Teoría de Números

Práctica 1

Lucio Santi
lsanti@dc.uba.ar

10 de septiembre de 2017

Ejercicio. *Asumiendo que el anillo* $\mathbb{Z}[\alpha = \frac{1+\sqrt{-19}}{2}]$ *es DFU, probar que* $(x, y) = (\pm 18, 7)$ *son las únicas soluciones enteras de la ecuación*

$$x^2 + 19 = y^3$$

Resolución. Si factorizamos $x^2 + 19$ en $\mathbb{Z}[\alpha]$, tenemos

$$\begin{aligned} x^2 + 19 &= (x + \sqrt{-19})(x - \sqrt{-19}) \\ &= ((x-1) + 2\alpha)\,((x+1) - 2\alpha) \\ &= \beta\dot{\gamma} \end{aligned}$$

Consideremos un $\delta = a + b\alpha \in \mathbb{Z}[\alpha]$ tal que $\delta|\beta$ y $\delta|\gamma$. Luego, se tiene que

$$\delta|\,((x-1) + 2\alpha) - ((x+1) - 2\alpha) = -2 + 4\alpha = 2(-1 + 2\alpha) = \eta$$

Puesto que $\mathbb{Z}[\alpha]$ es un dominio de factorización única, η es expresable como producto de primos de forma única (salvo asociados). Por ende, supongamos que δ es un divisor primo de η. De esta forma, $\delta|2$ o bien $\delta| -1 + 2\alpha$, de lo que sigue que $N(\delta)|N(2) = 4$ o bien $N(\delta)|N(-1 + 2\alpha) = 19$, siendo $N(u + v\alpha) = u^2 + uv + 5v^2$ la norma de $\mathbb{Z}[\alpha]$. Observemos que, como función de u, $f(u) = N(u + v_0\alpha) = u^2 + uv_0 + 5v_0^2$ es decreciente hasta $u = -v_0/2$, donde alcanza su mínimo, y luego creciente. De esta forma,

$$N(u + v\alpha) = u^2 + uv + 5v^2 \geq (-v/2)^2 + (-v/2)\,v + 5v^2 = 19/4\,v^2$$

Además, si buscamos que $\delta|2$ o que $\delta| -1 + 2\alpha$, necesariamente debe ocurrir que $b \neq 0$ si nos proponemos encontrar divisores no triviales. Así, $N(\delta) \geq 19/4 > 4$, por lo que $\delta|2$ sólo si δ es una unidad de $\mathbb{Z}[\alpha]$. Por otro lado, siempre que $|b| > 2$, $N(\delta) > 19$, de manera que $b = \pm 2$ si buscamos un divisor no unidad de $-1 + 2\alpha$. No obstante, en tales casos los únicos valores de δ posibles son precisamente $-1 + 2\alpha$ y $1 - 2\alpha$. En consecuencia, puesto que $\delta = \pm(-1 + 2\alpha)$ no puede ser divisor simultáneo de β y de γ, se tiene que β y γ son coprimos en $\mathbb{Z}[\alpha]$ o bien el único divisor no unidad que comparten es 2. En el primer caso, deben ser β y γ cubos simultáneamente de forma tal de satisfacer la ecuación deseada. En particular, deben existir ciertos $c, d \in \mathbb{Z}$ tales que

$$\begin{aligned} \beta = (x-1) + 2\alpha &= (c + d\alpha)^3 \\ &= \left(c^3 - 5d^3 - 15cd^2\right) + \left(3c^2d - 4d^3 + 3cd^2\right)\alpha \end{aligned}$$

de lo que, por unicidad de escritura, sigue que

$$d(3c^2 - 4d^2 + 3cd) = 2$$

y esto vale si y sólo si $d = 1$ y $c \in \{1, -2\}$. De esta forma,

$$x = 1 + c^3 - 5d^3 - 15cd^2 \in \{-18, 18\}$$

lo cual permite concluir que, en cualquier caso, $y = 7$ reemplazando en la ecuación original.

Finalmente, si β y γ comparten a 2 como único divisor común no unidad, es posible considerar $\beta' = 2\beta$ y $\gamma' = \frac{\gamma}{2}$ siendo β' y γ' coprimos en $\mathbb{Z}[\alpha]$. A través de un razonamiento similar al anterior, puede arribarse a la conclusión de que no existe una forma de expresar como cubo en $\mathbb{Z}[\alpha]$ a γ'. Por ende, esto termina de probar que las únicas soluciones posibles a la ecuación planteada son las descriptas anteriormente. □

Ejercicio. *Caracterizaremos los primos que son suma de dos cuadrados. Probaremos que, si p es un primo impar, entonces $p = x^2 + y^2$ si y sólo si $p \equiv 1 \, mod \, 4$.*

I. *Sea p primo impar tal que p se escribe como suma de dos cuadrados. Probar que -1 es un cuadrado módulo p. Concluir que $p \equiv 1 \, mod \, 4$.*

II. *Sea p primo impar, $p \equiv 1 \, mod \, 4$. Tomar $n \in \mathbb{Z}$ tal que $n^2 \equiv -1 \, mod \, p$. Como $p|n^2 + 1$ en $\mathbb{Z}$, tenemos que $p|(n + i)(n - i)$ en $\mathbb{Z}[i]$. Probar que p no es primo de $\mathbb{Z}[i]$ y, por lo tanto, es reducible.*

III. *Sabiendo que $p = \alpha\dot{\beta}$, $\alpha, \beta \in \mathbb{Z}[i]$ no unidades, concluir que p es suma de dos cuadrados.*

Resolución. TBD □

Ejercicio. *Caracterización de los irreducibles de $\mathbb{Z}[i]$.*

I. *Probar que $2 = (-i)(1 + i)^2$ y que $1 + i$ es irreducible.*

II. *Sea $p \equiv 3 \, mod \, 4$. Probar que $p = x^2 + y^2$ no tiene soluciones en $\mathbb{Z}$. Concluir que p es irreducible en $\mathbb{Z}[i]$.*

III. *Utilizar el ejercicio anterior para probar que, si $p \equiv 1 \, mod \, 4$, entonces p se factoriza en $\mathbb{Z}[i]$ como producto de dos irreducibles no asociados.*

IV. *Probar que, si π es un irreducible de $\mathbb{Z}[i]$, entonces π es asociado a alguno de los irreducibles mencionados en los ítems anteriores (sug.: si π es irreducible, existe un primo $p \in \mathbb{Z}$ tal que $p|N(\pi) = \pi\bar{\pi}$ y usar factorización única).*

Resolución. TBD □

Ejercicio. *Factorizar como producto de irreducibles los elementos $7 + 4i$ y $23 + 14i$ en $\mathbb{Z}[i]$.*

Resolución. Inmediato usando SageMath ☺:

```
sage: K.<i> = QuadraticField(-1)
sage: factor(7 - 4*i)
(i) * (-i - 2) * (2*i + 3)
sage: factor(23+14*i)
(-i - 2)^2 * (-2*i + 5)
```

□