10. RAICES PRIMITIVAS, INDICES MODULARES Y SISTEMAS

10.1 Raíces primitivas

1.1 Raíz primitiva: definición.

Dados m, n tales que $mcd(m,n) = 1$, el menor g tal que $n^g \equiv 1(mód.m)$ se denomina *gaussiano* de n respecto de m. Si m es un primo y n es un número cualquiera tal que $m \nmid n$, y el gaussiano de n es $m-1$, entonces se dice que n es una raíz primitiva de m.
El número de raíces primitivas de m viene determinada por la función $\varphi(m-1)$, siendo $(m-1) = m_1^{a1} \cdot m_2^{a2} \cdot \ldots \cdot m_r^{ar}$. Si en α se cumple que $\alpha^{(p-1)/p_1} \not\equiv 1(mód.p)$, con p primo, y también en $\alpha^{(p-1)/pr} \not\equiv 1(mód.p)$ entonces, α es la raíz primitiva de *p*. En efecto. Notemos que si $p \nmid n$, entonces $n^{p-1} \equiv 1(mód.p)$, con lo que, si el gaussiano de n no es $p-1$, deberá ser un divisor de $p-1$. Pero en este caso, si el gaussiano se descompone en factores primos como $p_1^{\beta_1} \ldots p_r^{\beta_r}$ donde alguno de los β_i puede ser cero, y suponiendo que $\beta_j < \alpha_j$, tenemos que $\alpha^{(p-1)/\beta_j} \equiv 1(mód.p)$ luego, el número de raíces primitivas de p viene determinado por $\varphi(p-1)$.
Dada n una raíz primitiva de p, se tiene que los valores $n^0, n^1, \ldots, n^{p-2}$ dan restos distintos dos a dos (*mód.p*). Dado a, si existe $\beta \in \{0, \ldots, p-2\}$ tal que $n^\beta \equiv a(mód.p)$, entonces se dice que β es índice modular de a en base n, y se denota como $\beta = I_n(a) = Ind_n a$.
No todos los módulos poseen raíces primitivas. Los casos en que existen raíces primitivas respecto de un módulo m, con $m > 1$ son, $m = \{2, 4, p^\alpha, 2p^\alpha\}$, en donde p es primo y $\alpha \geq 1$.

1.2 Calcular la raíz primitiva de 11.

Para calcular la raíz primitiva de 11, empezaremos por descomponer en factores primos $\varphi(p-1) = 10 = 2 \cdot 5$, $10/2 = 5$ y $10/5 = 2$. Por consiguiente, para que un número α no sea divisible por 11, sea raíz primitiva respecto del módulo 11, es necesario y suficiente que este número α no satisfaga a ninguna de las congruencias $\alpha^2 \equiv 1(mód.11)$ o $\alpha^5 \equiv 1(mód.11)$. Para $\alpha = 2$, $2^{(10/2)} = 2^5 \equiv -1(mód.11)$ no es congruente con 11, y para $2^{(10/5)} = 2^2 \equiv 4(mód.11)$, tampoco es congruente con 11, luego *2 es la raíz primitiva de 11.*

1.3 Calcular la raíz primitiva de 13.

Sea $p = 13$. $\varphi(p-1) = 12 = 2^2 \cdot 3 = 2 \cdot 6$, $12/2 = 6$ y $12/6 = 2$, que para $\alpha = 2$, tenemos $2^{(12/2)} = 2^6 \equiv -1(mód.13)$ y $2^{(12/6)} = 2^2 \equiv 4(mód.13)$. Ninguna de las dos congruencias satisface, ni a $\alpha^2 \equiv 1(mód.13)$ ni a $\alpha^6 \equiv 1(mód.13)$ luego, *la raíz primitiva de 13 es 2***.**

1.4 Calcular la raíz primitiva de 17.

Tenemos que $p = 17$ y $\varphi(p-1) = 16 = 2^4 = 2 \cdot 8$, donde $16/2 = 8$ y $16/8 = 2$. Para $\alpha = 3$, $3^{(16/2)} = 3^8 \equiv 16 \equiv -1(mód.17)$ y para $3^{(16/8)} = 3^2 \equiv 9(mód.17)$, que no satisfacen a $\alpha^2, \alpha^8 \equiv 1(mód.17)$ por tanto, *la raíz primitiva de 17 es 3.*

1.5 Calcular la raíz primitiva de 23.

Tenemos que $p=23$ y $\varphi(p-1)=22=2\cdot 11,$ donde $22/2=11$ y $22/11=2.$ Para $\alpha=3,$ $3^{(22/2)}=3^{11}\equiv 1(mód.23)$ que es congruente y $3^{(22/11)}=3^{2}\equiv 9(mód.23)$ que no es congruente con *1 módulo 23* y, por tanto, 3 no es raíz primitiva de *23*. Probamos con $\alpha=5.$ Tenemos que, $5^{(22/2)}=5^{11}\equiv 22(mód.23)$ y $5^{(22/11)}=5^{2}\equiv 2(mód.23)$, ambas son *incongruentes* con *1 módulo 23*, luego *5 es la raíz primitiva de 23.*

1.6 Calcular las raíces primitivas de los enteros $n<100$.

Utilizando el programa $Mathematica\ versión\ 6.1$, las raíces primitivas de los enteros comprendidos entre el 1 y 99, son,

n	0	1	2	3	4	5	6	7	8	9
0		*0*	*1*	*2*	*3*	*2*	*5*	*3*		*2*
1	*3*	*2*		*2*	*3*			*3*	*5*	*2*
2			*7*	*5*		*2*	*7*	*2*		*2*
3		*3*			*3*			*2*	*3*	
4		*6*		*3*			*5*	*5*		*3*
5	*3*			*2*	*5*				*3*	*2*
6		*2*	*3*					*2*		
7		*7*		*5*	*5*					*3*
8		*2*	*7*	*2*			*3*			*3*
9					*5*			*5*	*3*	

Nota: Las casillas en blanco son números que *no tienen* raíz primitiva.

1.7 Demostrar la no existencia de raíces primitivas $mód.2^{\alpha}$ para $\alpha\geqq 3$.

Sea x un entero impar. Si $\alpha\geqq 3,$ tenemos que $x^{\varphi(2^{\alpha})/2}\equiv 1(mód.2^{\alpha})$ luego, no existen raíces primitivas *mód*. 2^{α}. Efectivamente, si $\alpha=3,$ la ecuación $x^{\varphi(2^{\alpha})/2}\equiv 1(mód.2^{\alpha})$ establece que $x^{2}\equiv 1(mód.2^{3})$ para x impar. Este hecho se comprueba fácilmente haciendo que $x=1,3,5,7$ u observando que $(2k+1)^{2}=4k^{2}+4k+1=4k(k+1)+1$ y teniendo en cuenta que $k(k+1)$ es par.

Supongamos que el teorema se cumple para α y queremos demostrar que también se cumple para $\alpha+1.$ La hipótesis de inducción nos dice que $x^{\varphi(2^{\alpha})/2}=1+2^{\alpha}t,\ t\in Z.$ Elevando ambos miembros al cuadrado obtenemos $x^{\varphi(2^{\alpha})}=1+2^{\alpha+1}t+2^{2\alpha}t^{2}\equiv 1(mód.2^{\alpha+1})$ ya que $2\alpha\geqq\alpha+1.$ Esto termina la demostración puesto que $\varphi(2^{\alpha})=2^{\alpha-1}=\varphi(2^{\alpha+1})/2.$

1.8 Demostrar en qué casos la congruencia $x^{n}\equiv\alpha(mód.m)$ tiene solución.

Supongamos que *p* es un número primo impar; $\alpha\geqq 1,$ *m* es uno de los números $p^{\alpha},\ 2p^{\alpha}$ y finalmente, $c=p-1$ y $mcd(n,c)=d,$ entonces $x^{n}\equiv\alpha(mód.m)$ admite solución sí, y sólo sí $(I)\alpha$ sea un múltiplo de d, esto es, α es un resto de grado *n* respecto del módulo *m*. Por tanto, si $x^{n}\equiv\alpha(mód.m)$ es soluble, ésta admite *d* soluciones.

Aplicando el *teorema de Fermat*, como $I(\alpha)\equiv 0(mód.c)$ es equivalente a $\alpha^{c/d}\equiv 1(mód.d)$ y, como $g^{c/q}\equiv 1(mód.m)$ será equivalente sí, y sólo sí *g* sea un no resto de grado *q* respecto del

módulo *m*, por la imposibilidad de que $g^{c/2} \equiv 1(mód.m)$, entonces $\alpha^{c/d} \equiv 1(mód.d)$ será congruente si, y sólo si α es un no resto de grado *d* respecto al módulo *d*.
Sea $x^8 \equiv 7(mód.13)$ y sea $g = 2$ la raíz primitiva de 13. Como $mcd(8,12) = 4$ y $I(7) = 11$, resulta que $4 \nmid 11$, luego la congruencia no admite ninguna solución.
Comprobamos para $I(7) = 11 \not\equiv 0(mód.12)$, donde $7^{12/4} = 7^3 = 343 \not\equiv 1(mód.4)$ y que $2^{12/4} = 2^3 = 27 \not\equiv 1(mód.13)$ por tanto, queda demostrado que la congruencia no admite ninguna solución si $I(a)$ no es múltiplo de d.

10.2 Índices modulares

2.1 Índices modulares: confección de tablas.

Si *m* tiene una raíz primitiva *g*, los números $1, g, g^2, \ldots, g^{\varphi(m)-1}$ forma un sistema residual reducido *mód*. *m*. Si $mcd(a,m) = 1$ existe un único entero k en el intervalo $0 \leqq k \leqq \varphi(m) - 1$ tal que $a \equiv g^k (mód.m)$. Este entero se llama índice de a en base g *mód*. *m*, y que escribimos como $k = ind_g a$ o simplemente $k = índ$ a cuando la base *g* se sobrentiende.
Los índices tienen propiedades análogas a las de los logaritmos. Efectivamente. Sea *g* una raíz primitiva *mód*. *m*. Si $mcd(a,m) = (b,m) = 1$ tenemos que:

$índ(ab) = índ(a) + índ(b)(mód.\varphi(m))$
$índ(q^n) \equiv n \cdot índ(a)(mód.\varphi(m))$ sí $n \geqq 1$.
$índ(1) = 0$ *e* $índ(g) = 1$.
$índ(-1) = \varphi(m)/2$ sí $m > 2$.

Si g' es también una raíz primitiva *mód*. *m* entonces

$$índ_g(a) \equiv índ_g(a) \cdot índ_g(g')(mód.\varphi(m))$$

Las *tablas de índices modulares* se confeccionan en dos partes: una para hallar el índice de un número dado, otra para hallar los números por el índice. Las primeras las denotamos como $N(n)$ y las segundas como $I(n)$.

2.2 Confeccionar la tabla de índices modulares del 11.

Sabemos que la raíz primitiva del número 11 es 2, esto es, $\alpha = 2$ por tanto, se trata de calcular por $\alpha^n \equiv r(mód.11)$ donde *n* es el conjunto $\{0,1,2,\ldots,p-1\}$, los restos potenciales, que para 11 resultan ser:

$2^0 \equiv 1$	$2^2 \equiv 4$	$2^4 \equiv 5$	$2^6 \equiv 9$	$2^8 \equiv 3$
$2^1 \equiv 2$	$2^3 \equiv 8$	$2^5 \equiv 10$	$2^7 \equiv 7$	$2^9 \equiv 6$

Se confecciona tabla $I_{(n)}$ para hallar el número, conociendo el índice, que es copia de la que se acaba de calcular, y tabla n para hallar el índice, conociendo el número:

n	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	1	2	4	8	5	10	9	7	3	6

$I_{(n)}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0		0	1	8	2	4	9	7	3	6
1	5									

Por ejemplo, si queremos conocer el número que corresponde al índice 4, en la tabla $I_{(n)}$, $I(4)=2$ y para conocer el índice del número 8, en la tabla, $n(8)=3$.

2.3 Resolver la ecuación $x^8 \equiv 5(mód.11)$.

Sea $m=p-1$ y $mcd(a,b)=d$, donde la congruencia $x^n \equiv a(mód.p)$ admite solución y por consiguiente, *a* es un resto de grado *n* respecto del *módulo p* cuando, y sólo cuando $I(a)$ es un múltiplo de d. Si la congruencia es soluble, ésta admite *d* soluciones en la forma $n \cdot I(x) \equiv I(a)(mód.m)$.
La solución de $x^8 \equiv 5(mód.11)$ requiere los siguientes pasos:

$a)$ El $mcd(8,10)=2$ y el índice que corresponde al número 5 es $I(5)=4$, que es divisible por 2 luego, la ecuación admite 2 soluciones.

$b)$ La congruencia $x^8 \equiv 5(mód.11)$ es equivalente a $8 \cdot I(x) \equiv 4(mód.10)$. Ahora dividimos todos los miembros por 2 que resulta $4 \cdot I(x) \equiv 2(mód.5)$, de donde $x \equiv 3(mód.5)$, o sea $x=3+5t$ por lo que $x \equiv 3,8(mód.10)$.

$c)$ Según la tabla n, los valores de 3 y 8 son $n(3,8)=8,3$ por tanto, la solución al sistema planteado es, $x \equiv 3,8(mód.11)$.

2.4 Resolver la ecuación $x^7 \equiv 11(mód.17)$.

Sabemos que la raíz primitiva de *17* es *3*, ahora calculamos las tablas de índices.

$3^0 \equiv 1$	$3^2 \equiv 9$	$3^4 \equiv 13$	$3^6 \equiv 15$	$3^8 \equiv 16$	$3^{10} \equiv 8$	$3^{12} \equiv 4$	$3^{14} \equiv 2$
$3^1 \equiv 3$	$3^3 \equiv 10$	$3^5 \equiv 5$	$3^7 \equiv 11$	$3^9 \equiv 14$	$3^{11} \equiv 7$	$3^{13} \equiv 12$	$3^{15} \equiv 6$

$I_{(n)}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

n	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

El $mcd(7.16)=1$ y el índice de $I(11)=7$ que divide a 1, esto es, $1|11$ luego, la ecuación admite al menos una solución. La ecuación es equivalente a $7 \cdot I(x) \equiv 7(mód.16)$, o sea, $I(x) \equiv 1(mód.16)$. Por la tabla n, $n(1)=3$ luego, la solución al sistema propuesto es $x \equiv 3(mód.17)$.

2.5 Resolver la ecuación $x^{16} \equiv 3(mód.13)$ **.**

Sabemos que la raíz primitiva de 13 es 2. Las tablas de índices que generan son:

$I_{(n)}$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

n	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

El $mcd(16,12) = 4$. Como $I(3) = 4$, que es múltiplo del mcd, la ecuación admitirá cuatro soluciones. La ecuación $x^{16} \equiv 3(mód.13)$ es equivalente a $16 \cdot I(x) \equiv 4(mód.12)$, que haciendo operaciones, $x = 1 + 3t$. Dando valores a *t* obtenemos para $I(x) = 1,4,7,10$ que, de acuerdo con las tablas de índice, resulta, $x \equiv 2,3,10,11(mód.13)$ como solución al sistema propuesto.

2.6 Resolver la ecuación $x^5 \equiv 3(mód.41)$ **.**

El $mcd(5,40) = 5$. Como $I(3) = 15$, que es múltiplo del mcd, luego la ecuación admite cinco soluciones. Sea $x^5 \equiv 3(mód.41)$ que equivale a $5 \cdot I(x) \equiv 15(mód.40)$, si dividimos toda la ecuación por 5, $I(x) \equiv 3(mód.8)$ o sea, $I(x) = 3 + 8t$. Damos valores a *t* y obtenemos, $I(x) = 3,11,19,27,35$ que, de acuerdo con las tablas de índice *n*, resulta para $x \equiv 11,12,28,34,38(mód.41)$, que son las soluciones del sistema propuesto.

2.7 Resolver la ecuación $x^5 \equiv 3(mód.65)$ **.**

La descomposición factorial del módulo es $65 = 5 \cdot 13$ por tanto, la ecuación tendrá solución si, y sólo si la tienen $x^5 \equiv 3(mód.5)$ y $x^5 \equiv 3(mód.13)$. Por simple observación la primera es equivalente a $x \equiv 3(mód.5)$ luego, $x = 3 + 5t$. Para la segunda, el $mcd(5,12) = 1$ y $I(3) = 4$ o sea, 1|4 por consiguiente admite una solución. La ecuación $x^5 \equiv 3(mód.13)$ es equivalente a $5 \cdot I(x) \equiv 4(mód.12)$, que operando se convierte en $I(x) = 8 + 12t$. Según las tablas de índices del 13, al 8 le corresponde 9, entonces, $x \equiv 9(mód.13)$, que escribimos como $x = 9 + 13t$.

Para la solución de $x^5 \equiv 3(mód.65)$ utilizaremos el *Teorema Chino de Restos*. Tomamos $3 + 5t_1 \equiv 9(mód.13)$, haciendo operaciones $t_1 = 9 + 13t$. Sustituimos para conocer *x*, $x = 3 + 5(9 + 13t) = 48 + 65t$, luego $x \equiv 48(mód.65)$ que es la solución buscada.

2.8 Resolver la ecuación $x^6 \equiv 17(mód.23)$ **.**

El $mcd(6,22) = 2$ y $I(17) = 7$. Como $2 \nmid 7$, la ecuación no admite ninguna solución.

2.9 Resolver la ecuación $x^{10} \equiv 9(mód.161)$ **.**

Como $161 = 7 \cdot 23$, la ecuación tendrá solución si y sólo si las tienen las ecuaciones $x^{10} \equiv 9(mód.7)$ y $x^{10} \equiv 9(mód.23)$.

Para $x^{10} \equiv 9(mód.7)$ equivalente a $x^{10} \equiv 2(mód.7)$, cómo $mcd(10,6) = 2$ y $I(2) = 2$, dado que $2 \mid 2$, la ecuación tendrá dos soluciones. Si $10 \cdot I(x) \equiv 2(mód.6)$ la dividimos por *2* resulta $5 \cdot I(x) \equiv 1(mód.3)$, donde $I(x) \equiv 2,5(mód.6)$. Por la tabla de índices n, los valores de $I(2,5)$ son equivalentes a *2* y *5*, que es la solución de $x^{10} \equiv 9(mód.7)$.

Para $x^{10} \equiv 9(mód.23)$, cómo $mcd(10,22) = 2$ y $I(9) = 10$, dado que $2 \mid 10$, la ecuación tendrá dos soluciones. Si $10 \cdot I(x) \equiv 10(mód.22)$ la dividimos por *2* resulta $5 \cdot I(x) \equiv 5(mód.11)$, donde $N(x) \equiv 1,12(mód.22)$. Por la tabla de índices n, los valores de $I(1,12)$ son equivalentes a 5 y 18, la solución de $x^{10} \equiv 9(mód.23)$.

Aplicando el *teorema chino de restos*, la solución de $x^{10} \equiv 9(mód.161)$ es de $5,51,110,156$.

10.3 Sistemas monovariables

3.1 Resolver el sistema $f(x) = 2^{500} \equiv r(mód.61)$.

Fermat nos dice que $a^{(p-1)} \equiv 1(mód.p)$, si ahora sustituimos resulta $2^{(61-1)} \equiv 1(mód.61)$. Para $2^{500} = 2^{480+20} = 2^{480} \cdot 2^{20} = 1^{480} \cdot 2^{20} = 2^{20}$. Éste último resultado aplicado a la ecuación propuesta resulta $2^{20} = 1048576 \equiv 47(mód.61)$ donde, $r = 47$.
A continuación comprobamos si este sistema tiene otras soluciones. Para ello resolvemos la función $x^{500} \equiv 47(mód.61)$ equivalente a $500 \cdot I(x) \equiv 47(mód.60)$. Por las tablas de índices modulares, $I(47) = 20$ por tanto, $20 \cdot I(x) \equiv 20(mód.60)$, o sea $I(x) \equiv 1(mód.3)$. Dando valores a $I(x) = 1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46,49,52,55,58$ por lo que obtenemos $f(x) \equiv 2,5,6,7,13,15,16,18,21,22,39,40,43,45,46,48,54,55,56,59(mód.61)$ que son las soluciones del sistema.

3.2 Resolver el sistema $f(x) = 13x^{40} + 23x^{25} \equiv 1(mód.11)$.

La ecuación $x = 13x^{40} + 23x^{25} \equiv 1(mód.11)$ podemos reducirla a $x = 2x^{40} + x^{25} \equiv 1(mód.11)$. Por la función de Euler, $\varphi(11) = 11 - 1 = 10$, por lo que podemos modificar los exponentes hasta convertir la ecuación a $x = 2 + x^5 \equiv 1(mód.11)$, de donde $x^5 \equiv 10(mód.11)$. Tomando índices, escribimos $5I(x) \equiv \mathrm{I}(10)(mód.10)$ que es equivalente a $5I(x) \equiv 5(mód.10)$ y que podemos escribir como $I(x) \equiv 1(mód.2)$. Para $I(x) = 1,3,5,7,9$ y para $n = 2,8,10,7,6$. Por tanto, la solución al sistema propuesto es $f(x) \equiv 2,6,7,8,10(mód.11)$.

3.3 Resolver el sistema $f(x) = x^{12} \equiv 37(mód.41)$.

Utilizando índices, $12I(x) \equiv I(37)(mód.40)$ que resulta $12I(x) \equiv 32(mód.40)$. Como el $mcd(12,32) = 4$, lo que indica que el sistema tiene cuatro soluciones. Dividiendo el resultado obtenido anteriormente por 4, tenemos $3I(x) \equiv 8(mód.10)$. Multiplicamos por 3 para despejar $I(x)$, obtenemos $I(x) \equiv 6(mód.10)$. Para $I(x) = 6,16,26,36$ que son equivalentes a $n = 39,18,2,23$ luego, la solución al sistema propuesto es $f(x) \equiv 2,18,23,39(mód.41)$.

3.4 Resolver el sistema $f(x)=x^{36}\equiv 36(mód.29)$.

La función propuesta la podemos escribir como $x^8\equiv 7(mód.29)$. Utilizando índices modulares, $8I(x)\equiv \mathrm{I}(7)(mód.28)$ que resulta $8I(x)\equiv 12(mód.28)$. Como el $mcd(8,12)=4,$ la ecuación tendrá 4 soluciones. Dividiendo $8I(x)\equiv 12(mód.28)$ por 4 obtenemos $2I(x)\equiv 3(mód.7)$ que simplificada resulta $I(x)\equiv 5(mód.7)$. Ahora podemos conocer los valores de $I(x)=5,12,19,29$ equivalentes a $n=3,7,26,22,$ de donde, las soluciones al sistema son $f(x)\equiv 3,7,22,26(mód.29)$.

3.5 Resolver el sistema $f(x)=5x^{85}+8x^{40}\equiv 13(mód.533)$.

El módulo se factoriza como $533=13\cdot 41$ luego, el sistema tendrá solución si y sólo si la tienen las ecuaciones $5x^{85}+8x^{40}\equiv 13(mód.13)$ y $5x^{85}+8x^{40}\equiv 13(mód.41)$.

Para $5x^{85}+8x^{40}\equiv 13(mód.13),$ que simplificamos como $5x+8x^4\equiv 0(mód.13),$ que podemos reducir a $12x^4+x\equiv 0(mód.13)$ y que se convierte finalmente en $x^4-x\equiv 0(mód.13)$.
Utilizando índices modulares, $4I(x)-I(x)\equiv \mathrm{I}(0)(mód.12),$ que se convierte en $3I(x)\equiv 0(mód.12)$. Como el $mcd(3,0)=3,$ la ecuación tendrá tres soluciones. Dividiendo por 3, $I(x)\equiv 0(mód.4),$ de donde $I(x)=0,4,8$ equivalentes a $n=0,1,3,9$ de donde las soluciones a la ecuación son $x_1=0+13t,\ x_2=1+13t,\ x_3=3+13t\ y\ x_4=9+13t.$

Para $5x^{85}+8x^{40}\equiv 13(mód.41),$ que simplificamos como $5x^5+8\equiv 13(mód.41),$ y que podemos reducir a $x^5\equiv 1(mód.41).$
Utilizando índices modulares, $5I(x)\equiv \mathrm{I}(1)(mód.40)$ equivalente a $5I(x)\equiv 0(mód.40)$. Como el $mcd(5,0)=5,$ la ecuación tiene cinco soluciones. Dividiendo por cinco y simplificando, tenemos $I(x)\equiv 0(mód.8),$ de donde $I(x)=0,8,16,24,32$ equivalentes a $n=1,10,18,16,37$ que son las soluciones a la ecuación y que escribimos en la forma $x_1=1+41t,\ x_2=10+41t,\ x_3=16+41t, x_4=18+41t\ y\ x_5=37+41t.$

Para $5x^{85}+8x^{40}\equiv 13(mód.533),$ como las ecuaciones parciales han dado cuatro y cinco soluciones, respectivamente, ésta tendrá veinte soluciones que se pueden encontrar utilizando el T*eorema Chino de Restos* y que son, $f(x)\equiv 1,16,42,78,92,100,133,139,165,182,211,247,256,338,$ $365,406,469,508,510,529\equiv (mód.533).$

3.6 Resolver el sistema $f(x)=7x^{90}+x^{63}\equiv 9(mód.6231)$.

Factorizamos el módulo como $6231=3\cdot 31\cdot 67.$

Para $7x^{90}+x^{63}\equiv 9(mód.3),$ simplificamos a $1+x\equiv 0(mód.3)$ que tiene como solución $x=2+3t.$

Para $7x^{90}+x^{63}\equiv 9(mód.31),$ simplificamos a $7+x^3\equiv 9(mód.31)$ que podemos escribir como $x^3\equiv 2(mód.31).$ Utilizando índices, $3I(x)\equiv \mathrm{I}(2)(mód.30)$ donde $3I(x)\equiv 24(mód.30).$ Como el $mcd(3,24)=3,$ tres serán las soluciones de la ecuación. Dividiendo la ecuación por 3, resulta

$I(x) \equiv 8(mód.10)$ de donde $I(x) = 8,18,28$ equivalentes a $n = 20,4,7.$ Las soluciones de la ecuación son $x_1 = 4 + 31t, x_2 = 7 + 31t$ *y* $x_3 = 20 + 31t.$

Para $7x^{90} + x^{63} \equiv 9(mód.67),$ simplificamos a $7x^{24} + x^{63} \equiv 9(mód.67).$ Para simplificar los exponentes hemos utilizado la función de Euler $\varphi(67) = 67 - 1 = 66,$ número que es mayor que el segundo coeficiente 63. Podemos forzar el coeficiente negativo haciendo que $63 - 66 = -3$ y reescribiendo la ecuación simplificada como $7x^{24} + x^{-3} \equiv 9(mód.67)$ equivalente a $7x^{24} + 1/x^3 \equiv 9(mód.67).$ Quitando denominadores, resulta $7x^{27} - 9x^3 + 1 \equiv 0(mód.67)$ que tiene como solución $x \equiv 17,24,26(mód.67),$ como podrá comprobar utilizando métodos anteriores.

Aplicando el teorema chino de restos, el sistema $f(x) = 7x^{90} + x^{63} \equiv 9(mód.6231)$ tiene como solución $f(x) \equiv 627,888,1089,1433,1632,1833,2438,2639,3510,4037,4515,4716,4781,5042,$ $5243,5786,5987,6114(mód.6231).$

3.7 Resolver el sistema $f(x) = x^{20} - 20x^{40} \equiv 2(mód.1127)$.

Empecemos por factorizar el módulo: $1127 = 7^2 \cdot 23.$

Para $x^{20} - 20x^{40} \equiv 2(mód.7),$ simplificamos a $x^2 + x^4 \equiv 2(mód.7)$ que podemos escribir como $x^2(x^2+1) \equiv 2(mód.7)$ y que tiene como solución $x \equiv 1,6(mód.7).$

Para $x^{20} - 20x^{40} \equiv 2(mód.23),$ simplificamos a $1/x^2 + 26/x^4 \equiv 2(mód.23)$ que quitando denominadores podemos escribir como $x^2 + 26 \equiv 2x^4(mód.23).$ Si ahora unificamos monomios, tenemos $2x^4 - x^2 \equiv 3(mód.23)$ que podemos transformar en $x^2(2x^2 - 1) \equiv 3(mód.23)$ que tiene como solución $x \equiv 6,17(mód.23).$

Para resolver la ecuación $x^{20} - 20x^{40} \equiv 2(mód.49),$ ya que conocemos las soluciones del módulo 7, utilizaremos la *formula de Taylor,* $Brook\ Taylor$ $(1685 - 1731),$ matemático inglés que la descubrió. Los valores de la ecuación $x^2 + x^4 \equiv 2(mód.7)$ y sus derivadas, son

$$f(x) = x^2 + x^4 = \begin{cases} f(1) = 2 \\ f(4) = 1332 \end{cases} \quad f'(x) = 2x + 4x^3 = \begin{cases} f(1) = 6 \\ f(4) = 876 \end{cases}$$

Ahora debemos resolver la ecuación $f(x) + f'(x)pt \equiv 0(mód.p^n),$ que sustituyendo los valores obtenidos, obtenemos $x \equiv 6,43(mód.49).$

Utilizando el *teorema chino de restos*, la solución al sistema planteado vendrá determinado por $f(x) \equiv 6,190,937,1121(mód.1127).$

3.8 Confeccionar tabla de números e índices módulo 13

Sabemos que la raíz primitiva de 13 es 2. Las restantes raíces primitivas se obtienen calculando los r tales que $mcd(r,12) = 1.$ Éstos resultan ser $r = 5,7,11,$ con lo que las raíces pedidas son, $2^5 \equiv 6(mód.13),$ $2^7 \equiv 11(mód.13)$ y $2^{11} \equiv 7(mód.13).$

Para pasar de un índice de base b a otro de base b'. Supongamos conocido $x = I_b(n)$ y queremos calcular $x' = I_{b'}(n)$, si $b'^{x'} \equiv n(mód.p)$, entonces $x' I_b(b') \equiv I_b(n)(mód.p-1)$, por lo que $x' \equiv I_b(b')^{-1} I_b(n)(mód.p-1)$. Por consiguiente, es suficiente calcular la columna $I_2(n)$ de la tabla siguiente, y, a partir de ella calcular las otras mediante $x' \equiv I_b(b')^{-1} I_b(n)(mód.p-1)$. Supongamos $I_6(n) \equiv (I_2(6)^{-1} I_2(n)(mód.12)$. Como $I_2(6) = 5,\ I_2(6)^{-1} = 1/5 \equiv 5(mód.12)$, ya que $5 \cdot 5 = 25 \equiv 1(mód.12)$. De la misma manera, si $I_2(11)^{-1} = 1/7 \equiv 7(mód.12)$, ya que $7 \cdot 7 = 49 \equiv 1(mód.12)$. Análogamente $I_2(7)^{-1} = 11$, ya que $11 \cdot 11 = 121 \equiv 1(mód.12)$. De esta manera la tabla nos queda de la siguiente forma:

n	$I_2(n)$	$I_6(n)$	$I_7(n)$	$I_{11}(n)$
1	0	0	0	0
2	1	5	11	7
3	4	8	8	4
4	2	10	10	2
5	9	9	3	3
6	5	1	7	11
7	11	7	1	5
8	3	3	9	9
9	8	4	4	8
10	10	2	2	10
11	7	11	5	10
12	6	6	6	6

Nota: Este supuesto aparece en la página 308 de Problemas y Ejercicios de Matemáticas Discreta de Antonio Vera López y Ramón Esteban Romero.

3.9 Confeccionar tabla de números e índices módulo 17

Sabemos que la raíz primitiva de 17 es $g = 3$ y los números que generan las nuevas raíces primitivas vendrán determinados por $mcd(n,16) = 1,3,5,7,9,11,13,15$. Con estos números índices se generan las raíces primitivas de la forma siguiente:

$$3^1 \equiv 3(mód.17),\ 3^3 \equiv 10(mód.17),\ 3^5 \equiv 5(mód.17),\ 3^7 \equiv 11(mód.17),$$
$$3^9 \equiv 14(mód.17),\ 3^{11} \equiv 7(mód.17),\ 3^{13} \equiv 12(mód.17),\ 3^{15} \equiv 6(mód.17)$$

donde las raíces primitivas, respecto al módulo 17, son $3,5,6,7,10,11,12,14$. Ahora podemos crear las tablas índices de estas raíces primitivas:

g	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
3	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6
5	1	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7
6	1	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3
7	1	7	15	3	4	11	9	12	16	10	2	14	13	6	8	5
10	1	10	15	14	4	6	9	5	16	7	2	3	13	11	8	12
11	1	11	2	5	4	10	8	3	16	6	15	12	13	7	9	14
12	1	12	8	11	13	3	2	7	16	5	9	6	4	14	15	10
14	1	14	9	7	13	12	15	6	16	3	8	10	4	5	2	11

10.4 Sistemas multidimensionales

4.1 Transformación a sistemas multivariables.

Sea una ecuación monovariable cuadrática $ax^2+bx=c,$ que tiene solución. Sea una ecuación multivariable $ax^2+by=c.$ Estas dos ecuaciones serán equivalentes sí, y sólo sí, c es restos cuadrático de ax^2 respecto al $módulo\ b.$

Supongamos $x^2+5x=2.$ Esta ecuación tiene como solución $x=\dfrac{-5\pm\sqrt{5^2+4\cdot 2}}{2}=\dfrac{-5\pm\sqrt{33}}{2},$ dos raíces reales. La ecuación $x^2+5y=2$ tendrá solución sí, y sólo sí, 2 es resto cuadrático respecto al módulo 5. Por el *criterio de Euler* $a^{(p-1)/2}\equiv 1(mód.p),$ aplicado a nuestro caso $2^{(5-1)/2}\equiv 3\not\equiv 1(mód.5),$ 2 no es resto cuadrático respecto al módulo 5 y, por tanto, los sistemas no son equivalentes ni transformables.

4.2 Transformar la ecuación $x^2+5x-4=0$.

La solución de $x^2+5x-4=0$ es $x=\dfrac{-5\pm\sqrt{5^2+4\cdot 4}}{2}=\dfrac{-5\pm\sqrt{41}}{2},$ dos raíces reales.

Para $x^2+5y-4=0,$ como $4^{(5-1)/2}\equiv 1(mód.5),$ el sistema es transformable y tendrá cuatro raíces, dos por cada variable.

A continuación exponemos un método de solución para estas ecuaciones.

Calcular **x** en función de **y**: Por ecuaciones modulares.
Sea $x^2+5y=4$ que transformamos en $x^2\equiv 4(mód.5)$. Como $x^2\equiv 2^2(mód.5)$, la ecuación tiene como solución $x\equiv 2(mód.5)$. De acuerdo con *Gauss*, si una ecuación cuadrática pura admite una raíz, también admitirá una segunda que será la inversa de aquella. En este caso, $x\equiv -2(mód.5)$. Como la inversa o complemento de -2, respecto al módulo 5 es 3, la segunda raíz será $x\equiv 3(mód.5)$ luego, la solución será, $x_1=2+5t\ y\ x_2=3+5t.$

Calcular **y** en función de **x**: Por sustitución.
En $x^2+5y=4,$ sustituyendo el valor de $x,$ obtenemos $(2+5t)^2+5y=4.$ Como $5y=4-(2+5t)^2$ es equivalente a $5y=4-(2+5t)^2$ resulta para $y_1=-(4t+5t^2)$. Referente a la segunda raíz, $5y=4-(3+5t)^2$ resulta para $y_2=-(1+6t+5t^2)$. El sistema propuesto tiene cuatro soluciones paramétricas que, como sistema indeterminado, genera infinitas soluciones que resumidas resultan:

$$x^2+5y=4\Rightarrow\begin{cases}x_1=2+5t\ \ y_1=-(0+4t+5t^2)\\ x_2=3+5t\ \ y_2=-(1+6t+5t^2)\end{cases}$$

4.3 A partir de la ecuación $5x^2+11x=3$ crear, si es posible, un sistema multidimensional.

La solución a $5x^2+11x-3=0$ es $x=\dfrac{-11\pm\sqrt{11^2-4\cdot5(-3)}}{2\cdot5}=\dfrac{-11\pm\sqrt{181}}{10}$, dos raíces reales.

Para $5x^2+11x-3=0,$ como $3^{(11-1)/2}\equiv1(mód.11),$ la ecuación es transformable en el sistema multivariable $5x^2+11y=3.$

Para la ecuación $5x^2+11x=3.$ Transformamos a una modular $5x^2+11x\equiv3(mód.11)$ que simplificada podemos escribir como $x^2\equiv5(mód.11).$ Esta ecuación tiene dos soluciones, $x_1=4+11t\ y\ x_2=7+11t.$ Por otra parte, la *función Euler* $\varphi(11)=11-1=10,$ soluciones que modifican los exponentes y que escribimos como $e_1=2+10s\ y\ e_2=1+10s.$ Por todo lo expuesto, la ecuación $5x^2+11x\equiv3(mód.11)$ se transforma en un sistema con infinitas soluciones mediante la modificación de los parámetros e y t que podemos escribir como:

$$f(x)=5x^{e_1}+11x^{e_2}\equiv3(mód.11)\ \begin{cases}x_1=4+11t & \begin{cases}e_1=2+10s\\ e_2=1+10s\end{cases}\\ x_2=7+11t\end{cases}$$

Para la ecuación $5x^2+11x=3.$ Transformamos en $5x^2+11y=3,$ una ecuación multivariable.

<u>Despejamos **x** en función de **y**</u>:
Sea $5x^2+11y=3$ que escribimos como $5x^2\equiv3(mód.11).$ Simplificada resulta $x^2\equiv5(mód.11)$ que sabemos tiene como solución $x_1=4+11t\ y\ x_2=7+11t.$

<u>Despejamos **y** en función de **x**</u>:
En la ecuación $5x^2+11y=3,$ sustituyendo los valores de $x,$ obtenemos $5(4+11t)^2+11y=3$ y $5(7+11t)^2+11y=3.$ Ahora, despejamos y en cada una de las ecuaciones:

$$y_1=\frac{-3+5(4+11t)^2}{11}=\frac{-3+5(16+88t+121t^2)}{11}=7+40t+55t^2$$

$$y_2=\frac{-3+5(7+11t)^2}{11}=\frac{-3+5(49+154t+121t^2)}{11}=22+70t+55t^2$$

Por la *función Euler* sabemos que $\varphi(11)=11-1=10,$ con $e_1=2+10s\ y\ e_2=1+10s,$ por tanto, la ecuación $5x^2+11y=3$ puede ser transformada en el siguiente sistema multidimensional:

$$f(x,y)=5x^{e_1}+11y^{e_2}\equiv3(mód.11)\ \begin{cases}x_1=4+11t & y_1=7+40t+55t^2 & \begin{cases}e_1=2+10s\\ e_2=1+10s\end{cases}\\ x_2=7+11t & y_2=22+70t+55t^2\end{cases}$$

4.4 A partir de la ecuación $x^3+7x=6$ crear, si es posible, un sistema multidimensional.

La ecuación $x^3+7x=6$ tendrá solución si, y sólo si 6 es resto cuadrático respecto al módulo 7. Como $6^{(7-1)}\equiv 1(mód.7)$, la ecuación tiene solución en la forma $x^3\equiv 6(mód.7)$.
Utilizando índices, como $3I(x)\equiv \mathrm{I}(6)(mód.6)$ es equivalente a $3I(x)\equiv 3(mód.6)$, que dividida por 3, resulta $I(x)\equiv 1(mód.2)$. Como para $I(x)=1,3,5$ equivalentes a $x=3,6$ y 5, la solución a la ecuación planteada resulta $x_1=3+7t$, $x_2=5+7t$ y $x_3=6+7t$.
Por la *función de Euler* sabemos que $\varphi(7)=6$ de donde $e_1=3+6s$ y $\mathrm{e}_2=1+6s$, por tala ecuación $x^3\equiv 6(mód.7)$ puede ser transformada en un sistema multidimensional como:

$$f(x)=x^{e_1}+7x^{e_2}\equiv 6(mód.7)\begin{cases}x_1=3+7t\\x_2=5+7t\\x_3=6+7t\end{cases}\begin{cases}e_1=3+6s\\e_2=1+6s\end{cases}$$

Para la ecuación $x^3+7y=6$, son válidas las soluciones anteriores de x, por tanto, sustituyendo esos valores en la ecuación, resulta $(3+7t)^2+7y=6$, $(5+7t)^2+7y=6$ y $(6+7t)^2+7y=6$, ecuaciones que tienen para y las siguientes soluciones:

$$y_1=\frac{-6+(3+7t)^3}{7}=3+27t+63t^2+49t^3$$

$$y_2=\frac{-6+(5+7t)^3}{7}=17+75t+105t^2+49t^3$$

$$y_3=\frac{-6+(6+7t)^3}{7}=30+108t+126t^2+49t^3$$

La ecuación $x^3+7y=6$ genera un sistema multivariable y multidimensional de la forma:

$$f(x,y)=x^{e_1}+7y^{e_2}\equiv 6(mód.7)\begin{cases}x_1=3+7t & y_1=3+27t+63t^2+49t^3\\x_2=5+7t & y_2=17+75t+105t^2+49t^3\\x_3=6+7t & y_3=30+108t+126t^2+49t^3\end{cases}\begin{cases}e_1=3+6s\\e_2=1+6s\end{cases}$$

4.5 A partir de la ecuación $7x^{51}+13x^{13}=4$ crear, si es posible, un sistema multidimensional.

Por la *función de Euler* sabemos que $\varphi(13)=12$. La ecuación $7x^{51}+13x^{13}=4$ podemos simplificarla a $7x^{51-12\cdot 4}+13x^{13-12}=4\Rightarrow 7x^3+13x=4$ y resolverla como $7x^3\equiv 4(mód.13)$. Ahora quitamos el coeficiente dependiente de x y obtenemos $x^3\equiv 8(mód.13)$. Observar que $x^3\equiv 2^3(mód.13)$, por tanto $x\equiv 2(mód.13)$. Si utilizamos índices, $3I(x)\equiv \mathrm{I}(8)(mód.12)$ equivalente a $3I(x)\equiv 3(mód.12)$, de donde $I(x)\equiv 1(mód.4)$. Como $I(x)=1,5,9$ y $x=2,6,5$ las soluciones de la ecuación, son $x_1=2+13t$, $x_2=5+13t$ y $x_3=6+13t$.

La ecuación $7x^3+13x=4$ genera un sistema monovariable y multidimensional de la forma:

$$f(x)=7x^{e_1}+13x^{e_2}\equiv 4(mód.13)\begin{cases}x_1=2+13t\\x_2=5+13t\\x_3=6+13t\end{cases}\begin{cases}e_1=3+12s\\e_2=1+12s\end{cases}$$

Sustituyendo en $7x^3+13y=4$ los valores de $x,$ obtenemos:

$$7(2+13t)^3+13y=4\Rightarrow y_1=4+84t+546t^2+1183t^3$$
$$7(5+13t)^3+13y=4\Rightarrow y_2=67+525t+1365t^2+1183t^3$$
$$7(6+13t)^3+13y=4\Rightarrow y_3=116+756t+1638t^2+1183t^3$$

La ecuación $7x^3+13y=4$ genera un sistema multivariable y multidimensional de la forma:

$$f(x,y)=7x^{e_1}+13x^{e_2}\equiv 4(mód.13)\begin{cases}x_1=2+13t,\ \ y_1=\ \ 4+84t+546t^2+1183t^3\\x_2=5+13t,\ \ y_2=\ 67+525t+1365t^2+1183t^3\\x_3=6+13t,\ \ y_3=116+756t+1638t^2+1183t^3\end{cases}\begin{cases}e_1=3+12s\\e_2=1+12s\end{cases}$$

4.6 A partir de la ecuación $x^3+7x^2=6$ crear, si es posible, un sistema multidimensional.

Si resolvemos la ecuación como $x^3+7x^2\equiv 6(mód.7),$ dado que $7x^2$ es múltiplo del módulo, la ecuación tiene como solución $x\equiv 3,5,6(mód.7),$ y los valores de y^2 vendrán determinados por

$$y_1=\pm\left(3+27t+63t^2+49t^3\right)^{1/2},$$
$$y_2=\pm\left(17+75t+105t^2+49t^3\right)^{1/2}$$
$$y_3=\pm\left(30+108t+126t^2+49t^3\right)^{1/2}$$

Que son los valores del supuesto $4.4.$

4.7 A partir de la ecuación $x^{10}+7x^2=4$ crear, si es posible, un sistema multidimensional.

La *función de Euler* determina que $\varphi(7)=6.$ Si resolvemos la ecuación como $x^{10}+7x^2\equiv 4(mód.7),$ dado que $7x^2$ es múltiplo del módulo y que $x^{10-6}=x^4,$ obtenemos una ecuación simplificada de $x^4\equiv 4(mód.7),$ que tiene como solución $x\equiv 3,4(mód.7).$ Sustituyendo estos valores en $x^{10}+7y^2\equiv 4,$ resulta para y^2

$$(3+7t)^4+7y^2=4\Rightarrow y_1=\pm\left(11+108t+378t^2+588t^3+343t^4\right)^{1/2}$$
$$(4+7t)^4+7y^2=4\Rightarrow y_2=\pm\left(36+256t+672t^2+384t^3+343t^4\right)^{1/2}$$

Un sistema multivariable y multidimensional.

4.8 Resolver la ecuación $x^{42}+55y^2=1$.

Si tomamos la ecuación como $x^{42}+55y^2\equiv 1(mód.55)$, dado que $55y^2$ es múltiplo del módulo y éste se factoriza $55=5\cdot 11$, tenemos $x^{42}+55y^2\equiv 1(mód.55)$ que es equivalente a $x^{42}+5y^2\equiv(mód.5)$ y $x^{42}+11y^2\equiv 1(mód.11)$. Si estas ecuaciones tienen solución, también las tendrá la ecuación que las ha generado.

Sea $x^{42}+5y^2\equiv 1(mód.5)$. El término $5y^2$ es múltiplo del módulo y por la *función Euler* sabemos que $\varphi(5)=4$, de donde $x^{42-4\cdot 10}=x^2$, por tanto $x^2\equiv 1(mód.5)$ es la ecuación a resolver y que, como fácilmente se puede comprobar, tiene como soluciones $x\equiv 1,4(mód.5)$.

Sea $x^{42}+11y^2\equiv 1(mód.11)$. El término $11y^2$ es múltiplo del módulo y por la *función Euler* sabemos que $\varphi(11)=10$, de donde $x^{42-10\cdot 4}=x^2$, por tanto $x^2\equiv 1(mód.11)$ es la ecuación a resolver y que tiene como soluciones $x\equiv 1,10(mód.11)$.

Sea $x^{42}+55y^2\equiv 1(mód.55)$. El término $55y^2$ es múltiplo del módulo. Por la *función Euler* sabemos que $\varphi(55)=40$, de donde $x^{42-40}=x^2$, luego $x^2\equiv 1(mód.55)$ es la ecuación a resolver. Por el *teorema chino de restos*, estas soluciones son $x\equiv 1,21,34,54(mód.55)$.

Conocidos los valores de x, los valores de y vendrán determinado mediante sustitución en $x^2-55y^2=1$,(*) esto es:

$$(1+55t)^2-55y^2=1,\ \Rightarrow y_1=\pm\left(0+2t+55t^2\right)^{1/2}$$
$$(21+55t)^2-55y^2=1,\ \Rightarrow y_2=\pm\left(8+42t+55t^2\right)^{1/2}$$
$$(34+55t)^2-55y^2=1,\ \Rightarrow y_3=\pm\left(21+68t+55t^2\right)^{1/2}$$
$$(54+55t)^2-55y^2=1,\ \Rightarrow y_4=\pm\left(53+108t+55t^2\right)^{1/2}$$

(*) Ponemos $55y^2$ en negativo ya que las soluciones que genera son en $\mathbb{Z}$.
Esta ecuación genera un sistema multivariable y multidimensional que podemos identificar como $x^{e_1}+55y^{e_2}\equiv 1(mód.55)$ con $e_1=2+40s$ y $e_2=2+40s$, iguales por pertenecer a exponentes originales iguales pero distintos, ya que pueden ser utilizados de forma independientes.

4.9 A partir de la ecuación $x^3+7y^2+11z=13$ crear, si es posible, un sistema multidimensional.

Dado que se trata de una ecuación con tres variables, la solución debe pasar por tomar dos variables principales, por ejemplo x y y, y una libre, z por tanto, la ecuación podremos plantearla como $x^3+7y^2=13-11z$.

Sea $x^3+7y^2=13-11s(mód.7)$ que reducimos a $x^3=6+3s(mód.7)$.

x recorre el sistema completo de restos respecto al módulo 7.
$6+3s$ debe ser resto cuadrático de x respecto al módulo 7.
z recorre parte del sistema completo de restos respecto a $11\equiv(mód.7)=5$.

Por tanteo obtenemos:

$$\{x=0,\ z=5\},\{x=1,\ z=3\},\{x=2,\ z=3\},\{x=3,\ z=0\}$$
$$\{x=4,\ z=3\},\{x=5,\ z=0\},\{x=6,\ z=0\}$$

Aplicando a la ecuación $x^3=6+3s(mód.7)$, resulta para x las siguientes soluciones:

$$x_1=0+7t,\ x_2=1+7t,\ x_3=2+7t,\ x_4=3+7t,$$
$$x_5=4+7t,\ x_6=5+7t,\ x_7=6+7t.$$

En función de estos resultados, las soluciones de y vendrán determinadas por:

$$(0+7t)^3+7y^2+11\cdot5=13\ \Rightarrow\ y_1=\pm\left\{6+49t^3\right\}^{1/2}$$
$$(1+7t)^3+7y^2+11\cdot3=13\ \Rightarrow\ y_2=\pm\left\{3+3t+21t^2+49t^3\right\}^{1/2}$$
$$(2+7t)^3+7y^2+11\cdot3=13\ \Rightarrow\ y_3=\pm\left\{4+12t+42t^2+49t^3\right\}^{1/2}$$
$$(3+7t)^3+7y^2+11\cdot0=13\ \Rightarrow\ y_2=\pm\left\{2+27t+63t^2+49t^3\right\}^{1/2}$$
$$(4+7t)^3+7y^2+11\cdot3=13\ \Rightarrow\ y_5=\pm\left\{12+48t+84t^2+49t^3\right\}^{1/2}$$
$$(5+7t)^3+7y^2+11\cdot0=13\ \Rightarrow\ y_6=\pm\left\{16+75t+105t^2+49t^3\right\}^{1/2}$$
$$(6+7t)^3+7y^2+11\cdot0=13\ \Rightarrow\ y_7=\pm\left\{29+108t+126t^2+49t^3\right\}^{1/2}$$

10.5 Sistemas criptográficos: Herramientas utilizadas

5.1 Orden multiplicativo.

Si a,m son dos enteros positivos $mcd(a,m)=1$, si $\varphi(m)=e$, entonces $a^e\equiv1(mód.m)$ y se denota como $ord_m=a$. El *orden multiplicativo* de a *módulo* m es el menor entero positivo e que cumple $a^e\equiv1(mód.m)$. Por ejemplo, para determinar el orden multiplicativo de 4 *módulo* 7, $4^2\equiv2(mód.7)$ y $4^3\equiv1(mód.7)$, por lo que $ord_7\,4=3$.
Algunas de las propiedades de los órdenes multiplicativos son:

1. Si $ord_m a=e$, entonces $a^n\equiv1(mód.m)$ sí, y sólo sí $e\mid n$.
2. Si p es primo, entonces $ord_m a\mid p-1$. En particular $ord_m a\mid\varphi(m)$.
3. Si $ord_m a=e$, entonces $a^s\equiv a^t(mód.m)$ sí, y sólo sí $s\equiv t(mód.e)$. Como $mcd(a,m)=1$, esto implica que $a^{|s-t|}\equiv1(mód.m)$.

Referente al ejemplo anterior, como $4^2 \equiv 2(mód.7)$ y $4^3 \equiv 1(mód.7)$, $4^2 \equiv 4^3(mód.7)$ equivalente a $4^2 - 4^3 \equiv 1(mód.7)$.

5.2 Grupo cíclico.

En teoría de grupos, un *grupo cíclico* es un grupo que puede ser generado por un solo elemento; es decir, hay un elemento g del grupo G, llamado "generador" de G, tal que todo elemento de G puede ser expresado como una potencia de g. Si la operación del grupo se denota aditivamente, se dirá que todo elemento de G se puede expresar como ng, para n entero.
En otras palabras, G es cíclico, con un generador g, si $G = \{g^n \mid n \in \mathbb{Z}\}$. Dado que un grupo generado por un elemento de G es, en sí mismo, un subgrupo de G, basta con demostrar que el único subgrupo de G que contiene a g es el mismo G para probar que éste es cíclico.
Por ejemplo, $G = \{e, g^1, g^2, g^3, g^4\}$ es cíclico. De hecho, G es esencialmente igual (esto es, isomorfo) al grupo $\{1,2,3,4\}$ bajo la operación de suma $módulo\ 5$. El isomorfismo se puede hallar fácilmente haciendo $g \to 1$.
Contrariamente a lo que sugiere la palabra "cíclico", es posible generar infinitos elementos y no formar nunca un ciclo real: es decir, que cada g^n sea distinto. Tal grupo sería un *grupo cíclico infinito*, isomorfo al grupo $\mathbb{Z}$ de los enteros bajo la adición.
Salvo isomorfismos, existe exactamente un grupo cíclico para cada cantidad finita de elementos, y exactamente un grupo cíclico infinito. Por lo anterior, los grupos cíclicos son de algún modo los más simples, y han sido completamente clasificados.
Por esto, los grupos cíclicos normalmente se denotan simplemente por el grupo "canónico" al que son isomorfos: si el grupo es de orden n, para n entero, dicho grupo es el grupo $\mathbb{Z}n$ de enteros $\{0,1,\ldots,n-1\}$ bajo la adición $módulo\ n.$. Si es infinito, éste es, como cabe esperarse, $\mathbb{Z}$. Ejemplo, comprobar la relación entre $ord_{13}7.$ y $ord_{13}5$. Como $mcd(5,13) = 1 = mcd(7,13)$, calculamos $5^e, 7^e \equiv 1(mód.13)$, donde e es igual a $5^1, 5^2, 5^3, 5^4 \equiv (mód.13) = 5,12,8,1$, por tanto $5^4 \equiv 1(mód.13)$ y el orden multiplicativo $ord_{13}5 = 4$.
Para $7^1, 7^2, 7^3, 7^4, 7^5, 7^6, 7^7, 7^8, 7^9, 7^{10}, 7^{11}, 7^{12} \equiv (mód.13) = 7,10,5,9,11,12,6,3,8,4,2,1$, por tanto $7^{12} \equiv 1(mód.13)$ y el orden multiplicativo $ord_{13}7 = 12$.
Ejemplo, encontrar todos los elementos de $ord_{21}5$. Como $\varphi(21) = \varphi(3)\varphi(7) = 2 \cdot 6 = 12$, los factores primos de 12, son $\{1,2,3,4,6,12\}$ suficientes para valorar $ord_{21}5$.
Como $5^1, 5^2, 5^3, 5^4, 5^6 \equiv (mód.21) = 5,4,20,16,1$, luego $5^6 \equiv 1(mód.21)$ y $ord_{21}5 = 6$ es el orden multiplicativo.

5.3 Raíz primitiva.

Si g es un entero positivo donde $mcd(g,m) = 1$, g será una raíz primitiva respecto al módulo m, si, y sólo si $ord_m g = \varphi(m)$. Comprobar sí 2 es raíz primitiva de 9.
Tenemos $\varphi(9) = 3^2 - 3^1 = 6$, donde $2^6 \equiv 1(mód.9)$ y $2^k \not\equiv 1(mód.9)$ sí $0 < k < 6$. Como $ord_9 2 = 1,2,3,6$, para $2^1, 2^2, 2^3, 2^6 \equiv (mód.9) = 2,4,8,1$ y para $ord_9 2 = 6$, se puede asegurar que 2 es raíz primitiva de 9. Las raíces primitivas restantes se obtienen calculando los restos r tales que $mcd(r,9) = 1$, en este caso 2 y 5.
Calcular las raíces primitiva de 11. Sea $\varphi(11) = 11 - 1 = 10$ y $mcd(r,10) = 1,3,7,9$. Como $2^1, 2^3, 2^7, 2^9 \equiv (mód.11) = 2,8,7,6$, éstas son las raíces primitivas, respecto al módulo 11.

5.4 Logaritmo discreto.

Si a es entero arbitrario relativamente primo con m, y g es una raíz primitiva de m, entonces existirá entre los número $\{0,1,2,\ldots,\varphi(m)-1\}$, donde $\varphi(m)$ es la función de Euler, un número μ que satisfaga a $a \equiv g^{\mu}(mód.n)$.
El número μ es denominado *logaritmo discreto* de a respecto a la base g módulo m, y se denota como $\mu \equiv \log_g(mód.m)$. Este número es utilizado frecuentemente en sistemas de seguridad y criptografía.
Confeccionar tabla de logaritmos discreto de $\mathbb{Z}_{11}$ sabiendo que las raíces primitivas son $2,6,7\ y\ 8.$

μ	0	1	2	3	4	5	6	7	8	9
$2^{\mu} \equiv (mód.11)$	1	2	4	8	5	10	9	7	3	6

μ	0	1	2	3	4	5	6	7	8	9	10
$\log_2$		0	1	8	2	4	9	7	3	6	5

g / μ	0	1	2	3	4	5	6	7	8	9
2	1	2	4	8	5	10	9	7	3	6
6	1	6	3	7	9	10	5	8	4	2
7	1	7	5	2	3	10	4	6	9	8
8	1	8	9	6	4	10	3	2	5	7

La tabla general de logaritmos discretos respecto a $\mathbb{Z}_{11}$, es

μ / g	$\log_2$	$\log_6$	$\log_7$	$\log_8$
1	0	0	0	0
2	1	9	3	7
3	8	2	4	6
4	2	8	6	4
5	4	7	2	8
6	9	1	7	3
7	7	3	1	9
8	3	6	9	1
9	6	4	8	2
10	5	5	5	5

5.5 Método de los cuadrados repetidos.

Para el cálculo de x^n, cuando n es suficientemente grande, se puede simplificar utilizando la descomposición de n en factores binarios, tales que $n = x^1 + x^2 + x^4 + x^8 + \ldots + x^n$.
Ejemplo: Calcular $19^{21} \equiv r(mód.17)$. Observamos que $19^{21} \equiv 2^{21} \equiv r(mód.17)$ y la descomposición del exponente resulta $21 = 2^4 + 2^2 + 1$. Ahora planteemos la solución de la ecuación $2^{21} \equiv r(mód.17)$ de la siguiente forma:

$$2^1 \equiv 2(mód.17)$$
$$2^2 \equiv 2^2 \equiv 4(mód.17)$$
$$2^4 \equiv 4^2 \equiv 16(mód.17)$$
$$2^8 \equiv 16^2 \equiv 1(mód.17)$$
$$2^{16} \equiv 1^2 \equiv 1(mód.17)$$
$$2^{21} \equiv 2^{16+4+1} \equiv 1 \cdot 16 \cdot 2 \equiv 32 \equiv 15(mód.17)$$

Teniendo en cuenta que, por la función de Euler $\varphi(17) = 17 - 1 = 16,$ la ecuación también se podría haber resuelto como $2^{21} \equiv 2^{21\text{-}16=5} \equiv r(mód.17),$ de donde $2^5 \equiv (mód.17) = 15.$
Ejemplo: Calcular $31^{73} \equiv r(mód.101).$ La descomposición del exponente es $73 = 2^6 + 2^3 + 1$ y la solución la planteamos como:

Exp	**Cuadrados sucesivos**
1	$31^1 \equiv 31(mód.101)$
	$31^2 \equiv 31^2 \equiv 52(mód.101)$
	$31^4 \equiv 52^2 \equiv 78(mód.101)$
8	$31^8 \equiv 78^2 \equiv 24(mód.101)$
	$31^{16} \equiv 24^2 \equiv 71(mód.101)$
	$31^{32} \equiv 71^2 \equiv 92(mód.101)$
64	$31^{64} \equiv 92^2 \equiv 81(mód.101)$
73	$31^{73} \equiv 31^{64+8+1} \equiv 81 \cdot 24 \cdot 31 \equiv 60264 \equiv 68(mód.101)$

La solución de este supuesto sería muy difícil aplicando métodos normales ya que el resultado de $31^{73} = 7402930120435182309838061067999977541338847655293867577988460115733182809088639813666435147650814205274159391$ sería imposible de manejar.

5.6 Matrices.

En criptografía la codificación de mensajes requiere, a veces, la agrupación en bloques de dichos códigos. Esto se puede llevar a cabo utilizando matrices de $2 \text{ x } 2,$ $3 \text{ x } 3$ ó $n \text{ x } n,$ dependiendo del tamaño del mensaje o del enmascaramiento que se quiera hacer de él.
Supongamos el sistema:

$$2 \text{ x } 2, \quad \begin{matrix} ax + by \equiv e(mód.m) \\ cx + dy \equiv f(mód.m) \end{matrix} \Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \equiv \begin{pmatrix} e \\ f \end{pmatrix} (mód.m)$$

para

$$\Delta \equiv ad - bc \equiv \begin{vmatrix} a & b \\ c & d \end{vmatrix} (mód.m),$$

si x_o e y_o son soluciones al sistema:

$$x_o \equiv \Delta^{-1}\left(ed-bf\right) \equiv \Delta^{-1}\begin{vmatrix} a & b \\ f & d \end{vmatrix}(mód.m) \text{ e } y_o \equiv \Delta^{-1}\left(af-cd\right) \equiv \Delta^{-1}\begin{vmatrix} a & e \\ c & f \end{vmatrix}(mód.m)$$

si, y sólo si $mcd(\Delta, m)=1$ con $\Delta \equiv ad-bc(mód.m)$ y $\Delta^{-1} \equiv \dfrac{1}{ad-bc} \equiv \dfrac{1}{\Delta}(mód.m)$, determinante e inversa, respectivamente.
Como ejemplo resolvemos el siguiente supuesto:

$$3x+13y \equiv 8(mód.55)$$
$$5x+21y \equiv 34(mód.55)$$

Para $\Delta \equiv 3\cdot 21-13\cdot 5 \equiv 53(mód.55)$ y $mcd(53,55)=1,$ el sistema tiene una única solución módulo 55. Como $\Delta^{-1} \equiv 27(mód.55)$ obtenemos:

$$x_0 \equiv \Delta^{-1}(de-bf) \equiv 27(21\cdot 8-13\cdot 34) \equiv 27(mód.55)$$
$$y_0 \equiv \Delta^{-1}(af-ce) \equiv 27(3\cdot 34-5\cdot 8) \equiv 24(mód.55)$$

Esto nos lleva a que $x \equiv 27(móm.55)$ e $y \equiv 24(móm.55)$ son las únicas soluciones que satisfacen a la ecuación.
Supongamos ahora un sistema lineal de $3\text{x}3$ de la forma

$$a_1x+b_1y+c_1z \equiv d_1(mód.m)$$
$$a_2x+b_2y+c_2z \equiv d_2(mód.m)$$
$$a_3x+b_3y+c_3z \equiv d_3(mód.m)$$

Este sistema tendrá solución en $mód.\ m$ si, y sólo si $mcd(\Delta, m)=1,$ donde

$$\Delta \equiv \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}(mód.m)$$

y con soluciones de

$$x \equiv \Delta^{-1}\begin{vmatrix} d_1 & b_1 & c_1 \\ d_2 & b_2 & c_2 \\ d_3 & b_3 & c_3 \end{vmatrix}(mód.m),\quad y \equiv \Delta^{-1}\begin{vmatrix} a_1 & d_1 & c_1 \\ a_2 & d_2 & c_2 \\ a_3 & d_3 & c_3 \end{vmatrix}(mód.m) \text{ y } z \equiv \Delta^{-1}\begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{vmatrix}(mód.m)$$

Por ejemplo, resolvemos el siguiente sistema:

$$3x+4y+7z \equiv 8(mód.23)$$
$$5x+6y+2z \equiv 7(mód.23)$$
$$3x+5y+11z \equiv 1(mód.23)$$

Aplicando el procedimiento descrito, obtenemos las siguiente solución al sistema:

$$x=20,\ y=13,\ z=18$$

BIBLIOGRAFIA:

BOLKER, Ethan D., Elementary Number Theory, ISBN: 0-486-45807-5
CRANTZ, Paul, Aritmética y Álgebra, Edición 1926
KOSHY, Thomas, Elementary Number Theory with Applications, ISBN: 978-0-12-372487-8
LANG, Serge, Algebraic Number Theory, ISBN: 0-387-94225-4
NATHANSON, Melvyn B. Elementary Methods in Number Theory, ISBN: 0-387-98912-9
PHILLIPS, BUTTS y SHAUGHNESSY, Álgebra con Aplicaciones, ISBN: 968-6034-93-5
TATTERSALL, James T., Elementary Number Theory in Nine Chapters, ISBN: 0-521-61524-0
VERA LÓPEZ, Antonio y otro, Problemas y Ejercicios de Matemática Discreta, ISBN: 84-605-4351-X

APOYO INTERNET

http://www.akiti.ca/Mathfxns.html (Solución de ecuaciones)
http://www.vadenumeros.es/actividades/division-por-ruffini.htm (Programa matemático)
http://www.vadenumeros.es/actividades/division-por-ruffini.htm (Soluciones Ruffini)
http://www.wolframalpha.com/examples/ (Programa matemático)
http://www.wolframalpha.com/examples/ (Soluciones algebraicas)
http://Hojamat.es
http://es.wikipedia.org/wiki/Ley_de_reciprocidad_cuadr%C3%A1tica
http://es.wikipedia.org/wiki/Residuo_cuadr%C3%A1tico