ADADLH

Apellidos y nombre

AMPLIACIÓN DE MATEMÁTICAS 2019-2020
TRABAJO PRÁCTICO 7: Algoritmo Extendido de Euclides.

Aplicamos el Algoritmo de Euclides realizando las sucesivas divisiones para hallar el máximo común divisor

Utiliza el **Algoritmo de Euclides** para hallar el máximo común divisor de 1527 y 1894. Deducir de ello una **identidad de Bezout**. A este procedimiento se le conoce usualmente por **Algoritmo Extendido de Euclides**.

$1894 = 1527 \cdot 1 + 367$

$1527 = 367 \cdot 4 + 59$

$367 = 59 \cdot 6 + 13$

$59 = 13 \cdot 4 + 7$

$13 = 7 \cdot 1 + 6$

$7 = 6 \cdot 1 + \boxed{1}$

$\text{mcd}(1894, 1527) = 1$

$1 = 7 - 6 \cdot 1 = 7 - (13 - 7 \cdot 1) \cdot 1 =$
$= 7 \cdot 2 - 13 \cdot 1 = (59 - 13 \cdot 4) \cdot 2 - 13 \cdot 1 =$
$= 59 \cdot 2 - 13 \cdot 9 = 59 \cdot 2 - (367 - 59 \cdot 6) \cdot 9 =$
$= 59 \cdot 56 - 367 \cdot 9 = (1527 - 367 \cdot 4) \cdot 56 -$
$- 367 \cdot 9 = 1527 \cdot 56 - 367 \cdot 233 =$
$= 1527 \cdot 56 - (1894 - 1527 \cdot 1) \cdot 233 =$
$= 1527 \cdot 289 + 1894(-233)$

de abajo a arriba obtenemos una identidad de Bezout

$$\boxed{1 = 1894 \cdot (-233) + 1527 \cdot 289}$$

El perverso Gárgamel tiene una pócima casi preparada que le permitirá capturar a todos los pitufos. Sólo le falta agregar exactamente 93ml de esencia de pitufresas. Su problema es que el regalito sorpresa que pitufo bromista le dejó antes de escapar la última vez explotó y ahora sólo tiene dos calderos (en uno de los cuales está preparando la pócima), el frasco de 2 litros de esencia de pitufresas y dos tubos de ensayo, uno de 9ml y otro de 12ml. ¿Conseguirá Gárgamel, a base de meter y quitar tubos de ensayo llenos de esencia de pitufresas al caldero vacío, los 93ml exactos que necesita? ¿Cómo? Justifica tu respuesta.

Sí, pues $\text{mcd}(12, 9) = 3 \mid 93$

↳ Los pasos a seguir son los siguientes:

1) Encontrar una identidad de Bezout:

$12 = 9 \cdot 1 + \boxed{3} \rightsquigarrow 3 = 12 - 9 \cdot 1$.

2) Multiplicar esta por $93/3 = 31$:

$$\boxed{93 = 12 \cdot (31) + 9(-31)}$$

↳ A saber; metemos en el tubo de ensayo de 12ml la esencia, quitamos 9ml pasándolos al otro tubo, y metemos los 3ml restantes al caldero vacío, repitiendo este procedimiento 31 veces.

Prueba que, para todo entero n dado, los números $n^3 - 7n + 7$ y $n - 1$ son coprimos.

Basta calcular $mcd(n^3-7n+7, n-1)$, $\forall n \in \mathbb{Z}$; entendiendo estos dos como polinomios en $\mathbb{Z}$ y comprobando que este es 1. Para ello, aplicamos el Algoritmo Extendido de Euclides

$$\begin{array}{l|l} n^3 \quad -7n+7 & n-1 \\ \cline{2-2} -n^3+n^2 & n^2+n-6 \\ \hline \quad n^2-7n+7 & \\ \quad -n^2+n & \\ \hline \qquad -6n+7 & \\ \qquad 6n-6 & \\ \hline \qquad \boxed{1} & \end{array}$$

q.d.

Calcula, empleando el **Algoritmo Extendido de Euclides**, el máximo común divisor y una identidad de Bezout para los polinomios en $\mathbb{Z}_5[x]$ dados por

$$f(x) = x^5 + 3x^3 + 4x + 2 \quad \textbf{y} \quad g(x) = x^4 + 2x^3 + 1.$$

1)
$$\begin{array}{l|l} x^5 \quad +3x^3 \quad +4x+2 & x^4+2x^3+1 \\ \cline{2-2} -x^5-2x^4 \qquad\quad -x & x+3 \\ \hline \quad 3x^4+3x^3 \quad +3x+2 & \\ \quad -3x^4-6x^3 \qquad -3 & \\ \hline \qquad 2x^3+3x+4 & \end{array}$$

2)
$$\begin{array}{l|l} x^4+2x^3 \qquad\quad +1 & 2x^3+3x+4 \\ \cline{2-2} -6x^4 \quad -9x^2-12x & 3x+1 \\ \hline \quad 2x^3 \quad x^2+3x+1 & \\ \quad -2x^3 \qquad -3x-4 & \\ \hline \qquad x^2 \quad +2 & \end{array}$$

3)
$$\begin{array}{l|l} 2x^3 \qquad +3x+4 & x^2+2 \\ \cline{2-2} -2x^3 \qquad -4x & 2x \\ \hline \qquad\quad +4x+4 & \end{array}$$

4)
$$\begin{array}{l|l} x^2 \qquad +2 & 4x+4 \\ \cline{2-2} -16x^2-16x & 4x+1 \\ \hline \quad 4x+2 & \\ \quad -4x-4 & \\ \hline \qquad \boxed{3} & \end{array}$$

Luego: $mcd(f(x), g(x)) = 3 \sim 1$ en $\mathbb{Z}_5[x]$

$$\boxed{1 = f(x)\cdot(2x^3+2x^2+2x+1) + g(x)\cdot(3x^4+2x^3+3x^2+2x+4)}$$

Identidad de Bezout: $1 = 3\cdot 2 = [(x^2+2) - (4x+4)(4x+1)]\cdot 2 =$

$= (x^2+2)\cdot 2 + (4x+4)\cdot(2x+3) = (x^2+2)\cdot 2 + [(2x^3+3x+4) - 2x(x^2+2)](2x+3) =$

$= (x^2+2)(x^2+4x+2) + (2x^3+3x+4)\cdot(2x+3) = [(x^4+2x^3+1) - (2x^3+3x+4)(3x+1)]\cdot$

$\cdot(x^2+4x+2) + (2x^3+3x+4)\cdot(2x+3) = g(x)\cdot(x^2+4x+2) + (2x^3+3x+4)\cdot$

$\cdot(2x^3+2x^2+2x+1) = g(x)\cdot(x^2+4x+2) + [(x^5+3x^3+4x+2) - (x^4+2x^3+1)(x+3)]\cdot$

$\cdot(2x^3+2x^2+2x+1) = f(x)\cdot(2x^3+2x^2+2x+1) + g(x)\cdot(3x^4+2x^3+3x^2+2x+4)]$