

Primer prueba: 29/04

Segunda Prueba: 22/05

Tercera Prueba: 01/07

Teoría de Números & Aritmética

trata en un principio, el estudio $\mathbb{Z} = \{0, \pm 1, \dots, \pm n, \dots\}$

anillo comunitativo con 1 y $ab=0 \Rightarrow a=0, b=0$

anillo comunitativo con 1 (pero no es dominio de integración)

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a, b \in \mathbb{Z} \right\} \cong \mathbb{R} \times \mathbb{R}$$

Podemos definir el cuerpo de números racionales (cuerpo cociente)

$$\mathbb{Q} = \left\{ \frac{a}{b}, a \in \mathbb{Z}, b \in \mathbb{Z} - \{0\} \right\}$$

Si se trabaja con $\mathbb{R}(x)$, $\text{Quot}(\mathbb{R}(x)) = \mathbb{R}(x) = \left\{ \frac{f(x)}{g(x)} \mid f, g \text{ pol. } g \neq 0 \right\}$.

\mathbb{Z} es un dominio Euclídeo.

existe $g: \mathbb{Z} \rightarrow \mathbb{N} \cup \{0\}$ (bien ordenado, cada subconjunto tiene un menor elemento)

Si $a, b \in \mathbb{Z}$, $\exists f, r \in \mathbb{Z}$ tal que: $a = bf + r$ con $g(r) < g(b)$ o $r=0$.

Sea $I \subseteq \mathbb{Z}$ ideal. Por definición de ideal

$$a, b \in I \rightarrow a+b \in I, \text{ si } a \in I, c \in \mathbb{Z} \Rightarrow ac \in I$$

$$I = n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\} = (n)$$

(\mathbb{Z} es un dominio de ideales principales)

Un elemento p se dice primo si $p | mn \Rightarrow p | m \circ p | n$.

P se dice irreducible. Si $ab=p \Rightarrow a \in \mathbb{Z}^*, b \in \mathbb{Z}^*$ ($\mathbb{Z}^* = \{\pm 1\}$)

Teoría algebraica de números analítica de números.

Si R es un dominio de integridad. n se dice producto de primos si: $n = p_1 \cdots p_r$, p_i primo.

R se dice factorial, si todo $n \in R - R^*$ es producto de primos.

Así \mathbb{Z}_L es un dominio factorial.

$\left(\begin{array}{ccc} \text{dominio} & \Rightarrow & \text{dominio Ideales} \\ \text{Euclídeo} & \Rightarrow & \text{Principales} \\ & & \Rightarrow \text{dominio} \\ & & \text{factorial} \\ & & (\text{DFU}) \end{array} \right)$

Prop: Todo dominio euclídeo $\in SADIP$.

Def: Se o R un anillo conmutativo, R satisface la condición de cadena ascendente (es noetheriano) si:

$$(*) I_1 \subseteq I_2 \subseteq \dots \subseteq I_n \subseteq \dots \quad I_i \text{ ideal}$$

implica que $\exists N > 0$ con:

$$I = I_N = I_{N+1} = I_{N+2} = \dots$$

dar otra demostración.

Lema: R es noetheriano si todo ideal es finitamente generado.

$(*) \Rightarrow I = \bigcup_{i=1}^{\infty} I_i$ es un ideal. ($a, b \in I$, $a \in I_i$, $b \in I_j \Rightarrow a+b \in I_j$)

$$\Rightarrow a+b \in I_j \subseteq I$$

$a-b$

ca

Si I es finitamente generado todos los generadores están en I_N para $N > 1$.

$I_N = I_{N+1} = \dots = I_N + a_1, a_2, \dots, a_n \in I$

Si existe un ideal J no finitamente generado. Sea $a_1, a_2, \dots, a_n, \dots \in J$

$$a_2 \notin (a_1), a_3 \notin (a_1, a_2)$$

Tome la cadena: $(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \dots$

Así todo dominio de ideales principales es Noetheriano.

Demonstración: Sea $I \subseteq R$ un ideal en R euclídeano. $\exists f(u)$

Sea $n \in I$ tal que $f(n)$ es minimal. ($f(n) = \min f(I - \{0\})$)

Así $1 \leq f(n)$.

Entonces: $I = (n)$.

(n) $\subseteq I$. Sea $m \in I$, pero $m = n + r$, $f(r) < f(n) \Rightarrow r = 0$.

Pero: $r = m - nf$, por lo tanto $r = 0$.

De esto se sigue que: $m = nf$, $(n) \supseteq I$, $(n) = I$.

Prop: Todo dominio de ideales principales es factorial.

Hecho: Todo ideal está contenido en un ideal maximal.

M $\neq R$ y si: $M \subseteq I \subseteq R \Rightarrow I = M \circ I = R$.

M es maximal ssi R/M es cuerpo

P es primo ssi R/P es dominio de integridad

✓ Así M maximal $\Rightarrow P$ primo.

(*) Un elemento $p \in P$ primo ssi (p) es primo.

(*) R un DIP, M maximal, $M = pR = (p)$, p primo.

✓ Sean n un elemento de R cualquiera. $(n) \subseteq M = (p)$, así $n \in (P)$ $\Rightarrow n = p, h_1$ (si $(n) \neq R$)

$(h_1) \neq R \Rightarrow h_1 = p_1 h_2$

iterando el procedimiento:

Asi: $n = p_1 p_2 \dots p_r$

Si $(h_r) = R$ ssi $n \in R^*$. Cuando es una unidad $p_1 p_2 \dots p_r$ es primo.

Falta ver que el procedimiento se detiene.

$(n) \subseteq (h_1) \subseteq (h_2) \subseteq \dots$

Como R es noetheriano $\Rightarrow (h_N) = (h_{N+1})$

$h_N = p_N h_{N+1}$, $t h_N = h_{N+1}$

$$P_{N+1} \in h_N = h_N$$

$$(P_{N+1} - 1) h_N = 0 \quad , \quad h_N \neq 0$$

$P_{N+1} = 1 \quad (\Rightarrow \Leftarrow)$ con P_{N+1} primo.

$\therefore (h_N) = R \quad , \quad h_N \in R^*, \quad h = h_N p_1 \cdots p_N$

Descomposición en primos:

Sea $(\text{Anillo comunitario}, \cdot, +)$ un producto de primos si:
(Dominio de int.) $n = u p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

Unididad, p_i primos.

Se dice que dos elementos del anillo son afines si:

$p_i \sim p_j$ ssi $p_i = u p_j$ (\Leftrightarrow relación de equivalencia, $a = 1 \cdot a$,

Si $a = u b \Rightarrow b = u^{-1} a$, si $a = u b$, $b = v c \Rightarrow a = (u v) c$)

[Podemos suponer que si $p_i \sim p_j \Rightarrow i = j$].

Ejemplo: $4 = 2^2 = (-2)^2 \Leftrightarrow -2 \sim 2$.

Proposición: Si C es un dominio, $n \in C$.

$n = u p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $u \in C^*$, p_i primos.

y $n = v f_1^{\beta_1} \cdots f_s^{\beta_s}$, f_i irreducible, $v \in C^*$

Entonces $r = s$. Procediendo, podemos suponer $p_i \sim f_i$ y $\alpha_i = \beta_i$

Demostración: Por inducción en $\alpha_1 + \alpha_2 + \cdots + \alpha_r$. ($\alpha_r > 0$)

Si $N = 1$, $n = u p_i$, así n es primo.

Lema: Primo \Rightarrow irreducible.

Si n es primo, $n = ab$, como $n | n \Rightarrow n | a$ o $n | b$.

(f.s.) $n | a \Rightarrow a = nt$, $a = abt \Rightarrow bt = 1$, $b \in C^*$ (análogo para b).

Si $n | b \Rightarrow b = nft$, $b = abt \Rightarrow at = 1$, $a \in C^*$.

Si n es primo y $n = v f_1^{\beta_1} \cdots f_s^{\beta_s} \Rightarrow s = 1$ ($\beta_i = 1$, por def. de irred.)

Supongamos $n = u p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $\alpha_r > 0$, entonces $n = p_r h$, con

$h = u p_1^{\alpha_1} \cdots p_{r-1}^{\alpha_{r-1}}$, así $N = \alpha_1 + \cdots + \alpha_{r-1} = N-1$.

Si $n = v f_1^{\beta_1} \cdots f_s^{\beta_s}$.

Como $p_r | n \Rightarrow p_r | f_i$ (olvídmelo), redondeando podemos suponer $i = s$.

Así $Pr \in fs$, luego: $fs = tPr \Rightarrow t \in C^*$ (pues pr no es unidado)
 $\therefore pr \sim fs$.

Es decir

$$n = (v f_1^{\beta_1} \dots f_s^{\beta_{s-1}}) fs$$

$$n = (v f_1^{\beta_1} \dots f_s^{\beta_{s-1}}) w pr$$

$$h_1 = (v f_1^{\beta_1} \dots f_s^{\beta_{s-1}}) w$$

$$h_1 = (vw) f_1^{\alpha_1} \dots f_r^{\alpha_{r-1}}$$

$$h_1 = n \cdot p_1 x_1 \dots p_r x_{r-1}$$

Casos: I) Si: $\alpha_r \geq 1, \beta_s > 1 \Rightarrow r=s$

reordenando podemos suponer que: $f_i \sim p_i$ y $\alpha_i = \beta_i$.

Como ya sabemos que $Pr \sim fs$ Sobreordenaremos $f_1 \dots f_{s-1}$.

$$\alpha_{r-1} = \beta_{s-1}, \alpha_r = \beta_s$$

II) Si: $\alpha_r = \beta_s = 1$.

$$h_1 = (vw) f_1^{\beta_1} \dots f_{s-1}^{\beta_{s-1}}$$

$$h_1 = n \cdot p_1^{\alpha_1} \dots p_{s-1}^{\alpha_{s-1}}$$

Así: $r-1 = s-1 \Rightarrow r = s$ y $f_i \sim p_i$ (reordenando), $\alpha_i = \beta_i, i \in \{1, \dots, r-1\}$

y $pr = fs \sim pr$, $\alpha_r = \beta_s = \beta_r = 1$.

III) Si: $\alpha_r > 1; \beta_s = 1$

$$Pr[n_1 = n \cdot p_1^{\alpha_1} \dots p_r^{\alpha_{r-1}}] \quad \alpha_r > 1$$

$$h_1 = (vw) f_1^{\beta_1} \dots f_{s-1}^{\beta_{s-1}}$$

entradas: $p_i | f_i$, $\alpha_i \neq \beta_i \quad 1 \leq i \leq s-1$,
 (no ocurre).

IV) $\alpha_r = 1; \beta_s > 1$.

$$Pr \sim fs \mid h_1 = (vw) f_1^{\beta_1} \dots f_s^{\beta_{s-1}} \quad \left(Pr \models \alpha = (vw) f_1^{\alpha_1} \dots f_s^{\alpha_{s-1}} \Rightarrow Pr \models \alpha = (tvw) \right)$$

Luego: $Pr \mid h_1 = n \cdot p_1^{\alpha_1} \dots p_{r-1}^{\alpha_{r-1}} \Rightarrow Pr \models p_i$ (\neq)

(no ocurre) \rightarrow M como se formaron las producciones

\S : Si tiene una descomposición en primos, esta es "esencialmente" la única descomposición en irreducibles.

Ejemplo: $\mathbb{Z}(\sqrt{-5}) = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$

$$21 = 3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5}).$$

$$\text{y } N(a + b\sqrt{-5}) = a^2 + 5b^2 \quad (\text{y } N(zw) = N(z)N(w) \text{ y } N(z) \in \mathbb{Z})$$

$$\text{Si } 3 = z_1 z_2 \Rightarrow N(3) = p = N(z_1)N(z_2)$$

$$(\text{Si } N(z) = 1 \Rightarrow z\bar{z} = 1 \Rightarrow z \in \mathbb{Z}(\sqrt{-5})^*)$$

$$\text{Así: } N(z_1) = N(z_2) = 3 \text{ y claramente } a^2 + 5b^2 \neq 3.$$

$\therefore 3$ es irreducible

$$\mathbb{Z}(\sqrt{-5}) / 3\mathbb{Z}(\sqrt{-5}) \text{ no es un dominio.}$$

Sin embargo, 3 no es primo en $\mathbb{Z}(\sqrt{-5}) \Rightarrow$

Def: C es un DFU si cada elemento en $C - C^*$ es un producto de primos.

Coro: Si C es un DFU la def. en irreducibles en C es válida.

Prop: En un DFU todo irreducible es primo.

Dem: Sea f irreducible.

$$f = \prod_{i=1}^r p_i^{e_i} \text{ Como } f \in C - C^* \Rightarrow r \geq 1$$

$$\therefore f \mid p_1.$$

obs: $\mathbb{Z}(\sqrt{-5})$ no es un DFU \Rightarrow no es un D.EP \Rightarrow no es un D. euclídeo.

Polinomios : en cualquier dominio de integridad:

$$D(x) = \{ a_n x^n + \dots + a_1 x + a_0 \mid a_i \in D\}$$

Si: $f(x) = a_n x^n + \dots + a_0$; $g(x) = b_m x^m + \dots + b_0$

$$f + g(x) := (a_n + b_m) x^{n+m} + \dots + (a_0 + b_0)$$

$$fg(x) := c_{n+m} x^{n+m} + \dots + c_0, \text{ donde } c_i = \sum_{i=j+k} a_j b_k$$

Si: Dominio: $\mathcal{Z}(fg) = \mathcal{Z}f \cdot \mathcal{Z}g$.

Dem: Si: $f(x) = a_n x^n + \dots + a_0$, $a_n \neq 0$, $g(x) = b_m x^m + \dots + b_0$, $b_m \neq 0$.

$$fg(x) = c_{n+m} x^{n+m} + \dots + \text{constant}, \text{ si } n+m > 0.$$

$$c_{n+m} = a_n b_m \neq 0.$$

Def:

• $\mathbb{Z}(x)$ no es dominio de ideales principales.

Sea x primo ($\mathbb{Z}(x)/x\mathbb{Z}(x) \cong \mathbb{Z}$, dominio de integridad)

Además: $\mathbb{Z}(x)/3\mathbb{Z}(x) \cong \mathbb{Z}_3[x]$ (en general $D/\mathbb{I}(x) \cong D(x)/\mathbb{I}(x)$)

∴ 3 es primo.

Sea $\mathbb{I} = (x, 3) = (d)$ entonces: $d \mid 3$, $d \mid x$ ($x \in (d)$ y $3 \in (d)$)

Así: $(d) = (1) \cong \mathbb{Z}(x)$

Pero: $\mathbb{Z}(x)/(3, x) \cong \frac{\mathbb{Z}(x)/(x)}{(3, x)/(x)} = \frac{\mathbb{Z}}{(3)} \cong \mathbb{Z}/3\mathbb{Z} \neq 0$

∴ $(3, x) \neq (1)$ ∴ no es un DIP.

Prof: D un DFU $\Rightarrow D(x)$ es un DFU. ↗ no se alcanza

Sean $n, m \in D$: $n = u p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $m = v p_1^{\beta_1} \dots p_r^{\beta_r}$

Se define $m \subset M = p_1^{\max\{\alpha_1, \beta_1\}} \dots p_r^{\max\{\alpha_r, \beta_r\}}$

$M \subset D = p_1^{\min\{\alpha_1, \beta_1\}} \dots p_r^{\min\{\alpha_r, \beta_r\}}$

Lo mismo puede ocurrir para definir $N(f)$ con los NCD de los elementos b_1, \dots, b_n .

Sea $f(x) = a_n x^n + \dots + a_0$. Sea $d = N(f) = \text{NCD}\{a_1, \dots, a_n\}$.
 $a_i = b_i d$

Así: $f(x) = (b_n x^n + \dots + b_0) d = d f_0(x)$, donde $f_0(x) = b_n x^n + \dots + b_0$

Definición de $N(f)$: $N(f_0) = 1$.

f_0 se dice primitivo si $N(f_0) = 1$.

(f_0 es primitivo si $p \in f_0$ para todo p primo de D).

Así: $f_0(x) \neq 0$ en $D(x)/P(D(x))$ para todo p primo de D .

Obs: El producto de dos polinomios es primitivo.
Si $f_0(x) p_0(x) = 0$ en $D(x)/P(D(x))$: algún p primo de D divide a $f_0(x)$ o a $p_0(x)$.
 $\Rightarrow f_0(x) = 0$ ó $p_0(x) = 0$.

Así si: $f(x) = N(f) f_0(x)$, $p(x) = N(p) p_0(x) \Rightarrow f p(x) = N(f) N(p) f_0 p_0(x)$
 $\Rightarrow N(f p) = N(f) N(p)$.

Si D es un dominio, se define el cuerpo de cocientes K :

$$K = \left\{ \frac{a}{b} ; a, b \in D, b \neq 0 \right\} \text{ y } \frac{a}{b} = \frac{c}{d} \text{ si } a d = b c$$

$D(x) \subset K(x) \subset D[\bar{P}]$ (entre ambos de división).

Sea $f(x) \in K(x)$: $f(x) = \frac{a_n x^n + \dots + a_0}{b_n x^n + \dots + b_0} = \frac{a_n b_{n-1} \dots b_0 x^n + \dots + a_0 b_{n-1} \dots b_0}{b_n \dots b_0}$

Así $f(x) = \frac{p(x)}{b}$, $p(x) \in D(x)$, $b \in D - \{0\}$.

(Se define). Entonces: $N(f) = \frac{N(p)}{b} \in K$ (el número es único).

Si $f(x) = \frac{f(x)}{b} = \frac{f'(x)}{b'} \Rightarrow b' p(x) = b p'(x)$

$$\text{Así } v(b^l p) = v(b p^l) \Rightarrow b^l v(p) = b v(p^l)$$

$$\Rightarrow \frac{v(p)}{b} = v(p^l).$$

Luego: $f(x) = \frac{g(x)}{b} = \frac{v(p)p_0(x)}{b} = v(f)p_0(x)$. \leftarrow Primitivo en D

$$f(x) = v(f)p_0(x) \quad (f_0(x) = p_0(x)). \quad \forall f \in K(x)$$

Resumen para el caso de salvo unididad:

Si $f(x) = u f_0(x)$, $u \in K$, f_0 primitivo.

$$\frac{1}{b} f_0(x) = \frac{1}{b} f_0(x) \quad (\text{salvo unid})$$

$$\text{y } f_0(x) = c_0 f_0(x) \Rightarrow f_0(x) = u f_0(x), u \in D^*$$

(*) Si $f(x) = f_0(x)h(x) \Rightarrow f_0(x) = f_0(x)h_0(x)$ en $D(x) \subset K(x)$
en $K(x)$.

Si $f_0(x)$ es irreducible en $D(x)$, entonces f es irreducible en $K(x)$.

Pero $K(x)$ es un D.F.U (irred \Rightarrow primo).

Ej.: Se $p(x)$ primitivo en $D(x)$ e irreducible en $K(x)$, entonces $p(x)$ es primo en $D(x)$.

(Lema de Gauss)

Dem: Sean $a(x), b(x) \in D(x)$ con $p(x) | a(x)b(x)$. Entonces $p(x) \in D(x) \subset K(x)$

Luego $p(x) | a(x)$ o $p(x) | b(x)$ en $K(x)$.

Supongamos que $p(x) | a(x) \Rightarrow a(x)^l = N(a), a_0(x) = v(a) P_0(x) f_0(x)$

$$= \dots = p(x) \underbrace{(N(a) f_0(x))}_{\in D(x)}$$

$$p(x) | a(x)$$

Luego p es primo en $D(x)$.

$$(x)^l q_0 = 1 \quad \text{y} \quad (x)^l = 1 \quad \text{y} \quad q_0 = 1$$

Prop: D es un DFU $\Rightarrow D(x)$ es un DFU.

Def: Sea $h(x) \in DFU$:

$h(x) = \lambda p_1^{d_1} \cdots p_r^{d_r}$ en $K(x)$, $\lambda \in K^*$, p_i primo en $K(x)$.

Pero:

$p_i(x) = N(p_i) P_{i0}(x) \leftarrow$ Primitivo.

$P_{i0}(x)$ es primo en $D(x)$ (Lema anterior).

Así:

$$h(x) = (\underbrace{\lambda N(p_1)^{d_1} \cdots N(p_r)^{d_r}}_{N(x) \in D}) P_{i0}^{d_1}(x) \cdots P_{r0}^{d_r}(x)$$

$$N(x) = u \cdot f_1^{B_1} \cdots f_r^{B_r} \xrightarrow{\text{primos en } D} \text{constantes}$$

$$h(x) = u \cdot f_1^{B_1} \cdots f_r^{B_r} P_{i0}^{d_1}(x) \cdots P_{r0}^{d_r}(x)$$

Ejemplo: $8x^2 - 8 = 2^3 (x+1)(x+1)$ en $\mathbb{Z}[x]$. $\mathbb{Z}[x] \cong \frac{\mathbb{Z}[x]}{(x+1)}$

$$\text{Puedemos } \mathbb{Z}[1/x] = \{f(1/x) | f \in \mathbb{Z}[x]\}$$

Sea:

$\Psi: \mathbb{Z}[x] \rightarrow \mathbb{Q}$ homomorfismo.

$$\therefore \mathbb{Z}[1/x] \leq \mathbb{Q} \text{ (Subanillo)}$$

$$\mathbb{Z}[1/x] \cong \frac{\mathbb{Z}[x]}{(x+1)}$$

Si $f \in \ker \Psi_{1/x} \Rightarrow f(1/x) = 0$ $\Leftrightarrow (x+1) \mid f(x) \Rightarrow f(x) = (2x+1) f_0(x)$ \leftarrow Primitivo

Así: $\ker \Psi_{1/x} = (2x+1)$, luego: $\mathbb{Z}[1/x] \cong \frac{\mathbb{Z}[x]}{(2x+1)} = (x+1) \cong \mathbb{Z}$

$$(x+1)^2 + (x+1)x^2 = (x^2 + 2x + 1) + (x^3 + x^2) = x^3 + 3x^2 + 2x + 1$$

Algoritmo de división para polinomios:

K cuerpo, $k[x]$, $m(x) = n(x)f(x) + r(x)$, $\deg r < \deg f$, $r=0$.

\mathbb{Z}_x (un anillo conmutativo).

$n, m \in \mathbb{C}[x]$, n monólico.

$$m(x) = n(x)f(x) + r(x)$$

Con $\deg r < \deg n$ o $r=0$.

además \mathbb{Z}_x es dominio, Esta descomp. es única.

Demo: Por inducción en el grado de $m(x)$.

Si $\deg m > \deg n$, $f = m$, $r = 0$.

Si $\deg m \leq \deg n$

$$m(x) = q_n x^n + \dots + q_0 \quad (-n \leq m < n)$$

$$n(x) = x^n + \dots + b_0$$

$$m_1(x) = m(x) - q_n n(x)x^{n-n} = \deg m < \deg n$$

Por hip. de inducción:

$$m_1(x) = n(x)q_1(x) + r(x) \Rightarrow r(x) = m_1(x) - n(x)q_1(x)$$

$$m(x) = n(x)(q_1(x) + q_n x^{n-n}) + r(x)$$

Unicidad:

$$\text{Si } m(x) = n(x)f(x) + r(x) = n(x)f'(x) + r'(x)$$

$$\text{Así: } n(x)(f(x) - f'(x)) = r'(x) - r(x) \quad (\text{grado aditivo, pues es dominio}).$$

$$\Rightarrow \deg n \leq \deg(r' - r) \leq \max\{\deg r, \deg r'\}$$

luego $f = f'$.

Ej: $\mathbb{Z}[i]$.

$$\mathbb{Z}[i] \cong \frac{\mathbb{Z}(x)}{(x^2+1)} \quad \text{si } f(x) \in \mathbb{Z}(x) \text{ es primo}$$

$$f(x) = (x^2+1) p(x) + (ax+b) \Rightarrow f(i) = ai+b$$

$$\text{Así: } \mathbb{Z}[i] = \mathbb{Z} \oplus i\mathbb{Z}.$$

(*) Si $\alpha \in \mathbb{Q}$, α es algebraico si $f(\alpha) = 0$, para algun $f \in \mathbb{Q}(x)$, $f \neq 0$.

Es decir $\varphi_\alpha: \mathbb{Q}(x) \rightarrow \mathbb{Q}$ no es inyectiva.

$\text{Ker } \varphi_{\alpha} \neq \{0\}$. (pues es D.E.)

$\text{Ker } \varphi_{\alpha} = \langle m_{\alpha}(x) \rangle$ (m_{α} es un polinomio). Se dice que el polinomio,

irreducible de α). ($m_{\alpha}(x) \in \mathbb{Q}(x)$ irreducible de α).

Así: $\mathbb{Q}(\alpha) \cong \frac{\mathbb{Q}(x)}{(m_{\alpha}(x))}$, polinomio irred. de α . (monico).

Def = Dimension de un entero algebraico. Si $m_{\alpha}(x) \in \mathbb{Z}(x)$

Si α es un entero algebraico, con $\deg m_{\alpha} = n$, entonces:

Se define: $\mathbb{Z}(\alpha) \cong \frac{\mathbb{Z}(x)}{(m_{\alpha}(x))}$

Si $m(x) \in \mathbb{Z}(x)$

$$m(x) = f(x) m_{\alpha}(x) + r(x)$$

$$m(\alpha) = r(\alpha) \text{ (unico } r, \text{ con } r < \deg m_{\alpha})$$

$$\therefore \mathbb{Z}(\alpha) \cong \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \dots \oplus \mathbb{Z}\alpha^{n-1}$$

Ej: $x^2+5 = m_{\alpha}(x)$
 $\mathbb{Z}(\sqrt{-5}) \cong \mathbb{Z} \oplus \mathbb{Z}(\sqrt{-5}) \cong \{a+b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.

$$x^3-2 = (m_{\alpha}(x))^{(3-2)} + (m_{\alpha}(x))^{(3-2)} + \dots + (m_{\alpha}(x))^{(3-2)} \cong \{a+b\sqrt[3]{2}+c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}.$$

$$\mathbb{Z}(\sqrt[3]{2}) \cong \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}\alpha^2$$

$$\mathbb{Z}(\sqrt[4]{2}) = \left\{ \frac{a}{2^t} \mid a \in \mathbb{Z}, t \in \mathbb{N}_0 \right\}.$$

Claramente: $\frac{q}{2^t} = f\left(\frac{1}{2}\right)$, con $f(x) = q \cdot x^t$.

$$\text{Sea } f(x) \in \mathbb{Z}[x] \Rightarrow f\left(\frac{1}{2}\right) = a_n\left(\frac{1}{2}\right)^n + \dots + a_0 = \frac{a_1 + \dots + a_0}{2^n}.$$

$\therefore \frac{1}{2}$ no es un entero algebraico.

$$+ m_{1/2}(x) = x - \frac{1}{2} \notin \mathbb{Z}[x].$$

Pr^oof: Sea $n, m \in D(x)$ el dominio

$$h(x) = a_N x^N + \dots + a_0 \in D$$

y S el conjunto de representantes de $D/(a_N)$ que incluye al cero.

Entonces existe $f(x), r(x) \in D(x)$, $s(x) \in S$ tal que:

$$2r < 2n \text{ con } m(x) = f(x)h(x) + s(x)x^{\deg n} + r(x)$$

y son suizas.

Dem: Por inducción en $\deg m$.

Si $2m < 2^n$, tomamos $f, s = 0$ y $r = m$.

$$\text{Si } m(x) = b_N x^N + \dots + b_0 \quad M > N.$$

$$b_N = s + a_N l, \quad s \in S, l \in D.$$

$$\text{Sea } m_1(x) = m(x) - s x^N - l h(x) x^{N-N}, \text{ luego } \deg m_1 < \deg m$$

$$\text{Luego: } m_1(x) = f_1(x)h(x) + s_1(x)x^N + r(x)$$

$$\text{Así: } m(x) = m_1(x) + s x^N + l h(x) x^{N-N}$$

$$= f_1(x)h(x) + s_1(x)x^N + r(x) + s x^N + l h(x) x^{N-N}$$

$$\therefore m(x) = m_1(x)(f_1(x) + l x^{N-N}) + (s_1(x) + s x^{N-N})x^N + r(x)$$

□

Si hubiesen dos expresiones:

$$f(x) \cdot h(x) + s(x) \cdot x^n + r(x) = f'(x) \cdot h(x) + s'(x) \cdot x^n + r'(x)$$

Algoritmo de división:

Si $m, n \in D$ - sol, existen $f, r \in D$ tales que $(m, n) = f(r) \cdot m + r(n)$
 $m = h \cdot f + r$ $r(n) < p(n)$

Tomemos el ideal: $(m, n) = (m) + (n) = \{a_m b_n | a, b \in D\}$

Como todo DE, es un DIP:

$$(m, n) = (f)$$

¿Cuales f ? Debe cumplir:

$$1) f|m \quad f|n \quad \text{y} \quad f \mid (m, n)$$

$$2) f = m + n \text{ si y solo si } f \in (m, n) \quad \text{y} \quad m + n = nf$$

y si $r|m$ y $r|n \Rightarrow r|f$.

f es el máximo común divisor.

Observaciones: Si $s = q(m + n) + r$, entonces $(n, m) = (m, r)$. (Esto ya fue)

$$n = u \cdot f, \quad m = v \cdot f, \quad r = w \cdot f$$

$$\text{Matricialmente: } \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ f & 1 \end{pmatrix} \begin{pmatrix} n \\ m \end{pmatrix}, \quad \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -f & 1 \end{pmatrix} \begin{pmatrix} n \\ m \end{pmatrix}$$

$$\text{Luego: } f = (s + t) \begin{pmatrix} u \\ m \end{pmatrix} = (s + t) \begin{pmatrix} 1 & 0 \\ f & 1 \end{pmatrix} \begin{pmatrix} n \\ r \end{pmatrix} = (s + t) + \begin{pmatrix} n \\ r \end{pmatrix} = n(s + t) + tr$$

$$\text{Así: } f = (n, m) = (n, r)$$

Escribo cada ideal como el menor (nodo-por) elemento (nodo) de los más pequeños en el sentido de \leq . (en D).

$$= \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix} \begin{pmatrix} 82 & -57 \\ -23 & 16 \end{pmatrix} \begin{pmatrix} 244 \\ 351 \end{pmatrix} = \begin{pmatrix} 82 & -57 \\ -351 & 244 \end{pmatrix} \begin{pmatrix} 244 \\ 351 \end{pmatrix} = \begin{pmatrix} 82 \cdot 244 - 57 \cdot 351 \\ 0 \end{pmatrix}$$

luego $= 82 \cdot 244 - 57 \cdot 351.$

si tenemos la fracción:

$$\frac{1}{244-351} = \frac{82 \cdot 244 - 57 \cdot 351}{244 \cdot 351} = \frac{82}{351} - \frac{57}{244}.$$

otro ejemplo:

$$\frac{1}{(x^2+1)(x^2+3)} = \frac{\frac{1}{2}((x^3+3)-(x^1+1))}{(x^2+1)(x^2+3)} = \frac{\frac{1}{2} \cdot \frac{1}{x^2+1}}{x^2+1} - \frac{\frac{1}{2} \cdot \frac{1}{x^2+3}}{x^2+3}.$$

$$\frac{x^2+3-x^2+1}{2} = \frac{4}{2} = 2$$

Congruencia: $x^2+3 \equiv x^2+1 \pmod{2}$

Def: Domínio. $I \subseteq D$ ideal $\Leftrightarrow I + D = D$

ssi: $b-a \in I \Leftrightarrow b \equiv a \pmod{I}$ (escribo como: $a \equiv b \pmod{I}$)

Esto es equivalente a decir que:

$$a+I = b+I$$

Si: $a \equiv b \pmod{I}$, $c \equiv d \pmod{I}$ (transpaso de los op. el anillo cociente)

$$a+c \equiv b+d \pmod{I}$$

$$ac \equiv bd \pmod{I}$$

$$a-c \equiv b-d \pmod{I}$$

Si: $a+x \equiv b \pmod{I}$: se $x \equiv b-a \pmod{I}$ (es solución).

Si tenemos: $a, x \equiv b \pmod{I}$: tiene solución única si a es invertible en el anillo cociente.

Si: $D = \mathbb{Z}$, $I = (\rho)$: $a, x \equiv b \pmod{\rho}$ tiene solución si $a \not\equiv 0 \pmod{\rho}$

$$(Ejemplo: \mathbb{Z}/(n) \cong \mathbb{F}_\rho \text{ para } \rho = n)$$

Más generalmente, si $(m, n) = 1$ entonces:

$$l = mt + ns.$$

$$l \equiv mt + ns \pmod{n}$$

$$l \equiv mt \pmod{n}$$

Así m es invertible \pmod{n} .

$$t \equiv m^{-1} \pmod{n}.$$

Un ejemplo: $244^{-1} \equiv 82 \pmod{351}$.

O sea si queremos resolver la ecuación:

$$244x \equiv 3 \pmod{351}$$

$$x \equiv 3 \cdot 82 \equiv 246 \pmod{351}.$$

Otro procedimiento:

$$244x \equiv 3 \pmod{351}.$$

$$244x + 351y \equiv 3, \text{ al puro } y \in \mathbb{Z}, x = \frac{3 - 351y}{244}.$$

$$107y \equiv 3(244).$$

$$107y + 244t = 3, \text{ al puro } t \in \mathbb{Z}, y = \frac{3 + 244 \cdot 32}{107}$$

$$244t \equiv 3(107) \pmod{107}$$

$$30t \equiv 3(107)$$

$$30(t + 107s) = 3 + 30s, t = -32$$

$$-107s \equiv 3(30) \pmod{30}$$

$$-107s \equiv 3(30) \pmod{30}$$

$$13u \equiv 3(17), u = 9$$

$$3u + 17v = 3, v = -5$$

$$-51v \equiv 3(13)$$

$$4v \equiv 3(13)$$

$$v = 4$$

Su permutación se puede calcular

$$13^{-1} \equiv x \pmod{243}$$

$$13 = 1+12 \quad \text{pues } 12^5 = 3^5 \cdot 4^5 \equiv 0$$

$$13^{-1} = 1 - 12 + 12^2 - 12^3 + 12^4 = \frac{1}{1+12}$$

$$= 1 - 12 + 144 - 27 + 81 = 226 - 39 = 187$$

$$\begin{aligned} 12^3 &= 268 \cdot 6 \\ &\equiv 45 \cdot 6 = 270 \equiv 27 \end{aligned}$$

$$12^4 = 27 \cdot 12 = 324 \equiv 81$$

funciona pues $x^r \equiv 0 \pmod{a}$.

$$\frac{1+x^r}{1+x} = 1 - x + x^2 - x^3 + x^4$$

$$\frac{1}{1+x} \equiv 1 - x + x^2 - x^3 + x^4 \pmod{a}.$$

Sea A anillo comunitativo y $a \in A$ nilpotente ($\exists r \in \mathbb{N}, a^r = 0$, sólo si $r \in \mathbb{N}_{\geq 0}$)
 $\ell: \mathbb{Z}[x] \rightarrow A$ tal que $\ell(x) = a$. (homomorfismo de anillos)

Aplicaremos esto:

$$\sqrt{13} \equiv x \pmod{27}$$

$$\sqrt{13} = \sqrt{1+12} = 1 + \binom{12}{1} x + \binom{12}{2} x^2$$

$$= 1 + \frac{1}{2} \cdot 12 - \frac{1}{8} \cdot 12^2$$

$$= 1 + 6 - 18 \equiv 16 \pmod{27}.$$

• $I+J \subseteq C$ son comaximales si $I+J = C$

Prop: Si I, J son comaximales entonces

$$IJ = I \cap J \iff I \subseteq C \text{ o } J \subseteq C$$

Dem: Claramente $I \supseteq IJ$, $J \supseteq IJ$, así $I \cap J \subseteq IJ$.

Sea $a \in IJ$: $a = \frac{i+j}{k}$

$$\text{entonces: } a = a \cdot 1_C = \frac{a \cdot i + a \cdot j}{k} \in I \cap J \iff a \in I \text{ y } a \in J$$

en un DIF: $(n)+(m) = (f+n)I \cap (g+m)J$

ssi n, m son relativamente primos.

Prop: (Teorema Chino de los Restos) Si $I, J \subseteq C$ son comaximales

$$\text{entonces: } C/IJ \cong C/I \times C/J$$

o bien: $C/IJ \cong C/I \times C/J$

Dem: Sea $\pi_1: C \rightarrow C/I$, $\pi_2: C \rightarrow C/J$ homomorfismos

$$\varphi = \pi_1 \times \pi_2: C \rightarrow C/I \times C/J$$

Demostremos que $\ker \varphi = IJ$.

$$\begin{aligned} \text{Observemos: } \ker \varphi &= \{ c \in C : c + I = I, c + J = J \} \\ &= \{ c \in C : c \in I, c \in J \} = IJ. \end{aligned}$$

Más intuitivamente: Sea $(b+I, a+J) \in C/I \times C/J$. pd: existe $\bar{c} \in C$:

$$c+I = b+I, c+J = a+J.$$

Sabemos que: $c = i+j \in I+J$

$$i \equiv b \pmod{J}, i \equiv 0 \pmod{I}$$

$$j \equiv a \pmod{I}, j \equiv 0 \pmod{J}$$

para encontrar

$$c \equiv b \pmod{I}$$

$$c \equiv a \pmod{J}$$

Sea $c = jb + ia$. Así:

$$c \equiv 1 \cdot b + 0 \cdot a \equiv b \pmod{I}$$

$$\therefore c \equiv 0 \cdot b + 1 \cdot a \equiv a \pmod{J}.$$

∴ φ es epíjetina

Prop: Si I, J son comunitiales, el sistema:

$$\begin{cases} x \equiv b \pmod{I} \\ x \equiv a \pmod{J} \end{cases}$$

Siempre tiene solución única módulo $I \cap J$.

Es única porque: c es única módulo $I \cap J$.

$$c \equiv d \pmod{I} \text{ por soluciones de (*)}$$

$$c \equiv d \pmod{J}$$

$$c - d \in I, c - d \in J \Rightarrow c - d \in I \cap J$$

Así:

Luego: $c - d \equiv 0 \pmod{I \cap J}$.

En un DIP: n, m primos relativos: $I = nt + ms$

$$\text{y tener el sistema: } \begin{cases} x \equiv b_1 \pmod{n} \\ x \equiv b_2 \pmod{m} \end{cases}$$

$$\Rightarrow x = a_1 nt + b_1 ms \pmod{mn}$$

$$x \equiv a_1 nt \pmod{m}$$

$$\therefore x \equiv a_1 nt \pmod{m} \quad (I)$$

$$(I) \text{ y } (II) \Rightarrow x \equiv a_1 nt + b_1 ms \pmod{mn}$$

$$(II) \text{ y } (III) \Rightarrow x \equiv a_1 nt + b_2 ms \pmod{mn}$$

$$(III) \text{ y } (I) \Rightarrow x \equiv a_1 nt \pmod{m}$$

Un ejemplo: $\begin{cases} x \equiv 5 \pmod{12} \\ x \equiv 7 \pmod{19} \end{cases}$

obsérvese:

$$19 = 12 \cdot 1 + 7$$

$$12 = 7 \cdot 1 + 5$$

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0.$$

luego:

$$x = -5 \cdot 19 + 8 \cdot 12 \pmod{12 \cdot 19}$$

luego:

$$x \equiv -5 \cdot 19 + 8 \cdot 7 \cdot 12 \pmod{12 \cdot 19}$$

$$\equiv -19 - 12 \pmod{12 \cdot 19}$$

$$\equiv -27 \pmod{12 \cdot 19}$$

otra forma:

$$x \equiv 7 \pmod{5}, x = 7 + 5k$$

$$7 + 5k \equiv 7 \pmod{12}$$

$$7 + 7k \equiv 7 \pmod{12}$$

$$7k \equiv 0 \pmod{12}, k \equiv 34 \pmod{12} \equiv 10 \pmod{12}$$

$$x \equiv 7 + 19 \cdot 10 \equiv 197 \pmod{12 \cdot 19}$$

Sistemas:

$$\begin{cases} x_1 \equiv 1 \pmod{12} \\ x_1 \equiv 0 \pmod{19} \end{cases}$$

$$19k \equiv 1 \pmod{12}$$

$$7k \equiv 1 \pmod{12}$$

$$k \equiv 7 \pmod{12} \Rightarrow x_1 \equiv 7 \cdot 19 \pmod{12 \cdot 19}$$

$$\begin{cases} x_2 \equiv 0 \pmod{12} \\ x_2 \equiv 1 \pmod{19} \end{cases}$$

$$12k \equiv 1 \pmod{19}$$

$$12k + 19r = 1$$

$$19r \equiv 1 \pmod{12} \Rightarrow r = -\frac{19 \cdot 7}{12} = -11$$

$$r = 7$$

$$x_2 \equiv 12 \cdot 11 \pmod{12 \cdot 19}$$

Sea $A = A_1 \times A_2$ producto de anillos unitarios.

$$P = (10)$$

$$1-P = (0,1) = P^c$$

$$P + P^c = 1$$

$$P \cdot P^c = 0$$

$$\text{P es idempotente} \quad P^2 = P \text{ y } (1-P)^2 = 1-2P+P^2 = 1-P$$

Si P es un idempotente, P/P^c es idempotente.

y PA, P^cA son ideales:

- $P = P + P^c$ Son comoduales

y ¿Qué es $P \cap P^c A$?

$$\text{Si } c = P \alpha = P^c b$$

$$Pc = PP\alpha = P\alpha \stackrel{\text{pues } P^2 = P}{=} c \stackrel{\text{pues } P^2 = P}{=} 0 \quad \text{y } P \alpha \in P \cap P^c A$$

$$Pc = PP^c b = 0 \quad \text{y } P^c A = P^c A$$

$$\text{Así: } A \cong A/\{0\} \cong A/P \cap P^c A \cong A/PA \times A/P^c A$$

Observación:

$$P + P^c = 1$$

$$P \equiv 0 \pmod{PA}$$

$$P \equiv 1 \pmod{P^c A}$$

(b) Se muestra si: $i+j=1 \Rightarrow \bar{i}, \bar{j}$ son idempotentes complejos unitarios en C/IJ .

$$\bar{i}^2 = \bar{i}^2 + \bar{i}\bar{j} = \bar{i}(\bar{i}+\bar{j}) = \bar{i}(1) = \bar{i}$$

$$j = \bar{i} - i$$

$\therefore \bar{i}, \bar{j}$ son idempotentes.

en el ejemplo anterior $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rightsquigarrow \frac{7 \cdot 19}{11 \cdot 12} \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Ejercicio: Corrobore que: $(7 \cdot 19)^2 \equiv 7 \cdot 19 \pmod{12 \cdot 19}$.

Ejemplo: $\mathbb{Z}/_{12\mathbb{Z}} \cong \mathbb{Z}/_4\mathbb{Z} \times \mathbb{Z}/_3\mathbb{Z}$

$$p_1 = 4 \pmod{12}$$

$$p_1^c = -3 = +9 \pmod{12}$$

luego todos los idempotentes son $4, 9, 10$.

$$\mathbb{Z}/_{30\mathbb{Z}} \cong \mathbb{Z}/_{12\mathbb{Z}} \times \mathbb{Z}/_3\mathbb{Z} \times \mathbb{Z}/_{5\mathbb{Z}}$$

$$6^2 \equiv 6 \pmod{30}$$

$$10^2 \equiv 10 \pmod{30}$$

$$(P+Q)^2 = P + 2PQ + Q = P + Q \text{ si } PQ = 0$$

$$\text{ssi: } 6, 10, 16, 25, 21, 15, 10$$

dependencias:

$$(100) \rightarrow 15$$

$$(010) \rightarrow 10$$

$$(001) \rightarrow 6$$

$$(110) \rightarrow 25$$

$$(101) \rightarrow 21$$

$$(011) \rightarrow 16$$

$$x \equiv q(2) \quad (a, b, c) \rightsquigarrow 15q + 10b + 6c.$$

Así si tenemos que resolver:

$$\begin{cases} x \equiv q(2) \\ x \equiv b(3) \\ x \equiv c(5) \end{cases}$$

Combinación de conjuntos:

$$A \subset X: \chi_A: x \rightarrow \mathbb{F}_2, \underbrace{\chi_A^2}_{\text{idempotente}} = \chi_A \wedge \chi_A \cdot \chi_B = \chi_{A \cap B}$$

$$(\chi_A^c = 1 - \chi_A)$$

$$\chi_{A \cup B} = \chi_{(A^c \cap B^c)^c} = 1 - \chi_{A^c \cap B^c} = 1 - \chi_{A^c} \cdot \chi_{B^c} = 1 - (1 - \chi_A)(1 - \chi_B) \\ = \chi_A + \chi_B - \chi_A \chi_B$$

Si P y Q son idempotentes. $P_{1\mathbb{Z}} = P\mathbb{Z}$
 $P_{\mathbb{Z}\mathbb{Z}} = P + Q - P\mathbb{Z}$. Son idempotentes.

Estabamor calculando: $12a \equiv x \pmod{12n}$

Sea: $a = a + tn$ ($a' \equiv a \pmod{n}$)

$$12a' = 12a + 12tn \equiv 12a \pmod{12n}$$

En general:

$$d = (a, n)$$

$$\begin{matrix} a = d \\ n = d \\ m \end{matrix}$$

$$dcx \equiv b \pmod{dm}$$

$$b \equiv dcx + tdm$$

$d \mid b$ o no hay solucion. Si $d \nmid b$: $b \equiv d e$:

$$dcx \equiv de \pmod{dm}$$

$$(x \equiv e \pmod{m})$$

hay d soluciones distintas modulo dm

Ejemplo: $12x \equiv 9 \pmod{15}$

$$4x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{5}$$

Luego $x \equiv 2 \pmod{15}$, $x \equiv 2 + 5(15) = 77$, $x \equiv 2 + 10(15) \equiv 12(15)$.

Ejemplo: $\begin{cases} x \equiv 7(15) \\ x \equiv 8(12) \end{cases}$

reemplazamos:

$$15k + 7 \equiv x \quad (1)$$

$$15k + 7 \equiv 8(12) \quad (2)$$

$$3k \equiv 1(12) \quad (3)$$

Luego no hay solución, pues $3 \nmid 12$.

La ecuación: $mx \equiv k \pmod{n}$ tiene solución si $d = \text{mcd}(m, n) \mid k$.

Si d divide a k :

$$m = dm'$$

$$n = dn'$$

$$k = dk'$$

Entonces: podemos simplificar d y obtener:

$$m'x \equiv k' \pmod{n'}$$

(Tiene d soluciones, a saber: $x_1, x_1 + n', \dots, x_1 + (d-1)n'$ módulo n).

Ejemplo: $\begin{cases} x \equiv 5(15) \\ x \equiv 8(12) \end{cases}$

reemplazando:

$$x = 15k + 5$$

$$15k + 5 \equiv 8(12)$$

$$15k \equiv 8(12) - 5 \equiv 1(12)$$

$$3k \equiv 1(12) \Rightarrow k \equiv 1(4)$$

Luego:

Entonces: $(60) = (12) \wedge (15)$ (ver)

y sucede: $(1+12), (1+15)$ no están en la imagen:

Ejercicio: $\text{Im } \varphi = \{(a+(12), b+(15)) ; \text{ con } a \equiv b \pmod{3}\}$. observe que $(3) = (12)+(15)$, $3 = \text{mcd}(12, 15)$

Demuestre en general.

Supongamos que queremos resolver la ecuación

$$x^2 \equiv 2 \pmod{161}$$

$$x^2 \equiv 2 \pmod{23 \cdot 7}$$

Como: $\mathbb{Z}_{(161)} \cong \mathbb{Z}_{(23)} \times \mathbb{Z}_{(7)}$

Módulo 7: $x_1 \equiv 3(7), x_2 \equiv 4(7)$

Módulo 23: $x_3 \equiv 5(23), x_4 \equiv 18(23)$

hay que resolver los 4 sistemas para encontrar todas las soluciones:

$$\begin{cases} x \equiv 3(7) \\ x \equiv 5(23) \end{cases}, \begin{cases} x \equiv 3(7) \\ x \equiv 18(23) \end{cases}, \begin{cases} x \equiv 4(7) \\ x \equiv 5(23) \end{cases}, \begin{cases} x \equiv 4(7) \\ x \equiv 18(23) \end{cases}$$

Encontrar los elementos nilpotentes:

$$\begin{cases} x \equiv 1(7) \\ x \equiv 0(23) \end{cases}$$

$$23k \equiv 1(7), k \equiv 4(7) \Rightarrow P = 92, P^C = 1 - 23 \cdot 4 = 70$$

Como ..

Así las 4 soluciones son:

$$y_1 \equiv 3 \cdot 92 + 5 \cdot 70 \pmod{161}$$

$$y_2 \equiv 3 \cdot 92 + 18 \cdot 70 \pmod{161}$$

$$y_3 \equiv 4 \cdot 92 + 5 \cdot 70 \pmod{161}$$

$$y_4 \equiv 4 \cdot 92 + 18 \cdot 70 \pmod{161}.$$

Este método no es general, pero solo aplica para potencias de primo.

Ejemplo: $x^2 \equiv 2 \pmod{49}$.

En particular: $x^2 \equiv 2 \pmod{7}$.

De esta ecuación: $x \equiv 3 \pmod{7}$,
 $x \equiv 4 \pmod{7}$.

Teniendo las primeras soluciones: $x = 7k + 3$

$$(7k+3)^2 \equiv 2 \pmod{49}$$

$$49k^2 + 2 \cdot 3 \cdot 7k + 9 \equiv 2 \pmod{49}$$

$$\therefore 2 \cdot 3 \cdot 7k + 7 \equiv 0 \pmod{49}$$

Así: $2 \cdot 3 \cdot k + 1 \equiv 0 \pmod{7}$

$$K \equiv 1 \pmod{7}$$

La otra solución sale de $x = 7k + 4$.

$$49k^2 + 2 \cdot 4 \cdot 7k + 16 \equiv 2 \pmod{49}$$

$$8k + 2 \equiv 0 \pmod{7}$$

$$\therefore k \equiv -2 \pmod{7}, K = 7t + 5$$

Por lo tanto $x = 49t + 39$, así $x \equiv 39 \pmod{49}$.

Problema: $x^2 \equiv 1 \pmod{8}$.

$$x^2 \equiv 1 \pmod{2}$$

$$x \equiv 1 \pmod{2}$$

Así: $(2k+1)^2 \equiv 1 \pmod{8}$

$$4k^2 + 4k + 1 \equiv 1 \pmod{8}$$

$$4k(k+1) \equiv k^2 + k \equiv 0 \pmod{2}, \text{ así } k_1 \equiv 0 \pmod{2}, k_2 \equiv 1 \pmod{2}$$

Las soluciones son: $x^2 \equiv 1 \pmod{8}$ si $x^2 \equiv 1 \pmod{2}$.

$$x^2 \equiv 3 \pmod{8} \text{ no tiene solución.}$$

No figura en el proce:

$$4k^2 + 4k + 1 \equiv 0 \pmod{4}$$

$$2k^2 + 2k + 1 \equiv 0 \pmod{4} \text{ (no tiene solución.)}$$

Sistema de ecuación:

$$f(x) \equiv 0 \pmod{p^2}$$

$$f(x+y) = f_0(x) + f_1(x)y + \dots + f_{t-1}(x)y^{t-1} + f_t(x)y^t + \dots$$

$$f_0(x) = f(x)$$

$$f_1(x) = f'(x)$$

$$(f(x+y)) \equiv f(x) + y f'(x) \pmod{y^2}$$

Si x_0 es solución de $f(x) \equiv 0 \pmod{p}$

Sea $X = x_0 + k_p$ y queremos que $f(X) \equiv 0 \pmod{p^2}$

$$f(x_0 + k_p) \equiv 0 \pmod{p^2}$$

$$\text{Caso } f(x_0) \equiv 0 \pmod{p}: f(x_0) = p \Rightarrow f'(x_0) \equiv 0 \pmod{p}$$

$$f(x_0 + k_p) \equiv 0 \pmod{p} \Rightarrow k_p \equiv -s f'(x_0)^{-1} \pmod{p}$$

Si $f'(x_0) \not\equiv 0 \pmod{p}$ existe una única solución para k módulo p .

\Rightarrow Unidad para X módulo p^2 , tal que $X \equiv x_0 \pmod{p}$, $k = -s f'(x_0)^{-1} + pa$

Si $f'(x_0) \equiv 0 \pmod{p}$ hay p sol. forcedas sol. módulo p .

$$\begin{aligned} & X = x_0 + p(-s f'(x_0)^{-1} + pa) \\ & X = x_0 + p(-s f'(x_0)^{-1}) + p^2 a \end{aligned}$$

y $f'(x_0) \not\equiv 0 \pmod{p}$

$$X_{t+1} = X_t + K_p t = x_0 + s b + p f'(x_0)^{-1} + p^2 a$$

Sea:

$$(s b + p f'(x_0)^{-1}) \equiv 0 \pmod{p^{t+1}}$$

$$f'(x_0 + k_p t) \equiv 0 \pmod{p^{t+1}}$$

$$p \cdot s + k_p t f'(x_0) \equiv 0 \pmod{p^{t+1}}$$

$$\text{así } S + k f'(x_t) \equiv 0 \pmod{p}$$

∴ existe una única solución módulo p^{t+1} :

$$\text{Compruebe } f'(x_{t+1}) \equiv f'(x_t) + k_p t \cdot f''(x_t) \not\equiv 0 \pmod{p}$$

Por inducción: Existe x_t con $f(x_t) \equiv 0 \pmod{p^t}$, $\forall t \in \mathbb{N}$.

Lema de Hensel: Si existe x_0 tal que: $f(x_0) \equiv 0 \pmod{p}$ y $f'(x_0) \not\equiv 0 \pmod{p}$

Entonces para cada $t \geq 1$ existe x_t con:

$f(x_t) \equiv 0 \pmod{p^t}$ y $x_t \equiv x_0 \pmod{p}$ y es único módulo p^t .

Ejemplo: $x^5 + x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod{64}$

$$f(x) = x^5 + x^4 + x^3 + x^2 + x + 1, \quad f'(x) = 5x^4 + 4x^3 + 3x^2 + 2x + 1$$

Si resolvemos la ec. módulo 2: $x_0 = 1$.

$$f(1) + 2k_1 f'(1) \equiv 0 \pmod{4} \Rightarrow 1 + 2k_1 \cdot 15 \equiv 0 \pmod{4}$$

$$15 \equiv 3 \pmod{4}$$

$$3 + 2k_1 \equiv 1 \pmod{2}$$

$$k_1 \equiv 1 \pmod{2} \quad \text{y} \quad x_1 = 3$$

$$x_2 = 3 + 4t \quad (t \in \mathbb{Z})$$

$$f(3 + 4t) \equiv 0 \pmod{16}$$

$$f(3) + 4t f'(3) \equiv 0 \pmod{16}$$

$$3 + 4t - 547 \equiv 0 \pmod{16}$$

$$91 + 547t \equiv 0 \pmod{16}$$

$$91 \equiv 13 \pmod{16}$$

$$13 + 547t \equiv 0 \pmod{16}$$

$$13 \equiv 5 \pmod{16}$$

$$5 + 547t \equiv 0 \pmod{16}$$

Bajo que condiciones se resuelve:

$$x^2 + ax + b \equiv 0 \pmod{p}, p \neq 2:$$

$$f'(x) = 2x + a$$

Si $(f'(x) = 2x + a \equiv 0 \pmod{p})$, entonces: $x = 2^{-1} \cdot a \pmod{p}$.

$$\text{Si } x = 2^{-1} \cdot a \quad (2^{-1} \cdot a)^2 + a(2^{-1} \cdot a) + b \equiv 0 \pmod{p}$$

$$a^2 + a^2 + b \equiv 0 \pmod{p}$$

$$\text{Entonces: } a^2 + a^2 + \frac{a^2}{4} \equiv 0 \pmod{p}$$

$$(x + \frac{a}{2})^2 \equiv 0 \pmod{p}$$

Si $f(x)$ tiene soluciones módulo p , las soluciones de $f(x) \equiv 0 \pmod{p}$

pueden calcularse usando el Lema de Hensel.

O sea si:

$\Delta = a^2 - 4b$. La ecuación $x^2 + ax + b \equiv 0 \pmod{p}$ tiene soluciones si Δ es cuadrado módulo p .

Módulo p .

(Cuáles son los cuadrados módulo p ?)

Si $p \neq 2$:

$$x^2 \equiv y^2 \pmod{p}$$

$$x^2 - y^2 \equiv 0 \pmod{p}$$

$$(x-y)(x+y) \equiv 0 \pmod{p}$$

Como $\mathbb{Z}/p\mathbb{Z}$ es cuerpo:

$$x-y \equiv 0 \pmod{p}$$

$$x+y \equiv 0 \pmod{p}$$

El nº de cuadrados perfectos en $\mathbb{Z}/p\mathbb{Z}$ es $\frac{p-1}{2} + 1 = \frac{p+1}{2}$.

$$\text{En } \mathbb{Z}/7\mathbb{Z} : \begin{array}{l} 1^2 = 1 \\ 2^2 = 4 \\ 3^2 = 9 \end{array} \Rightarrow \text{mádador} = \{ \bar{1}, \bar{4}, \bar{2} \}.$$

$$\text{Guia: } \begin{cases} 1: 1-5 \\ 2: 1-10 \\ 3: 1-9 \end{cases}$$

$$\text{Ej: } f(x) = x^3 - 8 \text{ Det. las soluciones de } f(x) \equiv 0 \pmod{7^2}$$

Claramente: $f(x) \equiv 0 \pmod{7}$ tiene $x \equiv 1 \pmod{7}$ y $x \equiv 2 \pmod{7}$ son soluciones.

Y como las soluciones unipro: $f(x) \equiv x^3 - 1 \pmod{7}$, $f'(x) = 3x^2$

teorema pie: $x \equiv 4 \pmod{7}$.

Paramos con: $x \equiv 1 \pmod{7}$, $x = 1 + 7t$.

$$f(x) \equiv 0 \pmod{7^2}$$

$$f(1 + 7t) \equiv 0 \pmod{7^2}$$

$$f(1) + 7t f'(1) \equiv 0 \pmod{7^2}$$

$$-7 + 7t \cdot 3 \equiv 0 \pmod{7^2}$$

$$-1 + 3t \equiv 0 \pmod{7}, 3t \equiv 1 \pmod{7}, t \equiv 5 \pmod{7}.$$

luego: $x \equiv 36 \pmod{49}$.

Para: $x \equiv 40 \pmod{49}$, $x = 4 + 7t$

$$f(x) \equiv 0 \pmod{7^2}$$

$$f(4 + 7t) \equiv 0 \pmod{7^2}$$

$$f(4) + 7t f'(4) \equiv 0 \pmod{7^2}$$

$$-16 + 7t \cdot 3 \cdot 16 \equiv 0 \pmod{7^2}$$

$$8 + 3 \cdot 16t \equiv 0 \pmod{7^2}$$

$$1 + 3 \cdot 2t \equiv 0 \pmod{7}, t \equiv 1 \pmod{7}$$

luego: $x \equiv 11 \pmod{49}$.

$$f(11 + 7t) \equiv 0 \pmod{7^2}$$

Un recuerdo: $|(\mathbb{F}_p^*)| = p-1$.

Si $\forall x \in \mathbb{F}_p^*$: $x^{p-1} - 1 = 0$

Sino es cíclico: $\mathbb{F}_p^* \cong A \times B$ con $(|A|, |B|) = 1$.

Queremos que G sea abeliano: $G \cong C_1 \times \dots \times C_r$, dif d_1, \dots, d_r

Otro camino: Prop: Si G es un grupo abeliano no cíclico,

existe $n \mid |G|$, $n \nmid |G|$ tal que: $p^n = 1 \Rightarrow \forall p \in G$.

Demo: Si \mathbb{F}_p^* no es cíclico entonces $p(x) = x^{p-1} - 1 = 0 \quad \forall x \in \mathbb{F}_p^*$ con $p > p-1$.
Existe $n \mid |G|$ tal que: $\forall p \in G$ existe elemento en \mathbb{F}_p^* es de orden n .
 $\therefore p(x)$ tiene más de n soluciones (pues todo elemento en \mathbb{F}_p^* es solución). \neq

Si: $|G| = p_1^{d_1} \cdots p_r^{d_r}$.

Para cada $|p| =$ menor r positivo: $p^r = 1$.

Entonces $n \mid p^r = 1$ si $\text{ord}(p) \mid n$.

Tomamos $m = \text{lcm}\{\text{ord}(p) \mid p \in G\}$.

Si: $\text{lcm}\{\text{ord}(p) \mid p \in G\} = m \Rightarrow G$ es cíclico.

Para cada p , existe $p \in G$ tal que: $p^m \mid \text{ord}(p)$.

Notación: Si: p es primo: $N_p(n) =$ mayor potencia de p que divide a n .
 $\alpha = N_p(n) \Leftrightarrow p^\alpha \mid n$, $p^{\alpha+1} \nmid n$.

Obs: $N_p(\text{lcm}\{h_1, \dots, h_r\}) = \max\{N_p(h_1), \dots, N_p(h_r)\}$.

Demo: Si: $m = p_1^{d_1} \cdots p_r^{d_r}$, $l = p_1^{\beta_1} \cdots p_r^{\beta_r}$

$$\text{lcm}(m, l) = p_1^{\max(d_1, \beta_1)} \cdots p_r^{\max(d_r, \beta_r)}$$

$$\Rightarrow N_p(\text{lcm}(m, l)) = \max\{\alpha_1, \beta_1\} = \max\{N_p(m), N_p(l)\}$$

$$\cup_{p \in G} \{ \text{ord}(p) \mid p \in G \} = d_i$$

$$\text{ord}(p) \leq d_i$$

$$\text{ord}(p) = d_i$$

Se p_i tal que $(p_i) = p_i^{d_i}$, si $(s_i, p_i) = 1$

$$\text{ord}(p_i s_i) = p_i^{d_i}$$

Sea $p = p_1^{r_1} \cdots p_r^{r_r}$, así $(p) = p_1^{d_1} \cdots p_r^{d_r}$

luego $\langle p \rangle = G \therefore G$ es cíclico.

$(\mathbb{Z}/(p))^\times$ ciclico de orden $p-1$ si p es primo.

Sea $U = \{ \overline{1+pr} \mid r \in \mathbb{Z}/p\mathbb{Z} \}$, claramente $|U| = p^t - 1$ para $x^t = 0$.

y $U \subseteq (\mathbb{Z}/p^t\mathbb{Z})^\times$ (haciendo expansión de Taylor de $(1+x)^{-1}$ para $x = 0$)

Af: U es cíclico, si $p \neq 2$

$$(1+pr)^p = 1 + p^2r + \binom{p}{2} p^2 r^2 + \sum_{i=3}^p \binom{p}{i} p^i r^i$$

Como $p \neq 2$: $\binom{p}{2} \equiv 0 \pmod{p}$

$$(1+pr)^p = 1 + p^2r + p^3r^2 + \dots \equiv 1 + p^2r \pmod{p^3}$$

$$N_p((1+p)^{p^t} - 1) = 2^t$$

$$A.S.T: (1+pr)^{p^t} = (1+pr)^p = 1 + p^3r + \binom{p}{2} p^2 r^2 + \dots \equiv 1 + p^3r \pmod{p^4}$$

Por inducción: $N_p((1+p)^{p^t} - 1) = 2^t$

Bajo las condiciones $(1+p)^{p^t} \equiv 1 \pmod{p^t} \Rightarrow p^t \mid (1+p)^{p^t} - 1$, así:

$$\text{sr. } N_p((1+p)^{p^t} - 1) \geq t$$

$$t+1 \geq t$$

$$\therefore \text{ord}(1+p) = p^{t+1} \therefore \langle \overline{1+p} \rangle = U.$$

Ejercicio: Si $n|m \Rightarrow N_p(n) \leq N_p(m)$, $\forall p$.

Luego \cup es cíclico de orden p^t .

$$x^{p-1} \equiv 1 \pmod{p}$$

tiene solución x_0 con x_0 de orden $p-1$.

$$\text{Sea } f(x) = x^{p-1} - 1, \quad f'(x) = (p-1)x^{p-2}, \quad f'(x_0) = -x_0^{p-2} \pmod{p} \not\equiv 0 \pmod{p}$$

Por teorema de Hensel, existe x_1 con $x_1^{p-1} \equiv 1 \pmod{p^t}$

$$x_1 \equiv x_0 \pmod{p} \quad x_1^{p-1} \not\equiv 1 \pmod{p^t}, \text{ si } n < p-1.$$

$$\text{Luego: } x_1^{p-1} \not\equiv 1 \pmod{p^t}, \text{ en } (\mathbb{Z}/p^t\mathbb{Z})^*$$

$$\text{Así: } \text{ord}(x_1) = p-1, \text{ en } (\mathbb{Z}/p^t\mathbb{Z})^*$$

$$\text{Luego: } \text{ord}(x_1(p+1)) = p + (p-1) = |(\mathbb{Z}/p^t\mathbb{Z})^*|$$

$$\text{Así: } (\mathbb{Z}/p^t\mathbb{Z})^* \text{ es cíclico. (Si } p \neq 2).$$

Ahora bien: Si $t \neq 1 \wedge p \neq 2 \Rightarrow |(\mathbb{Z}/(p^t\mathbb{Z})^*)^*| = p^t(p-1)$ es par.

$$(\mathbb{Z}/(p^t\mathbb{Z})^*)^* \cong \langle u \rangle \cong C_{2t}.$$

$$\bar{a} = \bar{u}^b \pmod{p^t}$$

para cualquier $a \in \mathbb{Z}$: $x^2 \equiv a \pmod{p^t}$ tiene solución si y sólo si $b \in \mathbb{Z}$ es par.

$$\text{Sea } x = \bar{u}^c, \quad \bar{x}^2 = \bar{u}^{2c} = \bar{u}^b \quad \text{ssi} \quad b \equiv 2c \pmod{2t} \Leftrightarrow b \text{ es par.}$$

$$\therefore N_p(a) = \frac{(p-1)(p-2)\dots(p-b)}{(p-1)(p-2)\dots(p-2c)} \cdot \frac{(p-1)(p-2)\dots(p-2c)}{(p-1)(p-2)\dots(p-2c)} = \frac{(p-1)(p-2)\dots(p-2c)}{(p-1)(p-2)\dots(p-2c)} = N_p(a)$$

$$= N_p(a)$$

$$= N_p(a)$$

$$U = \langle T \rangle$$

Luego la mitad de los elementos de $(\mathbb{Z}/pt\mathbb{Z})^*$ son cuadrados.

$$(\mathbb{Z}/pt\mathbb{Z})^* \cong U \times \langle \bar{x}_1 \rangle \cong C_{p-1} \times C_{p-1}$$

$$\bar{a} \mapsto (1+rp, x_1^l)$$

$$a \equiv x_1^l (1+rp) \pmod{pt}$$

Así:

• Cuando a es cuadrado?

$$a \equiv x_1^{2m} (1+rp) \pmod{pt}$$

$$x_1^{2m} \equiv x_1^l \pmod{p}$$

Así:

$$(1+sp)^2 \equiv 1+rp \pmod{p}$$

tiene solución.

✓ Ejercicio: En un grupo de orden impar (cada elemento es cuadrado).

Así: a es cuadrado módulo p si es cuadrado módulo p .

$$a \equiv x_1^l (1+rp) \pmod{pt}$$

Pues:

$$a \equiv x_1^l \pmod{p}$$

(pero en el toro, basta estudiar $f(x) = x^2 - a$)

Def: Sea p un primo impar y $a \in \mathbb{Z}$, con $pt \nmid a$, definimos:

$$\left(\frac{a}{p} \right) = \begin{cases} 1, & \text{si } a \text{ es cuadrado.} \\ -1, & \text{si no.} \end{cases}$$

$$\text{Prof: } \left(\frac{a}{p} \right) = a^{\frac{p-1}{2}} \pmod{p}$$

$$\text{Sea } a \equiv u^b, \text{ luego: } a^{\frac{p-1}{2}} \equiv u^b \left(\frac{p-1}{2} \right)$$

$$\text{Primera obs: } a^{\frac{p-1}{2} \cdot 2} \equiv a^{p-1} \equiv 1, \text{ así: } a^{\frac{p-1}{2}} \in \{1, -1\}$$

$$\text{Luego } a^{\frac{p-1}{2}} = 1 \text{ si: } p-1 = \text{ord}(u) \mid b \cdot \frac{p-1}{2}.$$

pero esto implica que: $2 \mid b$, luego a es cuadrado.

$$\therefore a^{\frac{p-1}{2}} = 1 \text{ si: } 2 \mid b \text{ si: } a \text{ es cuadrado}$$

$$\psi : (\mathbb{Z}/\mathbb{Z})^* \rightarrow \{1, -1\}$$

Corolario: La función $\bar{a} \mapsto \left(\frac{a}{p}\right)$ es un homomorfismo.

Multiplicativo.

$$(\bar{a}\bar{b})_p \mapsto \bar{ab}$$

Ej: $q \in \mathbb{Z}/\mathbb{Z}$ and dito $\bar{q} \in (\mathbb{Z}/\mathbb{Z})^*$

$$q^{\frac{p-1}{2}} = q^5 \equiv (-2)^5 \equiv -2^5 \equiv -(-1) \equiv 1 \pmod{p}.$$

$$\text{Otra forma: } \left(\frac{q}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{3}{p}\right)^2 = 1.$$

Si queremos calcular: $\left(\frac{-3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) \rightarrow$ simbolo de Legendre y cosi.

Luego

$$\left(\frac{-1}{p}\right) = \left(\frac{p+1}{2}\right) = \left(\frac{p-1}{2}\right) = \left(\frac{1}{2}\right) = 1$$

$$\text{y} \left(\frac{2}{p}\right) = \left(\frac{p-2}{2}\right) = \left(\frac{1}{2}\right) = 1$$

$$\text{y} \left(\frac{3}{p}\right) = \left(\frac{p-3}{2}\right) = \left(\frac{1}{2}\right) = 1$$

$$\text{entonces } \left(\frac{-3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot 1 \cdot 1 = 1$$

$$\text{entonces } \left(\frac{-3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot 1 \cdot 1 = 1$$

$$\text{entonces } \left(\frac{-3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot 1 \cdot 1 = 1$$

$$\text{entonces } \left(\frac{-3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot 1 \cdot 1 = 1$$

$$\text{entonces } \left(\frac{-3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot 1 \cdot 1 = 1$$

$$\text{entonces } \left(\frac{-3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot 1 \cdot 1 = 1$$

$$\text{entonces } \left(\frac{-3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot 1 \cdot 1 = 1$$

$$\text{entonces } \left(\frac{-3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot 1 \cdot 1 = 1$$

$$\text{entonces } \left(\frac{-3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot 1 \cdot 1 = 1$$

$$\text{entonces } \left(\frac{-3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot 1 \cdot 1 = 1$$

$$\text{entonces } \left(\frac{-3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot 1 \cdot 1 = 1$$

$$\text{entonces } \left(\frac{-3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot 1 \cdot 1 = 1$$

$$\text{entonces } \left(\frac{-3}{p}\right) = \left(\frac{6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = 1 \cdot 1 \cdot 1 = 1$$

Una aplicación: $\left(-\frac{1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } p \equiv 1(4) \\ -1 & \text{si } p \equiv 3(4) \end{cases}$

Otra demostración: $-1 = x^2$ ssi $x = 4$ ssi $4 \mid p-1$ o $4 \nmid \frac{24}{p-1}$ ssi $4 \nmid p-1$.

Proposición: $\left(\frac{2}{p}\right) \stackrel{p \equiv 1(4)}{=} (-1)^{\frac{p-1}{8}} = (-1)^{\frac{1}{2}} = \begin{cases} 1 & \text{parte real} \\ i & \text{parte imaginaria} \end{cases}$

Calcular en $\mathbb{Z}[i] \cong \mathbb{Z} \oplus i\mathbb{Z}$.

$$\frac{2}{p} = \frac{2 \oplus i0}{p} = \frac{2 \oplus 0i}{p} \stackrel{\text{parte real}}{\oplus} \stackrel{\text{parte imaginaria}}{i} \left(\frac{24}{p-1}\right)$$

$$\text{pero } \left(\frac{24}{p-1} \oplus i0\right) \stackrel{p-1 \equiv 0(4)}{=} \frac{24 \oplus 0i}{p-1} \stackrel{\text{parte real}}{\oplus} i \left(\frac{24}{p-1}\right)$$

Obs: 1) $2 = (-i)(1+i)^2$, $2^{\frac{p-1}{2}} \stackrel{p-1 \equiv 1(4)}{=} (-i)^{\frac{p-1}{2}} (1+i)^{p-1}$, $2^{\frac{p-1}{2}} (1+i) \stackrel{p-1 \equiv 1(4)}{=} (-i)^{\frac{p-1}{2}} (1+i)^2$
 hay que calcular $(-i)^{\frac{p-1}{2}} = (\pm i)^{\frac{p-1}{2}}$

Caso I: $p \equiv 1(8)$: $2^{\frac{p-1}{2}} (1+i) \equiv 1+i \pmod{p}$
 así: $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ (terminando parte real).

Caso II: $p \equiv 5(8)$: entonces $(-i)^{\frac{p-1}{2}} = -1$, $i^8 = 1$

Así: $2^{\frac{p-1}{2}} (1+i) \equiv -(1+i)$
 $2^{\frac{p-1}{2}} \equiv -1$

Caso III: $p \equiv 3(8)$: entonces $(-i)^{\frac{p-1}{2}} = i$, $i^8 = -1$

Así: $2^{\frac{p-1}{2}} (1+i) \equiv -i(1-i) = -1-i$
 $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

Caso IV: $P \equiv 7(8)$, $(-i)^{\frac{p-1}{2}} = i$

$$\text{Así: } 2^{\frac{p-1}{2}}(1+i) \equiv i(1-i) \equiv 1+i$$

Luego: $\left(\frac{2}{P}\right) \equiv 1 \pmod{P}$ con $f=8$ (o sea $\chi^8 \equiv 1 \pmod{P}$)

y como: $\left(\frac{2}{P}\right) = (-1)^{\frac{P-1}{8}} = \begin{cases} 1, & \text{si } P \equiv 1, 7(8) \\ -1, & \text{si } P \equiv 3, 5(8) \end{cases}$

Ejercicio: terminar:
intentávase encontrar una forma de evaluar $\left(\frac{p}{q}\right)$ para p primo impar.

Proposición: Si q, p son primos distintos y de reciprocidad cuadrática:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right)$$

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \equiv \left(\frac{q+8}{q}\right) \equiv \left(\frac{q+8}{q}\right)^{\frac{p-1}{2}} \left(\frac{14}{q}\right)$$

Un ejercicio ilustrativo: $\left(\frac{83}{97}\right) = (-1)^{\frac{97-1}{2} \cdot \frac{83-1}{2}} \left(\frac{83}{97}\right)$

$$\begin{aligned} \left(\frac{83}{97}\right) &= \left(\frac{2}{97}\right) \left(\frac{7}{97}\right) = (-1) \left(\frac{7}{97}\right) = (-1)^{\frac{97-1}{2} \cdot \frac{83-1}{2}} \left(\frac{83}{97}\right) \\ &= -(-1) \left(\frac{-1}{97}\right) = \left(\frac{-1}{97}\right) = (-1)^{\frac{97-1}{2}} = -1 \end{aligned}$$

$\therefore 97$ no es un cuadrado módulo 83 o bien: $x^2 \equiv 97(83)$ no tiene solución.

DJS: Supongamos que quisieramos resolver:

$$x^2 \equiv 17 \pmod{31 \cdot 11}$$

Como: $\mathbb{Z}/_{341}\mathbb{Z} \cong \mathbb{Z}/_{31}\mathbb{Z} \oplus \mathbb{Z}/_{11}\mathbb{Z}$

y además

$$\begin{aligned} \mathbb{Z}/_{341}\mathbb{Z} &\rightarrow \mathbb{Z}/_{11}\mathbb{Z} \quad \text{es un homomorfismo} \\ \bar{a} = a + 341\mathbb{Z} &\mapsto \bar{a} = a + 11\mathbb{Z} \end{aligned}$$

Es suficiente resolver:

$$\begin{cases} x^2 \equiv 17 \pmod{31} \\ x^2 \equiv 17 \pmod{11} \end{cases}$$

Demonstración: (Seg. Y. Kim)

$T \subseteq \mathbb{Z}$ finito $A_T = \prod_{a \in T} a$

$$\Phi = \left\{ n \mid 1 \leq n \leq \frac{p-1}{2} \text{ tal que } (a, p) = 1 \right\}$$

$$\Psi = \left\{ n \mid 1 \leq n \leq \frac{p-1}{2} \text{ tal que } (a, p) = 1 \right\}$$

$$X = \left\{ qt \mid 1 \leq t \leq \frac{p-1}{2} \right\}$$

obs: $\Psi = \Phi \cup X$ pues: $\Phi = \left\{ n \in \Psi \mid q+n \right\}$, $X = \left\{ n \in \Psi \mid q \mid n \right\}$

$$\Rightarrow \Phi \cap X = \emptyset$$

$$A_\Phi A_X = \prod_{a \in \Phi} a \cdot \prod_{a \in X} a = \prod_{a \in \Phi \cup X} a = A_\Psi$$

para cada t : $\Psi_t = \{n+pt \mid 1 \leq n \leq \frac{p-1}{2}\}$

$$\Psi_t^1 = \{n+pt \mid 1 \leq n \leq \frac{p-1}{2}\}$$

$$\Psi = \bigcup_{t=0}^{\frac{p-3}{2}} \Psi_t \cup \Psi_{\frac{p-1}{2}}$$

$$A_\Psi = \left(\prod_{a=0}^{\frac{p-3}{2}} A_{\Psi_t^1} \right) A_{\Psi_{\frac{p-1}{2}}} = \mathbb{F}_{p-1}^{p-1} \mathbb{F}_{p-1}^{p-1}$$

Nota: $(-1)! \equiv -1 \pmod{p}$
Así $A_{\Psi_t} \equiv -1 \pmod{p}$, pues $A_{\Psi_t} = (pt+1)(pt+2) \cdots (pt+(p-1)) \equiv (-1)^t \equiv -1 \pmod{p}$

$$A_\Psi \equiv (-1)^{\frac{p-1}{2}} \cdot A_{\Psi_{\frac{p-1}{2}}} \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2} \right)!$$

$$A_X \equiv \frac{p-1}{2} \left(\frac{p-1}{2} \right)! \equiv \left(\frac{q}{p} \right) \left(\frac{p-1}{2} \right)!$$

$$A_\Psi = A_X A_\Phi, \text{ así: } (-1)^{\frac{p-1}{2}} \left(\frac{p-1}{2} \right)! \equiv \left(\frac{q}{p} \right) \left(\frac{p-1}{2} \right)! A_\Phi \pmod{p}$$

$$A \Phi = (-1)^{\frac{p-1}{2}} \left(\frac{q}{p} \right) (\text{mod } p)$$

Per simetria:

$$A \Phi = (-1)^{\frac{p-1}{2}} \left(\frac{p}{q} \right) (\text{mod } q)$$

$$\underline{\text{Caso I}}: A \Phi \equiv 1 (\text{mod } p), A \Phi \equiv 1 (\text{mod } q) \Rightarrow A \Phi \equiv 1 (\text{mod } pq)$$

$$\underline{\text{Caso II}}: A \Phi \equiv -1 (\text{mod } p), A \Phi \equiv -1 (\text{mod } q)$$

$$\Rightarrow A \Phi \equiv -1 (\text{mod } pq)$$

$$\underline{\text{Caso III y IV}}: A \Phi \equiv 1 (\text{mod } p), A \Phi \equiv -1 (\text{mod } q)$$

$$\text{el sistema da una soluci\'on si } K^2 \equiv 1 (\text{mod } pq) \text{ es decir } K \equiv \pm 1 (\text{mod } pq)$$

$$\text{Luego: } A \Phi \equiv \pm 1 (\text{mod } pq) \text{ si}$$

$$(-1)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} \left(\frac{q}{p} \right) \left(\frac{p}{q} \right) \equiv \pm 1 (\text{mod } pq)$$

$$\text{Pd: } A \Phi \equiv \pm 1 \text{ si } p \equiv q \equiv 1 (\text{mod } 4).$$

$$(-1)^{\frac{p-1}{2}} \cdot \frac{q-1}{2} = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{q-1}{2}} \equiv \pm 1, \text{ si no}$$

$$\text{De la afirmaci\'on } (-1)^{\frac{p-1}{2}} (-1)^{\frac{q-1}{2}} = \left(\frac{p}{q} \right) \left(\frac{q}{p} \right) \text{ si } p \equiv q \equiv 1 (\text{mod } 4) \text{ o } p \equiv q \equiv 3 (\text{mod } 4)$$

$$\text{Dem. de la afirmaci\'on: Sean } p, q \in \mathbb{N} \text{ entonces existe un \'unico } u \in \mathbb{Z} \text{ tal que } u^2 \equiv 1 (\text{mod } pq)$$

$$\text{Def: si } u \in \mathbb{Z} \text{ definimos } u^{-1} \text{ tal que } u \cdot u^{-1} \equiv 1 (\text{mod } pq) \text{ si } u^{-1} \equiv 1 (\text{mod } p) \text{ y } u^{-1} \equiv 1 (\text{mod } q)$$

$$\text{Existe un \'unico elemento en } \{u \in \mathbb{Z} \mid u^2 \equiv 1 (\text{mod } pq)\} \text{ que est\'a en } \mathbb{Z}/pq\mathbb{Z} \text{ y } u^{-1} \equiv 1 (\text{mod } p) \text{ y } u^{-1} \equiv 1 (\text{mod } q)$$

$$u^{-1} = (u^{-1})^* = (u^{-1})^{-1} = (u^{-1})^{-1} \cdot u^{-1} = 1 \cdot 1 = 1$$

Sea $\mathcal{R} = \{n \in \mathbb{Z} / n^2 \equiv u \pmod{p^f}\}$

$A\Phi \equiv \pm A\mathcal{R} \pmod{p^f}$, pues $A\Phi = \underbrace{u_1 u_1' u_2 u_2' \dots u_r u_r'}_{\pm 1} \pmod{p^f}$

Caso: $p \equiv f \equiv 1 \pmod{4}$

$n \in \mathcal{R}$ ssi $n^2 \equiv \pm 1 \pmod{p^f}$

$(n^2 \equiv 1) \Leftrightarrow (n \in \{-1, 1, K, -K\})$ con $\begin{cases} K \equiv 1 \pmod{p} \\ K \equiv -1 \pmod{p} \end{cases}$

$$\text{Pues } \mathcal{R}/p^f \cong \mathcal{R}/p \times \mathcal{R}/p \cong \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \times \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\text{Si } n^2 \equiv 1 \pmod{p^f} \Leftrightarrow \begin{cases} n^2 \equiv -1 \pmod{1} \\ n^2 \equiv 1 \pmod{p^f} \end{cases} \quad (*)$$

Si $f \equiv 1 \equiv p \pmod{4}$: hay 4 soluciones: $\{L, -L, KL, -KL\}$

$$L = (a, b), -L = (-a, -b), KL = (a, -b), -KL = (-a, b)$$

$$\mathcal{R} = \{1 \pm K, -1 \pm KL\}$$

$$\text{Así: } A\lambda = \pm KL^2 \equiv \pm 1 \pmod{p^f}$$

Si $p \not\equiv 1 \pmod{4}$ o $f \not\equiv 1 \pmod{4}$:

luego $(*)$ no tiene soluciones, $\Rightarrow \mathcal{R} = \{1 \pm K\}$

$$A\lambda \equiv \pm K \pmod{p^f} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\not\equiv \pm L \pmod{p^f}$$

Ejemplo: 147 es un cuadrado módulo 181.

$$\left(\frac{147}{181} \right) = \left(\frac{3}{181} \right) \left(\frac{7^2}{181} \right)^{-1} = \left(\frac{3}{181} \right) = \left(\frac{181}{3} \right) = \left(\frac{1}{3} \right) = 1$$

Definición: Símbolo de Jacobi:

Si $n = p_1^{d_1} \cdots p_r^{d_r}$ primos distintos ($n, m \neq 1$)

impar. $m = 2^{\beta_0} p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ ($\beta_0 \geq 0$)

$$\left(\frac{m}{n}\right) = \prod_{i=1}^r \left(\frac{m}{p_i}\right)^{d_i} = \prod_{i=1}^r \left(\frac{2^{\beta_0} p_1^{\alpha_1} \cdots p_s^{\alpha_s}}{p_i}\right)^{d_i} = \prod_{i=1}^r \left(\prod_{j=1}^s \left(\frac{p_j}{p_i}\right)^{\alpha_j \beta_i}\right)$$

Es fácil comprobar que: $\left(\frac{n_1 n_2}{n}\right) = \left(\frac{n_1}{n}\right) \left(\frac{n_2}{n}\right)$.

$$\left(\frac{m}{n_1 n_2}\right) = \left(\frac{m}{n_1}\right) \left(\frac{m}{n_2}\right) \quad (\text{por } (1))$$

Si $n_1 = p_1^{d_1} \cdots p_r^{d_r} = p_1^{d_1} \cdots p_r^{d_r}$ ($d_1 < d_2$) $\Rightarrow n_1 n_2 = p_1^{d_1+1} \cdots p_r^{d_2} \cdots p_t^{d_t}$

$n_2 = p_1^{d_1} \cdots p_t^{d_t}$ ($d_1 < d_2$)

$$\text{Luego: } \left(\frac{m}{n_1 n_2}\right) = \prod_{i=1}^r \left(\frac{m}{p_i}\right)^{d_1+1+d_2} = \prod_{i=1}^r \left(\frac{m}{p_i}\right)^{d_1+1} \cdot \prod_{i=1}^r \left(\frac{m}{p_i}\right)^{d_2} = \left(\frac{m}{n_1}\right) \left(\frac{m}{n_2}\right).$$

Queremos que: $\left(-\frac{1}{n}\right) = \left(\frac{-1}{p_1}\right)^{\frac{n-1}{2}}$

$$\left(-\frac{1}{n}\right) = \prod_{i=1}^r \left(-\frac{1}{p_i}\right)^{d_i} = \left(\prod_{i=1}^r \left(-\frac{1}{p_i}\right)^{\frac{p_i-1}{2}}\right)^{d_i} = \lambda$$

$$= (-1)^{\sum_{i=1}^r d_i \left(\frac{p_i-1}{2}\right)} = (-1)^{\frac{n-1}{2}}$$

$$\left(\frac{-1}{p_1}\right) = \left(\frac{1}{p_1}\right) = \frac{1}{\left(\frac{p_1}{p_1}\right)} = \left(\frac{1}{p_1}\right) \left(\frac{1}{p_1}\right) = \left(\frac{1}{p_1}\right)^2$$

Proposición: Si a y b son impares: $\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod{2}$

Dem: $a = 2t+1, b = 2s+1$

$$\frac{(2t+1)(2s+1)-1}{2} = \frac{4ts+2(t+s)}{2} = 2ts+t+s \equiv t+s \pmod{2}$$

Aplicando esto repetidamente: $\prod_{i=1}^r \frac{p_i^{x_i}-1}{2} \equiv \sum_{i=1}^r x_i \left(\frac{p_i-1}{2} \right)$

$$\left(\frac{a^2-1}{2} \equiv \frac{a^2-1}{2} \left(\frac{a-1}{2} \right) \equiv 3 \left(\frac{a-1}{2} \right) \right)$$

$$\therefore \left(\frac{-1}{n} \right) = \left(-1 \right)^{\frac{n-1}{2}}$$

$$\text{y } \left(\frac{2}{n} \right) = \prod_{i=0}^r \left(\frac{-1}{p_i} \right)^{x_i} = \prod_{i=0}^r \left[(-1)^{\frac{p_i-1}{2}} \right]^{x_i} = (-1)^{\sum_{i=0}^r x_i \left(\frac{p_i-1}{2} \right)}$$

Proposición: Si a y b son impares:

$$\frac{a^2b^2-1}{8} \equiv \frac{a^2-1}{8} + \frac{b^2-1}{8} \pmod{2}$$

$$a^2 = 8t+1 \Rightarrow \frac{a^2b^2-1}{8} = \frac{64ts+8(t+s)}{8} = 8ts+t+s \equiv t+s \pmod{2}$$

$$\therefore \left(\frac{2}{n} \right) = (-1)^{\frac{\sum p_i^{x_i}-1}{8}} = (-1)^{\frac{n-1}{8}}$$

Si p es primo:

$$\left(\frac{p}{n} \right) = \prod_{i=1}^r \left(\frac{p}{p_i} \right)^{x_i}$$

$$\left(\frac{n}{p} \right) = \prod_{i=1}^r \left(\frac{p_i}{p} \right)^{x_i}$$

$$\begin{aligned} \left(\frac{p}{n} \right) \left(\frac{n}{p} \right) &= \prod_{i=1}^r \left(\frac{p}{p_i} \right)^{x_i} \left(\frac{p_i}{p} \right)^{x_i} \\ &= \prod_{i=1}^r \left[(-1)^{\frac{p-1}{2}} \cdot \frac{p_i-1}{2} \right]^{x_i} \\ &= (-1)^{\frac{p-1}{2} \sum_{i=1}^r x_i \cdot \frac{p_i-1}{2}} = (-1)^{\frac{p-1}{2} \cdot \frac{n-1}{2}} \end{aligned}$$

$$u = \prod_{j=1}^s f_j \beta_j$$

$$\begin{aligned} \left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= \prod_{i=1}^s \left(\frac{f_i}{n}\right)^{\beta_i} \prod_{i=1}^s \left(\frac{n}{f_i}\right)^{\beta_i} \\ &= \prod_{i=1}^s \left[\left(\frac{f_i}{n} \right) \left(\frac{n}{f_i} \right) \right]^{\beta_i} \\ &= \prod_{i=1}^s \left[(-1)^{\frac{f_i-1}{2} \cdot \frac{n-1}{2}} \right]^{\beta_i} = (-1)^{\frac{n-1}{2} \sum_{j=1}^s \beta_j \cdot \frac{f_i-1}{2}} = (-1)^{\frac{n-1}{2} \cdot \frac{m-1}{2}}. \end{aligned}$$

obs: $\left(\frac{m}{n}\right) = 1$ no significa que $x^2 \equiv m \pmod{n}$ tiene solución.

(*) Si n es impar: $x^2 \equiv n \pmod{n}$ tiene solución si $\left(\frac{m}{p}\right) = 1 \forall p \mid n$.

Ejemplo: $\left(\frac{147}{181}\right) = \left(\frac{147}{147}\right) = \left(\frac{34}{147}\right) = \left(\frac{147}{34}\right) = \left(\frac{147}{2}\right) \left(\frac{147}{17}\right) = (-1)^{\frac{147-1}{2}} \left(\frac{147}{17}\right) = \left(\frac{1}{17}\right)$

$$\begin{aligned} \left(\frac{147}{181}\right) &= \left(\frac{181}{147}\right) = \left(\frac{34}{147}\right) = \left(\frac{147}{2}\right) \left(\frac{147}{17}\right) = (-1)^{\frac{147-1}{2}} \left(\frac{147}{17}\right) = \left(\frac{1}{17}\right) \\ &= -\left(\frac{17}{147}\right) = -\left(\frac{11}{17}\right) = -\left(\frac{6}{11}\right) = -(-1)^{\frac{11-1}{2}} \left(\frac{3}{11}\right) = \left(\frac{3}{11}\right) \end{aligned}$$

$$= (-1) \left(\frac{11}{3}\right) = (-1) \left(\frac{12}{3}\right) = 6 \cdot \frac{1}{5} \cdot \frac{1}{5} \cdot \frac{1}{6} = \frac{1}{5} \cdot \frac{1}{3} = \frac{1}{15}.$$

Para que esto sea cierto: $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right)^2 \cdot \frac{m-1}{2} \cdot \frac{n-1}{2}$ / numeros primos relativos.

$$\left(\frac{1}{17}\right) = \left(\frac{-1}{17}\right) \left(\frac{1}{17}\right)^{\frac{17-1}{2}} = \frac{1-17+41}{17} = (1-1) \cdot \left(\frac{1}{17}\right) = 0 \cdot \left(\frac{1}{17}\right) = 0.$$

$$\left(\frac{1}{17}\right) \left(\frac{1}{17}\right)^{\frac{17-1}{2}} = \left(\frac{1}{17}\right) \left(\frac{1}{17}\right)^8 = \left(\frac{1}{17}\right)^9 = \left(\frac{1}{17}\right) \left(\frac{1}{17}\right)^8 = \left(\frac{1}{17}\right)^9.$$

$$\left[\left(\frac{1}{17}\right)^2 \cdot (-1)\right] \left(\frac{1}{17}\right) =$$

$$\left(\frac{1}{17} \cdot \frac{1}{17}\right) \cdot (-1) = \frac{1-17+41}{17} \cdot (-1) = (1-1) \cdot (-1) = 0 \cdot (-1) = 0.$$

Enteros Algebraicos:

$x \in \mathbb{C}$ es entero algebraico si satisface una ecuación

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0, \quad a_i \in \mathbb{Z} \text{ irred.}$$

Entonces $\mathbb{Z}[x] = \underbrace{\mathbb{Z} \oplus \mathbb{Z}x \oplus \dots \oplus \mathbb{Z}x^{n-1}}_{\cup} \oplus \mathbb{Z}[x^{n+1}]$

$$x^n = -a_{n-1}x^{n-1} - \dots - a_0 \in \cup$$

Así $1, x, x^2, \dots, x^n \in \cup$

$$x^{n+1} = -a_{n-1}x^n - a_nx^{n-1} - \dots - a_0x \in \cup$$

Por inducción: $x^r \in \cup \quad \forall r \in \{0, 1, \dots\}$

Ejemplo: $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}, \quad x^2 + 1 = 0$.

$$\mathbb{Z}(\sqrt{2}) = \{a+b\sqrt{2} \mid a, b \in \mathbb{Z}\}, \quad x^2 - 2 = 0$$

$$\mathbb{Z}(\sqrt[3]{2}) = \{a+b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}, \quad x^3 - 2 = 0$$

$\frac{1}{\sqrt{2}}$ no es entero algebraico. Si $n = \frac{1}{\sqrt{2}} \Rightarrow 2n^2 - 1 = 0 \Rightarrow x^2 - \frac{1}{2} = 0$

$\Rightarrow \frac{1}{\sqrt{2}}$ no es entero algebraico.

Así: $\mathbb{Z}\left[\frac{1}{\sqrt{2}}\right] \neq \{a + b\frac{1}{\sqrt{2}} \mid a, b \in \mathbb{Z}\}$

donde $\mathbb{Z}(x) = \{f(x) \mid f(x) \in \mathbb{Z}[x]\}$.

Preguntas:

Es i un primo en $\mathbb{Z}(i)$?

$$\mathbb{Z}(i) \cong \frac{\mathbb{Z}[x]}{(x^2 + 1)}$$

$$\frac{\mathbb{Z}(i)}{(2)} \cong \frac{\mathbb{Z}(x)}{(4x^2 + 1)} \cong \frac{\mathbb{F}_2(x)}{(x^2 + 1)} \text{ no es dominio.}$$

que $x+1 \neq 0$ en $\mathbb{F}_2[x]$ pero $0 = x^2 + 1 = (x+1)^2$ en $\frac{\mathbb{F}_2[x]}{(x+1)}$.

$$\text{Pero como: } \frac{\mathbb{F}_2[x]}{(x^2+1)} \cong \frac{\mathbb{F}_2[x]}{(x+1)^2} \cong \frac{\mathbb{F}_2[y]}{(y^2)} \cong \mathbb{F}_2 \oplus \mathbb{F}_2$$

Pregunta: $x+1$ es primo en $\mathbb{Z}(i)$?

$$\mathbb{Z}(i) \cong \frac{\mathbb{Z}(x)}{(x^2+1)} \cong \frac{\mathbb{Z}(x)}{(x+1, x+1)} \cong \frac{\mathbb{Z}(-1)}{(-1+1)} \cong \frac{\mathbb{Z}}{(2)} \cong \mathbb{F}_2$$

Doblando

Usar el resultado de la página anterior.

Entonces $x+1$ es primo.

Otro caso: $\mathbb{Z}(\sqrt{-r})$

$$\mathbb{Z}(\sqrt{-r}) \cong \frac{\mathbb{Z}(x)}{(3, x+1)} \cong \frac{\mathbb{F}_3(x)}{(x^2 - 1)} \cong \frac{\mathbb{F}_3(x)}{(x-1)} \cong \frac{\mathbb{F}_3(x)}{(x+1)} \cong \mathbb{F}_3 \times \mathbb{F}_3$$

Así: $\varphi: \mathbb{Z}(\sqrt{-r}) \rightarrow (\mathbb{F}_3, \mathbb{F}_3)$

$$\ker \varphi = (3)$$

$$\ker \varphi_1 = (3, \sqrt{-r} - 1)$$

ideales maximales

$$\ker \varphi_2 = (3, \sqrt{-r} + 1)$$

$$(3) = (3, \sqrt{-r} - 1) \cap (3, \sqrt{-r} + 1)$$

$$\mathbb{Z}(-\sqrt{-r}) \quad 3, 3_2 \leftarrow \text{ideales primos}$$

Diseño

decomposición

(1+x)

raizificada

$$\text{dim}_{\mathbb{F}_2} \mathbb{Z}(i) = \frac{(x-1)}{(1+x)} \cong \frac{(x-1)}{(1+x)} \cong \frac{(1-1)}{(1)} = 0$$

$$\text{Ultimo caso: } \frac{\mathbb{Z}(i)}{(3)} \cong \frac{\mathbb{Z}(x)}{(x^2+3)} \cong \frac{\mathbb{F}_3[x]}{x^2+3} \cong \mathbb{F}_3(i)$$

$$\mathbb{Z}(i) \quad (3)$$

$$\begin{array}{c|c} & \text{inverte} \\ \mathbb{Z} & (3) \end{array}$$

$$\text{Tarea: } \text{Grado} = 2^4$$

$$\text{Grado}_2 = 2^6$$

$$\rightarrow \text{Grado} = 2^7$$

Entero algebraico: ssi

1) x satisface un polinomio monico con coeficientes enteros

2) $\mathbb{Z}(x)$ es finitamente generado como grupo abeliano

3) \exists un grupo abeliano f.p. $M \subseteq \mathbb{C}$ con $\mathbb{Z} \subseteq M \oplus (M \neq 0)$

Dem.: 2) \Rightarrow 3) obvio

1) \Rightarrow 2) Demostreado. Entero $\Rightarrow x^n, \dots \in \langle 1 \rangle_d, \dots, \langle x^{n-1} \rangle$

3) \Rightarrow 1) Supongamos que $M = \langle m_1, \dots, m_r \rangle$

$\forall m_i \in M$, $\exists x_1, \dots, x_r \in \mathbb{Z}$ $\exists x \in \mathbb{Z}$ tal que

$$x m_i = \sum_{j=1}^r a_{ij} m_j$$

$$x m_i = \underbrace{\sum_{j=1}^r a_{ij} m_j}_{\in M} = \underbrace{A \tilde{m}}_{\in M} \quad (\because I - A) \tilde{m} = 0 \text{ por (*)}$$

Matricialmente si $M = \begin{pmatrix} m_1 & \dots & m_r \end{pmatrix}$

De (*)

$B \in \mathcal{M}_n(\mathbb{C})$, $B B^* = \det B \cdot I$

matriz transpuesta de los cofactores

$\det(xI - A) \tilde{m} = 0$ luego $\det(xI - A) = 0$ \leftarrow polinomio monico con coeficientes enteros.

Más generalmente, si D es un dominio de integridad:

$D \subseteq L$ (cuerpo)

$\alpha \in L$ se dice entero sobre D si $\sqrt{}$ es raíz de una ecuación algebraica monómica, con coeficientes en D :

$$\alpha^n + d_{n-1} \alpha^{n-1} + \dots + d_0 = 0.$$

* Ejercicio:

Estos:

2) $D[\alpha]$ es finitamente generado como D -módulo

3) \exists un D -módulo f.p. $\Pi \subseteq L$ con $\alpha \in \Pi$

* $(\Pi \in \text{un } D\text{-módulo}, \forall \alpha \in \Pi, \text{ si es grupo abeliano}) \Rightarrow \dim_{D[\alpha]} \Pi = \dim_{D[\alpha]} \Pi \otimes_D L$

Prop: Si $D \subseteq L$ satisfacen: (D , o dominios, L cuerpo)

1) $\alpha \in L$ es entero sobre D .
2) Cada elemento de O es entero sobre D .
Entonces α es entero sobre D .

Dem:

caso I: O es finitamente generado sobre D .

α entero sobre $O \Rightarrow \alpha^n \in \langle 1, \alpha, \dots, \alpha^n \rangle, \forall n \geq 0$.

$$O[\alpha] \subseteq \bigoplus_{i=0}^n \alpha^i O$$

Con mayor rango $\exists M \in D[\alpha] \subseteq \bigoplus_{i=0}^n \alpha^i O = M$

M f.p. con $\alpha M \subseteq M$

M es α -módulo $\Rightarrow M \in \text{sf}(D)$ -módulo

$\therefore \alpha$ es entero sobre D .

caso general: Si α es entero sobre Θ

$$\alpha^n + \alpha^{n-1} u_{n-1} + \dots + u_0 = 0, \quad u_i \in \Theta, \quad i \in \{0, \dots, n-1\}.$$

Sea $\Theta' = D[u_0, \dots, u_{n-1}] \subseteq \Theta$ (pues $D \subseteq \Theta$ y $u_i \in \Theta$)

Basta ver que Θ' es f.p. como D -módulo, pues α es entero sobre Θ' .

Lemma: Si u_0, u_1, \dots, u_n son enteros sobre D

$\Theta' = D[u_0, \dots, u_n]$ es f.p. como D -módulo.

Dem: Por inducción:

Si $n=0$: $\Theta' = D[u_0]$, por definición de entero.

Supongamos que $D[u_0, \dots, u_i]$ es f.p.

u_{i+1} es entero sobre D , luego sobre $D[u_0, \dots, u_i]$

Esto nos dice que $D[u_0, \dots, u_i][u_{i+1}] = \bigoplus_{j=0}^i D[u_0, \dots, u_i] u_{i+1}^{j+1}$ f.p.

$\therefore D[u_0, \dots, u_{i+1}]$ es f.p. como D -módulo.

y como todo elemento de Θ es entero sobre $D \Rightarrow \alpha$ es entero sobre D

$\Rightarrow D[u_0, \dots, u_n]$ es un D -módulo f.p. y se concluye como

en el caso anterior.

Def: Si cada elemento de Θ es entero sobre D diremos que Θ es entero sobre D .

Prop: Si x_1, \dots, x_n son enteros sobre D , entonces $D(x_1, \dots, x_n)$ es entero sobre D .

Demo: $\Pi = D[x_1, \dots, x_n]$ es f.g como D -módulo.

Luego si $d \in D[x_1, \dots, x_n]$ entonces $\exists f_i \in D$ tales que $d = \sum f_i x_i$.
 $\left. \begin{array}{l} \Pi \text{ es } D\text{-m\'odulo} \\ \Pi \text{ es f.p.} \end{array} \right\} \Rightarrow d \text{ es entero sobre } D$

Def: Sea $D \subseteq L$ (D dominio, L cuerpo) y sea

$\text{Lent} = \{x \in L \mid x \text{ entero sobre } D\}$.

Entonces Lent es un anillo. (D dominio de independencia).

Demo: Si $x_1, x_2 \in \text{Lent}$.

entonces $D[x_1, x_2]$ es entero sobre D (que x_1, x_2 enteros) y $x_1 + x_2, x_1 \cdot x_2 \in D[x_1, x_2]$, luego son enteros.

Si $K \mid \mathbb{Q}$ es una extensión finita, diremos que K es un Cuerpo de Números (o Cuerpo de Números Algebraicos). \mathbb{Q} es el anillo de enteros.

$\mathcal{O}_K = \{x \in K \mid x \text{ entero}\}$ es un anillo. (Anillo de enteros de K)

(Esto ya que K es cuerpo y $K \subseteq \mathbb{C}$)

Si $\mathfrak{U} \subseteq K \subseteq L$ ext. finita y $x \in L$ es un entero sobre \mathcal{O}_K

entonces $x \in \mathcal{O}_L$. (resultado anterior).

Por tanto \mathcal{O}_L es un anillo de enteros sobre \mathcal{O}_K .

Por lo tanto \mathcal{O}_L es un anillo de enteros sobre \mathbb{Z} .

Por lo tanto \mathcal{O}_L es un anillo de enteros sobre \mathbb{Z} .

Si d es entero $\Rightarrow \mathbb{Z}(\sqrt{d}) \subseteq \Theta_K$
 $(\forall \in K)$

Caso 1: K/\mathbb{Q} es una extensión cuadrática

Prop: Si K/\mathbb{Q} es una extensión cuadrática

$K = \mathbb{Q}(\sqrt{d})$, d libre de cuadrados, entonces

$$\Theta_K = \begin{cases} \mathbb{Z}(\sqrt{d}), & \text{si } d \equiv 2 \text{ o } 3 \pmod{4} \\ \mathbb{Z}\left(\frac{1+\sqrt{d}}{2}\right), & \text{si } d \equiv 1 \pmod{4}. \end{cases}$$

Dem: \Rightarrow queremos saber cuándo $a+b\sqrt{d} \in \Theta_K$, si $a, b \in \mathbb{Z}$

$$p(x) = (x - a - b\sqrt{d})(x + a + b\sqrt{d}) = x^2 - 2ax + (a^2 - b^2d)$$

he destratamos saber cuándo $p(x)$ tiene coef. enteros.

$$2a, a^2 - b^2d \in \mathbb{Z}$$

$$2a \in \mathbb{Z} \Rightarrow 4a^2 \in \mathbb{Z} \Rightarrow 4b^2d = 4(a^2 - d(a^2 - b^2d)) \in \mathbb{Z}$$

Si $b = \frac{m}{n}$, $d = \frac{l}{r} \Rightarrow 4\frac{m^2l}{n^2r} \in \mathbb{Z} \Rightarrow n^2 \mid 4l$, pero $4l$ es libre de cuadrados
 $\Rightarrow (m, n) = 1$

Comparando dcsc. en primos: $n \in \{1, 2\}$, así $2b \in \mathbb{Z}$.

$$\text{Si } a = \frac{t}{2}, b = \frac{s}{2}$$

$$a+b\sqrt{d} = \frac{t+s\sqrt{d}}{2} \in \Theta_K$$

$$\text{así: } p(x) = x^2 - 2ax + (a^2 - b^2d) = x^2 - tx + \frac{t^2 - 4s^2}{4} = 0$$

¿Cuándo $\frac{t^2 - 4s^2}{4} \in \mathbb{Z}$?

Caso 1: t, s pares.

Caso 2: t impar, s par \Rightarrow no puede ser

Caso 3: t par, s impar $\Rightarrow t^2 \pmod{4} \equiv 0, 1 \pmod{4}$, $s^2 \equiv 1 \pmod{4} \Rightarrow$ no puede ser

Caso 4: t, s impares $\Rightarrow t^2, s^2 \equiv 1 \pmod{4}$.

$$0 \equiv t^2 \pmod{d} \Rightarrow 1 \equiv 1 \pmod{d}$$

$$\therefore d \equiv 1 \pmod{4}$$

a) Si $d \not\equiv 1 \pmod{4}$

a, b son enteros: $a+b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$

b) Si $d \equiv 1 \pmod{4}$

entonces $a+b\sqrt{d} \in O_K$ si $a, b \in \mathbb{Z}$ bien: $(a+\frac{t}{2})+b\frac{s}{2}\sqrt{d} = \frac{1}{2}(2a+t)+\frac{s}{2}(\sqrt{d})$, si impares.

entonces:

a) $a+b \in \mathbb{Z}(\sqrt{d})$

enteros

b) $\frac{t}{2} + \frac{s}{2}\sqrt{d} \in \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$

y ademas: $O_K \subseteq \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ como $\frac{1+\sqrt{d}}{2}$ es entero: $O_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$

Ejemplo: $K = \mathbb{Q}(\sqrt{-3})$ entonces $O_K = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}] = \mathbb{Z}[\frac{1-\sqrt{-3}}{2}]$.

o sea $O_K = \mathbb{Z}(\omega)$ donde ω raiz cúbica de la unidad.

Definición: A dominio se dice normal si

$K_{\text{int}} = \{x \in K \mid x \text{ es entero sobre } A\}$

donde A es el cuerpo de cocientes de K , satisface:

$K_{\text{int}} = A$

O_K es el entero sobre de K , que satisface

1) O_K es entero sobre \mathbb{Z} .

2) O_K es normal.

3) $K = \text{El int}(O_K)$.

entonces $O_K = \{x \in K \mid x \text{ es entero sobre } \mathbb{Z}\}$

$(a, b \in \mathbb{Z}) \Leftrightarrow (a/b \text{ entero}, a \in \mathbb{Z})$

Proposición: Un DFU es normal.

Dem: Sea D un DFU. $K \subseteq \text{Quot}(D)$

Sea $\frac{m}{n} \in K$ entero sobre D , $(m, n) = 1$

entonces $\frac{m}{n}$ satisface:

$$X^n + d_{n-1} X^{n-1} + \dots + d_0 = 0$$

Sea $p | n$ primo.

$$\left(\frac{m}{n}\right)^n + d_{n-1} \left(\frac{m}{n}\right)^{n-1} + \dots + d_0 = 0$$
$$\underbrace{m^n + d_{n-1} m^{n-1} n + \dots + d_0 n^n}_{\not\equiv 0(p)} = 0 \quad (\ast)$$

(pues $p | n \Rightarrow p | m$).

entonces $n \in D^*$ $\Rightarrow \frac{m}{n} \in D$ $\# \text{ Quot}(D)_{\text{ent}} \subseteq D$ y claramente:

$D \subseteq \text{Quot}(D)_{\text{ent}} \Rightarrow D = \text{Quot}(D)_{\text{ent}}$.

*Ejercicio: $\mathbb{Z}(\sqrt{-5}) = \bigcup \mathcal{U}(\sqrt{-5})$.

$\mathbb{Z}(\sqrt{-5})$ y $\mathbb{Z}[\omega]$ son dominios de factorización única, basta ver que

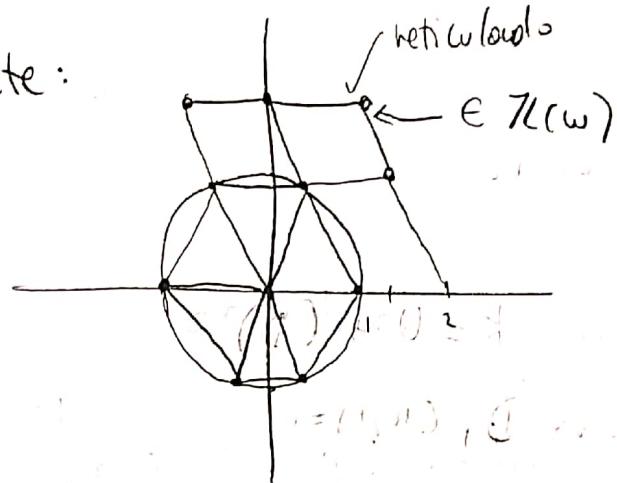
para cada $m, n \in \mathbb{Z}[\omega]$ existen f, r con

$$m = n f + r \quad \# \|r\| < \|n\| \quad r = 0.$$

Como son números complejos: $\frac{m}{n} = f + \frac{r}{n}$ con $\|\frac{r}{n}\| < 1 \Rightarrow r = 0$.

Basta ver que todo elemento de $\mathbb{Q}[\omega]$ está a distancia menor al de un elemento de $\mathbb{Z}(\omega)$.

Gráficamente:



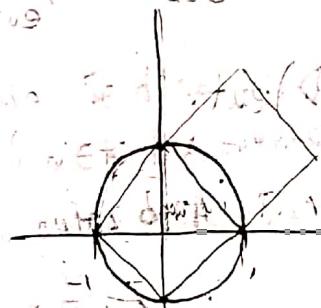
$$\|u-w\| \leq \frac{1}{2} \text{ al punto } z$$

Euler triángulos centrales $\sigma =$

$$l = \frac{1}{\sqrt{3}} < 1.$$

* Ejercicio: Hacer para $\pi(\sqrt{-1})$.

Gráficamente:



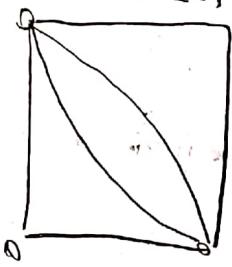
$$\|u-w\| \leq \frac{1}{2} \text{ al punto } z$$

$$(l \cos 30^\circ = \frac{\sqrt{3}}{2} \Rightarrow l = \frac{\sqrt{3}}{\cos 30^\circ} = \frac{\sqrt{3}}{\sqrt{3}} = 1)$$

(w) $\pi(\sqrt{-1})$

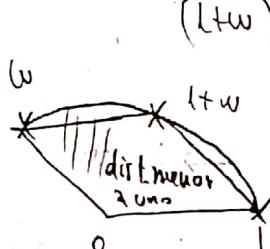
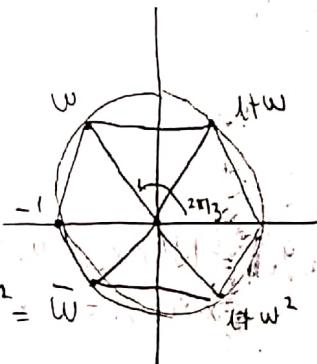
Si $t, A, B \in \mathbb{Z}$: $t^2 + At + B = 0 \Rightarrow \|z\| = B$ pues
 $x^2 + Ax + B = (x - t)(x - \bar{t}) \Rightarrow |t| = \|z\| = B$.

i) Para $\mathbb{Z}(i)$:



todos los puntos del cuadrado están a distancia menor o igual a 1
 que son puntos del reticulado.

Para $\mathbb{Z}(\omega) = \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$, $\mathbb{Z}(\omega) \subseteq \mathbb{C}$, $\omega = -\frac{1-i\sqrt{3}}{2}$, $\omega^2 + \omega + 1 = 0$.



y $1+\omega, \omega, 1$ están en el reticulado.

Ejercicio: $\mathbb{Z}(\sqrt{-2})$ hacerlo mismo.

Otro tipo de problemas: $\mathbb{Z}(\sqrt{2})$ denses en \mathbb{R}

$\mathbb{F} = \{a+b\sqrt{2} \mid 0 \leq a, b \leq N\} \subseteq [0, N+\sqrt{2}] \subseteq [0, \frac{5N}{2}]$, además:

$$\#\mathbb{F} = (N+1)^2 > N^2$$

Hay al menos dos elementos de \mathbb{F} a distancia menor a $\frac{1}{N^2}$.

Existen $a, b, c, d \in \mathbb{Z}$

$$|(a+b\sqrt{2}) - (c+d\sqrt{2})| \leq \frac{N}{2}$$

$$|(a-c) + (b-d)\sqrt{2}| \leq \frac{N}{2}$$

luego $\mathbb{Z}(\sqrt{2})$ es denso en \mathbb{R} .

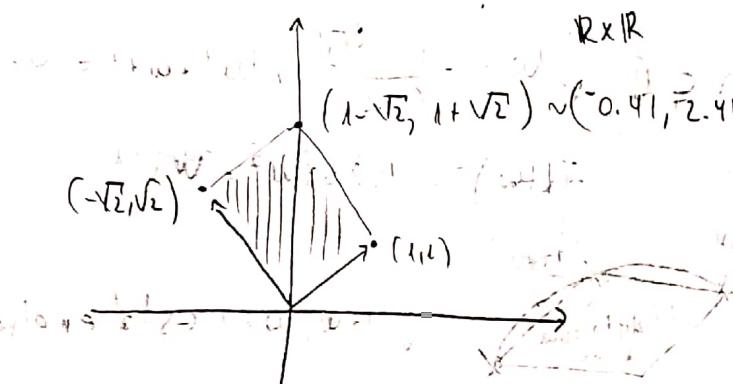
$$\mathbb{Z}(\sqrt{2}) \hookrightarrow \mathbb{R} \times \mathbb{R}$$

$$(a, b)(c, d) = (ac, bd)$$

Como? $\Phi: \mathbb{Z}(\sqrt{2}) \longrightarrow \mathbb{R} \times \mathbb{R}$

$$\begin{aligned} 1 &\mapsto (1, 1) \\ \sqrt{2} &\mapsto (-\sqrt{2}, +\sqrt{2}) \end{aligned}$$

$$(-\sqrt{2}, +\sqrt{2})^2 = (2, 2) \quad \therefore \Phi \text{ es bi\'univoque definida (como h\'an de serlos).}$$



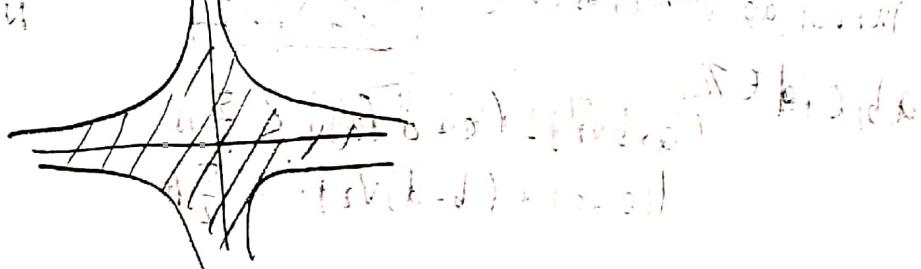
$$\begin{aligned} N(x_1y_1) &= xy, \quad (\text{multiplicaci\'on}) \quad N((x_1, y_1)(x_2, y_2)) = N(x_1x_2, y_1y_2) \\ p(a+b\sqrt{2}) &= |N(x_1y_1)| \quad = x_1x_2y_1y_2 = N(x_1y_1)N(x_2y_2) \end{aligned}$$

$$\begin{aligned} \Phi(a+b\sqrt{2}) &= a\Phi(1) + b\Phi(\sqrt{2}) \\ &= a(1, 1) + b(-\sqrt{2}, +\sqrt{2}) \end{aligned}$$

$$p(\Phi(a+b\sqrt{2})) = |(a+b\sqrt{2})(-\sqrt{2}, +\sqrt{2})| = |a^2 - 2b^2|$$

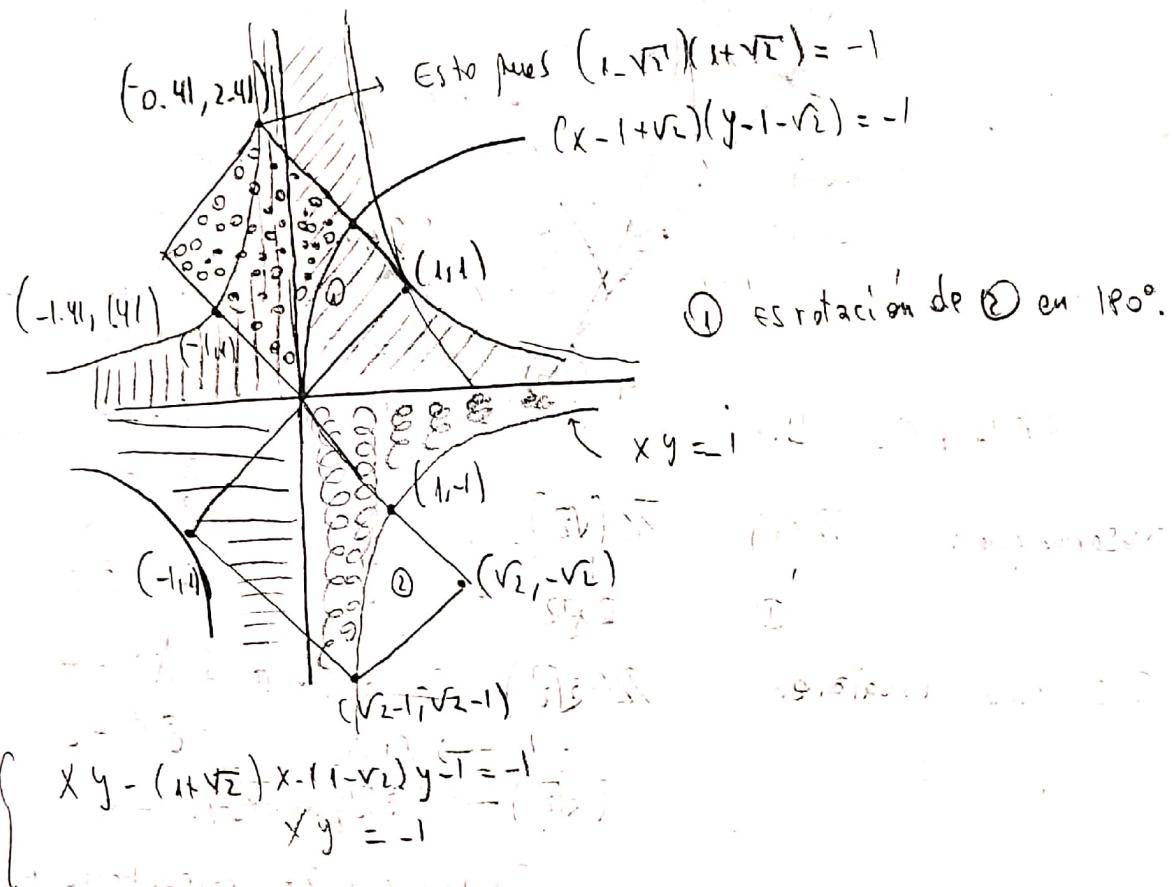
$$N(a+b\sqrt{2}) = |a^2 - 2b^2|.$$

Queremos ver donde $p(x_1y_1) < 1 \Rightarrow xy = 1, xy = -1$. $x_1 \in \mathbb{Z}(\sqrt{2})$



$$|a\sqrt{2}(k-j) + b\sqrt{2}| < 1$$

Basta con estudiar un paralelepípedo. (Los otros son desplazamientos de este).



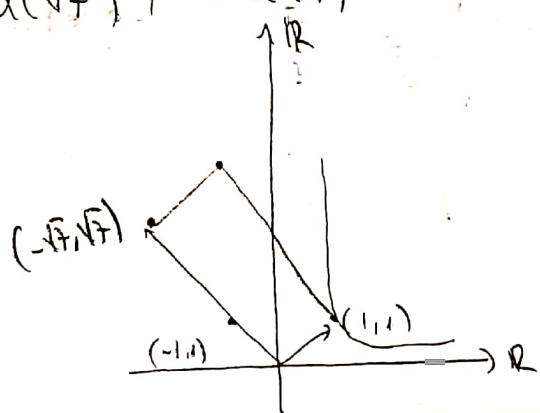
$$\begin{aligned} \frac{-1}{xy} &= \frac{-1}{1+\sqrt{2}} - \frac{1-\sqrt{2}}{1+\sqrt{2}} y \\ -1 &= -y \frac{(1-\sqrt{2})y}{1+\sqrt{2}} \Rightarrow \frac{(1-\sqrt{2})y + (1-\sqrt{2})}{1+\sqrt{2}} y^2 = 0 \end{aligned}$$

$$y \Delta P = 1 + 4(1+\sqrt{2})(1-\sqrt{2}) = -3 \therefore \text{no hay solucion.}$$

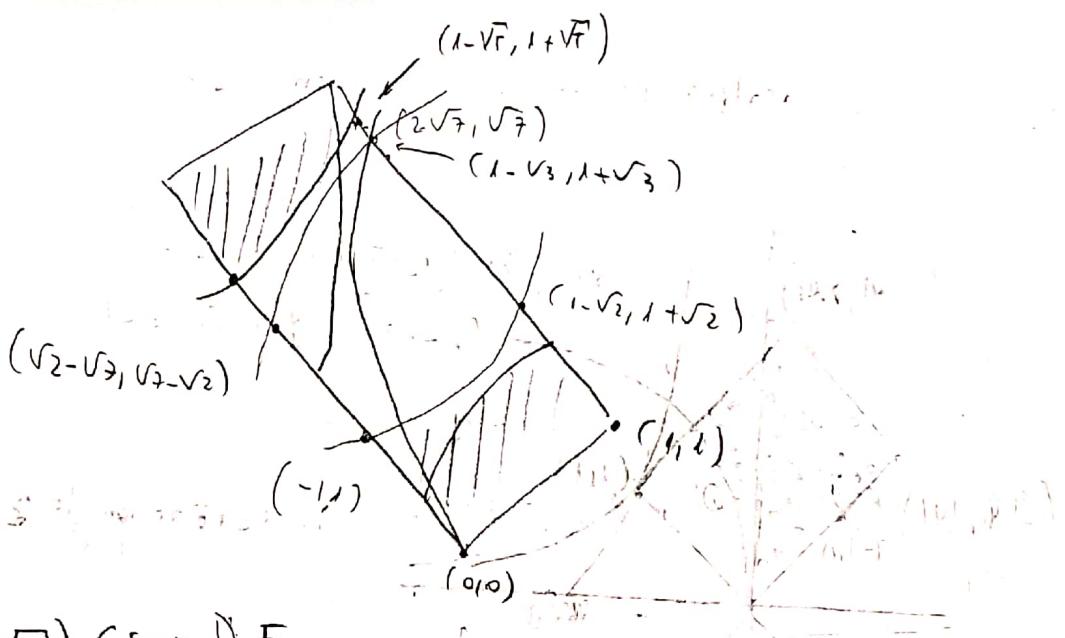
$\therefore \mathcal{L}(\sqrt{f})$ es D.E.

O Ejercicio: Pensar $\mathcal{L}(\sqrt{f})$.

Otro caso: $\mathcal{L}(\sqrt{f})$, $0 \mathcal{L}(Nf) = \mathcal{L}(Nf)$



Ampliando:



$\therefore \mathcal{L}(\sqrt{f}) \in \text{sun D.E.}$

Observe que : $\mathcal{R}(i)$

Sí queremos trabajar en

$\pi(\sqrt{2})$

$\mathbb{R} \times \mathbb{R}$

$$\mathcal{U}(\sqrt[3]{2}) \hookrightarrow \mathbb{R} \times \{1\}$$

$$f = \lambda x. \tilde{y} M$$

$$(\sqrt[3]{2}) \mapsto (\sqrt[3]{2}, \omega\sqrt[3]{2})$$

en $\mathbb{Z}(d)$, si $m_d(x)$ tiene raíces reales y 2 raíces no reales

$\mathbb{R} \times \dots \times \mathbb{R} \times \mathbb{C}$

$$x \mapsto (x_1, \dots, dx_1, \beta_1, \dots, \beta_{r_2}).$$

raíces reales \Leftrightarrow uno de cada par de raíces

función de probabilidad f(x) $\in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$

2^o de la de P-áfricano
extensión de ETCulares.

$$(\text{d}x^1, \dots, \text{d}x^n) = \text{d}(x^1, \dots, x^n) = (\text{d}x^1, \dots, \text{d}x^n)$$

Anillos de fracciones.

A anillo conmutativo

$S \subseteq A$ tal que $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$ conjunto multiplicativo.

$$S^{-1}A = \left\{ \frac{a}{s} \mid a \in S \right\}$$

dos fracciones son iguales $\frac{a}{s} = \frac{a'}{s'}$ si existe $s'' \in S$ tal que:

$$s''(as' - a's) = 0.$$

Ejercicio: Es relación de equivalencia en $A \times S$

$$\text{Ejemplo: 1)} \quad \frac{a}{s} = \frac{a''s''}{s''s''}$$

$$2) \quad a s' = a' s \Rightarrow \frac{a}{s} = \frac{a'}{s'}$$

$$\text{Ejemplo: 1)} \quad A = \mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$$

$$S = \{3\}$$

$$S^{-1}A = \left\{ \frac{0}{3}, \frac{1}{3}, \frac{2}{3}, \dots, \frac{5}{3} \right\} \text{ Algunos son iguales:}$$

$$\frac{2}{3} = \frac{0}{3} \text{ pues } 2 \cdot 3 = 0 \cdot 3, \quad \frac{5}{3} = \frac{3}{3}, \quad \frac{6}{3} = \frac{0}{3}, \quad \frac{1}{3} = \frac{1}{3}$$

$$S^{-1}A = \left\{ \frac{0}{3}, \frac{1}{3} \right\}$$

$$2) \quad A = \mathbb{Z}/6\mathbb{Z} = \frac{0}{2} = \frac{2}{2} = \frac{4}{2} = \frac{6}{2} = 0$$

$$S = \{1, 3\} = \frac{1}{2} = \frac{3}{2} = \frac{5}{2} = \frac{7}{2}$$

$$0 = \frac{0}{2} = \frac{1}{2} + \frac{3}{2} = \frac{1}{2} + \frac{5}{2} = \frac{1}{2} + \frac{7}{2} = 0$$

$$\frac{1}{2} = \frac{1}{2} + \frac{3}{2} = \frac{1}{2} + \frac{5}{2} = \frac{1}{2} + \frac{7}{2} = 0$$

Se puede ver antes como: $\left\{ \frac{0}{2}, \frac{1}{2}, \frac{3}{2}, \frac{5}{2}, \frac{7}{2} \right\} \Rightarrow \frac{1}{2} = \frac{3}{2} \Rightarrow$ Es que ampliar

$$\frac{3}{2} = \frac{3}{1}$$

hacer: $A_S = S^{-1}A = \left\{ \frac{0}{3}, \frac{1}{3} \right\}$.