Ley de reciprocidad cuadrática

En esta sección p representa siempre un primo impar

59. Sea $m \neq 2$ tal que hay raíces primitivas módulo m y $4|\phi(m)$. Hallar el número de soluciones $0 < x < m$ de $x^2 + 1 \equiv 0\ (m)$. ¿Cómo se pueden expresar las soluciones en términos de una raíz primitiva?

60. Probar que $x^2 + 1$ tiene 4 raíces en $\mathbb{Z}_{65}$ (no es necesario hallarlas). ¿Cómo puede ser si tiene grado 2?

61. Hallar m tal que $x^2 + 1 \equiv 0\ (m)$ tenga 16 soluciones $0 < x < m$.

62. Demostrar $2^2 \cdot 4^2 \cdot \cdots \cdot (p-1)^2 \equiv 1^2 \cdot 3^2 \cdot \cdots \cdot (p-2)^2 \equiv (-1)^{(p+1)/2}\ \ (p)$.

63. ¿La suma de tres cuadrados consecutivos puede ser un múltiplo de 19?

64. ¿Cuántas soluciones $(x, y) \in \mathbb{Z}_p^2$ tiene $x^2 + y^2 = \overline{0}$?

65. Un primo p tal que $q = 2p+1$ también es primo se dice que es *primo de Germain* (en honor a la matemática del siglo XIX Sophie Germain). Demostrar que si $p > 3$ es un primo de Germain tal que $p \equiv 3\ (4)$, entonces $2^p - 1$ no es primo. *Indicación*: Probar que 2 es residuo cuadrático módulo q y utilizar el criterio de Euler.

66. Calcular $\left(\frac{3}{p}\right)$ en términos de las clases de congruencias de p módulo 12.

67. Describir los primos para los que 13 es residuo cuadrático.

68. Caracterizar los p para los que $x^2 - 2x + 6 \equiv 0\ (p)$ tiene solución.

69. Utilizando las identidades $4(x^4 - x^2 + 1) = (2x^2 - 1)^2 + 3$ y $x^4 - x^2 + 1 = (x^2 - 1)^2 + x^2$, demostrar que si p divide a $n^4 - n^2 + 1$ para algún $n \in \mathbb{Z}$, entonces $p \equiv 1\ (12)$.

70. Demostrar que el número de soluciones $(x, y) \in \mathbb{Z}_p^2$ de $x^2 - y^2 = \overline{a}$ viene dado por $p + \sum_{y=0}^{p-1} \left(\frac{y^2+a}{p}\right)$. Deducir una fórmula sencilla para el valor del sumatorio probando directamente que el número de soluciones es $p-1$ si $p \not| a$ y $2p-1$ si $p|a$.

71. Gauss introdujo la suma $G_N(n) = \sum_{m=1}^{p} e^{2\pi i n m^2/N}$ y demostró el profundo y difícil resultado $G_N(1) = (1+i)(1+i^{-N})\sqrt{N}/2$ para N impar, y dedujo que $G_p(n) = \left(\frac{n}{p}\right)G_p(1)$ si $p \not| n$

a) Comprobar las fórmula de Gauss para $p = 3$ y $n = 1, 2$.

b) Demostrar que si $q \neq p$ es un primo impar, $G_p(q)G_q(p) = G_{pq}(1)$, donde $G_{pq}(1)$. *Indicación*: Si m recorre todos los restos módulo p y n recorre todos los restos módulo q, entonces $qm + pn$ los recorre módulo pq y además $(qm + pn)^2 \equiv q^2m^2 + p^2n^2\ (pq)$.

c) Deducir de la fórmula de Gauss y del apartado anterior la ley de reciprocidad cuadrática. (Nota: Esencialmente esta es la sexta prueba de dicha ley que realizó Gauss, y al parecer la que más esfuerzo le requirió).

72. Calcular los símbolos de Legendre $\left(\frac{175}{257}\right)$, $\left(\frac{15}{103}\right)$, $\left(\frac{136}{137}\right)$.

73. Calcular los símbolos de Jacobi $\left(\frac{3}{35}\right)$, $\left(\frac{403}{803}\right)$, $\left(\frac{133}{169}\right)$.

74. Comprobar que $x^2 \equiv 32\ (33)$ no tiene solución y sin embargo $\left(\frac{32}{33}\right) = 1$.

75. Decidir si 2006 es un residuo cuadrático módulo 365.

76. En la lista anterior se probó que $p \,|\, 4n^2+1 \ \Rightarrow\ p \equiv 1\ (4)$. Rehacer la demostración empleando residuos cuadráticos.

77. Demostrar por inducción $a^{\phi(p^k)/2} \equiv \left(\frac{a}{p}\right)\ (p^k)$ para $k \in \mathbb{Z}^+$.

78. Demostrar que si $p = 2^n + 1$, esto es, si es primo de Fermat, entonces r es una raíz primitiva módulo p si y sólo si r es no residuo módulo p.

79. En uno de los primeros microordenadores personales, el ZX-Spectrum, la n-ésima vez que se accedía a su generador de números aleatorios se obtenía el número $\texttt{RND}(n) = (x_n - 1)/65536$ donde $x_n \equiv 75^n\ (65537)$ con $0 < x_n < 65537$. Sabiendo que $65537 = 2^{16} + 1$ es primo, averiguar el valor de $\texttt{RND}(32768)$. ¿Cuándo se repiten por primera vez los números generados por $\texttt{RND}(n)$? *Indicación*: Utilizar el problema anterior

80. Eisenstein demostró la ley de reciprocidad cuadrática con un ingeniosos argumento a partir de la igualdad $\prod_{n=1}^{(p-1)/2} \operatorname{sen}(2\pi qn/p) = \left(\frac{q}{p}\right) \prod_{n=1}^{(p-1)/2} \operatorname{sen}(2\pi n/p)$ para p y q primos impares distintos. Demostrar esta fórmula empleando el lema de Gauss.

81. Demostrar que si $8|k-1$ entonces $x^2 \equiv k\ \ (2^n)$ tiene solución para todo $n \in \mathbb{Z}^+$.

Enteros algebraicos e ideales

82. Demostrar que $\left((1+\sqrt{5})/2\right)^n + \left((1-\sqrt{5})/2\right)^n \in \mathbb{Z}$ para todo $n \in \mathbb{Z}^+$. *Indicación*: Probar que es racional y entero algebraico.

83. Decidir si $(1 + \sqrt[3]{3})/2$ es un entero algebraico.

84. Sea $n \in \mathbb{Z}^+$. Demostrar que $2\operatorname{sen}(\pi/n)$ y $2\cos(\pi/n)$ son enteros algebraicos.

85. Si $\alpha_1, \alpha_2, \alpha_3$ son las raíces de cierto polinomio $x^3+ax^2+bx+c \in \mathbb{Z}[x]$, probar que $\alpha_1^n+\alpha_2^n+\alpha_3^n \in \mathbb{Z}$ para todo $n \in \mathbb{Z}^+$. Comprobar el resultado para el polinomio x^3-3. *Indicación*: Es conveniente recordar el teorema de los polinomios simétricos o la teoría de Galois del curso de Álgebra II.

86. Demostrar que cada término de la sucesión $x_{n+1} = \sqrt{2+\sqrt{3+x_n}}$ con $x_0 = 0$, es un entero algebraico. ¿Es también $\lim x_n$ un entero algebraico?

87. Comprobar que $(3+2\sqrt{2})^n$, $n \in \mathbb{Z}^+$, son unidades distintas en $\mathbb{Z}[\sqrt{2}]$ y utilizarlas para demostrar que $x^2 - 2y^2 = 7$ tiene infinitas soluciones. Hallar tres con $x, y > 0$.

88. Hallar un polinomio $P \in \mathbb{Z}[x]$ mónico de segundo grado tal que $P(\sec(2\pi/5)) = 0$. *Indicación*: Escribir $\cos(2\pi/5) = (\zeta + \zeta^{-1})/2$ con $\zeta^5 = 1$ y ajustar los coeficientes de P.

89. Se sabe que $\mathbb{Z}[\sqrt{6}]$ es un dominio de factorización única, ¿entonces cómo puede ser que $(4 + \sqrt{6})(4 - \sqrt{6}) = 2 \cdot 5$?

90. Factorizar $3 + 11i$ en $\mathbb{Z}[i]$.

91. Si $\pi/4 < \alpha_1 < \alpha_2 < \pi/2$ son los argumentos de dos primos Gaussianos, demostrar que $\lambda\alpha_1 + \mu\alpha_2 \neq 0$ para $(\lambda, \mu) \in \mathbb{Z}^2 - \{(0,0)\}$. Deducir que $\operatorname{arc\,tg} 2/\operatorname{arc\,tg}(3/2) \notin \mathbb{Q}$. *Indicación*: Se puede

suponer que λ y μ son coprimos $\mu < 0 < \lambda$. Probar que si π_1 y π_2 son los dos primos y $\lambda\alpha_1 + \mu\alpha_2 = 0$, entonces $\pi_1^{\lambda}\pi_2^{-\mu} \in \mathbb{Z}$.

92. Sea I el subanillo formado por los enteros $a + b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ con $2|a+b$. Estudiar si es un ideal y, en su caso, si es principal y si es primo.

93. Sea $I = (3, 1+\sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}]$. Probar que $I = \{a + b\sqrt{-5} \ : \ a \equiv b \ (3)\}$ y deducir que I es un ideal primo.

94. Estudiar si el ideal $(29, 13+\sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}]$ es principal y si es primo.

95. ¿Son todos los subanillos de $\mathbb{Z}[\sqrt{2}]$ ideales? *Indicación*: Considérese el subanillo más sencillo.

96. Hallar todas las unidades del anillo de enteros de $\mathbb{Q}(\sqrt{3})$.

97. Sea $\zeta = e^{2\pi i/n}$ con n impar. Empleando que las raíces n-ésimas de la unidad (distintas de 1) son raíces de $x^{n-1} + x^{n-2} + \cdots + x + 1$ probar que $1 + \zeta$ es una unidad de $\mathbb{Z}[\zeta]$. *Indicación*: Sustituir $x = -1$.

98. Factorizar los ideales (3), (5), (13), (45) y (65) en el anillo de enteros de $\mathbb{Q}(\sqrt{3})$.

99. Repetir el problema anterior pero ahora en el anillo de enteros de $\mathbb{Q}(\sqrt{5})$.

100. Demostrar que si $\zeta = e^{2\pi i/p}$ con p primo, entonces $(1-\zeta)$ es un ideal primo en $\mathbb{Z}[\zeta]$. *Indicación*: Hallar su norma.

101. Sean los ideales $I = (2, 1+\sqrt{-5})$ y $J = (3, 1+\sqrt{-5})$. Probar que $I \cdot J$ es principal dando un generador.

Representación por formas cuadráticas

$\mathcal{H}_d$ es el grupo de clases del anillo de enteros de $\mathbb{Q}(\sqrt{d})$, con d libre de cuadrados

102. Hallar el número de representaciones como suma de dos cuadrados de 29000000.

103. Hallar al menos dos soluciones de $x^2 + y^2 = 9945 = 3^2 \cdot 5 \cdot 13 \cdot 17$ con $0 < x < y$.

104. Demostrar que $r(n) = 4\sum_{(2k+1)|n}\left(\frac{-1}{2k+1}\right)$, donde $r(n)$ es el número de representaciones de n como suma de dos cuadrados. ¿Es $r(n)/4$ multiplicativa?

105. Sea $\widetilde{r}(n) = \left|\{(a,b) \in \mathbb{Z}^2 : a^2 + b^2 = n, \text{ con } a \text{ y } b \text{ primos entre sí (coprimos)}\}\right|$ demostrar que $r(n) = \sum_{d^2|n}\widetilde{r}(n/d^2)$ y deducir $\widetilde{r}(n) = \sum_{d^2|n}\mu(d)r(n/d^2)$.

106. Utilizar las soluciones obvias de $x^2 + 37y^2 = 38$ y $x^2 + 37y^2 = 41$ para hallar una solución de $x^2 + 37y^2 = 1558 = 38 \cdot 41$.

107. Demostrar de manera elemental, sin usar la teoría de ideales, que si $\left(\frac{d}{p}\right) = -1$, con p primo impar y $d < 0$, entonces la ecuación $x^2 - dy^2 = p^{\alpha}$ no tiene solución si α es impar, y si α es par las únicas soluciones son $(\pm p^{\alpha/2}, 0)$.

108. Demostrar que si I es un ideal en el anillo de enteros de $\mathbb{Q}(\sqrt{d})$, $d < -3$, entonces $I^{|\mathcal{H}_d|}$ es principal. Deducir el siguiente resultado similar a uno probado por Jacobi antes

de que naciera la teoría de ideales: Si $d \equiv 1\ (p)$ con p primo impar, $x^2 - dy^2 = 4p^{|\mathcal{H}_d|}$ tiene solución.

109. Suponiendo que $|\mathcal{H}_d| = 1$ y $\left(\frac{d}{p_1}\right) = \left(\frac{d}{p_2}\right) = \cdots = \left(\frac{d}{p_k}\right) = 1$, con $p_j \not| d$ primos impares distintos, hallar una fórmula para el número de divisores de $p_1 p_2 \dots p_k$ en el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ para $d < -3$.

110. Repetir el problema anterior suponiendo además que ninguna de las ecuaciones $x^2 - dy^2 = 4p_j$ tiene solución y que ahora $|\mathcal{H}_d| = 2$.

111. Hallar el número de clases de $\mathbb{Z}[\sqrt{-10}]$, esto es, $|\mathcal{H}_{-10}|$ y calcular el número de soluciones de $x^2 + 10y^2 = 7^n$.

112. Sea $I = (3, 1 + \sqrt{-17})$. Demostrar que $I^2 = (9, 1 + \sqrt{-17})$ no es principal y que $I^4 = (8 - \sqrt{-17})$. Concluir (sin hallarlo) que el número de elementos de $\mathcal{H}_{-17}$ es múltiplo de 4.

113. Factorizar (3) y (41) en $\mathbb{Z}[\sqrt{-5}]$ y hallar el número de soluciones de $x^2 + 5y^2 = 123^n$.

114. Sabiendo que $\mathcal{H}_{-26} \approx \mathbb{Z}_6$ y que el ideal $(5, 2 + \sqrt{-26})$ corresponde a $\overline{1}$, hallar el número de soluciones de $x^2 + 26y^2 = 5^{10}$.

115. Hallar, en general, el número de soluciones de $x^2 + 26y^2 = 5^n$ en función de n.

116. Comprobar que si $2x^2 + 2xy + 3y^2 = n$ equivale a $(3y + x)^2 + 5x^2 = 3n$. Utilizar este hecho para demostrar que si $x^2 + 5y^2 = p$ tiene solución entonces $2x^2 + 2xy + 3y^2 = p$ no la tiene.