Teoría de Números

Práctica 1

Lucio Santi
lsanti@dc.uba.ar

16 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

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

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 δ no puede ser un divisor no trivial de 2 en $\mathbb{Z}[\alpha]$. Por otro lado, siempre que $|b| > 2$, $N(\delta) > 19$, de manera que $b = \pm 2$. 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 primo 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 primo, es posible considerar $\beta' = 2\beta$ y $\gamma' = \frac{\gamma}{2}$ siendo así β' y γ' coprimos en $\mathbb{Z}[\alpha]$ (notar que $\gamma' = \frac{x+1}{2} - \alpha$ no es divisible por 2). 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 $p = \alpha \cdot \beta$, $\alpha, \beta \in \mathbb{Z}[i]$ no unidades, concluir que p es suma de dos cuadrados.*

IV. *Caracterizar los $n \in \mathbb{N}$ que son suma de dos cuadrados.* ***Nota:*** *excluyo deliberadamente al 0 de la suma para hacer el ejercicio más interesante (de lo contrario, quedan cubiertos muchos casos que simplifican los razonamientos –en particular, todos los cuadrados perfectos).*

Resolución.

I. Sea p primo impar tal que $p = x^2 + y^2$ para ciertos $x, y \in \mathbb{Z}$. Como p es impar, debe ser $x \equiv 0 \bmod 2$ y $y \equiv 1 \bmod 2$ o viceversa. Sin pérdida de generalidad, tomemos entonces $x \equiv 0 \bmod 2$ y $y \equiv 1 \bmod 2$. Observemos que $x^2 \equiv 0 \bmod 4$ y $y^2 \equiv 1 \bmod 4$. Veamos cuánto vale el símbolo de Legendre de -1:

$$\begin{aligned} \left(\frac{-1}{p}\right) &= (-1)^{\frac{p-1}{2}} \\ &= (-1)^{\frac{x^2+y^2-1}{2}} \\ &= (-1)^{\frac{x^2}{2}} (-1)^{\frac{y^2-1}{2}} \\ &= 1 \end{aligned}$$

De esta manera, queda probado que -1 es un cuadrado módulo p. Como consecuencia, debe ser necesariamente $p \equiv 1 \bmod 4$ pues, en caso contrario, $\left(\frac{-1}{p}\right) \neq 1$.

II. Sea p primo impar, $p \equiv 1 \bmod 4$, y sea $n \in \mathbb{Z}$ tal que $n^2 \equiv -1 \bmod p$ (un tal n debe existir puesto que $\left(\frac{-1}{p}\right) = 1$). Como $p|n^2 + 1$ en $\mathbb{Z}$, se tiene que $p|(n + i)(n - i)$ en $\mathbb{Z}[i]$. Supongamos que p es primo en $\mathbb{Z}[i]$. Luego, $p|n + i$ o bien $p|n - i$. En el primer caso, se tiene que $n + i = p\gamma$ para cierto $\gamma = a + bi \in \mathbb{Z}[i]$. Luego, $n + i = pa + pbi$, con lo cual debe ser $1 = pb$, lo cual es un absurdo puesto que $p, b \in \mathbb{Z}$ y $p > 1$. El otro caso puede argumentarse de manera análoga. Por ende, p no puede ser primo en $\mathbb{Z}[i]$ y, por lo tanto, no es irreducible (siendo $\mathbb{Z}[i]$ un DFU).

III. En el contexto del ítem anterior, tenemos que $p = \alpha \cdot \beta$, con $\alpha, \beta \in \mathbb{Z}[i]$ no unidades. Luego,

$$N(p) = N(\alpha \cdot \beta) = N(\alpha)N(\beta)$$

Considerando $\alpha = a + bi$ y $\beta = c + di$ para ciertos $a, b, c, d \in \mathbb{Z}$, tenemos entonces

$$p^2 = (a^2 + b^2)(c^2 + d^2)$$

Al ser p primo en $\mathbb{Z}$, tenemos las siguientes posibilidades:

- $a^2 + b^2 = 1$ y $c^2 + d^2 = p^2$,
- $a^2 + b^2 = p^2$ y $c^2 + d^2 = 1$, o bien
- $a^2 + b^2 = p$ y $c^2 + d^2 = p$

Observar que los dos primeros casos no pueden suceder puesto que, de ser así, α o β serán una unidad de $\mathbb{Z}[i]$. Luego, del último ítem se desprende lo que buscábamos.

IV. Veremos que $n \in \mathbb{N}$ es suma de dos cuadrados positivos si y sólo si

- n es libre de cuadrados y $p|n \Rightarrow p = 2$ o $p \equiv 1 \bmod 4$, o bien
- $n = m^2 u$ para ciertos $m, u \in \mathbb{N}$ tales que $u > 1$ y $p|u \Rightarrow p \equiv 1 \bmod 4$ o $p = 2$ y $4 \nmid u$.

En definitiva, la primera condición es redundante puesto que se desprende de la segunda tomando $m = 1$ y u libre de cuadrados. Es decir, lo que hay que ver es que n es suma de dos cuadrados si y sólo si $n = m^2 u$ para ciertos $m, u \in \mathbb{N}$ tales que $u > 1$ y $p|u \Rightarrow p \equiv 1 \bmod 4$ o $p = 2$ y $4 \nmid u$.

Observemos primero que, si n y m son impares y suma de dos cuadrados, entonces nm también lo es. Notar que, si $n = a^2 + b^2$ y n es impar, entonces $a \neq b$, de lo que sigue que, si $m = c^2 + d^2$ es también impar, entonces $ac \neq bd$ o bien $ad \neq bc$. Luego, suponiendo lo primero,

$$nm = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ac - bd)^2$$

Además, si $n = 2 = 1^2 + 1^2$,

$$2m = 2(c^2 + d^2) = (c + d)^2 + (c - d)^2$$

Veamos ahora que, dado $n = m^2 u$ para ciertos $m, u \in \mathbb{N}$ tales que $u > 1$ y $p|u \Rightarrow p \equiv 1 \bmod 4$ o $p = 2$ y $4 \nmid u$, n es suma de dos cuadrados. Por las observaciones anteriores y los ítems previos del ejercicio, tenemos que $u = a^2 + b^2$ para ciertos $a, b \in \mathbb{Z}$. Luego,

$$m^2 u = m^2(a^2 + b^2) = (ma)^2 + (mb)^2$$

Finalmente, consideremos $n = a^2 + b^2$ para $a, b \in \mathbb{Z}$. Supongamos primero que n es libre de cuadrados y que p es un primo que divide a n tal que $p \equiv 3 \bmod 4$. Por el ejercicio siguiente, p es pues primo en $\mathbb{Z}[i]$ y $p|n = (a + bi)(a - bi)$, de manera que $p|a + bi$ o bien $p|a - bi$. En cualquier caso, $p^2|a^2 + b^2 = n$, lo cual contradice el hecho de que n sea libre de cuadrados. De esta forma, n debe ser producto de primos pares o congruentes a 1 módulo 4. Por ende, basta tomar $m = 1$ para ver que $n = m^2 u$ con las restricciones solicitadas.

Supongamos ahora que n no es libre de cuadrados. De esta forma, podemos agrupar todas las potencias pares de primos que dividen a n en un único factor m^2 y dejar otro factor u libre de cuadrados. Así, $n = m^2 u$, con $u \geq 1$. Tomemos $u > 1$ y supongamos que existe cierto primo p tal que $p|u$, $p|m$ y $p \equiv 3 \bmod 4$. De esta forma,

$$n = m^2 u = p^{2k+1} m'^2 u'$$

para algún $k > 0$. Al igual que antes, tenemos que p es primo en $\mathbb{Z}[i]$ y, por ende, debe dividir a $a + bi$ o $a - bi$. No obstante, observar que todo entero z que divide a $a + bi$ debe necesariamente dividir también a $a - bi$. Así, si $p^r | a + bi$, $p^r | a - bi$, de lo que sigue que $p^{2r} | a^2 + b^2 = n$. Se ve pues que la potencia de p no puede ser impar, de lo que se desprende que p no puede ser congruente a 3 módulo 4 y dividir a u.

Por último, supongamos que $u = 1$, de lo que sigue que n es un cuadrado. De haber al menos un primo divisor de m congruente a 1 módulo 4, podemos tomar $m = m'^2 z^2$, de forma que todos los primos divisores de n pares o congruentes a 3 módulo 4 queden agrupados totalmente en m'. Se ve así que n queda expresado en la forma que buscamos tomando $u = z^2 > 1$. De no haber ningún primo divisor de m congruente a 1 módulo 4, se puede ver que debe ser $a + bi = a - bi$, lo cual no puede ocurrir siendo $b \neq 0$.

□

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.

I. La cuenta es inmediata:
$$(-i)(1+i)^2 = (-i)(1 + 2i - 1) = 2$$
Consideremos ahora los divisores de $1 + i$ en $\mathbb{Z}[i]$. Sea entonces $\alpha \in \mathbb{Z}[i]$ tal que $\alpha | 1 + i$, de manera que $N(\alpha) | N(1 + i) = 2$. Luego, $N(\alpha) \in \{1, 2\}$. No obstante, todos los elementos de $\mathbb{Z}[i]$ con norma 2 son asociados de $1 + i$, con lo cual se concluye que $1 + i$ es irreducible en dicho anillo.

II. Sea p primo en $\mathbb{Z}$ tal que $p \equiv 3 \bmod 4$. Consideremos un divisor primo $\alpha = a + bi \in \mathbb{Z}[i]$ de p. Debe ocurrir que $N(\alpha) | N(p) = p^2$, por lo que $N(\alpha) \in \{p, p^2\}$. No obstante $N(\alpha) = a^2 + b^2 \neq p$ como consecuencia del ejercicio anterior (esto sólo es posible cuando $p \equiv 1 \bmod 4$). Luego, debe ser $N(\alpha) = p^2$. Pero, entonces,
$$p^2 = N(p) = N(\alpha \cdot \beta) = N(\alpha) N(\beta) = p^2 \, N(\beta)$$
de manera que $N(\beta) = 1$. Por ende, β es unidad y p es asociado a α, por lo que es irreducible en $\mathbb{Z}[i]$.

III. Dado p primo en $\mathbb{Z}$ tal que $p \equiv 1 \bmod 4$, del ejercicio anterior tenemos que $p = x^2 + y^2$ para ciertos $x, y \in \mathbb{Z}$. Luego, $p = (x + yi)(x - yi)$ en $\mathbb{Z}[i]$. Sea $\alpha = a + bi \in \mathbb{Z}[i]$ un divisor primo de $x + yi$. Luego, $N(\alpha) | N(x + yi) = p$, de lo que se desprende que $N(\alpha) = a^2 + b^2 = p$. Entonces,
$$(a + bi)(a - bi) = (x + yi)(x - yi)$$

Y, escribiendo $x + yi = \alpha \cdot \beta$,

$$\alpha(a - bi) = \alpha \cdot \beta(x - yi)$$

Al ser $\mathbb{Z}[i]$ un DFU y α primo, tenemos que $a - bi = \beta(x - yi)$, con lo cual

$$\begin{aligned} p &= N(a - bi) \\ &= N(\beta(x - yi)) \\ &= N(\beta)N(x - yi) \\ &= N(\beta)p \end{aligned}$$

Por ende, se tiene que $N(\beta) = 1$ o, en otras palabras, β es una unidad. Así, $x + yi$ es asociado de α, de manera que es irreducible en $\mathbb{Z}[i]$. Un argumento similar puede darse para la irreducibilidad de $x - yi$. Observar que ambos son no asociados puesto que ninguna unidad ν del anillo es tal que $x + yi = \nu(x - yi)$.

IV. Sea π un irreducible de $\mathbb{Z}[i]$. Puesto que $N(\pi) > 1$, debe existir algún primo $p \in \mathbb{Z}$ tal que $p|N(\pi) = \pi\bar{\pi}$, es decir, $\pi\bar{\pi} = pq$ para algún $q \in \mathbb{Z}$. Primero notemos que, si $\bar{\pi} \in \mathbb{Z}$, se tiene que $\pi = \bar{\pi} \in \mathbb{Z}$, con lo que necesariamente $\pi = \pm p$. Así, por factorización única en $\mathbb{Z}[i]$, π debe ser tal que $\pi \equiv 3 \bmod 4$. Ahora consideremos $\bar{\pi} \notin \mathbb{Z}$. De ser así, existe por lo menos un factor irreducible de p que no aparece en $\bar{\pi}$. Dicho factor, pues, debe ser necesariamente asociado a π, de nuevo valiéndonos de la factorización única en $\mathbb{Z}[i]$.

□

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)
```

□