AM

HOJA 5ª

PROBLEMA 1º) Sean los números 2597 y 1369

Para calcular su máximo común divisor, usamos el algoritmo de Euclides:

$$\begin{array}{r|l} 2597 & 1369 \\ \hline 1228 & 1 \end{array} \qquad \begin{array}{r|l} 1369 & 1228 \\ \hline 0141 & 1 \end{array} \qquad \begin{array}{r|l} 1228 & 141 \\ \hline 100 & 8 \end{array}$$

$$\begin{array}{r|l} 141 & 100 \\ \hline 41 & 1 \end{array} \qquad \begin{array}{r|l} 100 & 41 \\ \hline 18 & 2 \end{array} \qquad \begin{array}{r|l} 41 & 18 \\ \hline 05 & 2 \end{array} \qquad \begin{array}{r|l} 18 & 5 \\ \hline 3 & 3 \end{array} \qquad \begin{array}{r|l} 5 & 3 \\ \hline 2 & 1 \end{array}$$

$$\begin{array}{r|l} 3 & 2 \\ \hline 1 & 1 \end{array} \qquad \begin{array}{r|l} 2 & 1 \\ \hline 0 & 2 \end{array}$$

Luego $m.c.d(2597, 1369) = 1$

Por lo tanto $m.c.m(2595, 1369) = \dfrac{2595 \times 1369}{1}$

Para calcular la identidad de Bezout formada hacemos la tabla

j	r	q	α	β
0	2597		1	0
1	1369		0	1
2	1228	1	1	−1
3	141	1	−1	2
4	100	8	9	−17
5	41	1	−10	19
6	18	2	29	−55
7	5	2	−68	129
8	3	3	233	−442
9	2	1	−301	571
10	1	1	534	−1013
	0	2		

con $r_j = r_{j-2} - q_j r_{j-1}$

$\alpha_j = \alpha_{j-2} - q_j \alpha_{j-1}$

$\beta_j = \beta_{j-2} - q_j \beta_{j-1}$

$j \geq 2$

Así $534 \times 2597 + (-1013)(1369) = 1$

AM

HOJA 5:

PROBLEMA 4: SI $mcd(a,b) = mcd(a,c) = 1$

ES DECIR a y b SON PRIMOS ENTRE SI

y a y c " " " "

ENTONCES

a) $mcd(ab, a) = a$ LUEGO NO TIENE POR QUE SER $1 = mcd(ab, a)$

b) $mcd(b,c) = 1$ NO TIENE POR QUE; SEA $a = 7$ $b = 3$ y $c = 9$

$mcd(7,3) = mcd(7,9) = 1$ y $mcd(3,9) = 3$.

c) $mcd(bc, a) = 1$ SI ES CIERTO; SI $d = mcd(bc, a) > 1$

$\exists\, p$ PRIMO CON $p \mid d$ y ASI $p \mid a$ y $p \mid bc$

PERO ENTONCES $p \mid b$ ó $p \mid c$ y ASI

O BIEN $mcd(a,b) \geq p > 1$ ó $mcd(a,c) \geq p > 1$

d) $mcd(ab, c) = 1$ NO ES CIERTO, SIRVE EL MISMO EJEMPLO QUE EN b $mcd(7 \times 3, 9) = 3 \neq 1$.

PROBLEMA 5: $a \equiv b \text{ mód } n \iff a - b = k_1 n = k_1 p_1^{\nu_1} \cdots p_n^{\nu_n}$

$a \equiv b \text{ mód } m \iff a - b = k_2 m = k_2 p_1^{\mu_1} \cdots p_n^{\mu_n}$

PARA CIERTOS $k_1, k_2 \in \mathbb{Z}$ y DONDE HEMOS ESCRITO LA FACTORIZACIÓN DE n y m

$$m.c.m[n, m] = p_1^{\max(\nu_1, \mu_1)} \cdots p_n^{\max(\nu_n, \mu_n)}.$$

LUEGO $\forall j = 1, 2 \ldots n$ $p_j^{\max(\nu_j, \mu_j)} \mid a - b$ y

ASI $m.c.m[n,m] \mid a - b$ LUEGO

$$a \equiv b \text{ mód } m.c.m[n,m].$$

PROBLEMA 7: $[7] \in \mathbb{Z}_{16}$ $mcd(7,16) = 1$, LUEGO POR EL EJERCICIO 6 EXISTE $[7]^{-1}$

ALGORITMO DE EUCLIDES

$16 = 7 \cdot 2 + 2$ $7 = 2 \cdot 3 + 1$ $2 = 1 \cdot 2 + 0$

r	q	α	β
16		1	0
7		0	1
2	2	1	-2
1	3	-3	7

$-3 \times 16 + 7 \times 7 = 1$ LUEGO

$[7]^{-1} = [7]$.

AM

HOJA 3:

PROBLEMA 9:] SEA $\mathbb{Z}_{15}$; LOS ELEMENTOS DE $\mathbb{Z}_{15}$ QUE TIENEN INVERSO RESPECTO DEL PRODUCTO SON AQUELLOS $n \in \{2,3 .. 14\}$ CON $m.c.d(n,15)=1$ SEGÚN EL PROBLEMA

COMO $15 = 3 \times 5$, LOS QUE TIENEN INVERSO SON

$2, 4, 7, 8, 11, 13, y\ 14.$

PROBLEMA 10:]

b) $5X \equiv 17 \pmod{15} \iff 5X \equiv 2 \mod 15$.

NO EXISTE $[5]^{-1} \mod 15$ YA QUE $5 = mcd(5,15)$ (SEGÚN EL PROBLEMA 6:). LUEGO PODEMOS HACER LA TABLA DE $(\mathbb{Z}_{15}, \times)$ Y VER SI EXISTE X TAL QUE $5X \equiv 2 \mod 15$ O BIEN:

$\forall n \in \mathbb{Z}$ $5 \times n$ TIENE SU ÚLTIMO CIFRA 0 Ó 5

$Y \forall m \in \mathbb{Z}$ $15 \times m$ " " " " 0 Ó 5

LUEGO SALVO 2 Y $m=0$ NO SE VERIFICA

$$5 \times n = m \times 15 + 2$$

ESTA ECUACIÓN EN CONGRUENCIAS NO TIENE SOLUCIÓN.

f) $211X \equiv 658 \pmod{900}$

COMO $900 = 3^2 \times 10^2 = 3^2 \times 2^2 \times 5^2$ Y 3, 2 Y 5 NO DIVIDEN A 211 SE SIGUE QUE $m.c.d(900, 211) = 1$ Y ASÍ EXISTE $[211]^{-1}$ Y LA SOLUCIÓN BUSCADA ES

$x = 658 \times [211]^{-1}$

900 | 211
056 4

211 | 56
43 3

56 | 43
13 1

43 | 13
04 3

13 | 4
1 3

4 | 1
0 4

i	r	q	α	β
0	900		1	0
1	211		0	1
2	56	4	1	-4
3	43	3	-3	13
4	13	1	4	-17
5	4	3	-15	64
6	1	3	49	-209
	0	4		

ASÍ

$49 \times 900 - 209 \times 211 = 1$

ASÍ $[211]^{-1} = [-209] =$

$= [691]$

LUEGO $X = [658] \times [691] =$

$= 454678 \equiv 178 \mod 900.$

AM

HOJA 5:

PROBLEMA 10:] c) $34x \equiv 60 \pmod{98}$.

Como $mcd(34,98) = 2$ no existe $[34]^{-1}_{98}$

Así no entrará no sabemos despejar x.

Dos caminos:

$34x = 2\times 17 \times x \equiv 60 \mod 98$ como sí existe

$[17]^{-1}_{98}$, realmente buscamos

$$2x \equiv 60\cdot[17]^{-1} \mod 98$$

$\begin{array}{r|l} 98 & 17 \\ \hline 13 & 5 \end{array}$ $\quad$ $\begin{array}{r|l} 13 & 4 \\ \hline 1 & 3 \end{array}$

$\begin{array}{r|l} 17 & 13 \\ \hline 4 & 1 \end{array}$ $\quad$ $\begin{array}{r|l} 4 & 1 \\ \hline 0 & 4 \end{array}$

i	r	q	α	β
	98		1	0
	17		0	1
	13	5	1	-5
	4	1	-1	6
	1	3	4	-23
	0	4		

Así $4\times 98 - (23\times 17) = 1$

Así $[17]^{-1} = [-23] =$
$= [75]$

Así $2x \equiv [60]\times[75] = [4500]_{98} \equiv [90]_{98} = 2\times 45 \equiv \mod 98$

Luego $x \equiv 45 \mod 98$.

Por otra parte,

$$34x \equiv 60 \mod 98 \iff \exists m \in \mathbb{Z}$$

con $34x = m98 + 60$

$\iff 17x = m49 + 30$

$\iff 17x \equiv 30 \mod 49$.

Como $mcd(17,49) = 1$ existe $[17]^{-1}_{49}$ y

Así $x \equiv 30 \times [17]^{-1}_{49} \mod 49$

$\begin{array}{r|l} 49 & 17 \\ \hline 15 & 2 \end{array}$ $\quad$ $\begin{array}{r|l} 15 & 2 \\ \hline 1 & 7 \end{array}$

$\begin{array}{r|l} 17 & 15 \\ \hline 2 & 1 \end{array}$ $\quad$ $\begin{array}{r|l} 2 & 1 \\ \hline 0 & 2 \end{array}$

i	r	q	α	β
	49		1	0
	17		0	1
	15	2	1	-2
	2	1	-1	3
	1	7	8	-23
	0	2		

Así $8\times 49 + (-23)\times 17 = 1$

Así $[17]^{-1}_{49} = [-23] = [26]$

Luego $x \equiv 30\times 26 \mod 49$

$\iff x \equiv 45 \mod 49$

Observemos que $45 \mod 49 \iff 45 \mod 98$.

AM

HOJA 5:

PROBLEMA 11: a) El sistema de congruencias

$x \equiv 2 \mod 4$

$x \equiv 4 \mod 5$ Dado que $1 = mcd(4,5)$, el teorema chino del resto no dice que el sistema tiene solución y nos dice como calcularla. Usando el lema de Bezout.

$$1 = 5 \times 1 + (-1)4$$

Así $(4-2) = (4-2)5 + (4-2)(-1)4$ reordenando

$$\underbrace{(4-2)5 + 4}_{x} = \underbrace{-(4-2)4 + 2}_{x} \qquad x = -6$$

o también todo $y = -6 + k20$ cad. $y \equiv x \mod (mcm(4,5))$

para $k = 1$, $y = 14$ también sería una solución posible

d) $x \equiv 3 \mod 17$

$x \equiv 4 \mod 18 = 3 \times 6$

$x \equiv 5 \mod 19$

Como 17, 18 y 19 son primos entre sí, el teorema chino del resto nos dice que el sistema tiene solución

Calculando identidad de Bezout.

r	q	α	β
18×19 = 342		1	0
17		0	1
2	20	1	−20
1	8	−8	161

$342 \div 17$: 02, 20; $17 \div 2$: 1, 8

Así $-8(18 \times 19) + 161 \times 17 = 1$

Así $-8(18 \times 19) \equiv 1 \mod 17$

r	q	α	β
17×19 = 323		1	0
18		0	1
17	17	1	−17
1	1	−1	18

$323 \div 18$: 143, 17, 17; $18 \div 17$: 1, 1

Así $-1(17 \times 19) + 18 \times 18 = 1$

y $-(17 \times 19) \equiv 1 \mod 18$

(*) del mismo modo se ve que

$-9(17 \times 18) \equiv 1 \mod 19$

(*)

Por tanto el x buscado es

$$x = 3((-8 \times 342) - 323 - (9 \times 306)).$$

AM

HOJA 5ª

PROBLEMA 12:) a) $18x + 5y = 48$ ¿$x, y \in \mathbb{N}-\{0\}$?

$\iff 5y = 48 - 18x = 12 + 2\times 18 - 18x = 12 + 18(2-x)$ (*)

ASÍ BUSCAMOS $5y \equiv 12 \mod 18$

COMO m.c.d $(5,18) = 1$ EXISTE $5^{-1} \mod 18$

(HACIENDO LA TABLA DE $\mathbb{Z}_{18}$: $5^{-1} \equiv 11 \mod 18$

$5\times 11 = 55$ y $3\times 18 = 54$)

ASÍ $y \equiv 12\times 11 \equiv 132 \mod 18$ LUEGO

$132 \underline{|18}$
$\underline{06}\ 7$

$y \equiv 6 \mod 18$

ASÍ $y = 6 + k18$ $k = 0, 1, \dots$

POR OTRO LADO $5y = 12 + 18(2-x)$ *)

$x > 0$; LUEGO O BIEN $x = 1$
O BIEN $x = 2$

$x = 1 \Rightarrow 18 + 12 = 30 = y5$ LUEGO $y \equiv 6$ COMPATIBLE CON $y = 6 + k18$

$x = 2 \Rightarrow 12 = y\cdot 5$ NO HAY SOLUCIÓN ENTERA.

LUEGO LA ÚNICA SOLUCIÓN ES $x = 1$ E $y = 6$.

PROBLEMA 13:) ¿$0 < c < 20$? TAL QUE $84x + 990y = c$ (*)

CON x, y ENTEROS

(*) $\iff 84x = c - 990y \iff 84x \equiv c \mod 990$

C NO PUEDE SER IMPAR YA QUE 84 Y 990 SON PARES

ASÍ SI C ES PAR

(*) $\iff 42x + 495y = c'$ c' TIENE QUE SER MÚLTIPLO DE 3 POR SERLO 42 Y 495

$:3$ $\iff 14x + 165y = c''$ CON $c = 12$ ó 18 y $c'' = 2$ ó 3.

m.c.d. $(14, 165) = 1$ LUEGO $x \equiv c'' \times 14^{-1} \mod 165$

POR EL ALGORITMO DE EUCLIDES $14^{-1} \equiv 59 \mod 165$

ASÍ $x \equiv (2 \text{ ó } 3) \times 59 \mod 165$.

A M

HOJA 5º

PROBLEMA 15º) Nº EQUIPOS N con $100 \leq N \leq 1500$

k núm de PAQUETES

m núm de FURGONETAS USADAS

ASÍ $N = 68 \times k$

$N = 20 \times m + 32 = 20 \times (m+1) + 12$

ASÍ $N \equiv 0 \mod 68$

$N \equiv 12 \mod 20$ como $4|68$, $4|20$ y $4|12$.

$\frac{N}{4} \equiv 0 \mod 17$

$\frac{N}{4} \equiv 3 \mod 5$ y $mcd(17,5) = 1$

UNA IDENTIDAD DE BEZOUT.

ES LA SIGUIENTE $-2 \times 17 + 7 \times 5 = 1$

LUEGO $[5]_{17}^{-1} = [7]_{17}$ y $[3]_5 \times [17]_5 = [1]_5$

ASÍ $\frac{N}{4} \equiv 0 \times 7 \times 5 + 3 \times 3 \times 17$ SEGÚN EL TEOREMA DEL RESTO.

ASÍ $N = 4 \times 3 \times 3 \times 17 + k(17 \times 5) =$

$= 612 + k85$

LUEGO N PUEDE TOMAR EL VALORES $k = -6, -5, \ldots 0, 1, \ldots, 9, 10$

PROBLEMA 16:) i) $(a+b)^2 = a^2 + 2ab + b^2 = a^2 + b^2$ en $\mathbb{Z}_2$

YA QUE $2 \equiv 0 \mod 2$.

ii) $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 = a^3 + b^3$ en $\mathbb{Z}_2$

YA QUE $3 \equiv 0 \mod 3$

iii) $\binom{p}{k} = \frac{p!}{k!\,(p-k)!} \in \mathbb{Z}$ y si $1 \leq k < p-1$ (en $k!$ ó $(p-k)!$ NO HAY FACTORES IGUALES QUE p) SI O PRIMO $p \nmid k!$, $p \nmid (p-k)!$

$\Rightarrow p \mid \binom{p}{k}$ (DE OTRA FORMA; como $p \mid p! = \frac{p!}{k!\,(p-k)!} k!\,(p-k)! \Rightarrow p \mid \frac{p!}{k!\,(p-k)!}$)

ASÍ $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = a^p + b^p$ en $\mathbb{Z}_p$

BINOMIO DE NEWTON

YA QUE $\binom{p}{k} \equiv 0 \mod p$ $\forall\, 1 \leq k \leq p-1$.

HOJA 5ª

AM

PROBL. 17ª

$$k28 = m100 + 16$$

$\Leftrightarrow$ $k28 - m100 = 16$ con $k, m \geq 0$

ECUACIÓN DIOFÁNTICA COMO LAS DEL EJERCICIO 12

$\Leftrightarrow$ $k7 - m25 = 4$

ASÍ $k7 \equiv 4$ mod 25 como mcd(7,25) = 1

y $-7 \times 7 + 2 \times 25 = 1$ $\Rightarrow$ ASÍ $[7]_{25}^{-1} = [-7]_{25} = [18]$

LUEGO $k \equiv 4 \times 18 = 72 \equiv 22$ mod 25

ASÍ $28(22 + r25)$ $r \geq 0$ TERMINA SIEMPRE EN 16

PROBLEMA 18ª

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

LUEGO $(n-1)(n^2+n-6) + 1 =$
$= n^3 - 7n + 7$.

POR EL ALGORITMO DE EUCLIDES

$$\text{mcd}(n^3 - 7n + 7,\ n-1) = 1.$$

HOJA 6. - PROBLEMA a) $(\mathbb{Z}_n - \{0\}, \times) = \{[1],[2], \ldots, [n-1]\}, \times)$

$[p] \in \mathbb{Z}_n$ y como $[p^k] = [p]^k \in \mathbb{Z}_n$; como $\mathbb{Z}_n$ tiene una cantidad finita de elementos, existen $j, m \in \mathbb{N}$ con $j > 1$ y $[p^j] = [p^{j+m}]$ (HAY DOS POTENCIAS DE p QUE SE REPITEN)

ASÍ $-[p]^j + [p]^{j+m} = [p]^j([p]^m - [1]) = 0$

e.d $[p^j(p^m - 1)] = 0 \Rightarrow n \mid p^j(p^m - 1)$ como $n \nmid p^j$ por ser p primo $\Rightarrow n \mid p^m - 1$.

AM

HOJA 5:

PROBLEMA 20:

a) $\varphi(m) \underset{\text{DEF}}{=} \text{Card}\,|\{[k]_m \in \mathbb{Z}_m : \text{mcd}(k,m)=1\}| =$

$\underset{\text{EJERCICIO 6}}{=} \text{Card}\,|\{[k]_m \in \mathbb{Z}_m : \exists [k]_m^{-1}\}|$

b) $\varphi(11) = 11 - 1 = 10$ YA QUE 11 ES PRIMO

$\varphi(25) = \varphi(5^2) = 5^2\left(1-\frac{1}{5}\right) = 25 - 5 = 20$

$\varphi(100) = \varphi(4 \times 25) = \varphi(4)\cdot\varphi(25) =$

$= 4\left(1-\frac{1}{2}\right)\cdot 25\left(1-\frac{1}{5}\right) =$

$= 2 \times 20 = 40.$

PROBLEMA 21:

a) 2^{333} LA ÚLTIMA CIFRA DE ESTE NÚMERO SERÁ $[2^{333}]_{10} \xrightarrow{\text{T}} \left([2^{333}]_2, [2^{333}]_5\right) =$

Ejercicio 14

NOTA:

$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16$
$2^5 = 32$
$2^6 = 64$ ...etc

$= \left([0]_2, [2^{4\times 83} \times 2]_5\right) =$ ($2^4 = 16 \equiv 1 \bmod 5$)

$$\begin{array}{r|l} 333 & 4 \\ 13 & 83 \\ 1 & \end{array}$$

$= \left([0]_2, [2]_5\right)$

ASÍ $[2^{333}]_{10} = [2]_{10}$

LUEGO LA ÚLTIMA CIFRA DE 2^{333} ES 2

PROBLEMA 20º

b) $2^{37\times 73} = k\,37 + r$ r resto

luego $2^{37\times 73} \equiv r \mod 37$

se puede ver que $2^{36} \equiv 1 \mod 37$ (ya que mcd$(2,37)=1$; ver algún teorema de Fermat en el capítulo de clases).

luego $[2^{(36+1)73}]_{37} = [(2^{36})^{73} \cdot 2^{73}]_{37} =$

$= [2^{36}]_{37}^{73} \cdot [2^{73}]_{37} = [2^{2\times 36+1}]_{37} =$

$= [2]_{37}$ luego $r = 2$

c)

$$\left.\begin{array}{l} 2 \\ 4 \to 4^2 \\ 8 \\ 16 \to 4^2 \\ 32 \end{array}\right\} 5$$

$$\left.\begin{array}{l} 64 \to 4^3 \\ 128 \\ 256 \\ 512 \\ 1024 \to 4^5 \\ 2048 \\ 4096 \to 4^6 \\ 8182 \end{array}\right\} 8$$

$16364 \quad 4^7$

32728

2^{4927}

buscamos $[2^{4927}]_{100} \xrightarrow{\Psi}$

$([2^{4927}]_4, [2^{4927}]_{25}) \stackrel{\uparrow}{=} \varphi(25) = 20$

$= ([2\times 2^{2(2463)}]_4, [2^{20\times 246+7}]_{25})$

$= ([0]_4, [2^7]_{25}) = ([0]_4, [3]_{25})$

luego $\Psi^{-1}([0]_4, [3]_{25}) = 28$

HOJA 5

AM

PROBLEMA 22.]

a) $f(x) = x^5 + 3x^3 + x^2 + 2x = x(x^4 + 3x^2 + x + 2) \in \mathbb{Z}_5[x]$

$\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.

ASÍ $x = 0$ ES RAIZ

SI y ES RAIZ DE $h(x) = x^4 + 3x^2 + x + 2 \Rightarrow y \mid 2$

LUEGO $y = \pm 1$ ó ± 2 ES DECIR PUEDEN SER 1, 4, 2 ó 3

$h(1) = 1 + 3 + 1 + 2 = 2 \neq 0$

$h(-1) = 1 + 3 - 1 + 2 = 0$ LUEGO 4 ES RAIZ

$h(2) = 2^4 + 3\,2^2 + 2 + 2 = 16 + 12 + 2 + 2 \equiv_5 1 + 2 + 2 + 2 \equiv_5 2$ NO ES RAIZ

$h(-2) = 16 + 12 - 2 + 2 = 1 + 2 - 2 + 2 = -2$ NO ES RAIZ

LUEGO LAS ÚNICAS RAICES SON $x = 0$ Y $x = 4$.

HOJA 5ª

AM

PROBLEMA 23:

a) y b)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	

$C(x) = x+6$ $\quad A=0 \Rightarrow C(0): 0+6 = G$

$V = 22 \Rightarrow C(22) = 22+6 = 28 \equiv 1 \mod 27$

luego $C(22) = B$.

ASÍ SI SE RECIBE

G Q Q E U A S K K J Ñ Y Q U B K

NOS DICEN A L L Y O U . . . .

c)

0 A	1 B	2 C	3 D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R														

PACIENCIA

SDFLHPFLD