AM PRÁCTICA-11

Nombre y apellidos.....

1.- Calcula el máximo común divisor (mónico) de los polinomios $f(x) = x^4 + x^3 + x^2 + x$ y $g(x) = x^2 + x - 1$ de $\mathbb{Z}_3[x]$. Exprésalo en la forma $a(x)f(x) + b(x)g(x) = m.c.d.(f, g)$.

USAMOS EL ALGORITMO DE EUCLIDES

$x^4 + x^3 + x^2 + x \;\big|\; x^2 + x - 1$

$-x^4 - x^3 + x^2 \qquad x^2 + 2$

$2x^2 + x$

$-2x - 2x + 2$

$2x + 2$

$x^2 + x - 1 \;\big|\; 2x + 2$

$-x^2 - x \qquad 2x$

2

	r_i	q_i	α_i	β_i
	$x^4+x^3+x^2+x$	x^2+x-1	$2x+2$	2
		x^2+2	$2x$	$x+1$
	1	0	1	x
	0	1	$2x^2+1$	$1-(2x)(2x^2+1)$ $= 2x^3+x+1$

LUEGO $m.c.d(f, g) = 2$ Y LA EXPRESIÓN BUSCADA ES

$2 = x(x^4+x^3+x^2+x) + (2x^3+x+1)(x^2+x-1) =$ $x^5+x^4+x^3+x^2+$

$+2x^5+x^3+x^2+2x^4+x^2+x-x^3-x-1 = -1 = 2.$

↓ COMPROBACIÓN

2.- Calcula el mínimo común múltiplo entre $P(x) = x^5 + x^4 + x$ y $Q(x) = x^3 + x^2 + 1$ en $\mathbb{Z}_2[x]$, y encuentra los polinomios $R(x)$ y $S(x) \in \mathbb{Z}_2[x]$ que satisfacen la ecuación:

$$R(x)P(x) + S(x)Q(x) = x.$$

1º) PRIMERO CALCULAMOS $m.c.d(P, Q)$, USANDO EL ALGORITMO DE EUCLIDES

$x^5 + x^4 + x \;\big|\; x^3 + x^2 + 1$

$-x^5 - x^3 - x^2 \qquad x^2$

$x^2 + x$

$x^3 + x^2 + 1 \;\big|\; x^2 + x$

$-x^3 - x^2 \qquad x$

1

LUEGO $1 = m.c.d(P, Q)$, ANALIZAMOS

	r	P	Q	x^3+x	1
	q		x^2	x	
	α	1	0	1	x
	β	0	1	x^2	$1+x^3$

LA EXPRESIÓN DE BÉZOUT NOS QUEDA

$$1 = x\,P(x) + (1+x^3)\,Q(x). \quad (*)$$

2º) COMO P, Q NO TIENEN FACTORES COMUNES

$$m.c.m(P, Q) = P \cdot Q.$$

3º) MULTIPLICANDO LA IGUALDAD $(*)$ POR x TENEMOS QUE

$$x^2 P(x) + (x + x^4)Q(x) = x \implies \boxed{R(x) = x^2} \text{ Y } \boxed{S(x) = x + x^4}$$

continuación.....

3.- Sea $\mathbb{F}$ un cuerpo y $m, n, p \in \mathbb{N}$. Prueba que son equivalentes:

- $m|n$
- $p^m - 1|p^n - 1$
- $x^{p^m-1} - 1|x^{p^n-1} - 1$.

Indicación: Divide $x^n - 1$ entre $x^m - 1$.

SEA $n = km + r$ $\quad 0 \le r < m$.

DIVIDIENDO $p^n - 1 \;\lfloor p^m - 1 \iff$

$$\begin{array}{l|l} p^{km+r} - 1 & p^m - 1 \\ -p^{km+r} + p^{(k-1)m+r} & p^{(k-1)m+r} + p^{(k-2)m+r} + \dots + p^r \\ \hline p^{(k-1)m+r} - 1 & \\ -p^{(k-1)m+r} + p^{(k-2)m+r} & \\ \hline p^{(k-2)m+r} - 1 & \\ \quad \ddots & \\ p^{m+r} - 1 & \\ -p^{m+r} + p^r & \\ \hline p^r - 1 & \end{array}$$

(1) SI $r = 0$ ($\iff m|n$) $\Rightarrow p^m - 1 | p^n - 1$

SI $r \neq 0$ ($\iff m \nmid n$) $\Rightarrow p^m - 1 \nmid p^n - 1$

— o —

SEA $n = km + r$ $\quad 0 \le r < m$

$$\begin{array}{l|l} x^{\overbrace{km+r}^{n}} - 1 & x^m - 1 \\ -x^{km+r} + x^{(k-1)m+r} & x^{(k-1)m+r} + x^{(k-2)m+r} + \dots + x^r \\ \hline x^{(k-1)m+r} - 1 & \\ -x^{(k-1)m+r} + x^{(k-2)m+r} & \\ \hline x^{(k-2)m+r} - 1 & \\ \quad \ddots & \\ x^{m+r} - 1 & \\ -x^{m+r} + x^r & \\ \hline x^r - 1 & \end{array}$$

(2) SI $r = 0$ ($\iff m|n$) $\Rightarrow x^m - 1 | x^n - 1$

SI $r \neq 0$ ($\iff m \nmid n$) $\Rightarrow x^m - 1 \nmid x^n - 1$

— • —

EN EL CASO PARTICULAR DE QUE $m' = p^m - 1$ Y $n' = p^n - 1$

$$m | n \underset{(1)}{\iff} p^m - 1 \,|\, p^n - 1 \underset{\substack{(2)\\ m'|n'}}{\iff} x^{m'} - 1 \,|\, x^{n'} - 1 \iff x^{p^m - 1} - 1 \,|\, x^{p^n - 1} - 1.$$