19/08/20

§ Ternas pitagóricas: soluciones enteras de $x^2+y^2=z^2$.

(x,y,z)
(cx,cy,cz)

$x,y,z>0$.

Ejemplos: $(3,4,5)$, $(5,12,13)$, $(7,24,25)$

Ternas pitagóricas $\Longleftrightarrow$ $\alpha = x+iy \in \mathbb{Z}[i]$ t.q. $N(\alpha)=z^2$.

$N(\alpha^2)=N(\alpha)^2$.

Ejemplos:
$(2+i)^2 = 3+4i$
$(3+2i)^2 = 5+12i$
$(4+3i)^2 = 7+24i$

$(a+bi)^2 = a^2-b^2+2abi$

$\Rightarrow (a^2-b^2,\ 2ab,\ a^2+b^2)$

def (x,y,z) es **primitiva** si $\mathrm{mcd}(x,y,z)=1$

$(\Leftrightarrow \mathrm{mcd}(x,y)=1)$

S.p.d.g. x es impar, y es par.

$1^2+1^2\equiv 2 \not\equiv \square \pmod{}$

Teorema Si (x,y,z) es una terna primitiva, x impar y y par

$\Rightarrow \exists\, a>b>0$, $\mathrm{mcd}(a,b)=1$ t.q.

$(x,y,z)=(a^2-b^2,\ 2ab,\ a^2+b^2)$

Dem $N(x+yi)=(x+yi)(x-yi)=z^2$

Ejercicio: Si $\mathrm{mcd}(x,y)=1$ y de diferente paridad

$\Rightarrow \mathrm{mcd}(x+yi,\ x-yi)=1$

Factorización única $\Rightarrow$ $x+yi \sim \alpha^2$ para $\alpha\in\mathbb{Z}[i]$

$x+yi = u\cdot(a+bi)^2$ $\quad u\in\{\pm1,\pm i\}$. $\quad -1=i^2 \Rightarrow$ basta tomar $u=1,i$.

$x+yi = u\cdot(a^2-b^2+(2ab)i)$

x impar $\Rightarrow u=+1$.

$x,y>0 \Rightarrow a>b>0$,

$\mathrm{mcd}(x,y)=1 \Rightarrow \mathrm{mcd}(a,b)=1$. ////

Punto clave en DFU, si $\mathrm{mcd}(\alpha,\beta)=1$,

$\alpha\cdot\beta=\gamma^2 \Rightarrow \exists\, \alpha',\beta'$ t.q. $\alpha\sim\alpha'^2$, $\beta\sim\beta'^2$

(Contra) ejemplo: $R = \mathbb{Z}[\sqrt{-5}]$. $R^\times = \{\pm 1\}$

$$\alpha = 2 + 3\sqrt{-5}, \qquad \bar{\alpha} = 2 - 3\sqrt{-5}.$$

$$\alpha\bar{\alpha} = N(\alpha) = 2^2 + 5\cdot 3^2 = 49 = 7^2$$

$a^2 + 5b^2 \neq 7 \implies \alpha$ y $\bar{\alpha}$ son irreducibles

$\alpha \neq \bar{\alpha}$ $\qquad \alpha\bar{\alpha} = 7^2$, pero no son $\mathcal{I}$ cuadrado.

$\mathbb{Z}[\sqrt{-5}]$ no tiene factorización única!

§ Ecuación de Fermat $x^3 + y^3 = z^3$

Euler: no hay soluciones enteras $xyz \neq 0$.

la prueba usa que $\mathbb{Z}[\sqrt{-3}]$ es un DFU.

Ejercicio: $\mathbb{Z}[\sqrt{-3}]$ no lo es!

$$\mathbb{Z}[\zeta_3] = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \supsetneq \mathbb{Z}[\sqrt{-3}].$$

sí es un DFU.

$$z^3 = x^3 + y^3 = (x+y)(x+\zeta_3 y)(x+\zeta_3^2 y)$$

Proposición $x^3 + y^3 = z^3$ no tiene sol. en $\mathbb{Z}[\zeta_3]$

con $\pi \nmid xyz$, donde $\pi = 1 - \zeta_3$.

Dem. Si $\pi \nmid x \implies x \equiv \pm 1 \pmod{\pi}$ $\qquad \mathbb{Z}[\zeta_3]/(\pi) \simeq \mathbb{F}_3$.

$$x \equiv \pm 1 \pmod{\pi} \xRightarrow[\text{ejercicio}]{} x^3 \equiv \pm 1 \pmod{\pi^4}$$

$$\pi \mid (x \pm 1) \implies \pi^4 \mid (x^3 \pm 1).$$

$\pi^4 \sim 9.$ $\qquad \mathbb{Z}[\zeta_3]/(\pi^4) \simeq \mathbb{Z}[\zeta_3]/(9).$

$\pi \nmid xyz.$ $\qquad x^3 + y^3 = z^3.$

$$\pm 1 \pm 1 \equiv \pm 1 \pmod{\pi^4}$$

esto es imposible! ∎

Descenso infinito para $v_\pi(z)$. (en las notas).

§ Puntos enteros en $y^2 = x^3 + t$.

$E: y^2 = x^3 + ax + b$. $\quad a, b \in \mathbb{Z}$. $\quad \Delta = 4a^3 + 27b^2 \neq 0$.

una curva elíptica.

Siegel: $\# \{ (x,y) \in \mathbb{Z}^2 \mid (x,y) \in E \} < \infty$.
(Silverman)

Ejemplo $y^2 = x^3 - 1$. tiene única solución entera $(1,0)$.

Demostración $x^3 - 1 \not\equiv 1 \pmod 4 \implies y$ es par.

Ejercicio: si y es par, entonces $\operatorname{mcd}(y+i, y-i) = 1$.

$$x^3 = (y+i)(y-i) \implies y+i = u \cdot (a+bi)^3.$$

$\pm i = (\mp i)^3 \implies$ s.p.d.g., $u = 1$.

$$y + i = (a+bi)^3 = a(a^2 - 3b^2) + b(3a - b^2)i$$

$$1 = b(3a - b^2) \implies (a,b) = (0,1)$$

$y = 0, x = 1$ ▦

Ejemplo $y^2 = x^3 - 19$. $\quad x^3 - 19 \not\equiv 1 \pmod 8$

$y^2 \equiv 1 \pmod 8$ si y impar.

y es par. En este caso

$$\operatorname{mcd}(y + \sqrt{-19}, y - \sqrt{-19}) = 1.$$

$$x^3 = (y + \sqrt{-19})(y - \sqrt{-19})$$

$$y + \sqrt{-19} = (a + b\sqrt{-19})^3 = a(a^2 - 57b^2) + \underbrace{b(3a^2 - 19b^2)}_{\neq 1}\sqrt{-19}$$

$\implies$ No hay soluciones enteras. (?!) $y^2 = x^3 - 19$

$7^3 - 19 = 324 = 18^2$ $\quad (7, \pm 18)$ SÍ es una solución.

$\mathbb{Z}[\sqrt{-18}]$ no es un DFU.

Pero $\mathbb{Z}\left[\frac{1+\sqrt{-18}}{2}\right]$ sí lo es,

Ocupando este anillo el mismo argumento nos da que los únicos puntos enteros son $(7, \pm 18)$.

En la tarea: $y^2 = x^3 - 4$

$$x^3 = y^2 + 4 = (y+2i)(y-2i)$$

§ Ecuación de Pell $x^2 - dy^2 = 1$

aquí $d > 0$ libre de cuadrados.

Ejemplo: $d = 3$. $\quad x^2 - 3y^2 = 1$.

Consideremos $\mathbb{Z}[\sqrt{3}]$.

la norma. $N(x+y\sqrt{3}) = (x+y\sqrt{3})(x-y\sqrt{3})$
$$= x^2 - 3y^2$$

$\mathbb{Z}[\sqrt{3}]^\times = \{\alpha \mid N(\alpha) = \pm 1\}$

$x^2 - 3y^2 \equiv x^2 + y^2 \not\equiv 3 \pmod 4$

No hay elementos de norma -1.

$\alpha\alpha^{-1} = 1$

$N(\alpha) . N(\alpha^{-1}) = 1$

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

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

$\alpha^{-1} = \pm\sigma(\alpha)$

$\alpha \cdot \sigma(\alpha) = N(\alpha)$

Conclusión:

$$\left\{\begin{array}{l}\text{Soluciones enteras de} \\ x^2 - 3y^2 = 1 \\ (x,y)\end{array}\right\} \longleftrightarrow \mathbb{Z}[\sqrt{3}]^\times$$
$$x + y\sqrt{3}$$

Ejemplo: $2 + \sqrt{3} \in \mathbb{Z}[\sqrt{3}]^\times \quad (2^2 - 3 \cdot 1^2 = 1)$

Notamos que si $u \in \mathbb{Z}[\sqrt{3}]^\times$, entonces

$\pm u^n \in \mathbb{Z}[\sqrt{3}]^\times$ para $n \in \mathbb{Z}$

Son diferentes unidades.

$u^m = u^n \Rightarrow u^{m-n} = 1.$ pero $\mathbb{Z}[\sqrt{3}] \subset \mathbb{R}$
y en $\mathbb{R}$ las únicas raíces de la unidad
son ± 1.

Lema $2+\sqrt{3}$ es la unidad más pequeña t.q.
en $\mathbb{Z}[\sqrt{3}]$.
$u > 1$.

Dem Tomamos $u = a + b\sqrt{3}$. t.q.

$$1 \leq u \leq 2+\sqrt{3}.$$

Tomando inversos, $u + u^{-1} = 2a$.

$$2-\sqrt{3} \leq u^{-1} \leq 1.$$

$$1 < 3-\sqrt{3} \leq \underbrace{u+u^{-1}}_{=2a} \leq 3+\sqrt{3} < 5.$$

$$\left.\begin{array}{l} u \cdot u^{-1} = 1 \\ u + u^{-1} = 2 \end{array}\right\} \Rightarrow u = 1 \qquad \left.\begin{array}{l} u \cdot u^{-1} = 1 \\ u + u^{-1} = 4 \end{array}\right\} \Rightarrow u = 2+\sqrt{3}.$$

$\blacksquare$

def Se dice que $u = 2+\sqrt{3}$ es la
unidad fundamental.

Teorema Todas las unidades en $\mathbb{Z}[\sqrt{3}]$ son
de la forma $\pm(2+\sqrt{3})^n$, $n \in \mathbb{Z}$.

$$\mathbb{Z}[\sqrt{3}]^\times \simeq \{\pm 1\} \times \langle 2+\sqrt{3} \rangle$$
$$\simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$$

Dem. $\pm(2+\sqrt{3})^n$ son unidades. Hay otras?

$u \in \mathbb{Z}[\sqrt{3}]^\times$. Pasando a $\pm u^{\pm 1}$, podemos
asumir que $u \geq 1$.

$\exists n$ t.q. $(2+\sqrt{3})^n \leq u < (2+\sqrt{3})^{n+1}$.

$$1 \leq u \cdot (2+\sqrt{3})^{-n} < 2+\sqrt{3}$$

lema $\Rightarrow$ $u = (2+\sqrt{3})^n$. $\blacksquare$

Acabamos de ver un caso particular del teorema de unidades de Dirichlet.

Ejemplo $x^2 - 2011y^2 = 1$.

Las soluciones se encuentran mediante la unidad fundamental de $\mathbb{Z}[\sqrt{2011}]^\times$. (un número muy grande)

- En PARI/GP quadunit.
- Veremos un algoritmo (fracciones continuas)

$\alpha \in R$ $\qquad \alpha \sim u\cdot\alpha, \quad u \in R^\times$.

Un número puede tener muchos asociados.

Mejor pasar a $R/\sim$

$(\alpha) = (\beta) \iff \alpha \sim \beta$.

En lugar de trabajar con elementos $\alpha \in R$, mejor trabajar con ideales como (α).

$\mathbb{Z}[\sqrt{3}]^\times \simeq \{\pm 1\} \times \langle u \rangle \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$,

En lugar de u, podemos tomar $-u$, u^{-1}, ó $-u^{-1}$.

Pero entre $u, -u, u^{-1}, -u^{-1}$ precisamente uno cumple $u > 1$

Pero en gral, tendremos

$$\underset{(R \text{ orden})}{R^\times} \simeq \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{r} \oplus \underbrace{T}_{\text{grupo finito}} \simeq \langle u_1 \rangle \times \cdots \times \langle u_r \rangle \times T$$

son unidades fundamentales