Teoría de Números

Práctica 1

Lucio Santi
lsanti@dc.uba.ar

10 de septiembre de 2017

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

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

Resolución. TBD □

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* $p \equiv 1 \bmod 4$.

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* $p \equiv 1 \bmod 4$.

II. *Sea* p *primo impar,* $p \equiv 1 \bmod 4$. *Tomar* $n \in \mathbb{Z}$ *tal que* $n^2 \equiv -1 \bmod p$. *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* $p \equiv 3 \bmod 4$. *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* $p \equiv 1 \bmod 4$, *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)
```

□