántos triángulos?

¿Cuántas regiones se forman al trazar n rectas en el plano?

$a_1 = 2$

$a_2 = 4$

$a_3 = 7$



$$\begin{cases} a_n = a_{n-1} + n \quad (\text{para } n \geq 2) \\ a_1 = 2 \end{cases}$$

¿Está bien definido?

Definiciones recursivas

$$\begin{cases} a_n = a_{n-1} + n \quad (\text{para } n \geq 2) \\ a_1 = 2 \end{cases}$$

Justificación

Supongamos que a_n NO está definido en un conjunto $S \subset N$
Por el axioma de buen orden, S tiene un elemento mínimo m
y así tenemos que a_m NO está definido
Como $m \neq 1$, resulta que $a_m = a_{m-1} + m$ pero aquí a_{m-1} SÍ está bien definido por la minimalidad de m, luego a_m está definido contradiciendo la suposición inicial.

Principio de inducción

Sea $S \subset \mathbf{N}$ tal que
(a) $1 \in S$,
(b) $\forall\, k \in \mathbf{N}$, si $k \in S$ entonces $k+1 \in S$.
Entonces, se cumple que $S = \mathbf{N}$

Dem.:
Por reducción al absurdo. Supongamos que $S \neq \mathbf{N}$
Así $S^c = \mathbf{N} - S = \{n \in \mathbf{N} / n \notin S\}$ es un conjunto no vacío, luego tiene un mínimo m

Como $1 \notin S^c$, resulta que $m \neq 1$ y $m - 1 \in S$
Por la condición (b) $m - 1 + 1 = m \in S$
Contradicción, tenemos que $m \in S$ y $m \notin S$

Principio de inducción

Sea $S \subset \mathbf{N}$ tal que
(a) $1 \in S$,
(b) $\forall\, k \in \mathbf{N}$, si $k \in S$ entonces $k+1 \in S$.
Entonces, se cumple que $S = \mathbf{N}$

Demostrar que para todo número natural n se verifica que

$$1 + 3 + 5 + 7 + \ldots + (2n - 1) = n^2$$

Expresión recursiva Expresión explícita

En la suma se “enmascara” la definición recursiva

$$s_1 = 1$$

$$s_n = s_{n-1} + (2n - 1)$$

Principio de inducción

Sea $S \subset \{n \in \mathbf{Z} / n \geq a\}$ tal que

(a) $a \in S$,

(b) $\forall\, k \geq a$, si $k \in S$ entonces $k+1 \in S$.

Entonces, se cumple que $S = \{n \in \mathbf{Z} / n \geq a\}$

Demostrar que si $n \geq 2$ entonces se cumple que $2^n > n + 1$

¿Para qué valores es cierto que $n! \geq 2^n$?

Principio de inducción

Si P es una propiedad que se puede afirmar para $n \in Z$ y se cumple que:
(1) P(1) es verdadera
(2) Siempre que P(k) es verdad para cualquier entero $k \geq 1$, entonces es verdadera para el siguiente entero, P(k+1).
Entonces P(n) es verdadera para todo $n \geq 1$

Si P es una propiedad que se puede afirmar para $n \in Z$ y se cumple que:
(1) P(a) es verdadera para un cierto $a \in Z$
(2) Siempre que P(k) es verdad para cualquier entero $k \geq a$, entonces es verdadera para el siguiente entero, P(k+1).
Entonces P(n) es verdadera para todo $n \geq a$

Basta considerar el conjunto
$S = \{a \in Z$ / P es verdadera para a$\}$

Principio de inducción

Inducción fuerte

Sean $a \in \mathbf{Z}$, $X = \{n \in \mathbf{Z} \mid n \geq a\}$ y $S \subset X$ tales que:

(a) $a \in S$,

(b) si $\{a, a+1, a+2, ..., k\} \subset S$ entonces $k+1 \in S$

En estas condiciones se cumple que S=X

Demostrar que la expresión recursiva

$$\begin{cases} a_n = 3a_{n-1} - 2a_{n-2} \quad (\text{para } n \geq 3) \\ a_1 = 3 \qquad a_2 = 5 \end{cases}$$

tiene como expresión explícita $a_n = 2^n + 1$

DIVISIBILIDAD

Si **a,b**$\in$**Z,** a$\neq$0, se dice que **a divide** a **b** si existe **c**$\in$**Z** tal que **b=ac** y se indica por **a** $\mid$ **b**. También se dice que **b** es múltiplo de **a**, o que **a** es un factor o divisor de **b**.

D_{20} = {1, 2, 4, 5, 10, 20} divisores positivos de 20
¿cuántos son? ¿cuánto vale su suma?

Propiedades: Si a,b,c$\in$Z, entonces:

1) $a \mid 0,\ 1 \mid a$
2) $a \mid a$
3) $a \mid b$ y $b \mid a \Rightarrow a = b$ ó $a = -b$
4) $a \mid b$ y $b \mid c \Rightarrow a \mid c$
5) $a \mid b$ y $a \mid c \Rightarrow a \mid b + c$

DIVISIÓN EN **Z**

Teorema

Sean $\mathbf{a} \in \mathbf{Z}$ y $\mathbf{b} \in \mathbf{N}$. Entonces existen $\mathbf{q},\mathbf{r} \in \mathbf{Z}$ tales que $\mathbf{a = bq + r}$, con $0 \leq r < b$. Además **q** y **r** son únicos.

$a = 26,\ b = 8$

$26 = 8 \cdot 3 + 2$

$26 = 8 \cdot 4 + (-6)$

$26 = 8 \cdot (-2) + 42$

$26 = 8 \cdot 2 + 10$

$a = -26,\ b = 8$

$-26 = 8 \cdot (-5) + 14$

$-26 = 8 \cdot 4 + (-58)$

$-26 = 8 \cdot (-2) - 10$

$-26 = 8 \cdot (-4) + 6$

DIVISIÓN EN **Z**

Teorema

Sean $\mathbf{a} \in \mathbf{Z}$ y $\mathbf{b} \in \mathbf{N}$. Entonces existen $\mathbf{q,r} \in \mathbf{Z}$ tales que $\mathbf{a = bq + r}$, con $0 \leq r < b$. Además **q** y **r** son únicos.

Dem.

$R = \{x \in N \cup \{0\} \,/\, a = by + x \text{ para algún } y \in Z\}$ R no es vacío

- si $a \geq 0$ $a = b0 + a$
- si $a < 0$ $a = ba + a – ba = ba + a(1 – b)$

Existe r mínimo de R, $a = bq + r$ $0 \leq r$

Si $r \geq b$ $a = b(q+1) + r – b$ $r – b < r$ pero r es mínimo en R !!

Unicidad

$a = bq + r = bq' + r'$ $0 \leq r < b$, $0 \leq r' < b$, $b(q – q') = r' – r$

Si $q > q'$ entonces $r' = r + b(q – q') \geq r + b \geq b$!!

$254 = 2\cdot 10^2 + 5\cdot 10 + 4$, $2326 = 2\cdot 10^3 + 3\cdot 10^2 + 2\cdot 10 + 6$

$25 = 2\cdot 3^2 + 2\cdot 3 + 1$ $\qquad 25_{10} = 221_3$

$25 = 1\cdot 2^4 + 1\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2 + 1$ $\qquad 25_{10} = 221_3 = 11001_2$

Sistema de numeración en base t

Si **t** es un número natural, **t≥2**, todo $x \in$ **N** se puede expresar de modo único en la forma

$$x = r_n t^n + r_{n-1} t^{n-1} + ... + r_1 t + r_0$$

$r_n \neq 0$ $\qquad 0 \leq r_i < t$ para todo $i=0, ..., n$

La expresión $\mathbf{(r_n\ r_{n-1}\ ....\ r_0)_t}$ constituye la expresión de **x** en el sistema de numeración en base **t**

Base 2,	BINARIA	{0, 1}
Base 8,	OCTAL	{0, 1, 2, 3, 4, 5, 6, 7}
Base 16,	HEXADECIMAL	{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F}

Paso de octal a binario

$$(1567)_8 = 1\cdot 8^3 + 5\cdot 8^2 + 6\cdot 8^1 + 7\cdot 8^0 =$$
$$= (2^0)\cdot(2^9) + (2^2 + 2^0)\cdot(2^6) + (2^2 + 2^1)\cdot(2^3) + (2^2 + 2^1 + 2^0)\cdot(2^0) =$$
$$= 2^9 + 2^8 + 2^6 + 2^5 + 2^4 + 2^2 + 2^1 + 2^0 =$$
$$= (1)(101)(110)(111)_2 = (1101110111)_2$$

Del mismo modo se puede efectuar la conversión

binario $\leftrightarrow$ hexadecimal

agrupando los dígitos de derecha a izquierda en grupos de 4

$$(A52C)_{16} \leftrightarrow (1010)(0101)(0010)(1100) \leftrightarrow (1010010100101100)_2$$

Máximo común divisor

Dados **a,b**$\in$**Z**-{0}**,** se dice que **d**>0 es el máximo común divisor de **a** y **b** si $d \mid a$, $d \mid b$ y cualquier otro $c \in \mathbf{Z}$ tal que $c \mid a$, $c \mid b$ verifica que $c \mid d$.

Se designa con $d = mcd(a,b)$

Algoritmo de Euclides (Procedimiento para obtener el mcd)

Dados **a,b**$\in$**Z –** {0} si $a = bq + r$ entonces $mcd(a,b) = mcd(b,r)$

$a = bq_1 + r_1$	$0 \le r_1 < b$	$mcd(a,b) = mcd(b,r_1)$
$b = r_1q_2 + r_2$	$0 \le r_2 < r_1$	$mcd(b,r_1) = mcd(r_1,r_2)$
$r_1 = r_2q_3 + r_3$	$0 \le r_3 < r_2$	$mcd(r_1,r_2) = mcd(r_2,r_3)$
.....	.....	.....
$r_{k-2} = r_{k-1}\, q_k + r_k$	$0 \le r_k < r_{k-1}$	$mcd(r_{k-2},r_{k-1}) = mcd(r_{k-1},r_k)$
$r_{k-1} = r_k\, q_{k+1}$	$r_{k-1} = 0$	$mcd(r_{k-1},r_k) = r_k$

$mcd(a,b) = r_k$ (último resto no nulo)

mcd(122, 18)

$$122 = 18\cdot 6 + 14$$
$$18 = 14\cdot 1 + 4$$
$$14 = 4\cdot 3 + 2$$
$$4 = 2\cdot 2$$

mcd(122, 18) = 2

Teorema de Bezout

Si d = mcd(a, b) entonces existen m, n enteros tales que

$$d = am + bn$$

$$2 = 14 - 4\cdot 3 = 14 - (18 - 14\cdot 1)3 = 14\cdot 4 - 18\cdot 3 =$$
$$= (122 - 18\cdot 6)\cdot 4 - 18\cdot 3 = 122\cdot 4 + 18\cdot(-27)$$

Los enteros m, n, NO son únicos

mcd (7,2) = 1

$$1 = 7\cdot 1 + 2\cdot(-3)$$
$$1 = 7\cdot(-1) + 2\cdot 4$$
$$1 = 7\cdot 3 + 2\cdot(-10)$$
$$1 = 7\cdot 5 + \ldots.$$

Algoritmo de Euclides

El nº de pasos efectuados en el algoritmo es, a lo sumo,

$$\log_2 a + \log_2 b$$

Lema

En cada iteración el producto de los números considerados baja, al menos, a la mitad

Consideremos el primer paso $(a, b) \rightarrow (b, r)$ $\quad a = bq+r \quad r<b$

$a = bq+r \geq b+r > 2r$, luego $ab > 2br$ es decir, $br < ab/2$

Tras k pasos el producto de los números con que se trabaja será $< \frac{ab}{2^k}$

$$1 \leq \frac{ab}{2^k} \quad \Rightarrow \quad 2^k \leq ab \quad \Rightarrow \quad k \leq \log_2 ab = \log_2 a + \log_2 b$$

Propiedades del máximo común divisor

i) Si $d = m.c.d.(a,b)$ entonces existen enteros m,n tales que
$d = ma + nb$

ii) $m.c.d.(a,b) = 1 \Leftrightarrow$ existen m y n enteros tales que $1 = ma + nb$
(Se dice que **a** y **b** son primos entre sí, o **coprimos**)

$\Leftarrow$) pues si $d|a$, $d|b$ entonces $d | ma + nb$, es decir, $d | 1$,
luego $d = 1$

iii) Si $a \mid bc$, $m.c.d.(a,b) = 1$ entonces $a \mid c$

$1 = ma + nb$, luego $c = mac + nbc$
$a \mid mac$, $a \mid bc$ luego $a \mid c$

Propiedades del máximo común divisor

iv) m.c.d.(a,b) = d $\Leftrightarrow$ d | a , d | b y m.c.d.(a/d, b/d) = 1

$\Rightarrow$) Si m.c.d.(a, b) = d entonces d|a, d|b y existen m, n tales que
ma + nb = d

Luego m(a/d) + n(b/d) = 1, es decir, m.c.d.(a/d, b/d) = 1

$\Leftarrow$) Si m.c.d.(a/d,b/d) = 1, existen m, n, con m(a/d) + n(b/d) = 1
ma + nb = d
Si c|a, c|b entonces c|d, luego d = mcd(a, b)

v) La reducción de fracciones a forma irreducible es única

a/b = a'/b' con mcd(a,b) = 1, mcd(a',b') = 1

ab' = a'b así b | ba' = ab' luego b | b'
y también, b' | ab' = ba' luego b' | b
Por tanto, b = b' y a = a'

ECUACIONES DIOFÁNTICAS

Las ecuaciones con coeficientes enteros y cuyas soluciones se buscan sólo dentro de **Z** se llaman *ecuaciones diofánticas*.

DIOFANTO siglo II

$24x + 10y = 7$ $24x^2 + 10y^2 = 6$

Ecuación de Pell $x^2 = 5\,y^2 + 1$

Ecuación pitagórica $x^2 + y^2 = z^2$

Fermat: La ecuación $x^n + y^n = z^n$ no tiene soluciones enteras salvo para n=2

Teorema de Wiles

ECUACIONES DIOFÁNTICAS DE PRIMER GRADO

$24x + 10y = 7$ $24x + 10y = 6$ ¿tienen solución?

$mcd(24,10) = 2$ $2(12x + 5y) = 7$ $2(12x + 5y) = 6$

Teorema
La ecuación diofántica **a**x + **b**y = **c,** tiene soluciones en **Z** si y sólo si $mcd(a,b) \mid c$

Dem.: Llamemos $d = mcd(a,b)$, $a = a'd$, $b = b'd$
Con esto la ecuación se puede escribir como $d(a'x + b'y) = c$

Si la ecuación tiene solución en **Z,** entonces la expresión del paréntesis es un entero y $d \mid c$

ECUACIONES DIOFÁNTICAS DE PRIMER GRADO

Teorema
La ecuación diofántica **a**x + **b**y = **c,** tiene soluciones en **Z** si y sólo si mcd(a,b) | c

Dem.:
Si d | c entonces la ecuación tiene solución. Veamos

Si a = a'd, b = b'd, c = c'd de ax + by=c se pasa a la ecuación

(*) a'x + b'y = c' donde mcd(a',b') = 1

existen m,n$\in$**Z**, a'm + b'n =1. Multiplicando por c', resulta
a'mc' + b'nc' = c'

Luego una solución de la ecuación diofántica es x_1 = mc' y_1 = nc'

Además todas las soluciones de la ecuación son de la forma
$x = x_1 + b't$ $y = y_1 + (-a')t$ $\forall\ t \in \mathbf{Z}$

ECUACIONES DIOFÁNTICAS DE PRIMER GRADO

$24x + 10y = 6$ $\qquad$ $\text{mcd}(24, 10) = 2 \mid 6$

Simplificamos por 2, resolvemos la ecuación equivalente

$$12x + 5y = 3$$

Como $\text{mcd}(12,5) = 1$ expresamos $1 = 12(-2) + 5 \cdot 5$

Multiplicando por 3, resulta $12(-2)3 + 5 \cdot 5 \cdot 3 = 3$

Luego una solución de la ecuación diofántica es $x_1 = (-2) \cdot 3$ $\quad y_1 = 5 \cdot 3$

Además todas las soluciones de la ecuación son de la forma

$$\begin{cases} x = -6 + 5t \\ y = 15 + (-12)t \end{cases} \qquad \forall\, t \in \mathbf{Z}$$

ECUACIONES DIOFÁNTICAS DE PRIMER GRADO

Teorema
La ecuación diofántica **a**x + **b**y = **c,** tiene soluciones en **Z** si y sólo si mcd(a,b) | c

Si (x_1, y_1) es una solución (particular) de la ecuación diofántica entonces todas las soluciones de la ecuación son de la forma

$x = x_1 + b't$
$y = y_1 + (-a')t \qquad \forall\, t \in \mathbf{Z}$

Sea (α, β) una solución de (*) entonces

$$a'x_1 + b'y_1 = c'$$
$$a'\alpha + b'\beta = c'$$

Luego $(\alpha - x_1, \beta - y_1)$ es una solución de $a'x + b'y = 0$ (ec. homogénea)

Las soluciones de la homogénea son de la forma $(b't, -a't)$ para $t \in \mathbf{Z}$

ECUACIONES DIOFÁNTICAS DE PRIMER GRADO

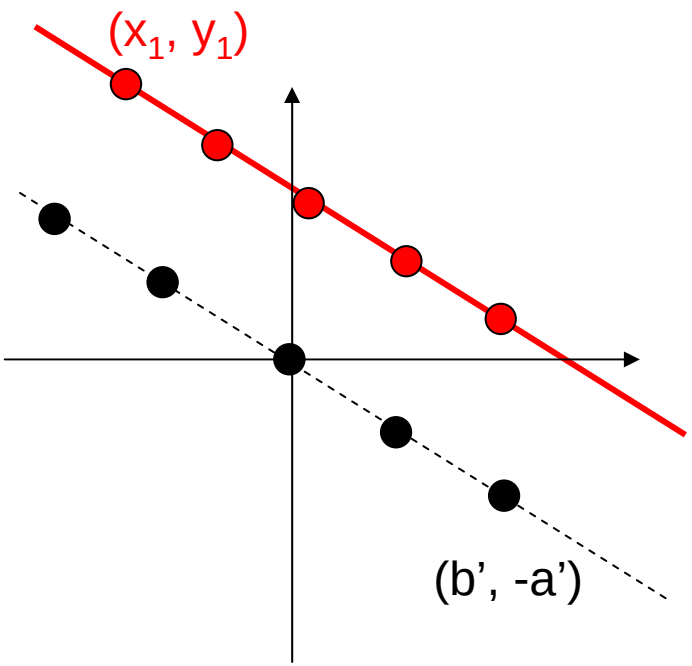
Interpretación geométrica de las soluciones

Si (x_1, y_1) es una solución (particular) de la ecuación diofántica entonces todas las soluciones de la ecuación son de la forma

$$\begin{cases} x = x_1 + b't \\ y = y_1 + (-a')t \end{cases} \qquad \forall\, t \in \mathbf{Z}$$

Las soluciones de la homogénea son los puntos de coordenadas enteras de la recta $y = (-a'/b')\, x$

Las soluciones de la ecuación son los puntos de coordenadas enteras de la recta paralela a la anterior por el punto (x_1, y_1)



NÚMEROS PRIMOS

Un número natural p es **primo** si p>1 y los únicos divisores positivos de p son 1 y p.

2, 3, 5, 7, 11, 13, 17, 19, ...

Propiedades

- Existen infinitos números primos.

Demostración: (Euclides)

Supongamos que hay una cantidad finita de primos. Así el conjunto $P= \{ p_1, p_2, p_3, \dots , p_n\}$ es finito

Consideramos el número natural $x = 1 + p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n$

Si x no es primo debe ser divisible por algún primo p_k

pero si $p_k \mid x$, como $p_k \mid p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n$ resulta que $p_k \mid 1$

Luego x es primo y no está en P, contradicción!!

NÚMEROS PRIMOS

Un número natural p es **primo** si p>1 y los únicos divisores positivos de p son 1 y p.

2, 3, 5, 7, 11, 13, 17, 19, ...

Propiedades

- Existen infinitos números primos.
- Si p es primo, $p \mid ab$ entonces, ó bien $p \mid a$ ó bien $p \mid b$.
- Si p es primo, $p \mid a_1 \ldots a_n$ entonces $p \mid a_i$ para algún i=1,...,n

Dem.:

Si $p \mid a$ ya está

Si $p \nmid a$ entonces mcd (a,p)=1,

luego existen m, n enteros tales que $am + np = 1$

Así, $amb + npb = b$, como p divide a los dos sumandos resulta que $p|b$

Teorema fundamental de la aritmética

Todo número natural n>1 se puede expresar de modo único, salvo el orden de los factores, como producto de números primos

Existencia de la descomposición

Sea A = { n >1 / n no factoriza como producto de números primos }
Si A es no vacío, por el axioma de buena ordenación, existe mín A = m.

O bien m es primo !! Absurdo
O bien m no es primo, pero entonces existen a, b < m, con m = ab
tanto a como b tendrán descomposición en primos
$a = p_1 \cdot \ldots \cdot p_k$ $b = p'_1 \cdot \ldots \cdot p'_j$
Luego $m = p_1 \cdot \ldots \cdot p_k \cdot p'_1 \cdot \ldots \cdot p'_j$ no está en A !!

Teorema fundamental de la aritmética

Todo número natural n>1 se puede expresar de modo único, salvo el orden de los factores, como producto de números primos

Unicidad de la descomposición

Sea B = { n >1 / n tiene dos factorizaciones en producto de primos }

Si B es no vacío, por el axioma de buena ordenación, existe mín B = s.

$s = p_1 \cdot \ldots \cdot p_k = p'_1 \cdot \ldots \cdot p'_j$ con p_i, p'_t primos

$p_1 \mid s = p'_1 \cdot \ldots \cdot p'_j$ luego p_1 divide a algún p'_t, por ejemplo, $p_1 \mid p'_1$

Como ambos son primos $p_1 = p'_1$

Así existe $r = p_2 \cdot \ldots \cdot p_k = p'_2 \cdot \ldots \cdot p'_j$ $r < s$ en contradicción con s = min B

Teorema fundamental de la aritmética

Todo número natural n>1 se puede expresar de modo único, salvo el orden de los factores, como producto de números primos

Ejercicio: $\sqrt{2}$ no es un número racional

Si $\sqrt{2} = \frac{m}{n}$ entonces $m^2 = 2n^2$ con m>0, n>0

La descomposición en primos de m y n serán

$m = 2^x h$, $n = 2^y g$

Luego $m^2 = 2^{2x} g^2$, $2n^2 = 2^{2y+1} h^2$

El factor 2 aparece un número par de veces en m^2 y un número impar en $2n^2$, luego $m^2 \neq 2n^2$

Resultados y conjeturas sobre primos

1. El intervalo entre primos consecutivos puede ser arbitrariamente grande
   (n+1)! + 2, (n+1)! + 3, …… (n+1)! +n+1 son compuestos y consecutivos.

2. Si mcd(a,b)=1, existen infinitos primos de la forma aq+b
   (Dirichlet, 1837)

3. Primos de Fermat
   Los números de Fermat son aquellos de la forma $F_n = 2^{2^n} + 1$
   Fermat conjeturó que todos eran primos
   Euler probó que $F_5 = 4294967297 = 641 \times 6700417$ es compuesto

4. ¿Cuántos primos hay menores que n?

$$\pi(n) \sim \frac{n}{\ln n}$$

Resultados y conjeturas sobre primos

Problemas de Landau (1912)

1. Conjetura de Goldbach, “Todo número par mayor que 2 es suma de dos números primos”.

   Comprobada experimentalmente hasta $n < 4 \cdot 10^{18}$
   Conjetura DÉBIL de Goldbach
   “Todo impar mayor que 5 es suma de tres primos”
   Demostrada por Hefgott en 2013

2. Conjetura de los primos gemelos. “Hay infinitos primos p tales que $p + 2$ es también un número primo”

   La mayor pareja conocida, septiembre 2016 (proyecto PrimeGrid), es $2996863034895 \cdot 2^{1290000} \pm 1$, que tiene 388342 cifras

   Zhang (2014) Existen infinitos pares de primos a distancia $N < 70 \cdot 10^6$
   Cota rebajada a 246 por Maynard y Tao

Resultados y conjeturas sobre primos

Problemas de Landau (1912)

3. Conjetura de Legendre. “Siempre existe un primo entre dos cuadrados perfectos”

   Ingham, 1937 demostró que si n>>0 entonces siempre hay un primo entre dos cubos consecutivos

4. Conjetura. “Hay infinitos primos de la forma $n^2 + 1$”

   Hay infinitos números de la forma $n^2 + 1$ que o bien son primos o bien tiene solo dos factores primos (Iwaniec, 1978)

Resultados y conjeturas sobre primos

Primos de Mersenne

Los números de Mersenne son aquellos de la forma $2^p - 1$, con p primo
Si además son primos se les llama primos de Mersenne.

Los primeros números de Mersenne son primos

$M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$, pero $M_{11} = 2047 = 23 \times 89$

Los primos conocidos con muchas cifras son siempre primos de Mersenne.
Proyecto GIMPS, búsqueda de grandes primos

Diciembre 2018 $2^{82589933} - 1$ (~24,8 millones de dígitos)
Es el primo de Mersenne número 51

POLINOMIOS CON COEFICIENTES ENTEROS

Lectura adicional

$x^3 + 7x^2 - 2$, $3x^4 - 8x + 5$

Los símbolos x, x^2, x^3, ... indican las posiciones de los coeficientes

(- 2, 0, 7, 1) (5, - 8, 0, 0, 3)

$(a_0, a_1, a_2, \ldots, a_n)$ sucesión finita de elementos de **Z,** es un polinomio con coeficientes en **Z**.

$f(x) = a_0 + a_1x + a_2x^2 + \ldots a_nx^n$

Conjunto de polinomios con coeficientes en **Z** **Z[x]**

coeficiente **principal** a_n (si es 1, polinomio **mónico**)

Suma de polinomios

Producto de polinomios

grado $(f(x) + g(x)) \leq \max\{\text{grado}(f(x)), \text{grado}(g(x))\}$

grado $(f(x) \cdot g(x)) = \text{grado}(f(x)) + \text{grado}(g(x))$

POLINOMIOS CON COEFICIENTES ENTEROS

División en Z[x].

Si f y g son polinomios en Z[x], no nulos, g(x) mónico, entonces existen polinomios únicos q(x) y r(x) tales que

$$f(x) = g(x)q(x) + r(x)$$

$$\text{grado}(r) < \text{grado}(g) \quad \text{o bien } r(x) = 0$$

Si $f(x) = g(x)q(x)$ decimos que g(x) es un **factor** o **divisor** de f(x), o que g(x) divide a f(x)

Consecuencias

1. Dado un polinomio f(x) y un entero c existe un único polinomio q(x) tal que $f(x) = (x - c)q(x) + f(c)$

Porque $f(x) = (x - c)q(x) + r$, luego $f(c) = r$

Luego, $x - c$ divide a $f(x) \Leftrightarrow f(c) = 0$

2. Si $f(c_1) = f(c_2) = \ldots = f(c_k) = 0$ entonces f(x) es divisible por $(x - c_1)\cdot(x - c_2)\cdot \ldots \cdot(x - c_k)$

Raíces de un polinomio $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$

El entero c es una raíz del polinomio f(x) si $f(c) = 0$

Un polinomio f(x) de grado n tiene a lo sumo n raíces distintas en **Z**

Teorema fundamental del álgebra (Gauss, 1799)
Un polinomio de grado n con coeficientes en **C** tiene siempre n raíces en **C**

Si c es raíz de f(x) entonces $c|a_0$

$0 = f(c) = a_0 + a_1c + a_2c^2 + ... + a_nc^n = a_0 + c(a_1 + a_2c + ... + a_nc^{n-1})$

Multiplicidad de una raíz

Orden de una raíz c es el mayor entero s tal que $(x - c)^s \mid f(x)$

Si s=1 c es raíz simple

Si s>1 c es raíz múltiple de orden s

Raíces de un polinomio $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$

Derivada de f

$f'(x) = a_1 + 2a_2x + 3a_3x^2 + ... + na_nx^{n-1}$

Dado f(x) no constante y una raíz c de f(x)

1) c es raíz simple de f(x) $\Leftrightarrow$ $f'(c) \neq 0$
2) c es raíz múltiple de f(x) $\Leftrightarrow$ $f'(c) = 0$

$f(x) = (x - c)^s g(x)$ siendo s= orden de c, con lo que $g(c) \neq 0$

Derivando, $f'(x) = s(x - c)^{s-1}g(x) + (x - c)^s g'(x)$

Luego, $s = 1 \Leftrightarrow f'(c) \neq 0$

$s > 1 \Leftrightarrow f'(c) = 0$

Además, c es raíz de orden s de f $\Rightarrow$ c es raíz de orden s – 1 de f '

POLINOMIOS CON COEFICIENTES ENTEROS

Máximo Común Divisor

Dados f(x) y g(x) polinomios en Z[x] no nulos, se llama **máximo común divisor** de f y g a un polinomio d(x) tal que

(1) d(x) | f(x) y d(x)| g(x)

(2) Si h(x) es otro divisor común, entonces h(x) | d(x)

Si además exigimos que sea mónico entonces mcd(f,g) es único

El algoritmo de Euclides permite obtener el máximo común divisor de polinomios con coeficientes en **Q**

$f(x) = x^4 - 2x^3 - 5x^2 + 4x + 6$ $\quad$ $g(x) = x^3 - 2x^2 - 2x + 4$

$f(x) = g(x)x - 3x^2 + 6$

$g(x) = (-3x^2 + 6)(-1/3x + 2/3)$

último resto no nulo es $-3x^2 + 6$

$\boxed{\text{mcd } (f,g) = x^2 - 2}$

POLINOMIOS CON COEFICIENTES ENTEROS

FACTORIZACIÓN E IRREDUCIBILIDAD EN **Z**[x]

Un polinomio f(x) es reducible en Z[x] si existen g y h, distintos de 1 y – 1 tales que f(x) = g(x)h(x)
En caso contrario se dice que f(x) es irreducible

Teorema
Todo polinomio f(x) en **Z**[x] se puede expresar como producto de factores irreducibles. La descomposición es única salvo constantes

Z[x] es un dominio de factorización única

$Z[\sqrt{-5}]$ = {a + b$\sqrt{-5}$ / a, b enteros}
no es dominio de factorización única

$$6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

POLINOMIOS CON COEFICIENTES ENTEROS

Criterio de Eisenstein

Sea $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ tal que $\text{mcd}(a_0, a_1, \ldots, a_n)=1$,
p primo tal que $p \mid a_0, a_1, \ldots, a_{n-1}$, p no divide a a_n y p^2 no divide a a_0
Entonces $f(x)$ es irreducible en $\mathbf{Z}[x]$ y en $\mathbf{Q}[x]$

Por ejemplo, $f(x) = 2 - 4x + x^3$ es irreducible ($p=2$).

Dem.: Supongamos que f es reducible, $f(x) = g(x)h(x)$
Sean $g(x) = b_0 + b_1x + b_2x^2 + \ldots + b_rx^r$ $b_r \neq 0$
$h(x) = c_0 + c_1x + c_2x^2 + \ldots + c_sx^s$ $c_s \neq 0$ $r + s = n$

$a_n = b_rc_s$, $p \nmid a_n$ luego $p \nmid b_r$ y $p \nmid c_s$
$a_0 = b_0c_0$, $p \mid a_0$, $p^2 \nmid a_0$ luego $p \nmid b_0$ ó $p \nmid c_0$ pero no ambos

Supongamos $p \mid c_0$, como $p \nmid c_s$, existe m mínimo tal que $p \nmid c_m$

$$a_m = \sum_{i+j=m} b_ic_j = b_0c_m + b_1c_{m-1} + \cdots + b_mc_0$$

No div. por p

Divisibles por p

Luego, $p \mid a_m$ contradicción!!