LA CRIBA DE CUERPOS DE NÚMEROS

↝ ES MÁS RÁPIDA QUE LA CRIBA CUADRÁTICA PARA FACTORIZAR NÚMEROS N CON $N > 10^{130}$

IDEA: SI $A, B \in \mathbb{Z}$ SON TALES QUE $A^2 \equiv B^2 \ (N)$, ES PROBABLE QUE $\gcd(A \pm B, N)$ SEA UN FACTOR NO TRIVIAL DE N.

(ÍDEM CRIBA CUADRÁTICA)

DE GRADO CHICO

1. BUSCAMOS $m \in \mathbb{Z} \setminus \{0\}$ Y $f \in \mathbb{Z}[X]$ MÓNICO E IRRED TAL QUE $f(m) \equiv 0 \ (N)$

OBS: SI $f(m) \equiv 0 \ (N)$ Y $f = g \cdot h$ CON $g, h \not\equiv \pm 1$, TENEMOS UNA FACT. DE N: $g(m) \cdot h(m) \equiv 0 \ (N)$
(SI $g(m), h(m) \neq \pm 1 \ldots$)

2. TOMAMOS $\beta \in \mathbb{C}$ RAÍZ DE f. SI $d = \deg f$, CONSIDERAMOS

$$\mathbb{Z}[\beta] := \left\{ c_0 + c_1\beta + \cdots + c_{d-1}\beta^{d-1} \in \mathbb{C} : c_i \in \mathbb{Z} \right\}$$

f IRRED $\Rightarrow$ ESCRIT. ÚNICA...

PROP: $\mathbb{Z}[\beta]$ ES UN ANILLO (UN SUBANILLO DE $\mathbb{C}$)

EJEMPLO: $f(X) = X^2 + 1$

ENTONCES $\beta = i$, $\mathbb{Z}[i] = \{ a + bi : a, b \in \mathbb{Z} \}$ "ANILLO DE ENTEROS GAUSSIANOS"

SUMA: $(a+bi) + (c+di) = (a+c) + (b+d)i$

PROD: $(a+bi) \cdot (c+di) = (ac - bd) + (ad + bc) \cdot i$

EJEMPLO: $f(X) = 1+X+X^2$. SEA β RAÍZ DE f.

- $\mathbb{Z}[\beta] = \{a+b\beta+c\beta^2\}$.

$\beta \in \mathbb{Z}[\beta] \Rightarrow \beta^3 \in \mathbb{Z}[\beta]$. ¿QUIÉN ES?

$1+\beta+\beta^2 = 0 \Rightarrow \beta+\beta^2+\beta^3 = 0 \Rightarrow \beta^3 = -\beta-\beta^2 \in \mathbb{Z}[\beta]$.

3. BUSCAMOS PARES DE ENTEROS (a_i, b_i) $(i=1,\dots,k)$

i. $\prod_{i=1}^{k}(a_i - b_i m)$ ES UN $\square$ EN $\mathbb{Z}$, DIGAMOS A^2

ii. $\prod_{i=1}^{k}(a_i - b_i \beta)$ ES UN $\square$ EN $\mathbb{Z}[\beta]$, DIGAMOS α^2,

SIMULTÁNEAMENTE.

LEMA: $\mathbb{Z}[\beta] \xrightarrow{\varphi} \mathbb{Z}/N\mathbb{Z}$

$c_0+c_1\beta+\cdots+c_{d-1}\beta^{d-1} \longmapsto c_0+c_1 m+\cdots+c_{d-1}m^{d-1}$

ES UN MORFISMO DE ANILLOS

(SE USA: $f(\beta)=0$, $f(m) \equiv 0 \pmod N$) ///

ASÍ, SI LLAMAMOS $B = \varphi(\alpha)$. TENEMOS

$$B^2 = \varphi(\alpha^2) = \varphi\left(\prod_{i=1}^{k}(a_i - b_i\beta)\right) = \prod_{i=1}^{k}(\varphi(a_i - b_i\beta))$$

$$= \prod_{i=1}^{k}(a_i - b_i m) = A^2 \text{ EN } \mathbb{Z}/N\mathbb{Z}$$

i.e., $A^2 \equiv B^2 \,(N)$

¿CÓMO RESOLVEMOS i. Y ii.?

- PARA i., HACEMOS LO MISMO QUE EN LA CRIBA CUADRÁTICA: BUSCAMOS (a_i, b_i) TALES QUE

a-b.m SEA PROD DE PRIMOS CHICOS (= B-SUAVE),
Y DENTRO DE LOS HALLADOS ELEGIMOS (a_i, b_i) TALES QUE
$\prod (a_i - b_i m)$ SEA UN $\square$ EN $\mathbb{Z}$ ($\Leftrightarrow$ LAS POT. DE PRIMOS QUE LO DIVIDEN SON PARES)

- PARA ii. ¿PODEMOS HACER LO MISMO EN EL ANILLO $\mathbb{Z}[\alpha]$? NO TAN FÁCILMENTE... (CAMBIAMOS α POR β...)

EN $\mathbb{Z}[\alpha]$ NO VALE EL TEO. FUND. DE LA ARITMÉTICA (PARA CIERTOS α SÍ VALE! EJ: $\alpha = i$)

EJEMPLO: SEA $f(X) = X^2 + 5$

TOMEMOS $\alpha \in \mathbb{C} / \alpha^2 = -5$. ENTONCES,

$$6 = 2 \cdot 3 = (1+\alpha)\cdot(1-\alpha)$$

AFIRMO: 2, 3, $1+\alpha$, $1-\alpha$ SON IRREDUCIBLES PERO NO SON ASOCIADOS ENTRE SÍ.

DEF: $N : \mathbb{Z}[\alpha] \to \mathbb{Z}$ "LA NORMA" EJ: $N(2) = 4$
$a + b\alpha \mapsto a^2 + 5b^2$ $N(1+\alpha) = 6$

PROP: N ES MULTIPLICATIVA, ie
$N(xy) = N(x)\cdot N(y) \quad \forall x, y \in \mathbb{Z}[\alpha]$. ///

SUPONGAMOS $2 = (a+b\beta)(c+d\beta)$. ENTONCES

$$2^2 = (a^2+5b^2)\cdot(c^2+5d^2)$$

$$\Rightarrow a^2+5b^2 = \begin{cases} 1 \to a = \pm 1,\ b = 0 \text{ ; LUEGO } c = \pm 2,\ d = 0 \\ 2 \to \text{NO} \\ 4 \to a = \pm 2,\ b = 0 \text{ ; LUEGO } c = \pm 1,\ d = 0 \end{cases}$$

/3

$\Rightarrow$ $a+b\beta = \pm 1$ y $c+d\beta = \pm 2$ ó

$a+b\beta = \pm 2$ y $c+d\beta = \pm 1$.

PARA $2, 3, 1+\alpha, 1-\alpha$: ÍDEM.

OBS: • DECIMOS QUE $x, y \in \mathbb{Z}[\alpha]$ SON ASOCIADOS SI $x = u \cdot y$, CON $u \in \mathbb{Z}[\alpha]$ UNIDAD

• DECIMOS QUE $u \in \mathbb{Z}[\alpha]$ ES UNIDAD SI $\exists\, v \in \mathbb{Z}[\alpha]$ / $u \cdot v = 1$.

→ CAMBIAR $\mathbb{Z}[\alpha]$ POR A ANILLO. $A^\times = \{\text{UNIDADES}\}$

EJ: • $\mathbb{Z}^\times = \{\pm 1\}$

• $\mathbb{Z}[\alpha]^\times = ?$ SEGURO $\pm 1 \in \mathbb{Z}[\alpha]$. ¿HAY MÁS?

NO: SEA $x \in \mathbb{Z}[\alpha]^\times$. TENGO $x \cdot y = 1$.

LUEGO, $1 = 1^2 = \underbrace{N(x)}_{\in \mathbb{Z}} \cdot \underbrace{N(y)}_{\in \mathbb{Z}}$

$\Rightarrow N(x) = \pm 1$; SI $x = a+b\alpha$, $N(x) = a^2 + 5b^2$

LUEGO $N(x) = \pm 1$ SII $b = 0$, $a = \pm 1$, i.e. SII $x = \pm 1$.

• CAMBIEMOS α: TOMAMOS $f(X) = X^2 - 5$.

EN ESTE CASO, LA NORMA VIENE DADA POR

$N(x) = a^2 - 5b^2$, SI $x = a + b\alpha$; TAMBIÉN ES MULTIPLICATIVA

(EN GRAL: SI $f(X) = X^2 - d$, LA NORMA VIENE DADA POR $N(x) = \underbrace{a^2 + db^2}_{= x \cdot \bar{x}}$, SI $x = a + b\alpha$, CON $\bar{x} = a - b\alpha$)

YA NO ES CIERTO QUE $N(x) = \pm 1$ SII $x = \pm 1$.

POR EJ, SI $x = 2+\alpha$ ENTONCES $N(x) = 4 - 5 = -1$

x ES UNA UNIDAD: $x \cdot \bar{x} = -1 \Rightarrow x(\underbrace{-\bar{x}}) = 1$

INVERSO DE x

$= -2+\alpha =: y$

OBS: x^m TAMBIÉN ES UNIDAD $\forall m \in \mathbb{N}$

(SU INVERSO: y^m); LAS UNIDADES x^m ($m \in \mathbb{N}$)

SON TODAS DISTINTAS: $x^m = 1 \Rightarrow |x|^m = 1 \Rightarrow |x| = 1$, ABS!

$\rightsquigarrow$ EN $\mathbb{Z}[\alpha]$ HAY INFINITAS UNIDADES. //

IDEALES

SEA $k \in \mathbb{Z}$. SEA $I = \{m \cdot k : m \in \mathbb{Z}\}$

$= \{m \in \mathbb{Z} : k \mid m\}$.

SABEMOS:

- SI $k \mid m_1$ Y $k \mid m_2$, ENTONCES $k \mid m_1 + m_2$

  PUES: $m_1 \in I$ Y $m_2 \in I \Rightarrow m_1 + m_2 \in I$

- SI $k \mid m$ Y $a \in \mathbb{Z}$, ENTONCES $k \mid a \cdot m$

  PUES: $m \in I$ Y $a \in \mathbb{Z} \Rightarrow a \cdot m \in I$.

DEF: A ANILLO, $\emptyset \neq I \subseteq A$ ES IDEAL SI

- $x, y \in I \Rightarrow x + y \in I$
- $x \in I, a \in A \Rightarrow ax \in I$

EJ: SI $x \in A$, $I = \{a \cdot x : a \in A\}$ ES IDEAL

NOT: $I = (x)$, Y LO LLAMAMOS IDEAL PPAL.

¿QUÉ ES UN IDEAL PRIMO?

VOLVAMOS A $A = \mathbb{Z}$, $I = \langle k \rangle$.

k ES PRIMO SI: $k \mid x \cdot y \Rightarrow k \mid x$ ó $k \mid y$

ie, SI: $xy \in I \Rightarrow x \in I$ ó $y \in I$

DEF: $I \subsetneq A$ IDEAL ES PRIMO SI

$xy \in I \Rightarrow x \in I$ ó $y \in I$.

EJEMPLO: $A = \mathbb{Z}[i]$. SEA $I = \langle 2 \rangle$.

I NO ES PRIMO: $(1+i)(1-i) = 2 \in I$,

PERO $1+i, 1-i \notin I$:

SI $1 \pm i = 2 \cdot (a+ib) = (2a) + (2b) \cdot i$ CON $a, b \in \mathbb{Z}$

$\Rightarrow 2a = 1$, $2b = \pm 1$ ABS!

ANTES: DADO A ANILLO, ¿ES TODO IDEAL DE LA FORMA $\langle x \rangle$ CON $x \in A$?

NO: SEA $A = \mathbb{Z}[\sqrt{5}]$, Y SEA

$I = \{ x \cdot 2 + y \cdot (1+\sqrt{5}) : x, y \in A \}$.

PARA ALGUNOS VALE. EJ: $A = \mathbb{Z}$, $A = \mathbb{Z}[i]$

I NO ES PPAL. SUPONGAMOS $I = \langle x \rangle$.

- $2 \in I \Rightarrow 2 = y \cdot x \Rightarrow 4 = N(y) \cdot N(x)$
  $\Rightarrow N(x) \mid 4$
- $1+\sqrt{-5} \in I \Rightarrow N(x) \mid N(1+\sqrt{5}) = 6$

$\Rightarrow N(x) \mid 4, 6 \Rightarrow N(x) \mid 2$

COMO $N(x) = a^2 + 5b^2$, NECESARIAMENTE $x = \pm 1$.

$\Rightarrow 1 \in I$. PERO ESTO ES ABSURDO.

PENSAR: SI $a+b\sqrt{5} \in I \Rightarrow a-b$ ES PAR. //

AÚN SI TODO IDEAL ES PPAL, LA ASIGNACIÓN (SURY.)

$$A \longrightarrow \begin{matrix}\text{IDEALES}\\ \text{DE } A\end{matrix}$$

$$x \longmapsto \langle x \rangle$$

NO ES BIYECTIVA, YA QUE $y = ux$ CON $u \in A^\times$ $\Leftrightarrow \langle y \rangle = \langle x \rangle$; Y VIMOS QUE $A^\times$ PUEDE SER NO TRIVIAL...

TEO: SI $A = \mathbb{Z}[i]$ Ó $\mathbb{Z}[\sqrt{5}]$ Y $I \subsetneq A$ ES IDEAL, ENTONCES

$$I = P_1^{e_1} \cdots P_r^{e_r}$$

PROD. A DEFINIR!

LOS P_i SON LOS DIVISORES PRIMOS DE I

CON P_i PRIMO, $e_i \in \mathbb{N}$; Y ESTA DESC. ES ÚNICA

MÁS AÚN, SI $A = \mathbb{Z}[\alpha]$ CON α RAÍZ DE f, $\exists\ \mathcal{O}_\alpha \supseteq A$ ANILLO EN EL QUE EL TEO VALE PARA $I \subseteq \mathcal{O}_\alpha$ IDEALES. ///

↝ TIENE SENTIDO HABLAR DE IDEALES B SUAVES: AQUELLOS I / $\underbrace{N(P_a)}_{\text{"NORMA"}} \leq B \quad \forall P$ / $P \mid I$.