Reto 8

Rafa Granero

Se tiene que

$$x^5 = (y + \sqrt{-14})(y - \sqrt{-14})$$

así que hemos de trabajar sobre

$$\mathbb{Z}[\sqrt{-14}]$$

que es el anillo de enteros de

$$\mathbb{Q}(\sqrt{-14})$$

No es un D.F.U. pues su grupo de clase no es el trivial, si no que es isomorfo a

$$\mathbb{Z}/4\mathbb{Z}$$

como se vio en clase. Debemos tratar con ideales. Sea $\mathfrak{p}$ un ideal primo dividiendo a $< y + \sqrt{-14} >$ y $< y - \sqrt{-14} >$ entonces dividirá a la resta $< 2\sqrt{-14} >$. El polinomio mínimo es

$$x^2 + 14$$

entonces

$$< 2 >=< 2, \sqrt{-14} >^2 = \mathfrak{p}_2^2$$

y

$$< 7 >=< 7, \sqrt{-14} >^2 = \mathfrak{p}_7^2$$

Si calculamos

$$\mathfrak{p}_2\mathfrak{p}_7 =< 2, \sqrt{-14} >< 7, \sqrt{-14} >=< 14, 2\sqrt{-14}, 7\sqrt{-14}, -14 >=< 2\sqrt{14}, 7\sqrt{-14} >$$

y nos gustaría ver que en realidad tenemos

$$< \sqrt{-14} >=< 2\sqrt{-14}, 7\sqrt{-14} >$$

Esto es fácil verlo. De entrada $\sqrt{-14} \in \mathfrak{p}_2\mathfrak{p}_7$ lo que nos da un contenido. El otro contenido es ver que

$$(a + b\sqrt{-14})2\sqrt{-14} + (a' + b'\sqrt{-14})7\sqrt{-14} = \sqrt{-14}(2a + 2b\sqrt{-14} + 7a' + 7b'\sqrt{-14})$$

Así

$$< 2\sqrt{-14} >=< 2 >< \sqrt{-14} >= \mathfrak{p}_2^3\mathfrak{p}_7$$

de donde $\mathfrak{p} = \mathfrak{p}_2$ o $\mathfrak{p}_7$.

Veamos el primer caso, $\mathfrak{p} = \mathfrak{p}_2$, entonces

$$< 2 >= \mathfrak{p}_2^2| < y + \sqrt{-14} >< y - \sqrt{-14} >=< x >^5$$

de donde x es par. Si x es par entonces y debe ser par. Si miramos la ecuación módulo 4 vemos que se tiene

$$0 = 2 \quad mod\ 4$$

Contradicción.

En el segundo caso tenemos $\mathfrak{p} = \mathfrak{p}_7$. Entonces

$$< y + \sqrt{-14} >= \mathfrak{p}_7^k \mathfrak{q}$$

conjugando

$$< y - \sqrt{-14} >= \mathfrak{p}_7^k \bar{\mathfrak{q}}$$

porque $\mathfrak{p}_7 = \bar{\mathfrak{p}}_7$ y donde $\bar{\mathfrak{q}}$ y $\mathfrak{q}$ son primos entre si (pues el único ideal que puede dividir a $< y - \sqrt{-14} >$ y $< y + \sqrt{-14} >$ es $\mathfrak{p}_7$). Luego

$$< x >^5 =< y - \sqrt{-14} >< y + \sqrt{-14} >= \mathfrak{p}_7^{2k} \mathfrak{q} \bar{\mathfrak{q}}$$

entonces $< y + \sqrt{-14} >= \mathfrak{s}^5$ para cierto ideal $\mathfrak{s}$. Argumentando con órdenes del grupo de clase, elórden de $\mathfrak{s}$ debe ser divisor de 4 (sin ser 4) y de 5, luego es 1, tenemos que $\mathfrak{s}$ es principal. En conclusión: $y + \sqrt{-14}$ es un elemento α a la quinta *i.e.*

$$\alpha^5 = (a + b\sqrt{-14})^5$$

Si escribimos las ecuaciones tenemos

$$\begin{cases} y = a^5 - 140a^3b^2 + 980ab^4 \\ 1 = b(5a^4 - 140a^2b^2 + 196b^4) \end{cases} \tag{1}$$

de la segunda ecuación obtenemos que $b = 1$ y $5a^4 - 140a^2 + 196 = 1$ o $b = -1$ y $5a^4 - 140a^2 + 196 = -1$. $5a^4 - 140a^2 + 196 = 1$ no tiene soluciones enteras, sus soluciones son

$$-\sqrt{14 + \sqrt{157}}, \sqrt{14 + \sqrt{157}}, -\sqrt{14 - \sqrt{157}}, \sqrt{14 - \sqrt{157}}$$

Las soluciones de $5a^4 - 140a^2 + 196 = -1$ son

$$\frac{-1}{5}\sqrt{350 + 15\sqrt{435}}, \frac{1}{5}\sqrt{350 + 15\sqrt{435}}, \frac{-1}{5}\sqrt{350 - 15\sqrt{435}}, \frac{1}{5}\sqrt{350 - 15\sqrt{435}}$$

que tampoco son enteras. Por lo tanto no existe solución entera del sistema y en consecuencia nuestra ecuación no tiene soluciones enteras.