# Teoría de números algebraicos en PARI/GP

## Parte II: ideales en el anillo de enteros

**28/09/2020**

# ¿Cómo especificar un ideal?

# Ideales principales

$\alpha\mathcal{O}_K$ se especifica por su generador:

- polinomio en $x$
  = $\alpha$ en la base $1, x, x^2, \ldots, x^{n-1}$ de $\mathbb{Q}[x]/(f)$
- vector $[a_1, \ldots, a_n]$~
  = $\alpha$ en la $\mathbb{Z}$-base de $\mathcal{O}_K$ calculada en $K$.zk

# Ideales en general

- $I \subseteq \mathcal{O}_K$ — $\mathbb{Z}$-submódulo libre.
- $I \longleftrightarrow$ matriz de una $\mathbb{Z}$-base de $I$ en términos de la base de $\mathcal{O}_K$.
- **Forma normal de Hermite** (HNF). `mathnf`$(M)$ en PARI/GP. ¡Canónica!

# Forma normal de Hermite

- $H \in M_{n\times n}(\mathbb{Z})$ triangular superior con elementos $\geq 0$.
- Coeficiente mayor de la fila = primer coeficiente no nulo.
- Coeficiente mayor está a la derecha del coeficiente mayor de la fila anterior.
- Elementos arriba del coeficiente mayor son estrictamente menor.
- Elementos abajo del coeficiente mayor son nulos.

Para toda $A \in M_{n\times n}(\mathbb{Z})$ existe única $U \in \mathrm{GL}_n(\mathbb{Z})$ tal que $H = UA$ está en la HNF.
Se calcula mediante LLL (= Lenstra–Lenstra–Lovász).

# Ejemplo

$$\underbrace{\begin{pmatrix} 0 & +1 & +1 \\ -1 & +1 & -1 \\ -1 & +1 & +2 \end{pmatrix}}_{U} \cdot \underbrace{\begin{pmatrix} +3 & -2 & 0 \\ +4 & +3 & -3 \\ 0 & -2 & +2 \end{pmatrix}}_{A} = \underbrace{\begin{pmatrix} 2 & 1 & 1 \\ 0 & 4 & 1 \\ 0 & 0 & 2 \end{pmatrix}}_{H}$$

# Pasando a la HNF

```
? K = nfinit (x^2-5);
? K.zk
% = [1, 1/2*x - 1/2]
? a = idealhnf(K, 4+x)
% =
[11 8]

[ 0 1]
```

Interpretación:

$$\mathcal{O}_K = \alpha_1\mathbb{Z} \oplus \alpha_2\mathbb{Z}, \quad \alpha_1 = 1, \quad \alpha_2 = \frac{\sqrt{5}-1}{2},$$

$$(4+\sqrt{5})\mathcal{O}_K = 11\alpha_1\mathbb{Z} \oplus (8\alpha_1 + \alpha_2)\mathbb{Z}.$$

# Ejemplo bien conocido

$K = \mathbb{Q}(i)$,
$\mathcal{O}_K = \mathbb{Z}[i]$ es un DIP.

```
? K = nfinit(x^2+1);
? K.zk
% = [1, x]
```

# Ideales en $\mathbb{Z}[i]$ como $\mathbb{Z}$-módulos

$$\begin{aligned}(m+ni) &= \{(c+di)(m+ni) \mid c,d \in \mathbb{Z}\} \\ &= \{c\cdot(m+ni) + d\cdot(-n+mi) \mid c,d \in \mathbb{Z}\} \\ &= (m+ni)\mathbb{Z} \oplus (-n+mi)\mathbb{Z}.\end{aligned}$$

$$(m+ni) \longleftrightarrow \begin{pmatrix} m & -n \\ n & m \end{pmatrix} \quad \text{(¡no es HNF!)}$$

```
? a = idealhnf(K, 2+3*x)
% =
[13 5]
[ 0 1]

? mathnf ([2, -3; 3, 2])
% =
[13 5]
[ 0 1]
```

# Igualdad de ideales

$$\mathfrak{a} = \mathfrak{b} \iff \texttt{idealhnf}(K, \mathfrak{a}) = \texttt{idealhnf}(K, \mathfrak{b})$$

```
? a = idealhnf(K, 2+3*x)
% =
[13 5]
[ 0 1]

? b = idealhnf(K, -3+2*x)
% =
[13 5]
[ 0 1]

? Mod ((2+3*x)/(-3+2*x), K.pol)
% = Mod(-x, x^2 + 1)
```

# Enumeración de ideales

`ideallist`$(K, N)$ = ideales $I \subseteq \mathcal{O}_K$ tales que $N_{K/\mathbb{Q}}(I) \leq N$
Salida: vector

[ideales de norma 0,
ideales de norma 1,
$\ldots$,
ideales de norma $N$]

# Ejemplo

```
? K = nfinit(x^2+1);
? L = ideallist(K,10)
% = [[[1, 0; 0, 1]],  /* norma 1: I=O_K */
     [[2, 1; 0, 1]],
     [],              /* no hay de norma 3 */
     [[2, 0; 0, 2]],
     [[5, 3; 0, 1], [5, 2; 0, 1]],
     [],              /* no hay de norma 6 */
     [],              /* no hay de norma 7 */
     [[4, 2; 0, 2]],
     [[3, 0; 0, 3]],
     [[10, 3; 0, 1], [10, 7; 0, 1]]]

? vector (#L,i,#L[i])
% = [1, 1, 0, 1, 2, 0, 0, 1, 1, 2]
? vecsum (%)
% = 9
```

# Problema de la tarea

¿Cuántos ideales de norma $\leq 10$ hay en $\mathcal{O}_K$ para $K = \mathbb{Q}(\sqrt[3]{17})$?

```
? K = nfinit(x^3 - 17);
? L = ideallist (K,10);
? vector (#L,i,#L[i])
% = [1, 1, 2, 2, 1, 2, 0, 2, 3, 1]
? vecsum(%)
% = 15
```

Ejemplo: no hay ideales de norma 7:
$\mathfrak{p} = 7\mathcal{O}_K$ es primo (= 7 es inerte).
$17 \equiv 3\ (7)$; los cubos mód 7 son 1 y $6 \equiv (-1)^3$.

# Operaciones con ideales

# Operaciones aritméticas

- `idealadd`$(K, \mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$
- `idealmul`$(K, \mathfrak{a}, \mathfrak{b}) = \mathfrak{a}\mathfrak{b}$
- `idealpow`$(K, \mathfrak{a}, n) = \mathfrak{a}^n$
- `idealinv`$(K, \mathfrak{a}) = \mathfrak{a}^{-1}$
- `idealintersect`$(K, \mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}$

# Ideal «abajo»

$$\begin{array}{ccc} \mathfrak{a} & \subseteq K & \mathcal{O}_K\text{-módulo} \\ & \Big| & \\ \mathfrak{a}\cap\mathbb{Q} & \subseteq \mathbb{Q} & \mathbb{Z}\text{-módulo} \end{array}$$

`idealdown`$(K,\mathfrak{a})$ = el $\mathbb{Z}$-ideal $\mathfrak{a}\cap\mathbb{Q}$

```
? K = nfinit(x^2+1);
? idealdown(K,1+x)
% = 2
? idealdown(K,3+3*x)
% = 6
```

# Norma

$$\texttt{idealnorm}(K, \mathfrak{a}) = N_{K/\mathbb{Q}}(\mathfrak{a})$$

```
? K = nfinit(x^2+1);
? idealnorm(K,1+x)
% = 2
? idealnorm(K,3)
% = 9
? idealnorm(K,3+3*x)
% = 18
```

# Maximalidad

```
? K = nfinit(x^2+1);
? idealismaximal(K,1+x)
% = [2, [1, 1]~, 2, 1, [1, -1; 1, 1]]
? idealismaximal(K,3+3*x)
% = 0

? L = nfinit(x^3-17);
? idealismaximal(L,7)
% = [7, [7, 0, 0]~, 1, 3, 1]
```

# Generación por dos elementos

Recordatorio: todo ideal en $\mathcal{O}_K$ tiene forma $(\alpha, \beta)$

```
? K = nfinit(x^3 - 2);
? a = [3,1,2; 0,1,0; 0,0,1]
% =
[3 1 2]
[0 1 0]
[0 0 1]

? idealtwoelt(K,a)
% = [3, [1, 1, 0]~]
? nfbasistoalg(K,%[2])
% = Mod(x + 1, x^3 - 2)
```

Significado: $\mathfrak{a} = (3, 1 + \sqrt[3]{2})$.

# ¿Ideales principales?

- $\mathfrak{a}$ principal $\iff [\mathfrak{a}] = [\mathcal{O}_K] = 0$ en $\mathrm{Cl}(K)$.
- $\mathcal{O}_K$ es un DFU $\iff \mathrm{Cl}(K) = 0$.
- Veremos después...

# Factorización de ideales

# Factorización

- `idealfactor`$(K, \mathfrak{a})$: factorizar $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$
- `idealprimedec`$(K, p)$: factorizar $\mathfrak{a} = p\mathcal{O}_K$

# Factorización de primos racionales

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s},$$

$$\texttt{idealprimedec}(K,p) = [P_1,\ldots,P_s],$$

- $P_i$`.e` = índice de ramificación
- $P_i$`.f` = grado del campo residual
- $P_i$`.gen = [`$p$`,` $\alpha$`]`, donde $\mathfrak{p}_i = (p, \alpha)$

# Ejemplo: $K = \mathbb{Q}(\sqrt{5})$

```
? K = nfinit(x^2 - 5);

? decK = idealprimedec(K,11)
% = [[11, [-3, 2]~, 1, 1, [5, 2; 2, 3]],
     [11, [5, 2]~, 1, 1, [-3, 2; 2, -5]]]
? #decK
% 2                /* dos factores */

? [decK[1].e, decK[1].f]
% = [1, 1]
? decK[1].gen
% = [11, [-3, 2]~]
? nfbasistoalg (K,%[2])
% = Mod(x - 4, x^2 - 5)
```

$$11\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2, \quad \mathfrak{p}_1 = (11, \sqrt{5} - 4),\ \mathfrak{p}_2 = (11, \sqrt{5} + 4),\ f_1 = f_2 = 1$$

# Ejemplo: $L = \mathbb{Q}(\zeta_5) \supset \mathbb{Q}(\sqrt{5})$

```
? L = nfinit(polcyclo(5));
? decL = idealprimedec(L,11);
? #decL
# 4                  /* 4 factores */
? vector (#decL,i, [decL[i].e, decL[i].f])
% = [[1, 1], [1, 1], [1, 1], [1, 1]]
```

$$11\mathcal{O}_L = \mathfrak{p}_1\,\mathfrak{p}_2\,\mathfrak{p}_3\,\mathfrak{p}_4$$

# Ramificación

```
? idealprimedec(K,5)
% = [[5, [1, 2]~, 2, 1, [1, 2; 2, -1]]]
? %[1].e
% = 2
? idealprimedec(L,5)
% = [[5, [-1, 1, 0, 0]~, 4, 1, [.....]]]
? %[1].e
% = 4
```

Significado: $5\mathcal{O}_K = \mathfrak{p}^2, 5\mathcal{O}_L = \mathfrak{q}^4$

# Ejemplo de Kummer

```
? K = nfinit(polcyclo(23));
? dec = idealprimedec(K,47);
? #dec
% = 22
```

$$47\mathbb{Z}[\zeta_{23}] = \mathfrak{p}_1 \cdots \mathfrak{p}_{22}$$

# *Pausa para el café*

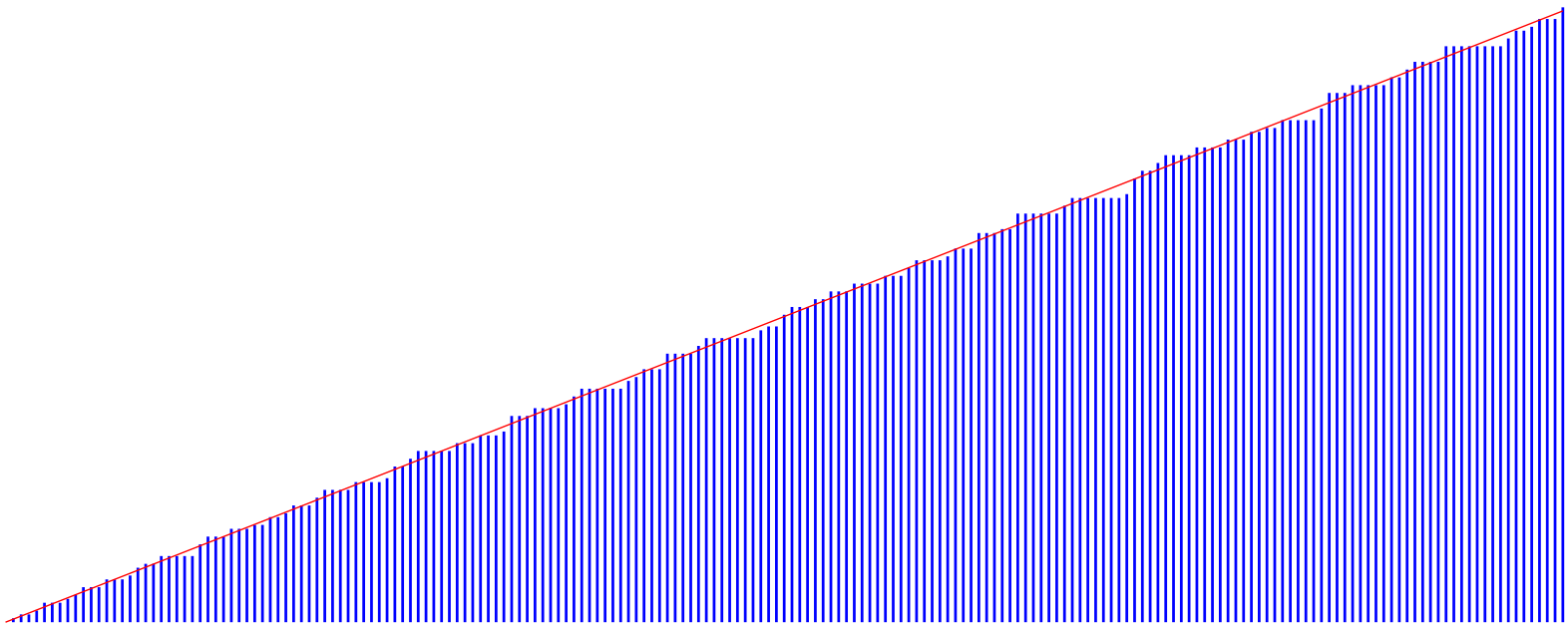
# Experimento:
# Ideales de norma $\leq N$

# Pregunta

Cómo se comporta la función

$$N \mapsto \#\{I \subseteq \mathcal{O}_K \mid N_{K/\mathbb{Q}}(I) \leq N\}$$

# Ejemplo: $K = \mathbb{Q}(i)$

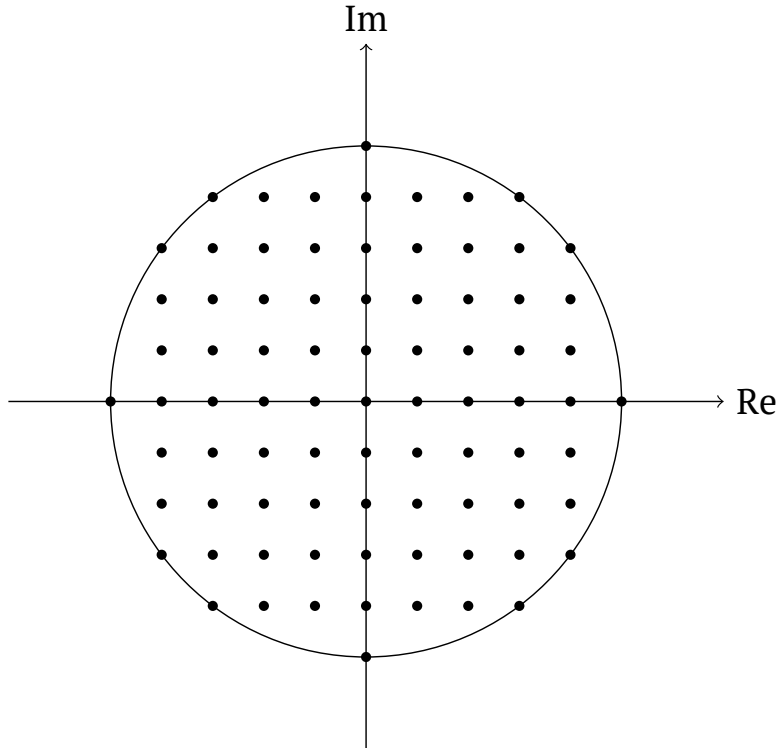


# Explicación

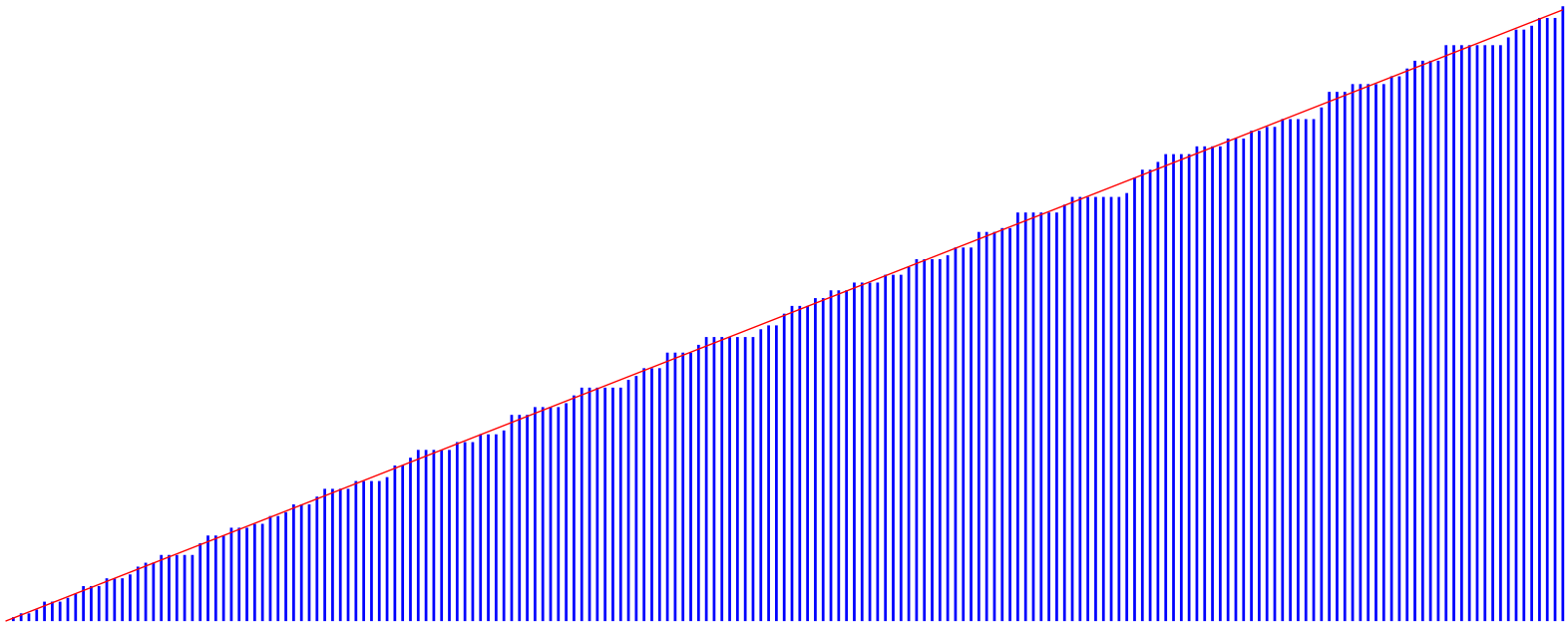
$$N_{K/\mathbb{Q}}(\alpha\mathbb{Z}[i]) = N_{K/\mathbb{Q}}((a+bi)\mathbb{Z}[i]) = a^2 + b^2$$

$$(\alpha) = (-\alpha) = (i\alpha) = (-i\alpha)$$

$$\#\{I \subseteq \mathbb{Z}[i] \mid N(I) \leq N\} = \frac{1}{4} \cdot \#\{(a,b) \in \mathbb{Z}^2 \mid a^2 + b^2 \leq N\}$$



# Explicación



$$\#\{\text{puntos dentro del círculo de radio } r\} \sim \pi r^2$$

$$\#\{\text{ideales de norma } \leq N\} \sim \tfrac{\pi}{4} N$$

# Algunos cálculos

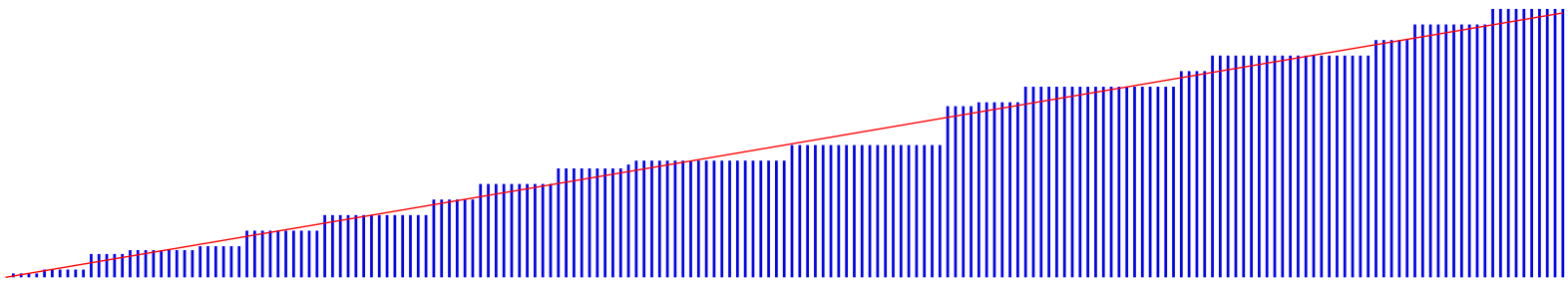
```
? K = nfinit(x^2+1);
? L = ideallist(K,20);

? vector (#L,s, sum(i=1,s,#L[i]))
% = [1,2,2,3,5,5,5,6,7,9,9, 9,11,11,11,12,14...]

? vector (20,i, ceil(Pi/4*i))
% = [1,2,3,4,4,5,6,7,8,8,9,10,11,11,12,13,14...]
```

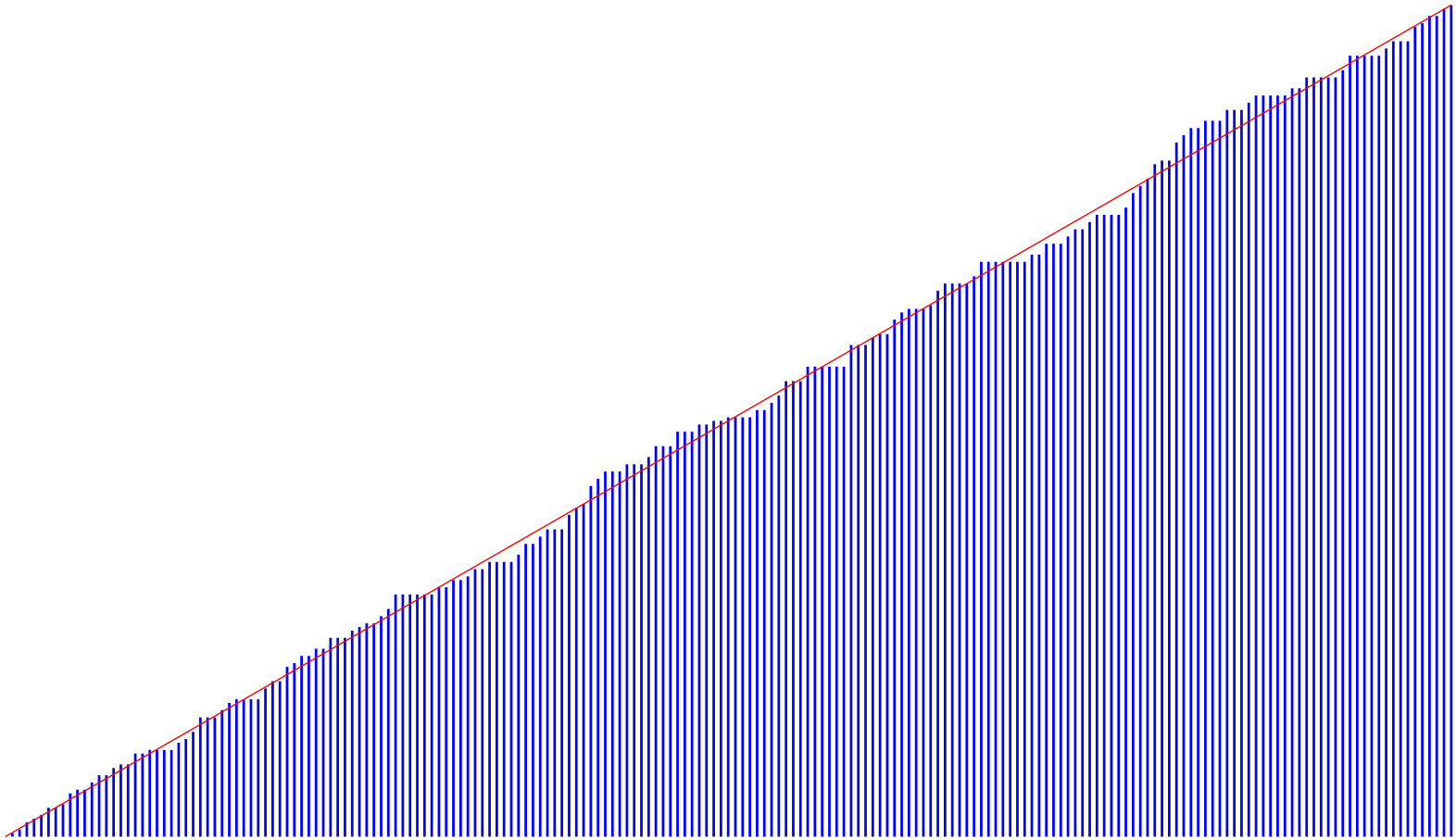
* Relacionado: **problema del círculo de Gauss**

# **Ejemplo:** $K = \mathbb{Q}(\zeta_5)$**,** $\mathrm{Cl}(K) = 0$**,** $|\mathcal{O}_K^\times| = \infty$



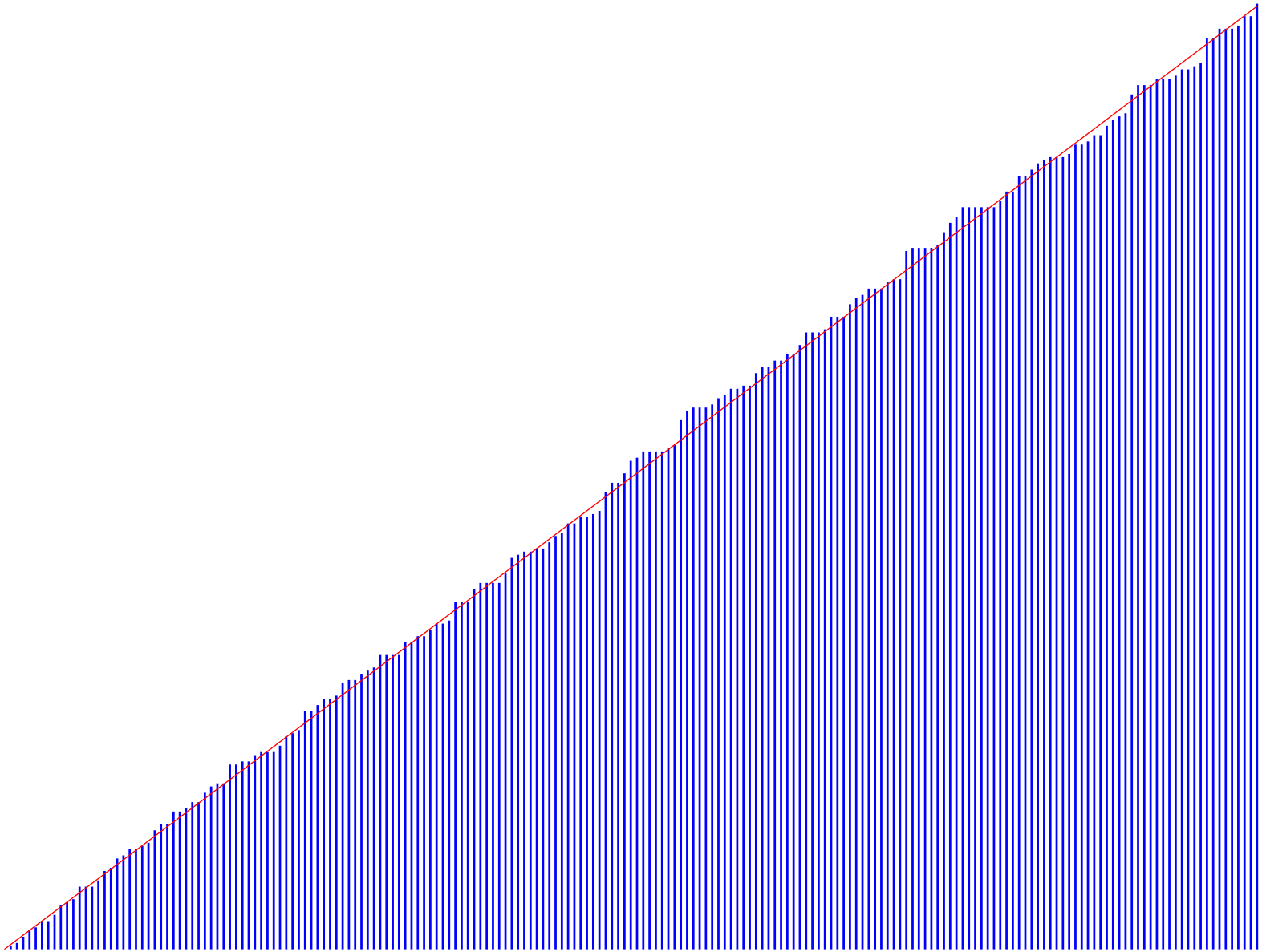
$\sim C \cdot N$, donde $C$ = ?????

# $K = \mathbb{Q}(\sqrt{10})$, $\mathrm{Cl}(K) \neq 0$, $|\mathcal{O}_K^\times| = \infty$



$\sim C \cdot N$, donde $C$ = ?????

# $K = \mathbb{Q}(\sqrt[3]{19})$, $\mathrm{Cl}(K) \neq 0$, $|\mathcal{O}_K^\times| = \infty$



$\sim C \cdot N$, donde $C$ = ?????

# Explicación breve: función zeta de Dedekind

- Función meromorfa

$$\zeta_K(s) = \sum_{\substack{I \subseteq \mathcal{O}_K \\ I \neq 0}} \frac{1}{N_{K/\mathbb{Q}}(I)^s}$$

  responsable por contar los ideales.
- $C$ = residuo en el polo $s = 1$
- $C$ trae información aritmética (fórmula del número de clase)

# Experimento: estadística sobre descomposiciones

# Pregunta

- Si $p$ no se ramifica en $K/\mathbb{Q}$:

$$p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_s.$$

- Número finito de ramificaciones ($p \mid \Delta_K$).
- $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$,

$$f_1 + \cdots + f_s = [K : \mathbb{Q}].$$

- ¿Con qué frecuencia surgen diferentes particiones de $[K : \mathbb{Q}]$?

# Ejemplo: $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

- $p = 2, 3$ se ramifican
  (ya se ramifican en $\mathbb{Q}(\sqrt[3]{2})$ y $\mathbb{Q}(\zeta_3)$)
- Algunos ejemplos

| $p$ | partición | $p$ | partición | $p$ | partición |
|---|---|---|---|---|---|
| 5 | $2+2+2$ | 41 | $2+2+2$ | 83 | $2+2+2$ |
| 7 | $3+3$ | 43 | $1+\cdots+1$ | 89 | $2+2+2$ |
| 11 | $2+2+2$ | 47 | $2+2+2$ | 97 | $3+3$ |
| 13 | $3+3$ | 53 | $2+2+2$ | 101 | $2+2+2$ |
| 17 | $2+2+2$ | 59 | $2+2+2$ | 103 | $3+3$ |
| 19 | $3+3$ | 61 | $3+3$ | 107 | $2+2+2$ |
| 23 | $2+2+2$ | 67 | $3+3$ | 109 | $1+\cdots+1$ |
| 29 | $2+2+2$ | 71 | $2+2+2$ | 113 | $2+2+2$ |
| 31 | $1+\cdots+1$ | 73 | $3+3$ | 127 | $1+\cdots+1$ |
| 37 | $3+3$ | 79 | $3+3$ | 131 | $2+2+2$ |

# Ejemplo: $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$

- Surge solo $1 + \cdots + 1, 2 + 2 + 2, 3 + 3$.
- ¿Estadística para los primeros $N$ primos?

| $N$ | $1+\cdots+1$ | $2+2+2$ | $3+3$ |
|---|---|---|---|
| 10 | 0.1000 | 0.5000 | 0.4000 |
| 100 | 0.1500 | 0.5200 | 0.3300 |
| 1000 | 0.1570 | 0.5080 | 0.3350 |
| 10000 | 0.1635 | 0.5011 | 0.3354 |
| 100000 | 0.1659 | 0.5004 | 0.3337 |

- Converge a $\frac{1}{6}, \frac{1}{2}, \frac{1}{3}$.

# Ejemplo que podemos entender: caso ciclotómico

- Consideremos $K = \mathbb{Q}(\zeta_7)$
- Factorización depende solo de $p \pmod 7$:

| $p$ (7) | factorización | partición |
|---|---|---|
| 1 | $\mathfrak{p}_1 \cdots \mathfrak{p}_6$ | $1 + \cdots + 1$ |
| 6 | $\mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3$ | $2 + 2 + 2$ |
| $2, 4$ | $\mathfrak{p}_1 \mathfrak{p}_2$ | $3 + 3$ |
| $3, 5$ | $\mathfrak{p}$ | $6$ |

- Dirichlet: $\frac{1}{6}$ primos cumplen $p \equiv a \pmod 7$ para $a = 1, 2, 3, 4, 5, 6$ fijo.

# Estadística

| $N$ | $1+\cdots+1$ | $2+2+2$ | $3+3$ | $6$ |
|---|---|---|---|---|
| 10 | 0.2000 | 0.1000 | 0.3000 | 0.4000 |
| 100 | 0.1700 | 0.1600 | 0.3200 | 0.3500 |
| 1000 | 0.1660 | 0.1660 | 0.3300 | 0.3380 |
| 10000 | 0.1662 | 0.1663 | 0.3324 | 0.3351 |
| 100000 | 0.1668 | 0.1669 | 0.3328 | 0.3336 |

Converge a $\frac{1}{6}$, $\frac{1}{6}$, $\frac{1}{3}$, $\frac{1}{3}$.

# Explicación muy breve

**«Teorema de densidad de Chebotarëv»**

**Videos:**

**cadadr.org/cimat-tna/chebotarev.html**

# ¡Gracias por su atención!