Ejercicio 51.-

1ª

					Z3
D	d	c	r	1 0	0 1
X^2-1	X^3-3x^2+6x-4	0	X^2-1	1	$-X^2+1$
X^3-3x^2+6x-4	X^2-1	x	**$x+2$**	$-x$	x^3+2x^2-x-2
X^2-1	$x+2$	x	0	**X^2+1**	

					Z5
D	d	c	r	1 0	0 1
X^2-1	X^3-3x^2+6x-4	0	X^2-1	1	$-X^2+1$
X^3-3x^2+6x-4	X^2-1	$X+2$	**$2x+3$**	$-x-2$	$2x^3+3x^2-2x-2$
X^2-1	$2x+3$	$3x+3$	0	**$3x^2+9x++7$**	

2ª

					Z3
D	d	c	r	1 0	0 1
x^2+2x+1	$X^3+7x^2+15x+9$	0	x^2+2x+1	1	$-x^2+2x+1$
$X^3+7x^2+15x+9$	x^2+2x+1	$X+5$	**$X+4$**	$-x-5$	$x^2+3x^2-11x-4$
x^2+2x+1	$X+4$	$X+1$	0	**x^2+6x+6**	

					Z5
D	d	c	r	1 0	0 1
x^2+2x+1	$X^3+7x^2+15x+9$	0	x^2+2x+1	1	$-x^2+2x+1$
$X^3+7x^2+15x+9$	x^2+2x+1	x	**$4x+4$**	$-x$	x^3-2x^2+x+1
x^2+2x+1	$4x+4$	$4x+4$	0	**$4x^2+4x+1$**	

3ª

					Z3
D	d	c	r	1 0	0 1
$X^5+5x^4+4x^3+3x^2+2x-1$	x^3-3x^2+2x-1	x^2+2x+2	**2**	1	$-x^2+2x+2$
x^3-3x^2+2x-1	2	$2x^3+x+1$	0	**-2x3-x-1**	

					Z5
D	d	c	r	1 0	0 1
$X^5+5x^4+4x^3+3x^2+2x-1$	x^3-3x^2+2x-1	x^2+3x+1	x^2+3x	1	$-x^2+3x+1$
x^3-3x^2+2x-1	x^2+3x	$X+4$	**4**	$-x-4$	$x^3+4x^2-10x-7$
x^2+3x	4	$4x^2+2x$	0	**$4x^3+18x^2+8x+1$**	

Ejercicio 32.-

Primera parte – Calculo de las ecuaciones que cumplen las tres condiciones:

a) $n \equiv 1 \pmod 2$ > $n \equiv 11 \pmod{2^2}$ > $n \equiv 3 \pmod 4$
b) $n \equiv 0 \pmod 3$ > $n \equiv 00 \pmod{3^2}$ > $n \equiv 0 \pmod 9$
c) $n \equiv 2 \pmod 5$ > $n \equiv 12 \pmod{5^2}$ > $n \equiv 7 \pmod{25}$

Sistema de ecuaciones:

$$\left.\begin{array}{l} n \equiv 3 \pmod 4 \\ n \equiv 0 \pmod 9 \\ n \equiv 7 \pmod{25} \end{array}\right\} \qquad n = 3+4k$$

· $3+4k = 0 \pmod 9$ > $4k = -6 \pmod 9$ > $k = 56 \pmod 9$ > $k = 6+9k'$

$$n = 3+4(6+9k') > n= 27+36k'$$

· $27+36k' = 7 \pmod{25}$ > $36k' = -20 \pmod{25}$ > $k^2 = 5+25k'$

$$n = 27+36(5+25k') > n = 207 + 900k$$

Segunda parte.- Enteros entre 1500 y 2500

$1500 \leq n \leq 2500$

Sustituimos la n por el valor que hemos sacado antes:

$1500 \leq 207+900k \leq 2500$
-207

$1293 \leq 900k \leq 2293$
$:900$

$1{,}436 \leq k \leq 2{,}547$

Entre 1,536 y 2,547 el único numero entero es el 2, por lo tanto k=2

Solución final= 900*2+207= 2007

Ejercicio 31.-

$$\begin{cases} 17834x \equiv 1870 \pmod{21989} \\ 89710x \equiv 10489 \pmod{8147} \\ 10022x \equiv 81984 \pmod{20984} \\ 20987x \equiv 10002 \pmod{11090} \\ 4094x \equiv 12353 \pmod{56271} \end{cases}$$

1ª.- 17834,1870,21989
    19316+21989k
2ª.- 89710*21989,10489-89710*19316,8147
    7922+ 8147k
3ª.- 19316+21989*7922,19316*8147
    174216174+157367452k
4º.- 10022*157367452,81984-10022*174216174,20984

NO TIENE SOLUCION

```
def ecuacion(a,b,m):
    d=xgcd(a,m)
    if b%d[0]==0:
        (a,b,m)=(a/d[0],b/d[0],m/d[0])
        b=b*d[1]
        return [b%m,m]
    else:
        return "No tiene solucion"

ec1=ecuacion (17834,1870,21989)
ec1
    [19316, 21989]

ec2= ecuacion(89710*ec1[1],10489-89710*ec1[0],8147)
ec2
    [7922, 8147]

ec3= (ec1[0]+ec1[1]*ec2[0],ec1[0]*ec2[1])
ec3
    (174216174, 157367452)

ec4= ecuacion(10022*ec3[1],81984-10022*ec3[0],20984)
ec4
    'No tiene solucion'
```

Ejercicio 37.-   3761373923x + 472926384y = 382734927

xgcd(3761373923,472926384)
(1,11997467, -95420685)

La primera solución es:

(3761373923*(11997467*382734927))
+
(472926384*(-95420685*382734927))
=
1*382734927

x0= 4591849656429909   y0= -36520828907764995

Resto de soluciones

X= 4591849656429909 + 472926384/1 * C

Y= -36520828907764995 - 3761373923/1 * C

Siendo C un numero entero

Solucion 2:
(3761373923*(4591849656429909 + 472926384*2))
+
(472926384*(-36520828907764995 – 3761373923*2))
=
382734927

Solucion 3:
(3761373923*(4591849656429909 + 472926384*3))
+
(472926384*(-36520828907764995 – 3761373923*3))
=
382734927

Solucion 4:
(3761373923*(4591849656429909 + 472926384*4))
+
(472926384*(-36520828907764995 – 3761373923*4))
=
382734927

Solucion 5:
(3761373923*(4591849656429909 + 472926384*5))
+
(472926384*(-36520828907764995 – 3761373923*5))
=
382734927

Ejercicio 42.-

x^4+1 irreducible en Zp[x] para p=(2,3,5,7,11,13,17)

- Z^2| $1^2 \equiv -1 \pmod 2$ $x^2(x^2-1)$
- Z^3| $1^2 \equiv -2 \pmod 3$ $(x^2+x-1)(x^2-x-1)$
- Z^5| $2^2 \equiv -1 \pmod 5$ $(x^2+2)(x^2-2)$
- Z^7| $3^2 \equiv 2 \pmod 7$ $(x^2+3x+1)(x^2-3x+1)$
- Z^{11}| $3^2 \equiv -2 \pmod{11}$ $(x^2+11x-1)(x^2-11x-1)$
- Z^{13}| $5^2 \equiv -1 \pmod{13}$ $(x^2+5)(x^2-5)$
- Z^{17}| $4^2 \equiv -1 \pmod{17}$ $(x^2+4)(x^2-4)$

Ejercicio 60.-

Demuestra que X^2+1 es irreducible en Z^3

	1	0	1
0		1	0
	1	0	**1**

	1	0	1
1		1	2
	1	2	**2**

	1	0	1
2		2	2
	1	1	**2**

Demuestra que X^3+x+1 es irreducible en Z^2

	1	1	1
1		0	0
	1	1	**1**

	1	0	1
1		1	0
	1	0	**1**

Describe todos los elementos y la aritmética de $Z^3[x]X^2+1$ y $Z^2[x]x^3+x+1$.

·X^2+1 = [0,1,2,x,x+1,x+2,2x,2x+1,2x+2]
·x^3+x+1 = [0,1,x,x+1,x^2,x^2+1,x^2+x,X^2+x+1]

Ejercicio 31.-

Simplifico las ecuaciones hasta el formato x≡a (mod b)

$\begin{cases} 17834x \equiv 1870 \pmod{21989} \\ 89710x \equiv 10489 \pmod{8147} \\ 10022x \equiv 81984 \pmod{20984} \\ 20987x \equiv 10002 \pmod{11090} \\ 4094x \equiv 12353 \pmod{56271} \end{cases}$	$\begin{cases} x \equiv 19316 \pmod{21989} \\ x \equiv 726 \pmod{8147} \\ x \equiv 6344 \pmod{10492} \\ x \equiv 1386 \pmod{11090} \\ x \equiv 13789 \pmod{56271} \end{cases}$

Tenemos el primer valor de x:

$$x = 19316+21989k^1$$

Resolvemos la segunda ecuación con el resultado de la primera:

$$19316+21989k^1 \equiv 726 \pmod{8147} \quad \Rightarrow \quad k^1 = 7922+8147k^2$$

Calculamos el nuevo valor de x con el resultado de la nueva ecuación:

$$x = 19316+21989(7922+8147k^2)$$
$$= 174176564 + 174176564\, k^2$$

Resolvemos la tercera ecuación con el resultado:

$$174176564 + 174176564\, k^2 \equiv 6344 \pmod{10492} \quad \Rightarrow \quad k^2 = 1460+2623k^3$$

Calculamos de nuevo el valor de x:

$$x = 174176564 + 174176564(1460+2623k^3)$$
$$= 261665502644 + 469788868704\, k^3$$

Resolvemos la 4º ecuación:

$$261665502644 + 469788868704\, k^3 \equiv 1386 \pmod{11090} \quad \Rightarrow k^3 = 3678+5545k^4$$

Ultimo valor de x:

$$x = 261665502644 + 469788868704(\ 3678+5545k^4)$$
$$= 1728145124595956+2604979276963680k^4$$

Resolvemos la 5º ecuación:

$$1728145124595956+2604979276963680k^4 \equiv 13789 \pmod{56271}$$
$$2604979276963680 \equiv -1728145124582167 \pmod{56271}$$

mcd (2604979276963680 y 56271) = 3
-1728145124582167 (mod 3)= 2

Como el mcd no divide a -1728145124582167 no tiene solución.