Def.- Dadas dos sucesiones $(a_1, a_2, \ldots)$ y $(b_1, b_2, b_3, \ldots)$ consideramos la sucesión

$$a_0, \quad a_0 + \frac{b_1}{a_1}, \quad a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2}}, \quad \ldots$$

y el límite de esta sucesión (si es que existe) es lo que entenderemos por la fracción continua infinita

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \ldots}}$$

En el estudio de este curso nos interesarán las llamadas fracciones continuas simples las cuales tiene $b_i = 1 \quad \forall i$

Teorema.- Todo número racional $\frac{a}{b}$ con $(a,b)=1$, tiene expansión en fracción continua simple ~~finita~~.

Dem.- Por el algoritmo de euclides $a = bq_1 + r_1$ y entonces $\frac{a}{b} = q_1 + \frac{r_1}{b}$

$$= q_1 + \frac{1}{\left(\frac{b}{r_1}\right)}$$

pero nuevamente por el algoritmo de euclides $b = r_1 q_2 + r_2 \Rightarrow \frac{b}{r_1} = q_2 + \frac{r_2}{r_1}$

y entonces $\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \frac{r_2}{r_1}}$

y como el algoritmo de euclides es finito

$\Rightarrow \frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots + \frac{1}{q_n}}}$ ∎

Notación para identificar una fracción continua utilizamos la notación $[a_1, a_2, \ldots, a_n]$ si es finita y $[a_1, a_2, \ldots]$ si es infinita y en caso de repetir patrón $[a_1, \overline{b_1, b_2, \ldots, b_k}]$

Def.- Dada una fracción continua simple $[a_1, \ldots, a_n]$, llamaremos convergentes a las sumas parciales $\delta_1 = [a_1]$, $\delta_2 = [a_1, a_2]$, ..., etc.

Podemos dar una fórmula explícita para cada convergente.

Definimos $P_0 = 1$, $Q_0 = 0$

$\delta_1 = q_1 = \frac{q_1}{1} = \frac{P_1}{Q_1}$

$\delta_2 = q_1 + \frac{1}{q_2} = \frac{q_2 \left(q_1 + \frac{1}{q_2}\right)}{q_2}$

$= \frac{q_2 q_1 + 1}{q_2} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{P_2}{Q_2}$

y así tendremos que

$$\delta_n = \frac{q_n P_{n-1} + P_{n-2}}{q_n Q_{n-1} + Q_{n-2}}$$

con

$$P_n = q_n \cdot P_{n-1} + P_{n-2} \quad y \quad Q_n = q_n \cdot Q_{n-1} + Q_{n-2}$$

$$P_0 = 1 \wedge Q_0 = 0$$

Proposición.- Dada la sucesión de fibonacci se tiene que $\frac{F_n}{F_{n-1}} = [\underbrace{1, 1, \ldots, 1}_{n \text{ veces}}] \quad \forall n \geq 2$

Dem.- Por inducción sobre n.

~~Se tiene que $\frac{F_2}{F_1} = \frac{1}{1} = 1 = [1]$, sup. que es válido para $k > 1$, entonces, sabemos que~~

$$~~[\underbrace{1, 1, \ldots, 1}_{k+1 \text{ veces}}] = 1 + [\underbrace{0, 1, \ldots}_{k}] = 1 + \frac{1}{1+1} \ldots = 1 + \frac{1}{[\underbrace{1, \ldots, 1}_{k-1 \text{ veces}}]}~~$$

$$~~= 1 + \frac{1}{\left(\frac{F_{k-1}}{F_{k-2}}\right)} = 1 + \frac{F_{k-2}}{F_{k-1}} = \frac{F_k}{F_{k-1}}~~$$

¿El ayudante lo escribió mal"

$$\frac{F_n}{F_{n-1}} = [\underbrace{1, 1, \ldots, 1}_{n-1 \text{ veces}}]$$

por lo anterior

$$\Rightarrow \lim_{n\to\infty} \frac{F_n}{F_{n-1}} = [\overline{1}] = 1 + \cfrac{1}{1+\cfrac{1}{1+\cdots}}$$

y sabemos que $\lim_{n\to\infty} \frac{F_n}{F_{n-1}} = \varphi$

$$\therefore \varphi = 1 + \cfrac{1}{1+\cfrac{1}{1+\cdots}}$$

Proposición: Si $B > C \Rightarrow [a, B] < [a, C]$

Dem: Como $B > C \Rightarrow \frac{1}{B} < \frac{1}{C}$

$\Rightarrow a + \frac{1}{B} < a + \frac{1}{C} \Rightarrow [a, B] < [a, C]$

Proposición: Si $[a, b] < [a, c] \Rightarrow [d, a, b] > [d, a, c]$

Dem: por lo anterior,

como $[a, b] < [a, c] \Rightarrow [d, [a, b]] > [d, [a, c]]$

pero $[d, [a, b]] = d + \frac{1}{[a, b]} = d + \cfrac{1}{a + \frac{1}{b}}$

$= [d, a, b]$

$\Rightarrow [d, a, b] > [d, [a, c]] = [d, a, c]$ $\blacksquare$

Teorema.- Sean $a_0 \in \mathbb{Z}$, $a_1, \dots, a_n, c \in \mathbb{Z}^+$.
Entonces $[a_0, \dots, a_n] > [a_0, \dots, a_n + c]$
si n es par.

Dem.- Para $n=0$, como $c \in \mathbb{Z}^+ \Rightarrow a_0 + c > a_0$
$\Rightarrow [a_0 + c] > [a_0]$ V

Para $n=1$, tenemos que $a_1 < a_1 + c$
$\Rightarrow \frac{1}{a_1+c} < \frac{1}{a_1} \Rightarrow a_0 + \frac{1}{a_1+c} < a_0 + \frac{1}{a_1}$
$\Rightarrow [a_0, a_1 + c] < [a_0, a_1]$ X

Def.- una fracción continua simple es:

$$[a_1, a_2, \dots, a_n] = a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}$$

Obs.- si simple se considera $a_n \neq 1$, pues $[a_0, \dots, a_n, 1] = [a_0, \dots, a_n + 1]$

$0 \le \{x\} < 1$

Obs.- $\forall a, b \in \mathbb{Z}$, $\frac{a}{b} = \lfloor \frac{a}{b} \rfloor + \{\frac{a}{b}\} = \lfloor \frac{a}{b} \rfloor + \frac{1}{\frac{1}{\{a/b\}}}$

y como $\{\frac{a}{b}\} < 1 \Rightarrow \frac{1}{\{\frac{a}{b}\}} > 1$

$$\Rightarrow \frac{a}{b} = \lfloor \frac{a}{b} \rfloor + \cfrac{1}{\lfloor \frac{1}{\{a/b\}} \rfloor + \{ 1/\{a/b\} \}}$$

... Así $a_0 = \lfloor \frac{a}{b} \rfloor \in \mathbb{Z}$ y $a_n \in \mathbb{Z}^+$

Obs.> Notemos qué pasa por a $\sqrt{2}$

$$\Rightarrow \sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + \cfrac{1}{\left(\frac{1}{\sqrt{2}-1}\right)} = 1 + \cfrac{1}{\left(\frac{1}{\sqrt{2}-1}\right) \cdot \frac{\sqrt{2}+1}{\sqrt{2}+1}}$$

$$= 1 + \frac{1}{\sqrt{2}+1} = 1 + \cfrac{1}{2 + (\sqrt{2}-1)} = 1 + \cfrac{1}{2 + \cfrac{1}{\sqrt{2}+1}}$$

$$= 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\sqrt{2}+1}}} = \dots$$

¿será que $\sqrt{2} = [1, 2, 2, \dots] = [1, \overline{2}]$?

Def.: (con el procedimiento de clases pasadas)

se definen h_n: $h_{-2}=0$, $h_{-1}=1$, $h_n = a_n h_{n-1} + h_{n-2}$

k_n: $k_{-2}=1$, $k_{-1}=0$, $k_n = a_n k_{n-1} + k_{n-2}$,

son tales que $\frac{h_0}{k_0} = a_0$, $\frac{h_1}{k_1} = \frac{a_1 a_0 + 1}{a_1 + 0}$

$= a_0 + \frac{1}{a_1}$

y así $\frac{h_n}{k_n} = [a_0, a_1, \dots, a_n]$

Propiedades:

- $[a_0, a_1, \dots, a_{n-1}, x] = \frac{x h_{n-1} + h_{n-2}}{x k_{n-1} + k_{n-2}}$
- $h_n k_{n-1} - h_{n-1} k_n = (-1)^{n-1}$
- $h_n k_{n-2} - h_{n-2} k_n = (-1)^n a_n$

Prop. Todo racional tiene una fracción continua finita y todo irracional una infinita

Dem.: (ayudantía)

para irracionales, α se definen

$a_0 = \alpha$, $a_n = \lfloor \alpha_n \rfloor$ con $\alpha_n = \frac{1}{\{\alpha_n\}}$

$\Rightarrow \alpha = \alpha_0 = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \cdots \alpha_g}}$ etc.

$\Rightarrow \alpha = [a_0, a_1, \dots, a_{n-1}, \alpha_n] = \frac{\alpha_n h_{n-1} + h_{n-2}}{\alpha_n k_{n-1} + k_{n-2}}$

Notemos que k_n es creciente,

para $n \geq 0$ afirmo que $\left|\alpha - \frac{h_n}{k_n}\right| \leq \frac{1}{k_n k_{n+1}}$

Demostremos que

$$\left|\alpha - \frac{h_n}{k_n}\right| = \left|\frac{\alpha_n h_{n-1} + h_{n-2}}{\alpha_n k_{n-1} + k_{n-2}} - \frac{h_n}{k_n}\right|$$

$$= \left|\frac{k_n[\alpha_n h_{n-1} + h_{n-2}] - h_n[\alpha_n k_{n-1} + k_{n-2}]}{k_n[\alpha_n k_{n-1} + k_{n-2}]}\right|$$

$$= \left|\frac{\alpha_n[k_n h_{n-1} - h_n k_{n-1}] + [k_n h_{n-2} - h_n k_{n-2}]}{\sim}\right|$$

$$= \left|\frac{\alpha_n[(-1)^{n-1}] + [-(-1)^n a_n]}{\sim}\right|$$

$$= \left|\frac{\alpha_n(-1)^n + (-1)^{n+1} a_n}{\sim}\right| = \left|\frac{(-1)^n[\alpha_n - a_n]}{\sim}\right| = \left|\frac{(-1)^n\{\alpha_n\}}{\sim}\right|$$

$$\leq \left|\frac{1}{k_n|\alpha_{n+1} k_n + k_{n+1}}\right| \leq \frac{1}{k_n k_{n+1}}$$

y así como k_n es creciente

$$\Rightarrow \lim_{n\to\infty}\left|\alpha_n - \frac{h_n}{k_n}\right| = 0 \Rightarrow \frac{h_n}{k_n} \xrightarrow[n\to\infty]{} \alpha \quad \blacksquare$$

8) - Tendremos entonces que el cociente $\frac{h_n}{k_n}$ es una muy buena aproximación para un irracional.

Además cada término sucesivo se aproxima más al irracional, es decir,

$$\left|\alpha - \frac{h_n}{k_n}\right| < \left|\alpha - \frac{h_{n-1}}{k_{n-1}}\right|$$

Proposición - Si $a, b \in \mathbb{Z}$, $b > 0$, α irracional con convergentes h_n/k_n, entonces

1) si $\left|\alpha - \frac{a}{b}\right| < \left|\alpha - \frac{h_n}{k_n}\right| \Rightarrow b > k_n$

2) si $|b\alpha - a| < |k_n\alpha - h_n| \Rightarrow b \geq k_{n+1}$

Dem -

- Recordemos que se vio que

$$* \text{ si } n \text{ par} \Rightarrow \frac{h_n}{k_n} < \alpha$$
$$* \text{ si } n \text{ impar} \Rightarrow \frac{h_n}{k_n} > \alpha$$

(2) ⇒ (1)

~~Por RA~~ sup. que $b \leq k_n$

$\Rightarrow$ como $\left|\alpha - \frac{a}{b}\right| < \left|\alpha - \frac{h_n}{k_n}\right|$

$\Rightarrow |b\alpha - a| < |k_n\alpha - h_n|$

$\Rightarrow b \geq k_{n+1} > k_n$! $\therefore b < k_n$

(1) ⇒ (2)

Sup. que $b < k_{n+1}$

Notemos que el sistema $\begin{cases} x k_n + y k_{n+1} = b \\ x h_n + y h_{n+1} = a \end{cases}$ tiene soluciones enteras, pues

$\det(A) = k_n h_{n+1} - k_{n+1} h_n = (-1)^n = \pm 1$ y por la regla de Cramer si tendremos soluciones enteras tales que $x \neq 0$ y $y \neq 0$, pues

• Si $x = 0 \Rightarrow$ ~~$x k_{n+1}$~~ $b = y k_{n+1}$ y como $b > 0$ y $k_{n+1} > 0 \Rightarrow y > 0$ $\therefore b = y k_{n+1} \geq k_{n+1}$!! pues $b < k_{n+1}$

• Si $y = 0 \Rightarrow a = h_n x \wedge b = k_n x$ y por hip. $\Rightarrow |k_n \alpha - h_n| > |b\alpha - a|$
$= |x k_n \alpha - x h_n| = |x| |k_n \alpha - h_n| \geq |k_n \alpha - h_n|$

$\therefore |k_n \alpha - h_n| > |k_n \alpha - h_n|$!! $\therefore y \neq 0$

Ahora

* Si $y < 0 \Rightarrow b - y k_n > 0 \Rightarrow x k_n > 0 \Rightarrow x > 0$

* Si $y > 0 \Rightarrow y k_{n+1} \geq k_{n+1} \overset{hip}{>} b \Rightarrow 0 > b - y k_{n+1} = x k_n$ y como $k_n > 0$, $\Rightarrow x < 0$

Ahora, $|b\alpha - a| = |(x k_n + y k_{n+1})\alpha - (x h_n + y h_{n+1})|$
$= |x(k_n \alpha - h_n) + y(k_{n+1}\alpha - h_{n+1})|$

$h_n < \alpha k_n$

Ahora si n par $\Rightarrow \frac{h_n}{k_n} < \alpha \Rightarrow$

$\Rightarrow \alpha k_n - h_n > 0$ y si n impar $\alpha k_n - h_n < 0$

Así como x e y tienen signos distintos entonces $x(k_n\alpha - h_n) \wedge y(k_{n+1}\alpha - h_{n+1})$ tienen el mismo signo, entonces como tienen el mismo signo

$$\Rightarrow |x(k_n\alpha - h_n) + y(k_{n+1}\alpha - h_{n+1})|$$
$$= |x(k_n\alpha - h_n)| + |y(k_{n+1}\alpha - h_{n+1})|$$
$$= |x||k_n\alpha - h_n| + |y||k_{n+1}\alpha - h_{n+1}|$$
$$> |x||k_n\alpha - h_n| \overset{x\neq 0}{\geq} |k_n\alpha - h_n|$$

$\therefore |b\alpha - a| > |k_n\alpha - h_n|$! caso contradice la hipo. $\therefore\ b \geq k_{n+1}$

Proposición: Si $|\alpha - \frac{a}{b}| < \frac{1}{2b^2}$ entonces $\frac{a}{b} = \frac{h_n}{k_n}$ para $n \in \mathbb{N}$. ($b > 0$, α irracional)

Dem:

- Sup. que $d = (a,b)$, $d > 1$.
$\Rightarrow a = d \cdot a' \wedge b = d \cdot b'$ y entonces $(a', b') = 1$, así podemos trabajar con primos relativos

- Spdg que $(a,b) = 1$ y sup. que $\frac{a}{b} \neq \frac{h_n}{k_n}\ \forall n$

Como la sucesión K_n es una sucesión de enteros estrictamente creciente con $K_{-1}=0$
$\Rightarrow \exists m \in \mathbb{N}$ t.q $K_m \leq b < K_{m+1}$.

Luego por la proposición anterior, como
$b < K_{m+1} \Rightarrow |b\alpha - a| \geq |K_m \alpha - h_m|$

con ello

$$0 \neq \left|\frac{a}{b} - \frac{h_m}{K_m}\right| = \left|\frac{a}{b} - \alpha + \alpha - \frac{h_m}{K_m}\right|$$

$$\leq \left|\frac{a}{b} - \alpha\right| + \left|\alpha - \frac{h_m}{K_m}\right| = \left|\alpha - \frac{a}{b}\right| + \left|\alpha - \frac{h_m}{K_m}\right|$$

$$< \frac{1}{2b^2} + \frac{|K_m \alpha - h_m|}{K_m} \leq \frac{1}{2b^2} + \frac{|b\alpha - a|}{K_m}$$

$$< \frac{1}{2b^2} + \frac{1}{2bK_m}$$

por otro lado

$$\left|\frac{a}{b} - \frac{h_m}{K_m}\right| = \frac{|aK_m - bh_m|}{bK_m} \quad \text{y como } \frac{a}{b} \neq \frac{h_m}{K_m}$$

$\Rightarrow aK_m - bh_m \neq 0 \Rightarrow |aK_m - bh_m| \geq 1$

$$\Rightarrow \left|\frac{a}{b} - \frac{h_m}{K_m}\right| \geq \frac{1}{bK_m}$$

$$\therefore \frac{1}{bK_m} \leq \left|\frac{a}{b} - \frac{h_m}{K_m}\right| < \frac{1}{2b^2} + \frac{1}{2bK_m}$$

$$\Rightarrow \frac{1}{bK_m} < \frac{1}{2b^2} + \frac{1}{2bK_m} \overset{\times 2b^2K_m}{\Rightarrow} 2b < K_m + b$$

$\Rightarrow b < K_m$!! pero teníamos que $K_m \leq b$

$\therefore \frac{a}{b} = \frac{h_m}{k_m}$ pra $n \in \mathbb{N}$.

más aún

Así como $(a,b)=1$ y como $(h_n, k_n)=1$

$\Rightarrow a = h_n$ y $b = k_m$ ■

Ayudante

Proposición.- Sea p primo t.q. $p \equiv 3 \pmod 4$
entonces $p \mid a^2+b^2 \Rightarrow p \mid a \wedge p \mid b$

Teorema.- Sea p primo con $p \equiv 1 \pmod 4$
Sea $u \in \mathbb{Z}$ t.q. $u^2 \equiv -1 \pmod p$
Entonces si $u/p = [a_0, a_1, \dots, a_n]$ e
$i_0 = \max\{i \in \{1, \dots, n\} : k_i < \sqrt{p}\}$ se tendrá
que $a = k_{i_0}$ y $b = h_{i_0} p - u k_{i_0}$
cumplen que $p = a^2+b^2$

Lema: Sea $f(x) = x + \frac{1}{x}$. Entonces

- $x < \frac{1+\sqrt{5}}{2} = \varphi \Leftrightarrow x + \frac{1}{x} < \sqrt{5}$
- $x > \frac{1+\sqrt{5}}{2} = \varphi \Leftrightarrow x + \frac{1}{x} > \sqrt{5}$

Lema.- Sea α irracional, entonces
si $\left|\alpha - \frac{h_{j-1}}{k_{j-1}}\right| \geq \frac{1}{\sqrt{5}\, k_{j-1}^2}$ y
$\left|\alpha - \frac{h_j}{k_j}\right| \geq \frac{1}{\sqrt{5}\, k_j^2} \Rightarrow \frac{k_j}{k_{j-1}} < \varphi$

Dem.- De la hip tenemos que

$$\left|\frac{h_n}{k_n}-\frac{h_{n-1}}{k_{n-1}}\right| = \frac{1}{k_n k_{n-1}} \geq \frac{1}{\sqrt{5}k_n^2}+\frac{1}{\sqrt{5}k_{n-1}^2}$$

$$\therefore \frac{1}{\sqrt{5}k_n^2}+\frac{1}{\sqrt{5}k_{n-1}^2} \leq \frac{1}{k_n k_{n-1}} \Rightarrow \frac{k_{n-1}}{k_n}+\frac{k_n}{k_{n-1}} \leq \sqrt{5}$$

Pero lo de la izquierda es racional

así que $\frac{k_n}{k_{n-1}}+\frac{k_{n-1}}{k_n} < \sqrt{5}$ $\therefore$ Si $x = \frac{k_n}{k_{n-1}}$

$$\Rightarrow x+\frac{1}{x} < \sqrt{5} \Rightarrow x < \frac{1+\sqrt{5}}{2}$$

$$\Rightarrow \frac{k_n}{k_{n-1}} < \varphi$$

Teorema (Hurwitz).- De cada 3 convergentes consecutivos alguno de ellos satisface que

$$\left|\alpha-\frac{h_n}{k_n}\right| < \frac{1}{\sqrt{5}k_n^2}$$

Dem.- Sean $\frac{h_{n-1}}{k_{n-1}}, \frac{h_n}{k_n}, \frac{h_{n+1}}{k_{n+1}}$ y SPG que ~~alguno~~ ninguno satisface lo anterior

$$\Rightarrow \left|\alpha-\frac{h_{n-1}}{k_{n-1}}\right| \geq \frac{1}{\sqrt{5}k_{n-1}}, \quad \ldots \quad y \quad \ldots$$

ent. por el lema anterior

$$\frac{k_n}{k_{n-1}} < \varphi \quad y \quad \frac{k_{n+1}}{k_n} < \varphi$$

$$\Rightarrow \varphi > \frac{k_{n+1}}{k_n} = \frac{a_{n+1}k_n+k_{n-1}}{k_n} = a_{n+1}+\frac{k_{n-1}}{k_n} \geq 1+\frac{k_{n-1}}{k_n}$$

$$> 1+\frac{1}{\varphi} = \varphi \quad \therefore \varphi > \varphi \; !$$

Proposición.- En el teorema de Hurwitz la constante $\sqrt{5}$ es la mejor, es decir, si $C > \sqrt{5}$, $\exists\, \alpha$ irracional t.q. $\left|\alpha - \frac{h_n}{k_n}\right| < \frac{1}{C k_n^2}$ solo se satisface para un número finito de convergentes.

Dem.- Sabemos que $\alpha = [\overline{1}] = \varphi$

y notemos que como $h_{-2} = 0$, $h_{-1} = 1$

y $h_{n+1} = h_n + h_{n-1}$, $k_{n+1} = k_n + k_{n-1}$

$\Rightarrow (h_n)_{n=1}^{\infty}$ es la sucesión de fibonacci

e igual $(k_n)_{n=0}^{\infty}$, así $k_{n+1} = h_n$

$\Rightarrow \lim_{n\to\infty} \frac{k_{n+1}}{k_n} = \lim_{n\to\infty} \frac{h_n}{k_n} = \varphi$

$\Rightarrow \lim_{n\to\infty} \left(\alpha + \frac{k_n}{k_{n+1}}\right) = \varphi + \frac{1}{\varphi} = \sqrt{5}$ y si $C > \sqrt{5}$

entonces a partir de una $N \in \mathbb{N}$

$\alpha + \frac{k_n}{k_{n+1}} < C \quad \forall n \geq N$

ó la desigualdad $\alpha + \frac{k_n}{k_{n+1}} \geq C$ solo puede ocurrir un número finito de convergentes

Falta

Def.- Definimos la sig. relación de equivalencia en $\mathbb{R}$. $x \sim y \iff x$ y y son racionales o x y y son irracionales y existen n, m t.q $a_{n+j} = b_{m+j}$ para $j = 1, 2, \ldots$ en su expansión como fracción continua.

Obs.- Así si tomo α irracional t.q $\alpha \not\sim \beta$ entonces existe $c \geq \sqrt{5}$ t.q $\left|\alpha - \frac{h_n}{k_n}\right| < \frac{1}{c k_n^2}$ para una infinidad de convergentes

Fracciones continuas periódicas

Son aquellas que se repiten a partir de un momento y lo denotaremos por $[a_0; a_1, a_2, \ldots, a_n, a_{n+1}, \ldots, a_{n+m-1}, a_n, a_{n+1}, \ldots]$
$= [a_0, a_1, \ldots, \overline{a_n, a_{n+1}, \ldots, a_{n+m}}]$

Obs.- Consideremos $\alpha = [\overline{a_0, a_1, \ldots, a_{n-1}}]$
$= [a_0, \ldots, a_n, \overline{a_0, \ldots, a_{n-1}}] = [a_0, a_1, \ldots, a_{n-1}, \alpha]$

$$= \frac{\alpha h_{n-1} + h_{n-2}}{\alpha k_{n-1} + k_{n-2}}$$

$$\Rightarrow \alpha^2 k_{n-1} + \alpha k_{n-2} = \alpha h_{n-1} + h_{n-2}$$

$$\Rightarrow \alpha^2 k_{n-1} + \alpha(k_{n-2} - h_{n-1}) - h_{n-2} = 0$$

$$\Rightarrow \alpha = \frac{h_{n-1} - k_{n-2} \pm \sqrt{(k_{n-2} - h_{n-1})^2 - 4k_{n-1}(-h_{n-2})}}{2 k_{n-1}}$$

pero $\alpha > 0 \Rightarrow$ tomo la raíz positiva

entonces $\alpha = \dfrac{a+\sqrt{b}}{c}$, con $a, b, c \in \mathbb{Z}$
y $b > 0$, $b \neq u^2$, $c \neq 0$

Obs.- Ahora consideremos $\alpha = [a_0, a_1, \dots, a_{n-1}, \overline{a_n, a_{n+1}, \dots, a_{n+m-1}}]$

si tomo $\beta = [\overline{a_n, a_{n+1}, \dots, a_{n+m-1}}]$

$\Rightarrow \beta = \dfrac{a+\sqrt{b}}{c}$ p.a $a, b, c \in \mathbb{Z}$.

$$\Rightarrow \alpha = [a_0, a_1, \dots, a_{n-1}, \beta]$$

$$= \frac{\beta h_{n-1} + h_{n-2}}{\beta k_{n-1} + k_{n-2}} = \frac{\frac{a+\sqrt{b}}{c} h_{n-1} + h_{n-2}}{\frac{a+\sqrt{b}}{c} k_{n-1} + k_{n-2}}$$

$$= \frac{a h_{n-1} + c h_{n-2} + h_{n-1}\sqrt{b}}{a k_{n-1} + c k_{n-2} + k_{n-1}\sqrt{b}}$$

$$= \frac{a' + d\sqrt{b}}{c'} \Rightarrow \alpha = \frac{a' + d\sqrt{b}}{c'} \quad \text{p.a } a', d, b, c' \in \mathbb{Z}.$$

$b > 0$, $b \neq u^2$, $c' \neq 0$

Obs.- Entonces toda fracción continua periódica es de la forma $\dfrac{a + b\sqrt{c}}{d}$

A estas expresiones se les conoce como irracional cuadrático

¿Si α es irracional cuadrático $\Rightarrow$ tiene fracción continua periódica?

Prop. Si α es irracional cuadrático, entonces su ~~fracción~~ la fracción continua es periódica.

Dem.: Consideramos $\alpha = \frac{a + d\sqrt{b}}{c}$, $a, b, c, d \in \mathbb{Z}$

$b > 0$, $b \neq y^2$, $c \neq 0$, $d \neq 0$

$\Rightarrow \alpha = \frac{sa + sd\sqrt{b}}{sc}$, $s = \pm 1$ / $s = 1$ si $d > 0$, $s = -1$ si $d < 0$

$\Rightarrow \alpha = \frac{sa + |d|\sqrt{b}}{sc} = \frac{sa + \sqrt{bd^2}}{sc}$

$\Rightarrow \frac{sa|c| + |c|\sqrt{bd^2}}{sc|c|} = \frac{sa|c| + \sqrt{bd^2c^2}}{sc|c|}$

$= \frac{m_0 + \sqrt{D}}{q_0}$

Así $D - m_0^2 = bd^2c^2 - a^2c^2 = c^2[bd^2 - a^2]$

Y notemos que $q_0 = c$ o $q_0 = -c$

y así $q_0 \mid D - m_0^2$.

Con ello $\alpha = \frac{m_0 + \sqrt{D}}{q_0}$, con $m_0, q_0 \in \mathbb{Z}$

$D > 0$, $D \neq y^2$, $q_0 \neq 0$ y $q_0 \mid D - m_0^2$

Falta nuevo de convergentes

Recordemos que si $d>0$ no cuadrado $\Rightarrow \sqrt{d} = [a_0, \overline{a_1, \dots, a_{r-1}, 2a_0}]$, con

$$\alpha_i = \frac{m_i + \sqrt{d}}{q_i}, \quad q_i \neq -1$$

$q_i = 1 \iff r \mid i$, r el periodo mínimo.

Def: Se define a la ecuación de Pell a la ecuación

$$x^2 - dy^2 = N$$

con $d>1$ y d libre de cuadrados, $d, N \in \mathbb{Z}$

Obs: Tenemos que $\sqrt{d} = [a_0; a_1, \dots, \alpha_i, \alpha_i]$ ✶

$$= \frac{\alpha_{i+1} h_i + h_{i-1}}{\alpha_{i+1} k_i + k_{i-1}} = \frac{\left(\frac{m_{i+1} + \sqrt{d}}{q_{i+1}}\right) h_i + h_{i-1}}{\left(\frac{m_{i+1} + \sqrt{d}}{q_{i+1}}\right) k_i + k_{i-1}}$$

$$= \frac{(m_{i+1} + \sqrt{d}) h_i + h_{i-1} q_{i+1}}{(m_{i+1} + \sqrt{d}) k_i + k_{i-1} q_{i+1}}$$

$$\Rightarrow \sqrt{d}\left[(m_{i+1} + \sqrt{d}) k_i + k_{i-1} q_{i+1}\right] = (m_{i+1} + \sqrt{d}) h_i + h_{i-1} q_{i+1}$$

$$\rightarrow \sqrt{d}\, m_{i+1} k_i + d\, m_{i+1} k_i + \sqrt{d}\, k_{i-1} q_{i+1} = m_{i+1} h_i + \sqrt{d}\, h_i + h_{i-1} q_{i+1}$$

$\Rightarrow$
- $d k_i = m_{i+1} h_i + h_{i-1} q_{i+1}$
- $m_{i+1} k_i + k_{i-1} q_{i+1} = h_i$

$\Rightarrow$ ~~k~~

por k_i : $d k_i^2 = m_{i+1} h_i k_i + h_{i-1} q_{i+1} k_i$

por h_i : $h_i^2 = m_{i+1} h_i k_i + h_i k_{i-1} q_{i+1}$

$$\Rightarrow \quad h_i^2 - d k_i^2 = q_{i+1} [h_i k_{i-1} - h_{i-1} k_i]$$
$$= q_{i+1} (-1)^{i+1}$$

$\Rightarrow \quad h_i^2 - d k_i^2$

Si $i+1 = r \cdot m$ entonces $q_{i+1} = 1$

$$\Rightarrow \quad h_{rm-1}^2 - d k_{rm-1}^2 = (-1)^{rm}$$

* Si r es par

$\Rightarrow \quad h_{rm-1}^2 - d k_{rm-1} = 1$

$\therefore \; (h_{rm-1}, k_{rm-1})$ es solución de la ecuación de Pell

* Si r impar

$$\Rightarrow \quad h_{rm-1}^2 - d k_{rm-1}^2 = \begin{cases} 1 & \text{si } m \text{ par} \\ -1 & \text{si } m \text{ impar} \end{cases}$$

$\Rightarrow \quad (h_{rm-1}, k_{rm-1})$ es solución

$x, y > 0$

Lema: Sean $x^2 - \delta y^2 = \gamma$ con δ, γ racionales, $\gamma > 0$ t.q. $\sqrt{\delta}$ es irracional con $0 < \gamma < \sqrt{\delta}$, entonces $\frac{x}{y}$ es un convergente de $\sqrt{\delta}$

Dem: Tenemos que $x^2 - \delta y^2 = \gamma$

$\Rightarrow (x + \sqrt{\delta}\, y)(x - \sqrt{\delta}\, y) = \gamma$

$\Rightarrow x - \sqrt{\delta}\, y = \dfrac{\gamma}{x + \sqrt{\delta}\, y} > 0 \Rightarrow x - \sqrt{\delta}\, y > 0$

$\Rightarrow x > \sqrt{\delta}\, y \Rightarrow \dfrac{x}{y} - \sqrt{\delta} > 0$

$\Rightarrow 0 < \dfrac{x}{y} - \sqrt{\delta} = \dfrac{\gamma}{y(x + \sqrt{\delta}\, y)} = \dfrac{\gamma}{y^2\left(\frac{x}{y} + \sqrt{\delta}\right)}$

$< \dfrac{\gamma}{y^2\, 2\sqrt{\delta}} < \dfrac{\gamma}{y^2\, 2\gamma} = \dfrac{1}{2y^2}$

$\Rightarrow \left| \dfrac{x}{y} - \sqrt{\delta} \right| < \dfrac{1}{2y^2}$

$\Rightarrow \dfrac{x}{y}$ es un convergente de $\sqrt{\delta}$

Teorema: Sea $x^2 - dy^2 = N$ con $0 < N < \sqrt{d}$ (d libre de cuadrados) entonces $\frac{x}{y}$ es convergente de $\sqrt{d}$

Dem: por el lema anterior como $0 < N < \sqrt{d}$ y $\sqrt{d}$ es irracional (pues d es libre de cuadrados) $\Rightarrow \dfrac{x}{y}$ es convergente de $\sqrt{d}$

Obs: para $N < 0$ consideramos $-\sqrt{d} < N < 0$

$\Rightarrow dy^2 - x^2 = -N \Rightarrow y^2 - \frac{1}{d}x^2 = -\frac{N}{d}$

y a esta nueva ecuación se aplica el lema, $\frac{y}{x}$ será convergente de $\sqrt{1/d}$

$\Rightarrow \frac{x}{y}$ es convergente de $\sqrt{d}$

Obs: Con esto tenemos que si $x, y \in \mathbb{Z}^+$ satisfacen la ecuación $x^2 - d\,y^2 = N$ con d libre de cuadrados, $d > 1$ y $N \in \mathbb{Z}$, $|N| < \sqrt{d}$ entonces $\frac{x}{y}$ es convergente de $\sqrt{d}$.

Obs: Si tomo $x^2 - dy^2 = N$ las hipótesis

$\Rightarrow \left(\frac{x}{y}\right)^2 = d + \frac{N}{y^2} \Rightarrow \left(\frac{x}{y}\right)^2 \approx d$

Obs: Si $N = \pm 1$, y $x, y \in \mathbb{Z}^+$ satisfacen

$x^2 - d\,y^2 = \pm 1 \Rightarrow (x, y) = 1$

$\Rightarrow \frac{x}{y} = \frac{h_i}{k_i}$ p.a. i (son convergentes)

$\Rightarrow x = h_i \wedge y = k_i$ pues $(x, y) = 1$

$\Rightarrow (-1)^{i+1} q_{i+1} = h_i^2 - d k_i^2 = \pm 1$

pero $q_{i+1} = \pm 1$ pues $q_{i+1} > 1$

$\Rightarrow q_{i+1} = 1 \Rightarrow r \mid i+1 \Rightarrow x = h_{rn-1}$

$y = k_{rn-1}$

Teorema.- Sean $d>0$ no cuadrado y r el periodo mínimo de $\sqrt{d}$. Si r es par, la ecuación

$$x^2 - dy^2 = -1$$

no tiene solución y todas las soluciones de $x^2-dy^2=1$ están dadas por (h_{rm-1}, k_{rm-1}) donde $\frac{h_n}{k_n}$ es el n-ésimo convergente de $\sqrt{d}$.

Si r es impar, todas las soluciones de $x^2-dy^2=1$ están dadas por (h_{2rm-1}, k_{2rm-1}) y las de $x^2-dy^2=-1$ están dadas por $(h_{(2m+1)r-1}, k_{(2m+1)r-1})$

Dem.- Notas

Proposición.- Definimos x_n, y_n por medio de la ecuación $x_n + y_n\sqrt{d} = (x_1+y_1\sqrt{d})^n$

siendo $x_0=1, y_0=0$ la solución trivial de $x^2-dy^2=1$ y x_1, y_1 las sig soluciones.

Entonces x_n, y_n son $\boxed{\text{todas}}$ las soluciones positivas de $x^2-dy^2=1$

Dem.- Tenemos que $x_1+y_1\sqrt{d} > 1$, con lo que $(x_1+y_1\sqrt{d})^n \xrightarrow[n\to\infty]{} \infty$ y es estrictamente creciente

Sean u, v una solución positiva de $x^2 - dy^2 = 1$, como $(x_1 + y_1\sqrt{d})^n$ es estrictamente creciente, entonces existe $n \in \mathbb{N}$ t.q

$$(x_1 + y_1\sqrt{d})^n \leq u + v\sqrt{d} < (x_1 + y_1\sqrt{d})^{n+1}$$

Si $(x_1 + y_1\sqrt{d})^n = u + v\sqrt{d} \Rightarrow x_n = u, \ y_n = v$ y terminamos

Sup. que $(x_1 + y_1\sqrt{d})^n < u + v\sqrt{d} < (x_1 + y_1\sqrt{d})^{n}$

y como $x_1^2 - dy_1^2 = 1 \Rightarrow (x_1 - y_1\sqrt{d})(x_1 + y_1\sqrt{d}) = 1$

entonces $x_1 - y_1\sqrt{d} > 0$

$\Rightarrow$ multiplicando la desigualdad por $(x_1 - y_1\sqrt{d})^n$

$$\Rightarrow (x_1^2 - y_1^2 d)^n < (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^n < (x_1^2 - dy_1^2)^n (x_1 + y_1\sqrt{d})$$

$$\Rightarrow 1 < (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^n < x_1 + y_1\sqrt{d}$$

Ahora sea $a + b\sqrt{d} = (u + v\sqrt{d})(x_1 - y_1\sqrt{d})^n$

$$\Rightarrow a - b\sqrt{d} = (u - v\sqrt{d})(x_1 + y_1\sqrt{d})^n$$

multipli.

$$\Rightarrow a^2 - db^2 = (u^2 - dv^2)(x_1^2 - dy_1^2)^n = 1 \cdot (1)^n = 1$$

$\Rightarrow (a, b)$ es solución

Ahora como $a^2 - d b^2 = 1 \Rightarrow (a + b\sqrt{d})(a - b\sqrt{d}) = 1$

y $a + b\sqrt{d} > 1 \Rightarrow a - b\sqrt{d} = \frac{1}{a + b\sqrt{d}} < 1$

$\Rightarrow 0 < a - b\sqrt{d} < 1$

$\Rightarrow 1 + 0 < a - b\sqrt{d} + a + b\sqrt{d} = 2a$

$\Rightarrow a > \frac{1}{2} \Rightarrow a > 0$

y $1 - 1 < a + b\sqrt{d} - a + b\sqrt{d} = 2b\sqrt{d}$

$\Rightarrow 2b\sqrt{d} > 0 \Rightarrow b > 0$ $\therefore$ $a > 0$, $b > 0$

$\therefore$ encontramos una solución positiva

por último como a, b son solución

$\Rightarrow a = h_s \geq h_1$, $b = k_s \geq k_1$ $\Rightarrow a + b\sqrt{d} \geq h_1 + k_1\sqrt{d} = x_0 + y_0\sqrt{d}$

lo que contradice que x_0, y_0 sean los más chicos $\therefore$ $u + v = (x_1 + y_1)^n$ p.a $n \in \mathbb{N}$.

por otro lado $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$

$x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$

$\Rightarrow x_n^2 - d y_n^2 = (x_1^2 - d y_1^2)^n = (1)^n = 1$ $\therefore$ los de esta forma son solución $\therefore$ todos los de esta forma son solución.

Obs.- De lo anterior se tiene que

$x_{n+1} = x_1 x_n + d\, y_1 y_n = a x_n + d b y_n$

$y_{n+1} = y_1 x_n + x_1 y_n = b x_n + a y_n$

Con a, b la solución positiva más pequeña después de $x_0 = 1$, $y_0 = 0$

Ahora.

$x_{n+2} = a x_{n+1} + d b y_{n+1}$

$= a x_{n+1} + d b [b x_n + a y_n]$

$= a x_{n+1} + d b^2 x_n + a d b y_n$

$= a x_{n+1} + d b^2 x_n + a [x_{n+1} - a x_n]$

$= a x_{n+1} + d b^2 x_n + a x_{n+1} - a^2 x_n$

$= 2a x_{n+1} - (a^2 - d b^2) x_n$

$= 2a x_{n+1} - (1) x_n = 2a x_{n+1} - x_n$

$\therefore\ x_{n+2} = 2a x_{n+1} - x_n$

Igualmente

$$y_{n+2} = b\,x_{n+1} + a\,y_{n+1}$$
$$= b[a x_n + d b y_n] + a y_{n+1}$$
$$= a b x_n + d b^2 y_n + a y_{n+1}$$
$$= a[y_{n+1} - a y_n] + d b^2 y_n + a y_{n+1}$$
$$= 2a y_{n+1} - (a^2 - d b^2) y_n = 2a y_{n+1} - y_n$$

$\therefore \quad y_{n+2} = 2a y_{n+1} - y_n$

$\therefore$ todas las soluciones positivas de $x^2 - d y^2 = 1$ cumplen ~~por~~ la relación

$x_0 = 1$, $y_0 = 0$, $x_1 = a$, $y_1 = b$ con a, b las soluciones positivas mas chicas

y $x_{n+2} = 2a x_{n+1} - x_n$, $y_{n+2} = 2a y_{n+1} - y_n$

Igualmente tenemos que $x_n + y_n \sqrt{d} = (x_1 + y_1\sqrt{d})^n$

$x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$

sumando $\Rightarrow$ $x_n = \dfrac{(x_1 + y_1\sqrt{d})^n + (x_1 - y_1\sqrt{d})^n}{2}$

restando $\Rightarrow$ $y_n = \dfrac{(x_1 + y_1\sqrt{d})^n - (x_1 - y_1\sqrt{d})^n}{2\sqrt{d}}$

Notemos que, por lo hecho antes,

$0 < x_1 - y_1\sqrt{d} < 1 \Rightarrow$ cuando $n \to \infty$ $(x_1 - y_1\sqrt{d})^n = 0$

por lo que para n muy grande

$$x_n \approx \frac{1}{2}(x_1 + y_1\sqrt{d})^n$$

y

$$y_n \approx \frac{1}{2\sqrt{d}}(x_1 + y_1\sqrt{d})^n$$

Ahora regresando a la solución general
$x^2 - dy^2 = n$.

Sean u, v ~~soluciones~~ soluciones, y sean a, b la mínima solución positiva de $x^2 - dy^2 = 1$

$$\Rightarrow (u + v\sqrt{d})(a + b\sqrt{d}) = r + s\sqrt{d}$$
$$(u - v\sqrt{d})(a - b\sqrt{d}) = r - s\sqrt{d}$$

$$\Rightarrow (u^2 - dv^2)(a^2 - db^2) = r^2 - ds^2$$

$$\Rightarrow n \cdot 1 = r^2 - ds^2 \Rightarrow r^2 - ds^2 = n$$

$\therefore$ (r, s) es solución de $x^2 - dy^2 = n$

Con lo anterior, si $x^2 - dy^2 = n$ tiene una solución, entonces tiene una infinidad de soluciones x_m, x_m dadas por

$$(u+v\sqrt{d})(a+b\sqrt{d})^m = x_m + y_m\sqrt{d}$$

Con (a,b) la solución positiva mínima de $x^2 - dy^2 = 1$

Ahora notemos que si (u,v) son soluciones positivas de $x^2 - dy^2 = n$, entonces

$$\frac{u+v\sqrt{d}}{a+b\sqrt{d}} = \frac{(u+v\sqrt{d})(a-b\sqrt{d})}{a^2 - db^2} = (u+v\sqrt{d})(a-b\sqrt{d})$$

$$= r + s\sqrt{d}$$

Dónde (r,s) será otra solución, con r, y s no necesariamente positivas.

Sea (a,b) la mínima solución positiva de $x^2 - dy^2 = 1$ y consideremos (u,v) una solución de $x^2 - dy^2 = m$ con $m > 0$ y $u > 0$, $v \geq 0$, tal que $(u+v\sqrt{d})(a-b\sqrt{d}) = r + s\sqrt{d}$

$\Rightarrow r = ua - vbd \iff u = ar + dbs$

$s = va - ub \qquad v = br + as$

$\Rightarrow$ $\Rightarrow br = v - as$ y si $s < 0$

$\Rightarrow br > 0 \Rightarrow r > 0$

$\Rightarrow ry - sx = a = bm > 0 \Rightarrow ry > sx$

si $s \geq 0 \Rightarrow sx \geq 0 \Rightarrow ry > 0 \Rightarrow r > 0$!

$\therefore s < 0 \Rightarrow r > 0$.

análogamente si $r < 0 \Rightarrow s > 0$

$\therefore (u + v\sqrt{d})(a - b\sqrt{d}) = r + s\sqrt{d}$ con $r < 0$ ó $s < 0$.

Más aún tendremos que
$$0 \leq v < b\sqrt{m}$$
$$\sqrt{m} \leq u < a\sqrt{m}$$

$\therefore$ si (u, v) es solución t.q.
$$0 \leq v < b\sqrt{a}$$
$$\sqrt{m} \leq u < a\sqrt{m}$$

$\Rightarrow$ todas las soluciones vendrán dadas por $(u + v\sqrt{d})(a + b\sqrt{d})$ ∎

Para el caso $x^2 - dy^2 = m$ con $m < 0$
se tiene que $-dx^2 + d^2y^2 = -dm$

sea $z = dy \Rightarrow z^2 - dx^2 = m'$ con $m' > 0$
$m' = -dm$

y tendremos lo mismo aplicado a m'
obteniendo que
$$0 \leq x < b\sqrt{-dm}$$
$$\sqrt{\frac{-m}{d}} \leq y < a\sqrt{\frac{-m}{d}}$$

Obs.- Teniendo la ecuación $x^2+y^2=z^2$

si $d=(x,y,z)$ $\Rightarrow$ $x=da$ $z=dc$
$y=db$

$\Rightarrow$ $d^2a^2+d^2b^2=d^2c^2 \Rightarrow a^2+b^2=c^2$

entonces $x^2+y^2=z^2$ tiene solución $\Leftrightarrow$ $a^2+b^2=c^2$ tiene solución

Obs.- considerando una forma primitiva (a,b,c); con $(a,b,c)=1$.

- si a y b son pares $\Rightarrow$ c es par (!)

- si a y b son impares $\Rightarrow$ $c^2=a^2+b^2\equiv 1+1 \equiv 2 \pmod 4$ (!)

$\therefore$ a y b tienen paridad distinta.

entonces podemos sup. spdg que a es impar y b es par, por lo que c es impar

Obs.- Teniendo $a^2+b^2=c^2$
$\Rightarrow$ $a^2=c^2-b^2=(c-b)(c+b)$

pero además $g=(c-b,c+b) \Rightarrow g\mid c-b \wedge g\mid c+b$
$\Rightarrow$ $g\mid 2c$ $\wedge$ $g\mid 2b$ $\Rightarrow$ $g\mid(2b,2c)$

$\Rightarrow$ $g\mid 2(b,c) \Rightarrow g\mid 2$ $\Rightarrow$ $g=1$ ó $g=2$

~~ya~~ pero como a y b son impares $\Rightarrow$ $c-b$ y $c+b$ son impares por lo que $g \neq 2$

$\therefore$ $g = 1$

$\therefore$ como $a^2 = (c-b)(c+b)$ y $(c-b, c+b) = 1$

necesariamente $c-b = r^2$ y $c+b = s^2$

para $r, s \in \mathbb{Z}$

$\Rightarrow$ $2c = r^2 + s^2$ $\Rightarrow$ $c = \dfrac{r^2+s^2}{2}$

$\Rightarrow$ $2b = s^2 - r^2$ $\Rightarrow$ $b = \dfrac{s^2-r^2}{2}$

$\Rightarrow$ $a^2 = c^2 - b^2 = r^2 s^2$ $\Rightarrow$ $a = rs$

b): Ahora regresando a $a^2 + b^2 = c^2$

$\Rightarrow$ $(a+bi)(a-bi) = c^2$ y tomando

$g = (a+bi, a-bi)$ sea lo que signifique

$\Rightarrow$ $g \mid a+bi \wedge g \mid a-bi$ $\Rightarrow$ $g \mid 2a \wedge g \mid 2bi$

$\Rightarrow$ $g \mid (2a, 2bi)$ $\Rightarrow$ $g \mid 2(a, bi)$ $\Rightarrow$ ¿$g \mid 2$?

$\Rightarrow$ ¿$g = 1$?

si fuera así $\Rightarrow$ ~~$a+bi = (r+si)^2$~~ ~~$a-bi = s^2$~~

$\Rightarrow a+bi = (r+si)^2 \Rightarrow a+bi = r^2 + 2rsi - s^2$

$$\Rightarrow \boxed{\begin{aligned} a &= r^2 - s^2 \\ b &= 2rs \\ c &= r^2 + s^2 \end{aligned}}$$

¡Soluciones reales!

Entonces con esto podríamos resolver la ecuación $x^2+y^2=z^2$ que en los enteros no podía factorizar de la primera manera pero en los complejos sí

Ej: Tenemos $x^2+y^2=2z^2 \Rightarrow x^2 = 2z^2 - y^2$

$\Rightarrow x^2 = (\sqrt{2}z+y)(\sqrt{2}z-y)$

¿En general que tenemos?

$x^n + y^n = z^n$

- Si n impar

$\Rightarrow$ Tenemos $x^n+y^n=0 \Rightarrow \left(\frac{x}{y}\right)^n + 1 = 0$

$\Rightarrow \frac{x}{y} = \alpha^n$ con α raíz primitiva de -1

$\therefore x^n + y^n = (x+y)(x-\alpha y)\cdots(x-\alpha^{n-1}y)$

¿Podemos generalizar los conceptos de los enteros a los complejos?

Tomando la construcción formal de polinomios

Si K es campo $\Rightarrow$ $K[x] = \{ (a_0, a_1, \dots, a_n, 0, \dots, 0, \dots)$

$| a_i \in K \} = \{ a_0 + a_1 x + \dots + a_n x^n \mid a_i \in$

y $x^n = \{ \underbrace{0, \dots, 0}_{n}, 1, \dots, 0, \dots)$

Así es mejor pues $f(x) = x^3$ y

$g(x) = x$ son iguales en $\mathbb{Z}_3$

pero con la construcción formal

x^3 y x no son lo mismo.

Esta es la ventaja.

:

polinomios

:

Def.- Un número complejo $z \in \mathbb{C}$ se llama algebraico si existe un polinomio $p(x) \in \mathbb{Q}[x]$ no cero t.q. $p(z) = 0$.

Obs.- Los números algebraicos forman un campo (subcampo de $\mathbb{C}$) que denotamos con $\mathbb{A}$

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{A} \subseteq \mathbb{C}$$

Obs.- $\mathbb{A}$ es numerable.

$P_1 \{a_1 x + a_0 \mid a_1, a_0 \in \mathbb{Q}\}$ es numerable

$\vdots$

$P_n = \{a_n x^n + \cdots + a_0 \mid a_i \in \mathbb{Q}\}$ es numerable

$\Rightarrow \bigcup_{n=1}^{\infty} P_n$ es numerable (y sus raíces son numerables).

Obs.- Un complejo no algebraico le llamaremos trascendente.

Proposición.- Si $p(x) \in \mathbb{Q}[x] \setminus \{\bar{0}\}$ t.q. $p(z) = 0$ y c es el coef. principal de $p(x)$
$\Rightarrow \frac{1}{c} p(x)$ es mónico y $\frac{1}{c} p(z) = 0$

- también con las mismas hip. existe $m \in \mathbb{Z}^+$ t. $m\, p(x) \in \mathbb{Z}[x]$ y $m\, p(z) = 0$

$\therefore$ en la def. de num. algebraico puedo cambiar $\mathbb{Q}[x]$ por $\mathbb{Z}[x]$.

Def.- El polinomio mínimo de un número algebraico z es el único polinomio mónico $p(x) \in \mathbb{Q}[x]$ t.q. $p(z)=0$ y $\operatorname{gra}(p(x))$ es mínimo.

Veamos que efectivamente es único de grado mínimo.

Sup. que $q(x) \in \mathbb{Q}[x] \setminus \{\bar{0}\}$ t.q. $q(z)=0$ y sea $c = \text{C.P.}[q]$ y definimos $p(x) = \frac{1}{c} q(x) \Rightarrow \operatorname{grad}(p) = \operatorname{gra}(q)$ con p mónico.

Entonces sea $t(x)$ otro polinomio mónico con $\operatorname{grad}(t) = \operatorname{grad}(p)$ y $t(z)=0$

$\Rightarrow t(x) = p(x)s(x) + r(x)$ con $\operatorname{grad}(r) < \operatorname{grad}(p)$

$\Rightarrow 0 = t(z) = \overset{0}{\cancel{p(z)}} s(z) + r(z) \Rightarrow r(z) = 0$

$\Rightarrow r(x) = \bar{0} \Rightarrow t(x) = p(x)s(x)$

$\Rightarrow p(x) \mid t(x)$

y analogamente $t(x) \mid p(x)$

$\Rightarrow p(x) = t(x)$ (pues son mónicos)

- para $z=3$, $p(x)=x-3$
- para $z=\frac{2}{3}$, $p(x)=3x-2$ No es mónico

$p(x)=x-\frac{2}{3}$ es el mínimo

- para $z=1+\sqrt{2}$, $p(x)=x^2-2x-1$

¿es de grado mínimo?

Si existiera tendría que ser de la forma $x+b$, con $b\in\mathbb{Q}$ $\Rightarrow$ $1+\sqrt{2}+b=0$ $\Rightarrow$ $\sqrt{2}=-b-1\in\mathbb{Q}$! $\therefore$ $p(x)$ es el mínimo.

- para $z=\sqrt{2}+\sqrt{3}$.

$z=\sqrt{2}+\sqrt{3} \Rightarrow z^2=5+2\sqrt{6} \Rightarrow z^2-5=2\sqrt{6}$

$\Rightarrow (z^2-5)^2=24 \Rightarrow z^4-10z^2+25=24$

$\Rightarrow z^4-10z^2+1=0$

$\therefore$ un candidato es $p(x)=x^4-10x^2+1$

Def.- El grado de un número algebraico es el grado de su polinomio mínimo.

- $gr(2/3)=1$
- $gr(r)=1$ $\forall r\in\mathbb{Q}$
- Si $r\in\mathbb{Q}$ y $\sqrt{r}\notin\mathbb{Q}$ $\Rightarrow$ $gr(\sqrt{r})=2$

Escaneado con CamScanner

Proposición.- A es subcampo de $\mathbb{C}$.

Demost. ... algebraicos ...

Todas las propiedades de asociatividad conmutatividad y distributividad se cumplen y $0 \in A$, $1 \in A$

$\therefore$ P.D. si $\alpha, \beta \in A \Rightarrow$ • $\alpha+\beta \in A$ • $-\alpha \in A$ • $\alpha-\beta \in A$ • $\frac{1}{\alpha} \in A$

1) Sea $p_\alpha(x) \in \mathbb{Q}[x]$ ...

$f_\alpha(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$

$$(-1)^n p_\alpha(-x) = (-1)^n(-x)^n + a_{n-1}(-1)^n(-x)^{n-1} + \dots + (-1)^n a_0$$

$$= x^n - a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + (-1)^{n-1} a_1 x + (-1)^n a_0$$

$\in \mathbb{Q}[x]$

$\Rightarrow g(-\alpha) = (-1)^n p(-(-\alpha)) = (-1)^n p(\alpha) = 0$

$\therefore -\alpha$ es algebraico y $g(x)$ es mínimo pues de no serlo así $p_\alpha(x)$ no sería el mínimo de α.

$gr(-\alpha) = gr(\alpha)$

2) P.D $\frac{1}{\alpha} \in A$.

Sea $p_\alpha(x) \in \mathbb{Q}[x]$. Tenemos que

$0 = p(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0$

$\underset{\alpha \neq 0}{\Rightarrow}$ $0 = \frac{1}{\alpha^n} p(\alpha) = 1 + a_{n-1}\frac{1}{\alpha} + a_{n-2}\left(\frac{1}{\alpha}\right)^2 + \dots + a_1\left(\frac{1}{\alpha^{n-1}}\right) + a_0\frac{1}{\alpha^n}$

$\Rightarrow$ Tomando ~~$g(x) =$~~ $f(x) = a_0 x^n + \dots + a_{n-1}x + 1$

$\Rightarrow f\left(\frac{1}{\alpha}\right) = 0 \quad \therefore \frac{1}{\alpha}$ es algebraico.

¿Es el mínimo? No

Si $a_0 = 0 \Rightarrow p(x) = x(x^{n-1} + a_{n-1}x^{n-2} + \dots + a_1)$

$\Rightarrow 0 = p(\alpha) = \alpha(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \dots + a_1)$

$\Rightarrow 0 = \alpha^{n-1} + a_{n-1}\alpha^{n-2} + \dots + a_1$! pues $p(x)$ era el polinomio mínimo.

$\therefore a_0 \neq 0$

$\Rightarrow \frac{1}{a_0} f(x) = x^n + \frac{a_1}{a_0}x^{n-1} + \dots + \frac{a_{n-1}}{a_0}x + \frac{1}{a_0}$

y este es el polinomio mínimo de $\frac{1}{\alpha}$

$gr\left(\frac{1}{\alpha}\right) = gr(\alpha)$

Def.- Sea $z \in \mathbb{C}$, decimos que z es un entero algebraico si existe $p(x) \in \mathbb{Z}[x]$ mónico distinto de 0 t.q. $p(z) = 0$.

Al conjunto de enteros algebraicos lo denotamos por $\mathbb{O}$

Proposición.- Sea $\alpha \in \mathbb{O}$ entonces su polinomio mínimo (como número algebraico) tiene coeficientes enteros

Dem.- Sea $p(x) \in \mathbb{Z}[x]$ mónico de grado mínimo t.q. $p(\alpha) = 0$.

Sea $q(x)$ el polinomio mínimo de α

$\Rightarrow p(x) = q(x) t(x) + r(x) \quad gr(r) < gr(q)$

$\Rightarrow p(\alpha) = q(\alpha) t(\alpha) + r(\alpha) \quad , \quad t(x), r(x) \in \mathbb{Q}[x]$

$\Rightarrow 0 = r(\alpha)$ pero $q(x)$ era el mínimo $\therefore r(x) = 0$

$\Rightarrow p(x) = q(\alpha) t(\alpha)$. pero como

$p(x) \in \mathbb{Z}[x]$ mónico y $q, t \in \mathbb{Q}[x] \Rightarrow t$ es mónico también y por hip q es mónico

$\therefore$ por el Lema de Gauss $q(x), t(x) \in \mathbb{Z}[x]$

pero entonces $q(x) \in \mathbb{Z}[x]$ y se anula en α y es mónico y es de grado mínimo $\therefore$ grad(p(x)) $\geq$ grad(q(x))

$\therefore$ grad(f(x)) = 1 , y como era mónico f(x) = 1 $\therefore$ p(x) = g(x)

Ejemplo

- $3/2 \notin \mathbb{O}$, pues su polinomio mínimo es $p(x) = x - 3/2$ y entonces $p(x) \notin \mathbb{Z}[x]$ $\therefore$ no puede haber un polinomio con coeficientes en los enteros mónico que se anule en $3/2$.

- $\mathbb{O} \cap \mathbb{Q} = \mathbb{Z}$.

$\supseteq)$ $n \in \mathbb{Z} \Rightarrow n \in \mathbb{Q}$ y $n \in \mathbb{O}$ ✓

$\subseteq)$ Si $\frac{r}{s} \in \mathbb{O} \cap \mathbb{Q}$, $r, s \in \mathbb{Z}$, $s \neq 0$.
Su polinomio mínimo es $p(x) = x - \frac{r}{s}$ y como $\frac{r}{s} \in \mathbb{O}$ necesariamente $p(x) \in \mathbb{Z}[x]$

$\therefore$ $\frac{r}{s} \in \mathbb{Z}$

- $\sqrt{2} \in \mathbb{O}$, pues $p(x) = x^2 - 2$

- $i \in \mathbb{O}$, pues $p(x) = x^2 + 1$.

Proposición.- $\mathbb{O}$ es dominio entero.

Dem.- Asociativa, conmutativa, distributiva ✓

$0 \in \mathbb{O}$ ✓, $1 \in \mathbb{O}$ ✓,

inversos aditivos ✓ Demostrado anteriormente cambiando $\mathbb{Q}$ por $\mathbb{Z}$.

$xy = 0 \Rightarrow x = 0$ o $y = 0$ ✓

P.D. Si $\alpha, \beta \in \mathbb{O} \Rightarrow \alpha+\beta, \alpha\cdot\beta \in \mathbb{O}$.

Lema.- Sea $z \in \mathbb{C}$. Si existen $w_1, \ldots, w_n \in \mathbb{C}$ no todos 0 t.q.

$$z w_1 = a_{11} w_1 + a_{12} w_2 + \cdots + a_{1n} w_n$$
$$z w_2 = a_{21} w_1 + a_{22} w_2 + \cdots + a_{2n} w_n$$
$$\vdots$$
$$z w_n = a_{n1} w_1 + a_{n2} w_2 + \cdots + a_{nn} w_n$$

Entonces

- Si $a_{ij} \in \mathbb{Q} \Rightarrow z$ es algebraico
- Si $a_{ij} \in \mathbb{Z} \Rightarrow z$ es entero algebraico

Dem.- Por hipótesis tenemos

$$(a_{11} - z) w_1 + a_{12} w_2 + \cdots + a_{1n} w_n = 0$$
$$a_{21} w_1 + (a_{22} - z) w_2 + \cdots + a_{2n} w_n = 0$$
$$\vdots$$
$$a_{n1} w_1 + a_{n2} w_2 + \cdots + (a_{nn} - z) w_n = 0$$

y tiene solución única $\Leftrightarrow$ $\det(A)=0$

y $\det(A) = p(z) \in \mathbb{Q}[z]$ o $\mathbb{Z}[z]$

$gr(z) \leq gr(p(x)) = n$

Proposición.- Si $\alpha, \beta \in \mathbb{A}$ ($\mathbb{D}$) entonces $\alpha+\beta$, $\alpha\cdot\beta \in \mathbb{A}$ ($\mathbb{D}$).

Dem.- Sean $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ el polinomio mínimo de α y $q(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ el polinomio mínimo de β.

Como $p(\alpha)=0 \Rightarrow \alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0$
y como $q(\beta)=0 \Rightarrow \beta^m = -b_{m-1}\beta^{m-1} - \cdots - b_1\beta - b_0$
y consideramos el conjunto $W = \{\alpha^r\beta^s \mid 0 \leq r \leq n,\ 0 \leq s \leq m\}$

Ahora notemos que si $\alpha^r\beta^s \in W$
$\Rightarrow \alpha^r\beta^s(\alpha+\beta) = \alpha^{r+1}\beta^s + \alpha^r\beta^{s+1}$

Si $r+1 < n$ y $s+1 < m \Rightarrow \alpha^r\beta^s(\alpha+\beta)$ es representado como elementos de W.

Si $r+1 = n$ y $s+1 < m \Rightarrow \alpha^{r+1} = \alpha^n = \cdots$
y nuevamente $\alpha^r\beta^s(\alpha+\beta)$ ~~representa~~ esta representado por combinaciones de elementos de W.

Igualmente si $r+1 < n$ y $s+1 = m$
$r+1 = n$ y $s+1 = m$

$\therefore$ Existen complejos t.q. $\forall\, r \in \mathbb{N}$, $0 \le s \le m$ / $\alpha^r \beta^s (\alpha+\beta)$ es combinación de elementos de W

$\therefore$ Por el lema $\alpha+\beta$ es algebraico

$\therefore$ Igual para $\alpha\beta$

$~~\ldots p(x-\beta) + q(x-\alpha)~~$?

Ejemplos

$\alpha = \sqrt{2}$, $\beta = \sqrt[3]{2}$

$p_\alpha(x) = x^2 - 2$ $\quad p_\beta(x) = x^3 - 2$

$gr(\alpha) = 2$ $\quad gr(\beta) = 3$

$\Rightarrow$ $\alpha+\beta = \sqrt{2} + \sqrt[3]{2}$ es de grado 6

$\alpha \cdot \beta = \sqrt{2}\sqrt[3]{2}$ es de grado 6

Teorema - Si $p(x) \in A[x]$, $grad(p(x)) > 0$ entonces tiene raíces en A, es decir, es algebraicamente cerrado.

Obs.- $\mathbb{A}$ es el subcampo algebraicamente cerrado mas pequeño de $\mathbb{C}$.

Obs.- Sea $\alpha \in \mathbb{A}$ de grado n, consideremos el conjunto

$$\mathbb{Q}(\alpha) = \{ a_m \alpha^m + a_{m-1}\alpha^{m-1} + \dots + a_1\alpha + a_0 \mid a_i \in \mathbb{Q} \text{ y } m \in \mathbb{N} \}$$

como la suma y el producto es cerrado en nos algebraicos $\mathbb{Q}(\alpha) \subseteq \mathbb{A}$.
y ademas sera subcampo,
todas las propiedades son inmediatas
excepto los inversos multiplicativos

Obs.- $\alpha \in \mathbb{A}$ de grado $n \Rightarrow$

$$\mathbb{Q}(\alpha) = \{ a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 \mid a_i \in \mathbb{Q} \}$$

$$= \bigcap \{ K \subseteq \mathbb{C} \mid \alpha \in K \text{ y } K \text{ campos} \} = F$$

Dem

$\Rightarrow)$ ✓

$\Leftarrow)$ Si K es un subcampo de $\mathbb{C}$ que contiene a $\alpha \Rightarrow 1 \in K, \alpha \in K, \alpha^2 \in K, \dots, \alpha^{n-1} \in K$ y sabemos que $\mathbb{Q} \subseteq K$

$\Rightarrow a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 \in K$ con $a_i \in \mathbb{Q}$

$\therefore \forall x \in \mathbb{Q}(\alpha) \Rightarrow x \in K$

$\therefore\ \mathbb{Q}(\alpha) \subseteq K \quad \forall K$ subcampo que contiene a $\alpha \Rightarrow \mathbb{Q}(\alpha) \subseteq F$

$\therefore\ F = \mathbb{Q}(\alpha)$

Obs: $\mathbb{Q}(\alpha) \cap \mathbb{O}$ es dominio entero.

En este dominio entero haremos teoría de números.

Veamos que podemos trasladar muchas cosas a dominios enteros.

Def: Sea D dominio entero y $a, b \in D$. Decimos que a divide a b si existe $c \in D$ t.q. $b = a \cdot c$, denotado $a | b$.

Prop.

- ~~Propiedades de la relación de equivalencia~~
- $a | a$
- $a | b$ y $b | c \Rightarrow a | c$
- $a | b$ y $b | a \Rightarrow a$ y b son asociados, i.e., existe $u \in D$ unidad t.q. $a = u b$ ó $a = b = 0$
- $a | b$ y $a | c \Rightarrow a | bx + cy \quad \forall x, y \in D$
- $1 | a \quad \forall a$
- $a | 0 \quad \forall a$
- Si $0 | a \Rightarrow a = 0$

asociados

- Si $a \sim c$ y $b \sim d$ ent. $a | b \iff c | d$.

Def.- Dados $a, b \in D$, un máximo común divisor de a y b es un elemento $d \in D$ que cumple:

- $d | a$ y $d | b$
- Si $c | a$ y $c | b \Rightarrow c | d$

Lo denotamos) $d = (a, b)$

Obs.- Si d_1 y d_2 son m.c.d de a y b $\Rightarrow d_1 \sim d_2$

Def.- Un elemento $a \in D$, $a \neq 0$, no unidad se llama irreducible si

$a = bc \Rightarrow$ b es unidad ó c es unidad
$(a \sim c)$ $(a \sim b)$

Def.- Un elemento $a \in D$, $a \neq 0$, no unidad se llama primo si

$a | bc \Rightarrow a | b$ ó $a | c$

- primo $\Rightarrow$ irreducible pero si p es irreducible no necesariamente es primo.

Def.- Sea D un Dominio entero, Decimos que D es un dominio de factorización única (DFU) si y solo si $\forall a \in D$, $a \neq 0$, no unidad existen $p_1, p_2, \dots, p_r \in D$ irreducibles t.q $a = p_1 \cdot p_2 \cdots p_r$. y dicha representación es única salvo el orden y salvo asociados.

Obs: • $a \mid b \Leftrightarrow b\mathbb{Z} \subseteq a\mathbb{Z}$

• $a\mathbb{Z} \cap b\mathbb{Z} = [a,b]\mathbb{Z}$

• $a\mathbb{Z} + b\mathbb{Z} = (a,b)\mathbb{Z}$

⋮

Ideales, ideales principales, DIP
Ideales, maximales, ideal primo, Dominio euclideano

Def.- Si α es algebraico con polinomio mínimo $p(x)$ entonces las otras raíces de $p(x)$ se conocen como los conjugados de α

Obs.- $\mathbb{Q}(\sqrt{2}) = \{a+\sqrt{2}b : a, b \in \mathbb{Q}\}$ es $\mathbb{Q}$ esp. vectorial sobre $\mathbb{Q}$ con base $\{1, \sqrt{2}\}$.

Sea $\alpha = a+\sqrt{2}b \in \mathbb{Q}(\sqrt{2})$ fijo y sea $T_\alpha : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ dada por $T_\alpha(v) = \alpha \cdot v$. Es transformación lineal

Veamos quién es $\det [T_\alpha]_\beta$

$T_\alpha(1) = \alpha = a+b\sqrt{2} = a\cdot 1 + b\cdot\sqrt{2}$

$T_\alpha(\sqrt{2}) = 2b + a\sqrt{2} = 2b\cdot 1 + a\cdot\sqrt{2}$

$\Rightarrow [T_\alpha]_\beta = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$

$\Rightarrow \det [T_\alpha]_\beta = a^2 - 2b^2 = (a+b\sqrt{2})(a-b\sqrt{2})$

Esto me da la motivación para la sig. def.

Def.- Sea α algebraico. La norma de α es el producto de α y sus conjugados

Obs.- Si $p(x)$ es el polinomio mínimo de α entonces

$$p(x) = (x-\alpha)(x-\alpha_2)\cdots(x-\alpha_n)$$

$\Rightarrow$ $p(0) = (-1)^n \alpha \alpha_2 \cdots \alpha_n$ por lo que es el término independiente de $p(x)$

Sea la norma de α es $(-1)^n p(0)$

Obs.- como $p(x) \in \mathbb{Q}[x]$ entonces la norma de α es un racional.

Notación $N(\alpha)$, es racional

Igualmente si α es entero algebraico entonces $N(\alpha) \in \mathbb{Z}$

Obs.- Sea $T_\alpha : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ dada por $T_\alpha = \alpha \cdot v$. Entonces $\det T_\alpha = N(\alpha)$

Proposición.- $N(\alpha\beta) = N(\alpha)N(\beta)$

Dem.-

Tenemos que $T_{\alpha\beta} v = \alpha\beta v = T_\alpha(T_\beta(v))$

$= T_\alpha \circ T_\beta (v)$

$N(\alpha\beta) =$

$\Rightarrow \det T_{\alpha\beta} = \det T_\alpha \det T_\beta = N(\alpha) N(\beta)$.

obs.: α es unidad $\Leftrightarrow N(\alpha) = \pm 1$

$(\Leftarrow)$

Dem.- si α es unidad $\Rightarrow \exists \beta \in \mathbb{Q}(\alpha)$ t.q.

$\alpha\beta = 1 \Rightarrow N(\alpha\beta) = N(1) = 1$

$\Rightarrow N(\alpha) = \pm 1$

Si $N(\alpha) = \pm 1 \Rightarrow \alpha \cdot (\alpha_2 \cdots \alpha_n) = \pm 1$

$\Rightarrow \alpha$ es unidad.

⋮ falta

Proposición.- $\alpha \in \mathbb{Q}(\sqrt{m}) \cap \mathbb{O}$, α es unidad $\Leftrightarrow N(\alpha) = \pm 1$

Dem.- Como $\alpha \in \mathbb{O} \Rightarrow N(\alpha) \in \mathbb{Z}$

$\Rightarrow \alpha \neq 0 \Rightarrow N(\alpha) \geq 1 = N(1) \Rightarrow N(\alpha) \leq N(\alpha\beta)$ $\forall \beta \in \mathbb{Q}(\sqrt{m}) \cap \mathbb{O}$

$\Rightarrow$ Sup. α unidad $\Rightarrow \exists \alpha^{-1}$ t.q.

$\alpha \cdot \alpha^{-1} = 1$ pero $N(\alpha) \leq N(\alpha \cdot \alpha^{-1}) = N(1) = 1$

$\Rightarrow 1 \leq N(\alpha) \leq 1 \Rightarrow N(\alpha) = 1$

proposición: Si $|N(\alpha)|$ es primo $\Rightarrow$ α es irreducible

prop. Si $\alpha \mid \beta \Rightarrow N(\alpha) \mid N(\beta)$

Teo.- ~~[illegible]~~ Sea $\alpha \in \mathbb{Q}(\sqrt{m}) \cap \mathbb{O}$
Entonces existe una factorización de α como producto de irreducibles (no unidad)

obs: $\mathbb{Q}(i) \cap \mathbb{O} = \mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$
son los enteros gaussianos.

$\mathbb{Z}[i]$ es dominio euclídeo con la Norma

obs.-

- 3 es primo en $\mathbb{Z}[i]$

- 5 No es primo en $\mathbb{Z}[i]$
pues $5 = (2+i)(2-i)$

obs) sabemos que si $p \equiv 1 \pmod 4$
p-primo $\Rightarrow$ $p = a^2+b^2$ p.a $a,b \in \mathbb{Z}$

$\Rightarrow p = (a+bi)(a-bi)$

y p no es primo en $\mathbb{Z}[i]$

α, β no unidades

Si $3 = \alpha\beta \Rightarrow N(3) = N(\alpha)N(\beta)$

$\Rightarrow 3^2 = N(\alpha)N(\beta) \Rightarrow N(\alpha) = N(\beta) = \pm 3$

$\Rightarrow N(\alpha) = N(x+iy) = x^2+y^2 \Rightarrow \pm 3 = x^2+y^2$!!

Obs.- En general si $p \equiv 3 \pmod 4$

p-primo en $\mathbb{Z} \Rightarrow p = \alpha\beta$ con α, β no unidades

$\Rightarrow p^2 = N(\alpha)N(\beta) \Rightarrow \pm p = N(\alpha) = N(\beta)$

$\Rightarrow x^2+y^2 = \pm p$!! pues $p \equiv 3 \pmod 4$ no es suma de dos cuadrados.

$\therefore p$ es primo en $\mathbb{Z}[i]$

Obs: Si $p \equiv 1 \pmod 4 \Rightarrow p = a^2+b^2$

$= (a+bi)(a-bi) \Rightarrow N(p) = N(a+bi)N(a-bi)$

$\Rightarrow a^2+b^2 = N(a+bi) = p$

$\Rightarrow$ tengo un numero complejo con norma un primo $\therefore$ es irreducible i.e. $a+bi$, $a-bi$ es primo.

Así que esta es la factorización única.

Obs.- Si $m = -1, -2, -3, -7, -11, 2, 3, 5, 13$ entonces $\mathbb{Q}(\sqrt{m})$ es euclideano

Dem.-

Caso 1: Si $m \not\equiv 1 \pmod 4$ i.e,
$m = -1, -2, 2, 3$.

Sean α, β con $\beta \neq 0$ y escribimos

$\frac{\alpha}{\beta} = u + v\sqrt{m}$ con $u, v \in \mathbb{Q}$.

Sean x, y enteros t.q
$|u - x| \leq \frac{1}{2}$ y $|v - y| \leq \frac{1}{2}$

y sea $\gamma = x + y\sqrt{m}$

$\Rightarrow N(\frac{\alpha}{\beta} - \gamma) = N(u + v\sqrt{m} - (x + y\sqrt{m}))$

$= N((u - x) + (v - y)\sqrt{m})$

$= (u - x)^2 - m(v - y)^2$

Por otro lado

$0 \leq (u - x)^2 \leq \frac{1}{4}$
$0 \leq (v - y)^2 \leq \frac{1}{4}$
$\Rightarrow \begin{cases} 0 \leq -m(v-y)^2 \leq \frac{-m}{4} & \text{si } m < 0 \\ 0 \geq -m(v-y)^2 \geq \frac{-m}{4}, & \text{si } m > 0 \end{cases}$

• Si $m < 0$

$\Rightarrow 0 \leq (u - x)^2 - m(v - y)^2 \leq \frac{1 - m}{4}$

y $\frac{1-m}{4} < 1 \iff m > -3$, pero como $m < 0 \Rightarrow m = -1$ o -2 y $m > -3$ ✓.

$\Rightarrow 0 \leq N\left(\frac{\alpha}{\beta} - \gamma\right) < 1 \Rightarrow \left|N\left(\frac{\alpha}{\beta} - \gamma\right)\right| < 1$ ∎

• si $m > 0$

$\Rightarrow -\frac{m}{4} \leq (u-x)^2 - m(v-y)^2 \leq \frac{1}{4}$

$\Rightarrow -\frac{m}{4} \leq N\left(\frac{\alpha}{\beta} - \gamma\right) \leq \frac{1}{4} < 1$

necesito que $-1 < \frac{-m}{4}$, $\Rightarrow -4 < -m$

$\Rightarrow m < 4$, pero como si $m > 0 \Rightarrow$

$m = 2, 3$ y se cumple que $m < 4$

$\Rightarrow -\frac{3}{4} < N\left(\frac{\alpha}{\beta} - \gamma\right) < 1 \Rightarrow \left|N\left(\frac{\alpha}{\beta} - \gamma\right)\right| < 1$ ∎

Caso 2: si $m \equiv 1 \pmod 4$

$\Rightarrow$ sea $\alpha, \beta \neq 0$, $\frac{\alpha}{\beta} = u + v\sqrt{m}$, $u, v \in \mathbb{Q}$

sea y entero t.q. $|2v - y| \leq \frac{1}{2}$

y x t.q. $x \equiv y \pmod 2$ y $|2u - x| \leq 1$

~~$\Rightarrow N\left(\frac{\alpha}{\beta} - \gamma\right) = N($~~

y sea $\gamma = \frac{x + y\sqrt{m}}{2}$

$\Rightarrow N\left(\frac{\alpha}{\beta} - \gamma\right) = N\left(\frac{2u - x}{2} + \left(\frac{2v - y}{2}\right)\sqrt{m}\right)$

$= \frac{1}{4}[(2u-x)^2 - m(2v-y)^2]$

p.D $|N(\frac{\alpha}{\beta} \quad)| < 1$.

- $0 \leq (2u-x)^2 \leq 1$

  $0 \leq (2v-y)^2 \leq \frac{1}{4} \Rightarrow \begin{cases} 0 \leq -m(2v-y)^2 \leq \frac{-m}{4}, & m>0 \\ 0 \geq -m(2v-y)^2 \geq -\frac{m}{4}, & m<0 \end{cases}$

- Si $m > 0$

  $\Rightarrow 0 \leq \frac{1}{4}[(2u-x)^2 - m(2v-y)^2] \leq \frac{1}{4} - \frac{m}{4}$

necesito que $\frac{1}{4} - \frac{m}{4} < 1 \Rightarrow -12 < m < 0$

y como $m<0 \Rightarrow m = -3, -7, -11$

$\therefore 0 \leq N(\frac{\alpha}{\beta} - \gamma) < 1 \Rightarrow |N(\frac{\alpha}{\beta} - \gamma)| \leq 1$.

- Si $m < 0$

  ⋮

Terminando la prueba.

Teorema.- Sea $\mathbb{Q}(\sqrt{m})$ de factorización única. Si α es un primo como entero algebraico ent. existe un único primo entero p t.q. $\alpha \mid p$

Proposición.- Si p es un primo entero ent. p es primo en $\mathbb{Q}(\sqrt{m})$ ó $p = \pi_1 \cdot \pi_2$, primos en $\mathbb{Q}(\sqrt{m})$.

Proposición.- Los primos de $\mathbb{Q}(\sqrt{m})$ se obtienen considerando los primos de $\mathbb{Z}$ que son primos en $\mathbb{Q}(\sqrt{m})$ juntos con los primos π_i que se obtienen al factorizar p que son compuestos en $\mathbb{Q}(\sqrt{m})$

Proposición.- Sea p primo impar t.q. $(p, m) = 1$. Entonces $p = \pi_1 \cdot \pi_2$, π_i primo $\Leftrightarrow$ $\left(\frac{m}{p}\right) = 1$

En este caso, $\pi_1 \not\sim \pi_2$ pero $\pi_1 \sim \overline{\pi_2}$

~~Proposición.- Sea $(2, m) = 1$ Si $m \equiv 3 \pmod 4$~~

Proposición.- Si $(2, m) = 1$ entonces:

- Si $m \equiv 3 \pmod 4 \Rightarrow 2 \sim \pi_1^2$
- Si $m \equiv 1 \pmod 8 \Rightarrow 2 = \pi_1 \cdot \pi_2$, $\pi_1 \not\sim \pi_2$
- Si $m \equiv 5 \pmod 8 \Rightarrow 2$ es primo

proposición: si $p \mid m$ entonces $p \sim \pi^2$ (asociado al cuadrado de un primo)

Dem: si $p \mid m = \sqrt{m}\sqrt{m} \Rightarrow p \nmid \sqrt{m}$

$\Rightarrow \frac{\sqrt{m}}{p} \notin$ [illegible]

$\Rightarrow p = \pi_1 \cdot \pi_2$

- si $m = \pm p$

$\Rightarrow p = \pm \sqrt{m}\sqrt{m} \Rightarrow \sqrt{m}$ primo

$\Rightarrow p \sim (\sqrt{m})^2$

- si $p < |m|$

Obs: Recordemos que si tenemos la ecuación $a^2+b^2=c^2$

- a, b de distinta paridad y c impar
- Sabemos que podemos simplificar con $(a,b,c)=1$

- Si $\exists p$ primo tq $p \mid a$ y $p \mid b \Rightarrow p \mid a^2+b^2=c^2$ $\Rightarrow p \mid c$!

$\therefore (a,b)=1$ y de forma análoga $(a,c)=1$, $(b,c)=1$.

- Tenemos que $c^2 = a^2+b^2 = (a+bi)(a-bi)$

Ahora tenemos que $(a+bi, a-bi) \mid 2a$ y $(a+bi, a-bi) \mid 2bi$

$\Rightarrow (a+bi, a-bi) \mid 2b$

$\Rightarrow (a+bi, a-bi) \mid 2ax+2by$

$\Rightarrow (a+bi, a-bi) \mid 2 = -i(1+i)^2$

$\Rightarrow (a+bi, a-bi) \sim \begin{cases} 1 \\ 1+i \\ (1+i)^2 \sim 2 \end{cases}$

- Si $g \sim 2 \Rightarrow g \mid a+bi$ $\Rightarrow g \mid a$ y $g \mid b \Rightarrow 2 \mid a$ y $2 \mid b$!

- Si $g \sim 1+i \Rightarrow N(1+i) \mid N(a+bi)$ $\Rightarrow 2 \mid a^2+b^2 = c^2$!

pero c es impar.

$\Rightarrow$) $g=2$: por la factorización única

$\Rightarrow a+bi = u(p+si)^2$

$\Rightarrow a-bi = u(r-si)^2$

- si $u=1$

$\Rightarrow a+bi = (r+si)^2 = r^2 - s^2 + 2rsi$

$\Rightarrow a = r^2 - s^2$, $b = 2rs$

- si $u=-1$

$\Rightarrow a+bi = -(r+si)^2 \Rightarrow a = s^2 - r^2$

$b = -2rs$

- si $u = i \Rightarrow a+bi = i(r+si)^2$

$= -2rs + (r^2 - s^2)i \Rightarrow a = -2rs$

$b = r^2 - s^2$

- si $u = -i \Rightarrow a+bi = -i(r+si)^2$

$\Rightarrow a = 2rs$

$b = s^2 - r^2$

- Ahora resolvamos $a^2+b^2=2c^2$

Obs:

- $(a,b,c)=1$
- si $\exists p$ primo $p \mid a$ y $p \mid b \Rightarrow p^2 \mid a^2$ y $p^2 \mid b^2$

$\Rightarrow p^2 \mid a^2+b^2 = 2c^2 \Rightarrow p^2 \mid c^2$

$\therefore (a,b)=1 \Rightarrow (a,c)=1$, $(b,c)=1$.

- Como $a^2+b^2=2c^2 \Rightarrow a^2+b^2$ par

pero a^2+b^2 no pueden ser pares al mismo tiempo $\Rightarrow$ a y b impares

- Así $a^2+b^2 \equiv 2 \pmod 4$

$\Rightarrow 2c^2 \equiv 2 \pmod 4 \Rightarrow c^2 \equiv 1 \pmod 4$

$\Rightarrow c$ impar.

$\therefore (a+bi)(a-bi) = 2c^2$ sabemos que $1+i \mid 2 \Rightarrow 1+i \mid (a+bi)(a-bi)$ pero $1+i$ es primo

$\Rightarrow 1+i \mid a+bi$ (sin perdida de generalidad)

$\Rightarrow 1-i \mid a-bi$

$\Rightarrow \dfrac{a^2+b^2}{2} = c^2 \Rightarrow \dfrac{a^2+b^2}{(1+i)(1-i)} = c^2$

$\Rightarrow \left(\dfrac{a+bi}{1+i}\right)\left(\dfrac{a-bi}{1-i}\right) = c^2$

Con $\left(\dfrac{a+bi}{1+i}, \dfrac{a-bi}{i-1}\right) = 1$

$\Rightarrow$) $\dfrac{a+bi}{1+i} = u(r+si)^2$

si $u=1$

$\Rightarrow a+bi = (1+i)(r+si)^2$

$= (1+i)(r^2-s^2+2rsi)$

$= r^2-s^2-2rs + (r^2-s^2+2rs)i$

$\Rightarrow a = r^2-s^2-2rs$

$b = r^2-s^2+2rs$

$\Rightarrow a^2+b^2 = c^2 \Rightarrow 2c^2 = 2(r^2+s^2)^2$

$\Rightarrow c^2 = (r^2+s^2)^2 \Rightarrow c = |r^2+s^2|$