ALDALDA H

Apellidos y nombre

AMPLIACIÓN DE MATEMÁTICAS 2019-2020
TRABAJO PRÁCTICO 8: Ecuaciones Diofánticas Lineales y Anillos Cociente

Una ecuación diofántica es aquella que se plantea sólo para encontrar las soluciones enteras. Considera la ecuación

$$ax + by = c,$$

donde x e y son las incógnitas y $a, b, c \in \mathbb{Z}$. Una ecuación así tiene solución si, y sólo si, se tiene que $d = \text{mcd}(a, b)$ divide a c (¿por qué?). De ese modo, si $d = ua + vb$ es una identidad de Bezout, es claro que $(x = uc/d, y = vc/d)$ es una solución de la ecuación. Además, si (x_0, y_0) es una solución entera, entonces **todas las demás soluciones enteras** son de forma $(x_0 - k\beta, y_0 + k\alpha)$ con $k \in \mathbb{Z}$ y donde $\alpha = a/d$ y $\beta = b/d$. Halla todas **las soluciones enteras** de las ecuaciones:

$$48x + 30y = 12 \iff 8x + 5y = 2$$

$\exists$ soluciones enteras dado que $\text{mcd}(8,5) = 1 \mid 2$.

- Algoritmo de Euclides: $8 = 5\cdot 1 + 3;\ 5 = 3\cdot 1 + 2;\ 3 = 2\cdot 1 + \boxed{1}$
- Identidad de Bezout: $1 = 3 - 2\cdot 1 = 3 - (5 - 3\cdot 1)\cdot 1 = 3\cdot 2 - 5\cdot 1 = (8 - 5\cdot 1)\cdot 2 - 5\cdot 1 = 8\cdot 2 + 5\cdot(-3) \Rightarrow \boxed{2 = 8\cdot \boxed{4} + 5\cdot \boxed{(-6)}}$

$$25x + 40y = 24$$

$\nexists$ soluciones enteras, pues $\text{mcd}(25, 40) = 5 \nmid 24$.

Resuelve la congruencia lineal $3x \equiv 4$ (mód 23). [Halla el inverso de 3 en $\mathbb{Z}_{23}$]

identidad Bezout: $3\cdot\boxed{8} + 23(-1) = 1$

$\Rightarrow \{x \equiv 9 \text{ (mód. } 23)\}$

resto de soluciones $(4 - 5\lambda, -6 + 8\lambda)$ con $\lambda \in \mathbb{Z}$

Determina los mínimos representantes positivos en $\mathbb{Z}_{1000000}$ de 276828181638 y 726297746268598.

181638 268598

Halla los inversos de 7 y 8 en $\mathbb{Z}_{15}$. ¿Qué pasa con 3 y 5?

→ $7\cdot 2 = 14 \iff 7\cdot(-2) = -14 \equiv 1 \pmod{15} \rightsquigarrow \{7^{-1} \equiv 13 \text{ (mod. } 15)\}$

→ $8\cdot 2 = 16 \iff 8\cdot 2 \equiv 1 \text{ (mod. } 16) \rightsquigarrow \{8^{-1} \equiv 2 \text{ (mod. } 15)\}$

→ $3\cdot 5 = 15 \equiv 0 \text{ (mod. } 15) \rightarrow$ son divisores de cero en $\mathbb{Z}_{15}$

Halla todos los elementos de $\mathbb{Z}_{45}$ que tienen inverso (es decir, halla $\mathbb{Z}_{45}^*$). Lo mismo para $\mathbb{Z}_{43}$.

$* \mathbb{Z}_{45}^* = \{a \in \mathbb{Z}_{45} \mid \text{mcd}(45, a) = 1\} = \{1, 2, 4, 7, 8, 11, 13, 14, 16, 17, 19, 22, 23, 26, 28, 29, 31, 32, 34, 37, 38, 41, 43, 44\}$

$(45 = 5\cdot 3^2)$

$\varphi(45) = \varphi(5)\cdot\varphi(3^2) = 4\cdot 6 = 24$

↳ {no múltiplos de 5 (acabados en 0, 5); no múltiplos de 3 (suma de dígitos múltiplo de 3); no múltiplos de 9 (suma de dígitos múltiplo de 9)}

$* \mathbb{Z}_{43}^* = \mathbb{Z}_{43} - \{0\}$ (43 es primo)

• 3 primo: NO $3 \mid 27 = (1+\sqrt{-26})(1-\sqrt{26})$ en A $\not\Rightarrow$ $3 \mid (1 \pm \sqrt{-26})$ en A

Esto es imposible en A

Prueba que $A = \mathbb{Z}[\sqrt{-26}] = \{a + b\sqrt{-26} \mid a, b \in \mathbb{Z}\}$ es un subanillo de $\mathbb{C}$. ¿Es ideal? Demuestra que 3 es irreducible en A. ¿Es 3 primo en A? (**Indicación**: Multiplica $1+\sqrt{-26}$ por su conjugado).

• Subanillo: $1 = 1 + 0\cdot\sqrt{-26} \in A$ (unitario); $0 = 0 + 0\cdot\sqrt{-26} \in A$ $\Big\}$ $A \neq \emptyset$

$x, y \in A$ $(x = a_x + b_x\sqrt{-26}\,;\ y = a_y + b_y\sqrt{-26})$ SI

(cerrado diferencia) $x - y = (a_x - a_y) + (b_x - b_y)\sqrt{-26} \in A$

(cerrado producto) $x \cdot y = (a_x a_y + 26 b_x b_y) + (a_x b_y + a_y b_x)\sqrt{-26} \in A$

• Ideal: NO $i \in \mathbb{C}$, $1 \in A$ $\Big\}$ $\Rightarrow i \cdot 1 \notin A$ (no se cumple la condición de ideal)

• 3 irreducible: $3 = (a + b\sqrt{-26})\cdot(c + d\sqrt{-26}) \Leftrightarrow \begin{cases} 3 = ac + 26bd \\ 0 = ad + bc \end{cases}$ $\not\Rightarrow$ SI

(no unidades (i.e. $\neq \pm 1$))

¿Es el anillo cociente $\mathbb{Z}_2[x]/(x^3 + x + 1)$ un cuerpo? Halla el inverso de $x^2 + x$ en caso afirmativo.

$x^3 + x + 1 \mid x^2 + x$ polinomio irreducible en $\mathbb{Z}_3[x]$

$-x^3 - x^2$ dado que tiene grado 3 en un cuerpo sin raíces

$x + 1$

$/\ x^2 + x + 1$

$-x^2 - x$

$/\ /\ 1$ → máximo común divisor

$\bar{0}^3 + \bar{0} + \bar{1} \neq \bar{0}$; $\bar{1}^3 + \bar{1} + \bar{1} \neq \bar{0}$

$\mathbb{Z}_2[x]/(x^3 + x + 1)$ es un cuerpo.

$(x^2 + x)^{-1} \equiv (x+1) \pmod{f}$

Identidad de Bezout: $(x^3 + x + 1) + (x+1)(x^2 + x) = 1$

Factoriza como producto de irreducibles $f(x) = 6x^2 - 12$ en $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ y $\mathbb{Z}_7[x]$.

• $f(x) = 2 \cdot 3(x^2 - 2)$ en $\mathbb{Z}[x]$ (irreducibles; irreducible (no raíces en $\mathbb{Z}$))

• $f(x) = 6(x - \sqrt{2})(x + \sqrt{2})$ en $\mathbb{R}[x]$ (unidad; polinomios de grado 1 irreducibles)

• $f(x) = 6x^2 - 12$ irreducible en $\mathbb{Q}[x]$ (no raíces en $\mathbb{Q}$)

• $f(x) \equiv (2 - x^2) \pmod{7} = (x-3)(x-4)$ polinomios de grado 1 irreducibles

puede verse también como todos los polinomios de $\mathbb{Z}_3[x]$ salvo los reducibles → aquellos que tienen raíces en $\mathbb{Z}_3$

Halla los polinomios irreducibles (luego primos) de grado menor o igual que 3 en $\mathbb{Z}_3[x]$.

$\{a_0 + a_1 x + a_2 x^2 + a_3 x^3 \mid a_i \in \mathbb{Z}_3\} \equiv \mathbb{Z}_3[x]$

↑ irreducibles $\Leftrightarrow$ no tienen raíces en $\mathbb{Z}_3[x]$. Estos son: 14

grado 1: x; $x + \bar{1}$; $x + \bar{2}$

grado 2: $x^2 + \bar{1}$; $x^2 + x + \bar{2}$; $x^2 + \bar{2}x + \bar{2}$

grado 3: $x^3 + \bar{2}x + \bar{1}$; $x^3 + \bar{2}x^2 + \bar{1}$; $x^3 + \bar{2}x + \bar{2}$; $x^3 + x^2 + \bar{2}$; $x^3 + x^2 + x + \bar{2}$; $x^3 + x^2 + 2x + \bar{1}$; $x^3 + \bar{2}x^2 + \bar{2}x + \bar{2}$; $x^3 + \bar{2}x^2 + x + \bar{1}$