Tarea 3 – Aritmética

Profesor: Pedro Montero, Ayudante: Tobías Martínez

Departamento de Matemática, Universidad Técnica Federico Santa María

Fecha de entrega:[1] Hasta el Domingo 11 de Junio de 2023 a las 23h59.

Esta Tarea puede ser realizada en grupos de 1 o 2 personas, y se debe **indicar el nombre de cada integrante**. Deben escoger 1 de los 2 problemas para resolver. Además, es posible realizar la tarea en grupos de 3 personas, pero en tal caso deben realizar **todos** los problemas.

Problema A: Extensiones cuadráticas y Ecuación de Pell (100 puntos)

El objetivo de este problema es utilizar propiedades del anillo de enteros de extensiones cuadráticas reales para estudiar la **ecuación de Pell** dada por

$$x^2 - dy^2 = 1,$$

donde $(x, y) \in \mathbf{Z}^2$ son las incógnitas, y con $d \in \mathbf{N}^{\geq 2}$ es un entero libre de cuadrados que fijaremos en lo que sigue. Para esto, consideramos $\mathbf{K} := \mathbf{Q}(\sqrt{d}) \subseteq \mathbf{R}$ y recordamos que $\mathbf{K}/\mathbf{Q}$ es una extensión galoisiana con grupo de Galois

$$\mathrm{Gal}(\mathbf{K}/\mathbf{Q}) = \langle \sigma : \mathbf{K} \to \mathbf{K},\ a + b\sqrt{d} \mapsto a - b\sqrt{d} \rangle \simeq \mathbf{Z}/2\mathbf{Z}.$$

Recordemos además que en este caso $\mathscr{O}_{\mathbf{K}} = \mathbf{Z} + \mathbf{Z}\omega_d$, donde

$$\omega_d = \begin{cases} \frac{1+\sqrt{d}}{2} & \text{si } d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{en otro caso.} \end{cases}$$

1. Sea $z \in \mathscr{O}_{\mathbf{K}}$. Probar que $z \in \mathscr{O}_{\mathbf{K}}^{\times}$ si y sólo si $\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(z) \in \{-1, 1\}$.

En lo que sigue, consideramos la función

$$\varphi : \mathscr{O}_{\mathbf{K}}^{\times} \longrightarrow \mathbf{R},\ z \longmapsto \log|z|.$$

2. Probar que φ es un morfismo de grupos y determinar $\ker(\varphi)$.

3. Probar que para todo $B \in \mathbf{R}^{>0}$ el conjunto

$$\{z \in \mathscr{O}_{\mathbf{K}}^{\times},\ |\varphi(z)| \leq B\}$$

es **finito**. Deducir que el grupo $\mathrm{Im}(\varphi)$ es cíclico (i.e., está generado por uno de sus elementos).

Indicación: Si $z = a + b\sqrt{d}$ con $a, b \in \frac{1}{2}\mathbf{Z}$, expresar $\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(z)$ como producto y acotar superiormente $|a|$.

Recordemos que si $x \in \mathbf{R}$ entonces su *parte entera* $\lfloor x \rfloor \in \mathbf{Z}$ es el entero más grande que es menor o igual a x, y que $\{x\} := x - \lfloor x \rfloor \in [0, 1[$ es la *parte fraccionaria* de x.

4. Sea $z \in \mathbf{R}$ y sea $N \in \mathbf{N}^{\geq 1}$. Probar que existen enteros j, k tales que $0 \leq j < k \leq N$ de tal suerte que

$$|\{kz\} - \{jz\}| < \frac{1}{N}.$$

Indicación: Considerar la función $\{0, \ldots, N\} \to \mathbf{Z},\ k \mapsto \lfloor N\{kz\} \rfloor$.

5. Probar que para todo $z \in \mathbf{R}$ y todo $N \in \mathbf{N}^{\geq 1}$ existen $p, q \in \mathbf{Z}$ con $0 < q \leq N$ y con $\mathrm{mcd}(p, q) = 1$ de tal suerte que

$$\left| z - \frac{p}{q} \right| < \frac{1}{Nq}.$$

6. Sea $z \in \mathbf{R} \setminus \mathbf{Q}$. Probar que existen infinitos $(p, q) \in \mathbf{Z}^2$ con $q \neq 0$ y con $\mathrm{mcd}(p, q) = 1$ de tal suerte que

$$\left| z - \frac{p}{q} \right| < \frac{1}{q^2}.$$

[1] Factor de retraso: 0.7 por 1 día de retraso, 0.55 por 2 días de retraso, 0.01 por 3 días de retraso.

7. Aplicando la pregunta anterior a $\sqrt{d}$, deducir que si $M := 1 + 2\sqrt{d}$ entonces el conjunto
$$\{(x, y) \in \mathbf{Z}^2,\ |x^2 - dy^2| \leq M \text{ y } \operatorname{mcd}(x, y) = 1\}$$
es **infinito**.

8. Pruebe que existen $m, x_0, y_0 \in \mathbf{Z}$ con $m \neq 0$ y tales que el conjunto de los $(x, y) \in \mathbf{Z}^2$ verificando que $\operatorname{mcd}(x, y) = 1$, $x > 0$, $y > 0$, $x^2 - dy^2 = m$ y tales que $x \equiv x_0 \pmod{m}$, $y \equiv y_0 \pmod{m}$ es **infinito**.

9. Pruebe que existen enteros $x_1, y_1, x_2, y_2 \in \mathbf{Z}$ tales que $\operatorname{mcd}(x_1, y_1) = \operatorname{mcd}(x_2, y_2) = 1$, $x_1 \neq x_2$, $x_1 \neq -x_2$, $x_1 \equiv x_2 \pmod{m}$, $y_1 \equiv y_2 \pmod{m}$, y tales que
$$x_1^2 - dy_1^2 = x_2^2 - dy_2^2 = m.$$

10. Considerando $(x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d})$, pruebe que existe $z \in \mathscr{O}_{\mathbf{K}}^{\times}$ tal que $z \in \mathbf{Z} + \mathbf{Z}\sqrt{d}$ y tal que $z \notin \{-1, 1\}$.

11. Pruebe que la ecuación de Pell $x^2 - dy^2 = 1$ tiene **infinitas** soluciones en $\mathbf{Z}^2$.

12. Pruebe que existe $(x_0, y_0) \in \mathbf{Z}^2$ con $x_0 - dy_0^2 = 1$ tal que, para toda solución $(x, y) \in \mathbf{Z}^2$ de la ecuación de Pell $x^2 - dy^2 = 1$ existe $\varepsilon \in \{-1, 1\}$ y $m \in \mathbf{Z}$ de tal suerte que
$$x + y\sqrt{d} = \varepsilon(x_0 + y_0\sqrt{d})^m.$$

Problema B: Extensiones ciclotómicas (100 puntos)

El objetivo de este problema es describir explícitamente la ramificación en ciertas extensiones ciclotómicas. Para ello, fijamos $p \geq 3$ número primo y consideramos $\zeta := e^{2\pi i/p}$ raíz p-ésima de la unidad. Entonces, $\mathbf{K} := \mathbf{Q}(\zeta)$ es el p-ésimo cuerpo ciclotómico con $\operatorname{Gal}(\mathbf{K}/\mathbf{Q}) \simeq (\mathbf{Z}/p\mathbf{Z})^{\times} \simeq \mathbf{Z}/(p-1)\mathbf{Z}$, y donde $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$ es el polinomio minimal de ζ sobre $\mathbf{Q}$. En todo lo que sigue, consideramos $\xi := \zeta - 1$.

1. Probar que $\mathbf{Z}[\zeta] \subseteq \mathscr{O}_{\mathbf{K}}$, y que $(1, \zeta, \ldots, \zeta^{p-2})$ es una base del $\mathbf{Z}$-módulo $\mathbf{Z}[\zeta]$. Deducir que $\mathbf{Z}[\zeta]$ es estable por la acción de $\operatorname{Gal}(\mathbf{K}/\mathbf{Q})$.

2. Probar que $(1, \xi, \ldots, \xi^{p-2})$ es una base del $\mathbf{Z}$-módulo $\mathbf{Z}[\zeta]$.

   Indicación: Describir la matriz de cambio de base.

3. Calcular $\operatorname{Tr}_{\mathbf{K}/\mathbf{Q}}\left(\sum_{i=0}^{p-2} a_i\zeta^i\right)$ para todo $(a_0, \ldots, a_{p-2}) \in \mathbf{Q}^{p-1}$.

4. Probar que $\mu_{\xi}^{\mathbf{Q}}(X) = \mu_{\zeta}^{\mathbf{Q}}(X + 1)$ y deducir el valor de $\operatorname{N}_{\mathbf{K}/\mathbf{Q}}(\xi)$.

5. Probar que ξ divide a $\zeta^i - 1$ en $\mathbf{Z}[\zeta]$ para todo $i \in \{1, \ldots, p-1\}$. Calcular $\operatorname{N}_{\mathbf{K}/\mathbf{Q}}\left(\dfrac{\zeta^i - 1}{\zeta - 1}\right)$.

6. Probar que para todo $\sigma \in \operatorname{Gal}(\mathbf{K}/\mathbf{Q})$ se tiene que $\sigma(\xi)/\xi \in \mathbf{Z}[\zeta]^{\times}$.

   Indicación: Pruebe que $z \in \mathscr{O}_{\mathbf{K}}$ es una unidad si y sólo si $|\operatorname{N}_{\mathbf{K}/\mathbf{Q}}(z)| = 1$.

7. Probar que existe $u \in \mathbf{Z}[\zeta]^{\times}$ tal que $p = u\xi^{p-1}$. Deducir que si $n \in \mathbf{Z}$ entonces ξ divide a n en $\mathscr{O}_{\mathbf{K}}$ si y sólo si n es un múltiplo de p.

   Indicación: Notar que si ξ divide a n entonces $\operatorname{N}_{\mathbf{K}/\mathbf{Q}}(\xi)$ divide a $\operatorname{N}_{\mathbf{K}/\mathbf{Q}}(n)$.

8. Pruebe (e.g. usando el ítem 2) que la inclusión canónica $\mathbf{Z} \hookrightarrow \mathbf{Z}[\zeta]$ induce un isomorfismo de anillos
$$\mathbf{Z}/p\mathbf{Z} \xrightarrow{\simeq} \mathbf{Z}[\zeta]/\langle\xi\rangle.$$

En lo que sigue, considere $x \in \mathscr{O}_{\mathbf{K}}$ y sea $(a_0, \ldots, a_{p-2}) \in \mathbf{Q}^{p-1}$ tal que $x = \sum_{i=0}^{p-2} a_i\zeta^i$.

9. Calcule $\operatorname{Tr}_{\mathbf{K}/\mathbf{Q}}((1 - \zeta)x)$ y pruebe que $pa_0 \in \mathbf{Z}$. Deduzca (e.g. inductivamente) que $pa_i \in \mathbf{Z}$ para todo $i \in \{1, \ldots, p-2\}$.

10. Pruebe que existe $(b_0, \ldots, b_{p-2}) \in \mathbf{Z}^{p-1}$ de tal suerte que
$$px = \sum_{i=0}^{p-2} b_i\xi^i.$$

11. Pruebe que p divide a b_0 y deduzca que $\mathscr{O}_{\mathbf{K}} = \mathbf{Z}[\zeta]$.

12. Calcule (e.g. utilizando resultados de la Tarea 2) el discriminante $d_{\mathbf{K}} \in \mathbf{N}$, y determine el índice de ramificación $e_{\mathfrak{q}}$ de $\mathfrak{q} := \langle\xi\rangle$ sobre $\mathbf{Z}$. ¿Existen otros primos $\mathfrak{q} \subseteq \mathscr{O}_{\mathbf{K}}$ que ramifiquen sobre $\mathbf{Z}$?