16. NÚMEROS PRIMOS: Genealogía y Grupos Multiplicativos

16.1 Genealogía Numérica

1.1 Concepto de Familia y de Generación Numérica

Hay un dicho popular que dice que el ser humano no debe estar solo. Es importante que tenga un origen y una familia que garantice, mediante parentescos, el futuro de su estirpe.

En el campo de los números ocurre algo parecido. Los números forman parte de familias, por ejemplo primos o compuesto. Mediante sus formas tienen una continuación a través de las secuencias generadas a partir de estas formas y/o estructuras.

Muchas civilizaciones primitivas compartieron diversos aspectos de la numerología que los pitagóricos llevaron al culto más extremo. Estas civilizaciones, como la de los pueblos mesopotámicos, influenciados por los relatos bíblicos, consideraban a los tres primeros números como símbolos de la creación divina. Para ellos, el número **uno** es el generador de los números y el número de la razón; el número **dos** es el primer número par, duplicación del primero, número masculino y de la opinión, y **tres** es el número femenino y número de la armonía por estar compuesto por la unidad y la diversidad. Según estos conceptos, los números, al igual que los seres humanos, se generan a partir del 2 y del 3, (nuestros primeros padres, según la numerología), formando con otros números primos combinaciones que, dependiendo de sus formas o estructuras, dieron lugar a las primeras o segundas generaciones de los números primos.

1.2 Concepto genealógico de los Números Primos

Todo número primo impar $p,\ p\geq 3,$ puede ser expresado como suma de dos mitades más uno, así $p=q+q+1=2(q)+1,$ donde q es el cociente de la división $p/2,$ demuestra su condición de número impar. Si lo denotamos como $\boxed{x=1+2t}$, $t\in Z,$ es un número algebraico que representa el primer cromosoma de cualquier número primo.

Todo número primo $p,\ p\geq 3,$ puede ser expresado en la forma $p=a(q)+b(q)+r=w(q)+r,\ w\in Z,$ donde q y r son, respectivamente, el cociente y resto de la división $p/w,$ y a,b la descomposición de w en su forma par e impar, esto es $w=a+(a+1)=a+b,$ que es la suma de dos números consecutivos, por tanto $p=a(q)+b(q)+r=w(q)+r$ representado por el algebraico $\boxed{y=r+wt}$, es el segundo cromosoma de p respecto a w.

Entonces, $\boxed{p=q+q+1=a(q)+b(q)+r=w(q)+r}$ forman parte del número impar primo, al igual que los números algebraicos $x=1+2t$ e $y=r+wt$.

Como los números algebraicos $x=1+2t$ e $y=r+wt$ son equivalentes pero independientes, ya que $mcd(2,w)=1,$ al igual que puede ser $mcd(1,r)=1,$ utilizando el Teorema Chino de Restos podemos determinar que $\boxed{z=u+2wt}$ es el único número algebraico que representa al número primo p y, por tanto, su ADN.

Ejemplo: Calcular x e y del número 19 para la 5^{a} generación.

El número 19 puede ser expresado como

$$19=q+q+1=2(q)+1=2(9)+1$$

por tanto, $\boxed{x=1+2t}$.

El número 5 puede ser expresado como

$$5=2+3$$

así, respecto al número 19

$$19=9+9+1=2(q)+3(q)+r=2(3)+3(3)+4=5(3)+4=5q+4$$

de donde $\boxed{y=4+5t}$.

En este caso, los algebraicos $x=1+2t$ e $y=4+5t$ tienen coeficientes independientes distintos, por lo que, mediante la utilización del Teorema Chino de Restos, obtenemos

$$1+2u\equiv 4(mód.5)\rightarrow 2u\equiv 3(mód.5)\rightarrow u\equiv 4(mód.5),\ u\in Z$$

y así

$$z=1+2(4+5t)=9+10t\rightarrow \boxed{z=9+10t}$$

Claramente podemos observar que $z=9+10t$ es una solución de $y=4+5t$, por lo que ambos son equivalentes.

De este número algebraico podemos generar la familia de números que serán antecesores y predecesores del 19, así

$$z=9+10t:\ 19,29,59,79,89,109,139,149,179,199,229,239,269,349,359,\ldots$$

publicados en la secuencia https://oeis.org/A030433, son primos que tienen la particularidad de que si se dividen por 2 dan como resto 1 y si se dividen por 5 dan como resto 4. Sin embargo, cada uno de ellos tiene su propia personalidad, así unos son de la forma $4k+1$ y otros de la forma $4k+3$.

1.3 Concepto de generación numérica

El concepto de generación de los números impares primos tendrá tantas ramificaciones como números tenga el sistema de resto de $\boxed{z=u+2wt}$, ya que u recorre todo el sistema $\{1,3,5,\ldots,2w-1\}$, respecto a $2w$. Así, en el supuesto de que $w=7$, como el sistema completo de restos es $\{1,3,5,\ldots,14-1\}$, los valores que tomaría y, serían

$$z=1+14t,\ z=3+14t,\ z=5+14t,\ z=9+14t, z=11+14t,\ z=13+14t$$

y las representaciones de cada familia

$$z=1+14t:\ 29,43,71,113,127,197,211,239,281,337,379,421,449,\ldots$$

ver https://oeis.org/A042967

$z = 3+14t:\ 3,17,31,59,73,101,157,199,227,241,269,283,311,353,367,\ldots$
ver https://oeis.org/A045437

$z = 5+14t:\ 5,19,47,61,89,103,131,173,229,257,271,313,383,397,439,\ldots$
ver https://oeis.org/A045458

$z = 9+14t:\ 23,37,79,107,149,163,191,233,317,331,359,373,401,443,\ldots$
ver https://oeis.org/A045392

$z = 11+14t:\ 11,53,67,109,137,151,179,193,263,277,347,389,431,487,\ldots$
ver https://oeis.org/A045471

$z = 13+14t:\ 13,41,83,97,139,167,181,223,251,293,307,349,419,433,461,\ldots$
ver https://oeis.org/A045473
números, por otra parte que pueden pertenecer a otras familias, pero no con estos antecesores y predecesores.

1.4 Metodología y análisis

En el ejemplo del apartado anterior hemos empleado un método numérico para determinar los distintos datos del supuesto. El cálculo de $x = 1+2t$ no plantea dificultades pero el de $y = r + wt,$ no sólo puede plantear dificultades sino que puede aportar formas distintas de solución.

Antes de seguir adelante, vamos a presentar el funcionamiento de una herramienta que nos será muy útil en nuestro trabajo.

Si a un número le sumamos y restamos otro número dado menor que él y calculamos la diferencia entre el mayor y el menor, el resultado es el doble del número dado.

Sean $m\ y\ q$ dos números enteros cualquieras, con $m > q.$ Si a la suma de $(m+q)$ le restamos la diferencia de $(m-q),$ resulta $(m+q)-(m-q) = 2q.$

En el caso resuelto anteriormente, si

$$19 = 9+9+1 = (9-5)+(9+5)+1 = 4+14+1$$

entonces

$$19 = 4+14+1 = 2(q)-2+3(q)+5+1 = 5(q)+4,\ q = 3$$

que representa otra forma distinta de estructura aditiva. Efectivamente, si en el caso anterior la función multiplicativa aditiva era

$$f(5q+4) = f(2q) + f(3q) + 4,\ q = 3$$

en el caso actual esta misma función es de resto unidad, ya que

$$f(5q+4) = f(2q-2) + f(3q+5) + 1,\ q = 3$$

La solución también puede ser abordada de forma algebraica, así

$$2q+3q+r = 19 \rightarrow 5q+r = 19 \rightarrow r = 19-5q$$

de donde $r = 4,$ y por sustitución obtener:

$$5q + 4 = 19 \rightarrow q = (19 - 4)/5 = 3$$

Ejemplo: Calcular x e y de 31 para la 7^{a} generación.

Expresamos el número 31 como

$$31 = q + q + 1 = 2(q) + 1 = 2(15) + 1$$

es un número impar y, por tanto, no divisible por 2. Se genera un número de la forma $\boxed{x = 1 + 2t}$.

Como 15 es la mitad del par de 31, $15 = 7 \cdot 2 + 1 = 7q + 1,$ donde $q = 2$ y $k = 2q = 4.$

Sabemos que $31 = 15 + 15 + 1.$ Si los valores de $q\ y\ k$ son, respectivamente 2 y 4, planteamos

$$31 = 15 + 15 + 1 = (15 - 2) + (15 + 2) + 1 = 13 + 17 + 1$$

y, como $k = 4$

$$31 = 13 + 17 + 1 = 3(4) + 1 + 4(4) + 1 + 1 = 7(4) + 3 = 7k + 3$$

que nos genera un número de la forma $\boxed{y = 3 + 7k}$.

Para $31 = 13 + 17 + 1,$ comprobamos este desdoblamiento:

$$13 = 6 + 6 + 1 = 4 + 8 + 1 = (4) + 2(4) + 1 = 3(4) + 1 = 3k + 1$$
$$17 = 8 + 8 + 1 = 2(4) + 2(4) + 1 = 4(4) + 1 = 4k + 1$$

por lo que

$$31 = 3k + 1 + 4k + 1 + 1 = 7k + 3$$

solución coincidente con la obtenida anteriormente.

Queda demostrado que el número 31 no es divisible ni por 2 ni por 7, pero genera dos números con estructuras distintas. Esto nos obliga a buscar un número de la forma $z = r + 14t$ a partir de los números encontrados anteriormente, esto es

$$\left.\begin{matrix} x = 1 + 2k \\ y = 3 + 7k \end{matrix}\right\} \rightarrow z = r + 14t$$

Mediante ecuaciones modulares, resolvemos

$$1 + 2u \equiv 3(mód.7) \rightarrow 2u \equiv 2(mód.7) \rightarrow u \equiv 1(mód.7)$$

$$z = 1 + 2(1 + 7t) = 3 + 14t \rightarrow \boxed{z = 3 + 14t}$$

El número $z=3+14t$ tiene el mismo coeficiente independiente que $y=3+7t$, lo que demuestra que el primero es un valor paramétrico del segundo. Dando valores a t, buscamos números primos que tengan la característica de que si se dividen por 2 o 7, dan como restos 1 o 3, respectivamente.

Veamos algunas representaciones:

$t\rightarrow$	0	1	4	8	10	14	22	28	...
$z=3+7t$	3	17	31	59	73	101	157	199	...

Aquí damos una secuencia más amplia de los primos relacionados con la familia del número 31.

$$z=3+14t:\ 3,17,31,59,73,101,157,199,227,241,269,283,311,353,367,...$$

ver https://oeis.org/A045437

La demostración de que tienen representación como funciones multiplicativas aditivas la encontramos en que

$$f(7q+3)=f(3q)+f(4q)+3,\ q=4$$
$$f(7q+3)=f(3q+1)+f(4q+1)+1,\ q=4$$

El número 73 se puede expresar como

$$73=36+36+1=2(36)+1=2k+1$$

El número 36, mitad del par de 73, genera los valores de $q=3$ y $k=2q=6.$

$$73=36+36+1=(36-3)+(36+3)+1=33+39+1$$
$$73=33+39+1=5(6)+3+6(6)+3+1=11(6)+7=11k+7$$

La comprobación de cada uno de estos números determina que

$$33=16+16+1=13+19+1=2(6)+1+3(6)+1+1=5(6)+3=5k+3$$
$$39=19+19+1=3(6)+1+3(6)+1+1=6(6)+3=6k+3$$

por lo que

$$73=5k+3+6k+3+1=11k+7$$

valor coincidente con el desarrollo anterior.

Como los números generados son $\boxed{x=1+2t}$ e $\boxed{y=7+11t}$, demostramos que el número resultante de la combinación de estos dos números, es un valor paramétrico de $\boxed{y=7+11t}$.

Sea $z=r+22t$ el número generado, entonces

$$1+2u\equiv 7(mód.11)\rightarrow 2u\equiv 6(mód.11)\rightarrow u\equiv 3(mód.11)$$

y, por tanto

$$z=1+2(3+11t)=7+22t\rightarrow \boxed{z=7+22t}$$

Este número es una representación paramétrica de $y=7+11t,$ cuando $t=2.$

La familia a la que pertenece el número 73 tiene la particularidad de que si sus miembros se dividen por 2 o por 11, dan como resto el 1 o el 7, respectivamente.

Veamos algunas representaciones:

$t\rightarrow$	0	2	6	12	20	24	26	30	32	...
$y=7+11t$	7	29	73	139	227	271	293	337	359	...

Aquí damos una secuencia más amplia de los primos relacionados con la familia del número 73.

$$z=7+22t:\ 7,29,73,139,227,271,293,337,359,491,557,601,...$$

ver https://oeis.org/A141854

1.5 Primera generación de números y grupos familiares

Si asumimos que todo número primo impar tiene como cromosomas $x=1+2t$ e $y=r+wt,$ y que estos generan el algebraico $z=u+2wt,$ al que llamaremos ADN, estaremos en disposición de determinar cuáles son las primeras generaciones de primos y los grupos familiares que tiene cada una de estas generaciones.

1.5.1 Primera generación con ADN igual a $z=r+2t$ y un grupo familiar.

Supongamos que no existe el cromosoma $y=r+wt$ y si existe, es de la forma $y=0+t,$ entonces $z=1+2t$ por tanto, un solo grupo familiar al que pertenecerían los primeros números primos:

$$z=1+2t:3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,...$$

que están representados por la secuencia https://oeis.org/A006005 y se conocen como números primos "seguros" debido a su relación con los primos fuertes. Son importantes en la criptografía debido a su uso en técnicas basadas en el logaritmo discreto como intercambio de claves Diffie-Hellman. Si $2p+1$ es un primo seguro, el grupo multiplicativo de los números $módulo(2p+1)$ tiene un subgrupo de orden primo grande.

1.5.2 Segunda generación con ADN igual a $z=r+4t$ y tres grupos familiares.

Si el cromosoma $y=1+2t$ es igual al cromosoma $x=1+2t,$ entonces el ADN es igual a $z=r+4t,$ donde $\{1,2,3\}$ es un grupo que recorre todo el sistema completo de restos respecto a $4t.$ El cromosoma $z=1+4t$ genera un primer grupo familiar al que pertenecen los siguientes números primos:

$$z=1+4t:\ 5,13,17,29,37,41,53,61,73,89,97,101,109,113,137,149,157,...$$

que recoge la secuencia https://oeis.org/A002144 y se conocen como primos pitagóricos o enteros de Gauss, ya que pueden ser representados como suma de dos cuadrados y forman parte del anillo $Z[i]$.

El segundo grupo familiar corresponde al ADN $z=2+4t$, pero como $mcd(2,4)=2\neq 1$, este se genera a partir de $z=1+2t$, equivalente a la primera generación de números primos, estudiada en el apartado anterior.

El tercer grupo familiar corresponde al ADN $z=3+4t$, y a él corresponden los siguientes números primos:

$z=3+4t$: 3,7,11,19,23,31,43,47,59,67,71,79,83,103,107,127,131,139,...

que están representados por la secuencia https://oeis.org/A002145 y se conocen como primos de Gauss, ya que no pueden ser representados como suma de dos cuadrados.

1.5.3 Tercera generación con ADN igual a $z=r+6t$ y cinco grupos familiares.

El primer grupo familiar correspondiente a esta tercera generación es $z=1+6t$ y al él corresponden los siguientes números primos:

$z=1+6t$: 7,13,19,31,37,43,61,67,73,79,97,103,109,127,139,151,157,163,...

El segundo grupo familiar corresponde al ADN $z=2+6t$, pero como $mcd(2,6)=2\neq 1$, los números primos se generan a partir de $z=1+3t$:

$z=1+3t$: 7,13,19,31,37,43,61,67,73,79,97,103,109,127,139,151,157,163,...

que como pueden comprobar, es análoga al primer grupo familiar, ya que son equivalentes los dos algebraicos $z=1+6t$ y $z=1+3t$.

Estos primos están recogidos en la secuencia https://oeis.org/A002476.

El tercer grupo familiar es $z=3+6t$, equivalente a $z=1+2t$ que corresponde al grupo familiar de la primera generación, ya estudiada.

El cuarto grupo familiar es $z=4+6t$, equivalente a $z=2+3t$ al que pertenecen los siguientes números primos:

$z=2+3t$: 2,5,11,17,23,29,41,47,53,59,71,83,89,101,107,113,131,137,149,...

El quinto grupo familiar respecto a esta tercera generación le corresponde como ADN $z=5+6t$, y estos son los números que les pertenecen:

$z=5+6t$: 2,5,11,17, 23,29,41,47,53,59,71,83,89,101,107,113,131,137,149,...

que son equivalentes a los del grupo cuarto.

Estos números están recogidos en la secuencia https://oeis.org/A003627.

1.6 En la quinta generación, calcular el grupo familiar al que pertenece el 67.

La quinta generación tiene como ADN $z = r + 10t$ y nueve grupos familiares.

El número 5 se representa como suma de dos números consecutivos, así $5 = 2 + 3,$ de donde

$$67 = 33 + 33 + 1 = 2(q) + 3(q) + r = 5(q) + r,\ con\ q = 13\ y\ r = 2$$

esto nos lleva a los números algebraicos $x = 1 + 2t$ e $y = 2 + 5t.$

Dado que los coeficientes independientes son distintos, utilizando el Teorema Chino de Restos, obtenemos

$$1 + 2u \equiv 2(mód.5) \rightarrow 2u \equiv 1(mód.5) \rightarrow u \equiv 3(mód.5)$$

de donde el valor de z vendrá determinado por

$$z = 1 + 2(3 + 5t) = 7 + 10t$$

luego, el número 67 pertenece al séptimo grupo familiar de la quinta generación, al que pertenecen los siguientes números primos:

$z = 7 + 10t$: 7,17,37,47,67,97,107,127,137,157,167,197,227,257,277,307,...

que tiene su representación en la secuencia https://oeis.org/A030432.

La función multiplicativa de este grupo familiar, viene dada por:

$$f(10t + 7) = f(2q) + f(3q) + 2,\ con\ t = 6\ y\ q = 13$$

El resto de grupos familiares de la quinta generación, son:

$1^o)\ z = 1 + 10t$: 11,31,41,61,71,101,131,151,181,191,211,241,251,271,281,311,...
$2^o)\ z = 1 + 5t$: 11,31,41,61,71,101,131,151,181,191,211,241,251,271,281,311,...
$3^o)\ z = 3 + 10t$: 3,13,23,43,53,73,83,103,113,163,173,193,223,233,263,283,...
$4^o)\ z = 2 + 5t$: 7,17,37,47,67,97,107,127,137,157,167,197,227,257,277,...
$5^o)\ z = 1 + 2t$: 3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,...
$6^o)\ z = 3 + 5t$: 3,13,23,43,53,73,83,103,113,163,173,193,223,233,263,283,293,...
$7^o)\ z = 7 + 10t$: 7,17,37,47,67,97,107,127,137,157,167,197,227,257,277,307,...
$8^o)\ z = 4 + 5t$: 19,29,59,79,89,109,139,149,179,199,229,239,269,349,359,...
$9^o)\ z = 9 + 10t$: 19,29,59,79,89,109,139,149,179,199,229,239,269,349,359,...

Los grupos 1º y 2º son equivalentes y tienen su representación en la secuencia https://oeis.org/A030430.

Los grupos 3º y 6º son equivalentes y tienen su representación en la secuencia https://oeis.org/A030431.

Los grupos 4º y 7º son equivalentes y tienen su representación en la secuencia https://oeis.org/A030432.

El grupo 5º tiene su representación en la secuencia https://oeis.org/A000040.

Los grupos 8º y 9º son equivalentes y tienen su representación en la secuencia https://oeis.org/A030433.

1.7 Calcular las generaciones y los grupos familiares a los que pertenece el 89.

Si tenemos en cuenta que la raíz cuadrada de 89 está comprendida entre $10^2 > 89 > 9^2$, tenemos

$$89 = q + q + 1 = 4(q) + 5(q) + r = 9(q) + r,\ con\ q = 9\ y\ r = 8$$

de donde $y = 8 + 9t$.

Si $x = 1 + 2t$ es el cromosoma masculino y universal e $y = r + wt$ el femenino, en nuestro caso $y = 8 + 9t$, mediante la utilización del Teorema Chino de Restos unificamos los dos algebraicos $1 + 2u \equiv 8(mód.9) \rightarrow 2u \equiv 7(mód.9) \rightarrow u \equiv 8(mód.9)$ y, por tanto $z = 1 + 2(8 + 9t) = 17 + 18t \rightarrow z = 17 + 18t$ es el ADN del número 89.

El 89 está implicado en nueve generaciones de números. Para conocer los grupos familiares o identitarios, partimos de $x = 1 + 2t$ y calculamos $y = r + wt$, esto nos va a permitir conocer el ADN $z = g + 2wt$, donde g será el grupo familiar.

El proceso es lento pero eficaz:

1ª generación: $89(mód.1) = 0, \rightarrow y = 0 + t, \rightarrow z = 1 + 2t$
2ª generación: $89(mód.2) = 1, \rightarrow y = 1 + 2t, \rightarrow z = 1 + 4t$
3ª generación: $89(mód.3) = 2, \rightarrow y = 2 + 3t, \rightarrow z = 5 + 6t$
4ª generación: $89(mód.4) = 1, \rightarrow y = 1 + 4t, \rightarrow z = 1 + 8t$
5ª generación: $89(mód.5) = 4, \rightarrow y = 4 + 5t, \rightarrow z = 9 + 10t$
6ª generación: $89(mód.6) = 5, \rightarrow y = 5 + 6t, \rightarrow z = 5 + 12t$
7ª generación: $89(mód.7) = 5, \rightarrow y = 5 + 7t, \rightarrow z = 5 + 14t$
8ª generación: $89(mód.8) = 1, \rightarrow y = 1 + 8t, \rightarrow z = 9 + 16t$
9ª generación: $89(mód.9) = 8, \rightarrow y = 8 + 9t, \rightarrow z = 17 + 18t$

Veamos las representaciones secuenciales:

$z = 1 + 2t$: 3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,83,89,...
no tiene registrada secuencia.

$z = 1 + 4t$: 5,13,17,29,37,41,53,61,73,89,97,101,109,113,137,149,...
secuencia https://oeis.org/A002144.

$z = 5 + 6t$: 11,17,23,29,41,47,53,59,71,83,89,101,107,113,131,137,...
secuencia https://oeis.org/A003627.

$z = 1 + 8t$: 17,41,73,89,97,113,137,193,233,241,257,281,313,337,353,...
secuencia https://oeis.org/A007519.

$z = 9 + 10t$: 19,29,59,79,89,109,139,149,179,199,229,239,269,349,359,...
secuencia https://oeis.org/A030433.

$z = 5 + 12t$: 5,17,29,41,53,89,101,113,137,149,173,197,233,257,269,...
secuencia https://oeis.org/A040117.

$z = 5 + 14t$: 5,19,47,61,89,103,131,173,229,257,271,313,383,397,439,...
secuencia https://oeis.org/A045458.

$z = 9 + 16t$: 41,73,89,137,233, 281,313,409,457,521,569,601,617,761,...
secuencia https://oeis.org/A105126.

$z = 17 + 18t$: 17,53,71,89,107,179,197,233,251,269,359,431,449,467,...
secuencia https://oeis.org/A061242.

16.2. Grupos Multiplicativos Permutables

2.1 Concepto de Grupo Multiplicativo

Sean m, a y b tres números enteros cualesquiera donde $m = ab$ con $a < b$ y $mcd(a,b) = 1 = a(\pm s) + b(\pm t),\ s,t \in Z.$

Sean i, j los restos de $x \equiv i(mód.a)$ e $y \equiv i(mód.b),$ donde $mcd(x,a) = 1$ y el $mcd(y,b) = 1.$

Si los valores de x e y pueden ser representados por los algebraicos $x = i + at$ e $y = j + bt,\ t \in Z,$ aplicando el Teorema Chino de Restos, éstos generan otro algebraico de la forma $z = r + abt \rightarrow z = r + mt$ que tiene como solución $z \equiv a(\pm s)i + b(\pm t)\, j(mód.m).$

Ejemplo: Generar un grupo multiplicativo a partir del número 67.

Como $9^2 > 67 > 8^2,$ tomamos $m = a \cdot b = 8 \cdot 9 = 72,\ mcd(8,9) = 1 = 8(-1) + 9(1)$ y $mcd(67,72) = 1,$ que representamos como $z = 67 + 72t, t \in Z.$ Este algebraico es equivalente a

$$x \equiv 67(mód.8) \rightarrow x = 3 + 8t \text{ e } y \equiv 67(mód.9) \rightarrow y = 4 + 9t$$

por tanto

$$67 = 8(-1)4(mód.72) + 9(1)3(mód.72) = 40 + 37$$

que tiene representación multiplicativa como

$$f(67) = f(40) + f(37)$$

Por ejemplo, para $z = 53 + 72t,$ como

$$z = 53 + 72t \rightarrow \begin{cases} x = 5 + 8t \\ y = 8 + 9t \end{cases}$$

podemos establecer que

$$53 = 8(-1)8(mód.72) + 9(1)5(mód.72) = 8 + 45$$

que tiene representación multiplicativa como

$$f(53) = f(8) + f(45)$$

En definitiva, la representación de la función multiplicativa aditiva viene determinada por

$$f(z) = f(x) + f(y)$$

2.2 Concepto de Grupo Multiplicativo Permutable

Referente al supuestos anterior, si partimos de $z = 67 + 72t$ y su desdoblamiento en $x = 3 + 8t$ e $y = 4 + 9t,$ planteamos

$$x = 8(-1)(4 + 9t) \equiv -32 - 72t \equiv 40 + 72t \equiv 40(mód.72)$$
$$y = 9(1)(3 + 8t) \equiv 27 + 72t \equiv 27(mód.72)$$

y, por tanto

$$z = (47 + 72t) \equiv 47(mód.72t) = 40(mód.72) + 27(mód.72)$$

con solución para cualquier valor de t.

La representación multiplicativa vendrá determinada por

$$f(47(mód.72)) = f(40(mód.72)) + f(27(mód.72))$$

En el caso de que $z = 53 + 72t,$ si $x = 5 + 8t$ e $y = 8 + 9t,$ tenemos

$$x = 8(-1)(8 + 9t) \equiv -64 - 72t \equiv 8(mód.72)$$
$$y = 9(1)(5 + 8t) \equiv 45 + 72t \equiv 45(mód.72)$$
$$z = 53 + 72t \equiv 53(mód.72) = 8 + 45(mód.72)$$

con solución para cualquier valor de t.

La representación multiplicativa, resulta

$$f(53(mód.72)) = f(8(mód.72)) + f(45(mód.72))$$

En definitiva, un grupo multiplicativo permutable puede ser expresado como

$$z = (r + mt)(mód.m) = a(\pm s)(j + bt)(mód.m) + b(\pm t)(i + at)(mód.m),\ t \in Z$$

2.3 Construcción de Grupos Multiplicativos .

Supongamos que partimos del número algebraico $z = 7 + 20t,\ t \in Z,$ donde el coeficiente dependiente de t es compuesto. Así $m = ab = 20 = 4 \cdot 5,\ x = i + at = 3 + 4t$ e $y = j + bt = 2 + 5t.$ Como $mcd(4,5) = 1 = 4(-1) + 5(1),$ buscamos todas las parejas $\{i, j\}$ correspondientes a $p,\ mcd(20, p) = 1,\ p \in P.$ Estos números deben estar comprendidos entre $m > p > b.$

La tabla siguiente recoge las parejas $\{i, j\}$ que son coprimos con a, b y $m = 20.$

i/j	1	2	3	4
1		17	13	9
3	11	7		19

De los 6 números que son coprimos con $4,5$ y $20,$ hay 5 que son primos, a saber:

$$7,11,13,17 \text{ y } 19$$

Algunos valores de $z,$ son

$$z = 4(-1)2 + 5\cdot 3 \equiv 12 + 15 \equiv 7(mód.20)$$
$$z = 4(-1)3 + 5\cdot 1 \equiv 8 + 5 \equiv 13(mód.20)$$
$$z = 4(-1)4 + 5\cdot 3 \equiv 4 + 15 \equiv 19(mód.20)\ ´$$

Y algunos valores permutables:

Para $x \equiv 4(-1)(2+5t) \equiv -8 - 20t \equiv 12(mód.20)$
Para $y \equiv 5(1)(3+4t) \equiv 15 + 20t \equiv 15(mód.20)$
Para $z \equiv 7(mód.20) = x \equiv 12(mód.20) + y \equiv 15(mód.20)$

por lo que

$$f(7(mód.20)) = f(12(mód.20)) + f(15(mód.20))$$

Si tenemos en cuenta que $z = p + 20t,$ donde p es cada uno de los elementos del grupo multiplicativo $m = 20,$ $\{7,11,13,17 \text{ y } 19\}$, cada uno de ellos puede generar una familia de números primos, por ejemplo:

$z = 7 + 20t$: 7,47,67,107,127,167,227,307,347,367,467,487,547,587,607,...
están representados por la secuencia https://oeis.org/A141882

$z = 11 + 20t$: 11,31,71,131,151,191,211,251,271,311,331,431,491,571,631,...
están representados por la secuencia https://oeis.org/A141884

$z = 13 + 20t$: 13,53,73,113,173,193,233,293,313,353,373,433,593,613,653,...
están representados por la secuencia https://oeis.org/A141885

$z = 17 + 20t$: 17,37,97,137,157,197,257,277,317,337,397,457,557,577,617,...
están representados por la secuencia https://oeis.org/A141886

$z = 19 + 20t$: 19,59,79,139,179,199,239,359,379,419,439,479,499,599,619,...
están representados por la secuencia https://oeis.org/A141887

Todas estas secuencias fueron publicadas por N.J.A. Sloane en 2008.
Neil James Alexander Sloane, es profesor de la Universidad de Melbourne y uno de los creadores y actual presidente de OEIS (On-Line Encyclopedia of Integer Sequence).
Ver http://en.wikipedia.org/wiki/Neil_Sloane

2.4 A partir de $z = 11 + 40t$ construir un grupo multiplicativo.

Como $m = ab = 40 = 5 \cdot 8,$ dónde $mcd(5,8) = 1 = 5(-3) + 8(2)$ y $mcd(11,40) = 1,$ $z = 11 + 40t$ es un algebraico que puede generar un grupo multiplicativo.

$z = 11 + 40t$ es equivalente a $x = 1 + 5t$ e $y = 3 + 8t,$ y esto es así porque, utilizando el Teorema Chino de Restos, tenemos

$$1 + 5u \equiv 3(mód.8) \rightarrow 5u \equiv 2(mód.8) \rightarrow u \equiv 2(mód.8)$$

que genera nuevamente el valor de z

$$z = 1 + 5(2 + 8t) = 11 + 40t \rightarrow z = 11 + 40t$$

Calculamos los distintos valores:

$$x = 5(-3)(3) \equiv 35(mód.40)$$
$$y = 8(2)(1) \equiv 16(mód.40)$$
$$z = 11(\text{mod}.40) = 35(mód.40) + 16(mód.40)$$

esto nos genera, para $f(z) = f(x) + f(y)$

$$f(11) = f(35(mód\,40)) + f(16(mód\,40)) = 35 + 16 \equiv 51 \equiv 11(mód.40)$$

o, también

$$f(11(mód.40)) = f(35(mód\,40)) + f(16(mód\,40))$$

En cuanto a los valores multiplicativos permutables:

$$x = 5(-3)(3 + 8t) \equiv -15(3 + 8t) \equiv 35(mód.40)$$
$$y = 8(2)(1 + 5t) \equiv 16(1 + 5t) \equiv 16(mód.40)$$
$$z = 35(mód.40) + 16(mód.40) \equiv 35 + 16 \equiv 11(mód.40)$$

que podemos escribir como

$$z = 11(mód.40) = 35(mód.40) + 16(mód.40) \equiv 35 + 16 \equiv 11(mód.40)$$

La tabla siguiente recoge las parejas $\{i, j\}$ que son coprimos con $m = 40,$ es

i/j	1	3	5	7
1		11	21	31
2	17	27	37	
3	33		13	23
4		19	29	39

De los 12 números que son coprimos con $5,8$ y $40,$ hay 8 que son primos, a saber:

$$11,13,17,19,23,29,31 \text{ y } 37$$

Mediante el algebraico $z = p + 40t$, para p $\{11,13,17,19,23,29,31 \text{ y } 37\}$, encontramos las siguientes familias de números primos:

$z = 11 + 40t$: 11,131,211,251,331,491,571,691,811,971,1051,1091,1171,1291,...
ver https://oeis.org/A142187

$z = 13 + 40t$: 13,53,173,293,373,613,653,733,773,853,1013,1093,1213,1373,...
ver https://oeis.org/A142188.

$z = 17 + 40t$: 17,97,137,257,337,457,577,617,857,937,977,1097,1217,1297,...
ver https://oeis.org/A142189.

$z = 19 + 40t$: 19,59,139,179,379,419,499,619,659,739,859,1019,1259,1459,...
ver https://oeis.org/A142190.

$z = 23 + 40t$: 23,103,223,263,383,463,503,743,823,863,983,1063,1103,1223,...
ver https://oeis.org/A142192.

$z = 29 + 40t$: 29,109,149,229,269,349,389,509,709,829,1069,1109,1229, 1429,...
ver https://oeis.org/A142194.

$z = 31 + 40t$: 31,71,151,191,271,311,431,631,751,911,991,1031,1151,1231,...
ver https://oeis.org/A142195.

$z = 37 + 40t$: 37,157, 197,277,317,397,557,677,757,797,877,997,1117,1237,...
ver https://oeis.org/A142197.

Todas estas secuencias fueron publicadas por N.J.A. Sloane en 2008.

2.5 A partir de $z = 13 + 72t$ construir en grupo multiplicativo.

El algebraico $z = 13 + 72t$ genera $x = 5 + 8t$ e $y = 4 + 9t$, donde $m = ab = 72 = 8 \cdot 9$ y $mcd(8,9) = 1 = 8(-1) + 9(1)$.

La tabla siguiente recoge las parejas $\{i, j\}$ que son coprimos con $m = 72$.

i/j	1	2	4	5	7	8
1		65	49	41	25	17
3	19	11	67	59	43	35
5	37	29	13		61	53
7	55	47	31	23		71

De los 21 números que son coprimos con $8,9$ y 72, hay 16 que son primos, a saber:

11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71

Algunos valores de z, son

$$z \equiv 8(-1)4 + 9 \cdot 5 \equiv 40 + 45 \equiv 13(mód.72)$$
$$z \equiv 8(-1)1 + 9 \cdot 5 \equiv 64 + 45 \equiv 37(mód.72)$$
$$z \equiv 8(-1)7 + 9 \cdot 5 \equiv 16 + 45 \equiv 61(mód.72)$$

Todos estos resultados tienen su representación como funciones multiplicativas aditivas.

Como en el algebraico $z = r + 72t$, r recorre el sistema completo de restos respecto a 72, $\{1,3,5,...,72-1\}$, se generan familias de números primos cuando r toma alguno de los siguientes valores: 11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71. Así, para

$z = 11 + 72t$: 83,227,443,587,659,947,1019,1091,1163,1307,1451,1523,1667,1811,...
$z = 13 + 72t$: 13,157,229,373,661,733,877,1021,1093,1237,1381,1453,1597,1669,...
$z = 17 + 72t$: 17,89,233,449,521,593,809,881,953,1097,1601,1889,2393,2609,...
$z = 19 + 72t$: 19,163,307,379,523,739,811,883,1171,1459,1531,1747,2179,2251,...
$z = 23 + 72t$: 23,167,239,311,383,599,743,887,1031,1103,1319,1607,1823,2039,...
$z = 29 + 72t$: 29,101,173,317,389,461,677,821,1109,1181,1613,1901,1973,2333,...
$z = 31 + 72t$: 31,103,463,607,751,823,967,1039,1327,1399,1471,1543,1759,1831,...
$z = 37 + 72t$: 37,109,181,397,541,613,757,829,1117,1549,1621,1693,2053,2269,...
$z = 41 + 72t$: 41,113,257,401,617,761,977,1049,1193,1409,1481,1553,1697,1913,...
$z = 43 + 72t$: 43,331,547,619,691,907,1051,1123,1483,1627,1699,1987,2131,...
$z = 47 + 72t$: 47,191,263,479,839,911,983,1487,1559,1847,2063,2207,2351,2423,..
$z = 53 + 72t$: 53,197,269,557,701,773,1061,1277,1493,1637,1709,1997,2069,...
$z = 59 + 72t$: 59,131,347,419,491,563,1283,1427,1499,1571,1787,1931,2003,...
$z = 61 + 72t$: 61,277,349,421,709, 853,997,1069,1213,1429,1789,1861,1933,2221,...
$z = 67 + 72t$: 67,139,211,283,499,571,643,787,859,1291,1579,1723,1867,2011,...
$z = 71 + 72t$: 71,359,431,503,647,719,863,1151,1223,1367,1439,1511,1583,1871,..

Ninguna de estas familias de números primos encuentra respuesta en el registro de secuencias OEIS.

2.6 Calcular, si lo tiene, el grupo multiplicativo para $m = 28$.

El valor de $m = ab$ se puede expresar como $m = 28 = 2 \cdot 14 = 4 \cdot 7$. En el caso de $28 = 2 \cdot 14$, como el $mcd(2,14) = 2 \neq 1$, no existe grupo multiplicativo. En cuanto a $28 = 4 \cdot 7$, como el $mcd(4,7) = 1 = 4(2) + 7(-1)$, se puede generar grupo multiplicativo con elementos p que sean coprimos con $4,7$ y 28, esto es $mcd(28, p) = 1$. Dichos elementos estarán comprendidos entre $m > p > b$, según la siguiente tabla:

i/j	1	2	3	4	5	6
1		9	17	25	5	13
3	15	23		11	19	27

Hay 10 números que son coprimos con $4,7$ y 28, de los que 6 son primos:

5,11,13,17,19 y 23

Dando valores a r en $z = r + 28t$, obtenemos las siguientes familias de primos:

$z = 5 + 28t$: 5,61,89,173,229,257,313,397,509,593,677,733,761,929,1013,1069,...
ver https://oeis.org/A141967

$z = 9 + 28t$: 37,149,233,317,373,401,457,541,569,653,709,821,877,1129,1213,...
ver https://oeis.org/A141968

$z = 11 + 28t$: 11,67,151,179,263,347,431,487,571,599,683,739,823,907,991,...
ver https://oeis.org/A141969

$z = 13 + 28t$: 13,41,97,181,293,349,433,461,601,769,797,853,881,937,1021,...
ver https://oeis.org/A141970

$z = 15 + 28t$: 43,71,127,211,239,379,463,491,547,631,659,743,827,883,911,...
ver https://oeis.org/A141971

$z = 17 + 28t$: 17,73,101,157,241,269,353,409,521,577,661,773,829,857,941,...
ver https://oeis.org/A141972

$z = 19 + 28t$: 19,47,103,131,271,383,439,467,523,607,691,719,859,887,971,...
ver https://oeis.org/A141973

$z = 23 + 28t$: 23,79,107,163,191,331,359,443,499,751,863,919,947,1031,1087,...
ver https://oeis.org/A141974

$z = 25 + 28t$: 53,109,137,193,277,389,557,613,641,809,977,1033,1061,1117,...
ver https://oeis.org/A141975

$z = 27 + 28t$: 83,139,167,223,251,307,419,503,587,643,727,811,839,1063,1091,...
ver https://oeis.org/A141976

Todas estas secuencias fueron publicadas por N.J.A. Sloane en 2008.

Para $z = 11 + 28t$, $x = 3 + 4t$ e $y = 4 + 7t$, calculamos el grupo multiplicativo de la forma siguiente:

$$x = 4(2)(4) \equiv 32 \equiv 4(mód.28) \rightarrow x = 4(2)(4 + 7t) \equiv 32 \equiv 4(mód.28)$$
$$y = 7(-1)(3) \equiv -21 \equiv 7(mód.28) \rightarrow y = 7(-1)(3 + 4t) \equiv -21 - 28t \equiv 7(mód.28)$$
$$z = 4 + 7 \equiv 11(mód.28)$$

El grupo multiplicativo aditivo podemos expresarlo como:

$$f(11(mód.28)) = f(4(mód.28)) + f(7(mód.28))$$

o lo que es los mismo:

$$f(11) = f(4) + f(7)$$

2.7 A partir de $z = 89 + 90t$, crear un grupo multiplicativo.

Sea $90 = m = ab = 9 \cdot 10$, donde $mcd(9,10) = 1 = 9(-1) + 10(1)$, que permite crear un grupo multiplicativo.

Los valores de x e y se determinan

$$x \equiv 89(mód.9) = 8 \rightarrow x = 8 + 9t \text{ e } y \equiv 89(mód.10) = 9 \rightarrow y = 9 + 10t$$

Los valores de las variables vendrán determinados por:

$$x = 8 + 9t = 9(-1)(9) \equiv -81 \equiv 9(mód.90)$$
$$y = 9 + 10t = 10(1)(8) \equiv 80(mód.90)$$
$$z = 89 + 90t = 9(mód.90) + 80(mód.90) \equiv 89(mód.90)$$

La función multiplicativa resulta:

$$f(89(mód.90)) = f(9(mód.90)) + f(80(mód.90))$$

Los valores de las variables, también pueden ser determinados como:

$$x = 8 + 9t = 9(-1)(9 + 10t) \equiv -81 \equiv 9(mód.90)$$
$$y = 9 + 10t = 10(1)(8 + 9t) \equiv 80(mód.90)$$
$$z = 89 + 90t = 9(mód.90) + 80(mód.90) \equiv 89(mód.90)$$

que tiene la misma representación multiplicativa para cualquier valor de t.

La tabla siguiente recoge las parejas $\{i, j\}$ que son coprimos a, b y $m = 90$.

i/j	1	3	7	9
1		73	37	19
2	11	83	47	29
4	31	13	67	49
5	41	23	77	59
7	61	43		79
8	71	53	17	89

De los 22 números que son coprimos con $9,10$ y $90,$ hay 20 que son primos, a saber:

11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83 y 89

3. Grupos Monovariables Modulares

3.1 Transformaciones lineales sobre los anillos $Zp.$.

Supongamos, que a partir del número 67, transformamos el sistema $5x + 6y = 67$ perteneciente al anillo Z_{11} al anillo Z_{13}. La solución del sistema resulta:

$$5x \equiv 67(mód.6) \rightarrow 5x \equiv 1(mód.6) \rightarrow x \equiv 5(mód.6)$$

que en forma algebraica denotamos como $x = 5 + 6t$. Ahora, por sustitución, calculamos la otra variable:

$$y = \frac{67 - 5(5 + 6t)}{6} = \frac{42 - 30t}{6} = 7 - 5t$$

por lo que, la solución al sistema es $67 = 5(5 + 6t) + 6(7 - 5t),\ t \in Z$ con tantas soluciones como valores se asignen a t.

El número 67 también puede ser representado como

$$67 = 5(q) + 6(q) + r = 11(q) + 1,\ con\ q = 6\ \rightarrow\ z = 1 + 11t$$

Para la transformación al anillo Z_{13}, como $w = a + b = 6 + 7 = 13,$ resulta

$$67 = 6(q) + 7(q) + r = 13(q) + 2,\ con\ q = 5\ \rightarrow\ z = 2 + 13t$$

Los valores de x e y se obtienen a partir de las soluciones del sistema anterior. Así, $x = 5 + 6t,$ ya que sus coeficientes son enteros y menores a 13. Para $y = 7 - 5t,$ como uno de los coeficientes es negativo, tomamos su inverso respecto a 13 y resulta $y = 7 + 8t.$

Ahora estamos en disposición del calcular los valores del grupo.

$$x = 5 + 6t = 5(5 + 6t) \equiv 12 + 4t(mód.13)$$
$$y = 7 + 8t = 6(7 + 8t) \equiv 3 + 9t(mód.13)$$
$$z = 2 + 13t = 12 + 4t(mód.13) + 3 + 9t(mód.13) = (12 + 4t) + (3 + 9t) \equiv 2(mód.13)$$

y la representación en el grupo multiplicativo:

$$f(2 + 13t) = f((12 + 4t)(mód.13)) + f((3 + 9t)(mód.13))$$

ver http://hojamat.es/parra/sistelin.pdf.

En esta exposición descubrimos dos secuencias:

$z = 1 + 11t$: 23,67,89,199,331,353,397,419,463,617,661,683,727,859,881,947,...
registrada como https://oeis.org/A141849.

$z = 2 + 13t$: 3,29,107,211,263,367,419,523,601,653,757,809,887,991,1069,1277,...
registrada como https://oeis.org/A100202.

3.2 Solución de una cuadrática monovariable

Supongamos $3x^2 + 4x + 3 = 0.$ Esta ecuación tiene como solución dos raíces complejas conjugadas $x = (-2 \pm \sqrt{5}i)/3, \in \mathbb{C}.$ Por el Criterio de Euler $a^{(p-1)/2} \equiv 1(mód.p),$ aplicado a nuestro caso $4^{(7-1)/2} \equiv -3 \equiv 4(mód.7)$ donde 4 es resto cuadrático respecto al módulo 7 y, por tanto, los sistemas son equivalentes y transformables.
ver http://hojamat.es/parra/raizprim.pdf.

La ecuación $3x^2 + 4x + 3 = 0(mód.7),$ equivalente a $3x^2 + 4x \equiv 4(mód.7),$ tiene como soluciones $x_1 = 3 + 7t$ y $x_2 = 5 + 7t.$ Cada una de estas soluciones tiene, como representación de la ecuación:

$$3(mód.7) - 4 = 3(2 + 7t)^2 \equiv (mód.7) + 4(2 + 7t) \equiv (mód.7) + 3$$

que tendrá tantas soluciones como valores se le asignen a $t.$

3.3 Transformación de una cuadrática monovariable

A partir de la forma $ax^2+bx+c\equiv 0(mód.p)$, si tenemos en cuenta que para cualquier número primo impar p, $p\geq 3$, $p=a(q)+b(q)+r=w(q)+r$ y $w=a+b$, podemos establecer qué $ax^2+bx+c\equiv 0(mód.w)$, y por tanto

$$a(x)^2+b(x)+c\equiv 0(mód.w)$$

que tendrá solución si, y sólo si c es resto cuadrático respecto a w.

Ejemplo: $7x^2+8x+6\equiv 0(mód.15)$ tiene como solución $x\equiv 4,7,9,12(mód.15)$. Pero, si tenemos en cuenta que el módulo es compuesto, $15=3\cdot 5$, cada uno de estos números generará sus propias soluciones, a saber.

$7x^2+8x+6\equiv 0(mód.3)$ se simplifica como $x^2+2x\equiv 0(mód.3)$ que tiene como soluciones $x\equiv 0,1(mód.3)$.

$7x^2+8x+6\equiv 0(mód.5)$ se simplifica como $2x^2+3x+1\equiv 0(mód.5)$ que tiene como soluciones $x\equiv 2,4(mód.5)$.

Si utilizamos el Teorema Chino de Restos, encontraremos las soluciones respecto al módulo 15.
ver http://hojamat.es/parra/modular.pdf.

Si tomamos $z=7+15t$, tenemos para $x=1+3t$ e $y=2+5t$. Soluciones que pueden comprobar por el desarrollo anterior. Si $m=ab=3\cdot 5$ y $mcd(3,5)=1=3(2)+5(-1)$, esto nos permite crear un grupo multiplicativo.

$$x=1+3t=3(2)(2+5t)\equiv 12(mód.15)$$
$$y=2+5t=5(-1)(1+3t)\equiv 10(mód.15)$$
$$z=7+15t=12+10\equiv 22\equiv 7(mód.15)$$

La representación multiplicativa de este grupo, es

$$f(7+15t)=f(12(mód.15))+f(10(mód.15))$$

$z=7+15t$: 7,37,67,97,127,157,277,307,337,367,397,457,487,547,577,607,727,...
secuencia registrada como https://oeis.org/A132231.

3.4 Resolver $5x^2+6x+1\equiv 0(mód.11)$.

Resolvemos $5x^2+6x+1\equiv 0(mód.11)$, que es equivalente a $5x^2+6x\equiv 10(mód.11)$ y tiene como soluciones $x\equiv 2,10(mód.11)$. La representación algebraica de estos resultados es $x_1=2+11t$ y $x_2=10+11t$ por tanto:

$$5(2+11t)^2+6(2+11t)\equiv 10(mód.11)$$
$$5(10+11t)^2+6(10+11t)\equiv 10(mód.11)$$

Los grupos multiplicativos, resultan para $z=2+11t$:

$$x = 9+11t = 5(2+11t)^2 \equiv 605t^2+220t+20 \equiv 9(mód.11)$$
$$y = 1+11t = 6(2+11t) \equiv 66t+12 \equiv 1(mód.11)$$
$$z = 10+11t = 9+1 \equiv 10(mód.11)$$

de donde $f(10+11t) = f(5(2+11t)^2)(mód.11)) + f(6(2+11t)(mód.11))$.

Y para $z = 10+11t$:

$$x = 5+11t = 5(10+11t)^2 \equiv 605t^2+1100t+500 \equiv 5(mód.11)$$
$$y = 5+11t = 6(10+11t) \equiv 66t+60 \equiv 5(mód.11)$$
$$z = 10+11t = 5+5 \equiv 10(mód.11)$$

de donde

$$f(10+11t) = f(5(10+11t)^2(mód.11)) + f(6(10+11t)(mód.11))$$

Estos dos algebraicos generan los siguientes grupos familiares de números primos:

$x_1 = 2+11t$: 2,13,79,101,167,211,233,277,409,431,541,563,607,673,739,761,... secuencia registrada https://oeis.org/A090187.

$x_2 = 10+11t$: 43,109,131,197,241,263,307,373,439,461,571,593,659,769,857,... secuencia registrada https://oeis.org/A141857.

3.5 Resolver $6x^2+7x+3 \equiv 0(mód.31)$.

La solución de $6x^2+7x+3 \equiv 0$, utilizando el programa Máxima*, resulta ser

$$x = \frac{-7 \pm \sqrt{23}\,i}{12}$$

dos raíces conjugadas e imaginarias.

La solución de $6x^2+7x \equiv 28(mód.31)$, es $x \equiv 11,24(mód.31)$ que algebraicamente podemos representar como $x_1 = 11+31t$ y $x_2 = 24+31t$.

Para el algebraico $x_1 = 11+31t$, los grupos multiplicativos resultan:

$$z = 28+31t = 6(11+31t)^2+7(11+31t) \equiv 28(mód.31)$$

de donde

$$x = 13+31t = 6(11+31t)^2 \equiv 5766t^2+4092t+726 \equiv 13(mód.31)$$
$$y = 15+31t = 7(11+31t) \equiv 217t+77 \equiv 15(mód.31)$$
$$z = 28+31t = 6(24+31t)^2+7(24+31t) \equiv 28(mód.31)$$

y la multiplicativa $f(28+31t) = f(6(24+31t)^2(mód.31)) + f(7(24+31t)(mód.31))$.

Para el algebraico $x_2 = 24+31t$, los grupos multiplicativos resultan:

$$6(24+31t)^2+7(24+31t)+3 \equiv 0(mód.31)$$

de donde

$$x = 15+31t = 6(24+31t)^2 \equiv 5766t^2+8928t+3456 \equiv 15(mód.31)$$
$$y = 13+31t = 7(24+31t) \equiv 217t+168 \equiv 13(mód.31)$$
$$z = 28+31t = (15+31t)+(13+31t) \equiv 28(mód.31)$$

y la multiplicativa $f(28+31t) = f((15+31t)(mód.31)) + f((13+31t)(mód.31))$.

Aquí se generan las siguientes secuencias de números primos:

$y = 13+31t$: 13,137,199,509,571,757,881,1129,1439,1811,1873,1997,2617,...
registrada como https://oeis.org/A142017.

$x = 15+31t$: 139, 263,449,821,883,1069,1193,1627,1999,2309,2371,2557,...
registrada como https://oeis.org/A142019.

$z = 28+31t$: 59,307,431,617,1051,1237,1361,1423,1609,1733,2477,2539,2663,...
registrada como https://oeis.org/A142032.

El número 31, en función de 13, podemos representarlo como:

$$31 = 6(q)+7(q)+r = 13(q)+5,\ con\ q = 2 \rightarrow z = 5+13t$$

Como $z = 5+13t$ genera una familia de números primos, tales que:

$z = 5+13t$: 5,31,83,109,239,317,421,499,577,733,811,863,941,967,1019,1097,...
registrada como https://oeis.org/A102732, en cuya secuencia se encuentra el número 31, podemos establecer que, para $z = 5+13t$:

$$x = 11+13t = 6(11+13t)^2 \equiv 1014t^2+1716t+726 \equiv 11(mód.13)$$
$$y = 12+13t = 7(11+13t) \equiv 91t+77 \equiv 12(mód.13)$$
$$z = 10+13t = 6(11+13t)^2+7(11+13t) \equiv 10(mód.13)$$

y la función multiplicativa $f(10+13t) = f(6(11+13t)^2(mód.13)) + f(7(11+13t)(mód.13))$.

Dejamos el resto de funciones multiplicativas en manos del lector.

*descargar gratis http://descargar.portalprogramas.com/Maxima.html.

Secuencias generadas por los siguientes algebraicos:

$z = 10+13t$: 23,101,127,179,257,283,439,491,569,647,673,751,829,881,907,1063,...
secuencia registrada como https://oeis.org/A140375.

$x = 11+13t$: 11,37,89,167,193,271,349,401,479,557,661,739,947,1051,1103,1129,...
secuencia registrada como https://oeis.org/A140373.

$y=12+13t$: 103,181,233,311,337,389,467,571,701,727,857,883,1013,1039,1091,... secuencia registrada como https://oeis.org/A141859.

3.6 Resolver $5x^2+13x+1\equiv 0(mód.17^2)$.

La ecuación $5x^2+13x+1\equiv 0(mód.17^2)$ tendrá solución si y sólo si la tiene:

$$5x^2+13x+1\equiv 0(mód.17)$$

Para $5x^2+13x+1\equiv 0(mód.17)$ las soluciones son:

$$x_1=3+17t \text{ y } x_2=8+17t$$

Los valores de estas raíces, para la ecuación y su derivada, son:

$$f_{(x)}=5x^2+13x+1\begin{cases}f_{(3)}=85\\ f_{(8)}=425\end{cases} \text{ y } f'_{(x)}=10x+13\begin{cases}f'_{(3)}=43\\ f'_{(8)}=93\end{cases}$$

Aplicando estos valores a la ecuación $f(x)+f'(x)\cdot p\cdot t_1\equiv 0(mód.p^n)$, resulta:

$$85+43\cdot 17t\equiv 0(mód.17^2)$$

que dividido por 17 obtenemos $5+43t\equiv 0(mód.17)$.

Despejando t, $t\equiv 7(mód.17)$ resulta para x:

$$x=3+17(7+17t)=122+17t^2$$

Ahora

$$425+93\cdot 17t\equiv 0(mód.17^2)$$

que divido por 17, $25+93t\equiv 0(mód.17)$.

Despejando t, $t\equiv 16(mód.17)$. Luego para x resulta:

$$x=8+17(16+17t)=280+17t^2$$

Las soluciones a la ecuación propuesta, son

$$x\equiv 122,280(mód.17^2)$$

ver http://hojamat.es/parra/cuadraticas.pdf.

Para $5x^2+13x+1\equiv 0(mód.17)$ equivalente a $5x^2+13x\equiv 16(mód.17)$, los valores de las variables, son:

$$x=3+17t=5(3+17t)^2\equiv 11(mód.17)$$
$$y=3+17t=13(3+17t)\equiv 5(mód.17)$$
$$z=16+17t=11+5\equiv 16(mód.17)$$

por lo que la función multiplicativa viene determinada por

$$f(16(mód.17)) = f(11(mód.17)) + f(5(mód.17))$$

Para $5x^2+13x+1\equiv 0(mód.17^2)$ equivalente a $5x^2+13x\equiv 288(mód.17^2)$, los valores de las variables, son:

$$x = 280+17^2t = 5(3+17^2t)^2 \equiv 116(mód.17^2)$$
$$y = 280+17^2t = 13(280+17^2t) \equiv 172(mód.17^2)$$
$$z = 288+17^2t = 116+172 \equiv 288(mód.17^2)$$

por lo que la función multiplicativa viene determinada por

$$f(288(mód.17^2)) = f(116(mód.17^2)) + f(172(mód.17^2))$$

16.4. Grupos Multivariables Modulares

4.1 Transformación de una cuadrática multivariable

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 si, y sólo si, c es resto cuadrático de ax^2 respecto al $módulo\ b$.
ver http://hojamat.es/parra/cuadraticas.pdf.

4.2 Resolver $6x^2+7y\equiv 3(mód.13)$.

La solución sobre el anillo Z_{13} o modular, es la siguiente:

$$x \equiv 0,1,2,3,4,5,6,7,8,9,10,11,12(mód.13)$$
$$y \equiv 6,7,10,2,9,5,3,3,5,9,2,10,7(mód.13)$$

Generalmente los valores de la variable x recorren todo el sistema completo de restos respecto al módulo 13. Los valores de y se obtienen por sustitución. Por ejemplo, para la pareja $x=3+13t$ e $y=2+13t$, planteamos:

$$6\cdot 3^2+7y\equiv 54+7y\equiv 2+7y\equiv 3(mód.13)\rightarrow 7y\equiv 1(mód.13)\rightarrow y\equiv 2(mód.13)$$

Para los valores de las variables:

$$x = 3+13t = 6(3+13t)^2 \equiv 2(mód.13)$$
$$y = 2+13t = 7(2+13t) \equiv 1(mód.13)$$
$$z = 3+13t = 6(3+13t)^2+7(2+13t) \equiv 1+2 \equiv 3(mód.13)$$

En general, la función multiplicativa vendrá determinada por:

$$f(3+13t) = f(6(3+13t)^2 (mód.13)) + f(7(2+13t)(mód.13))$$

La solución algebraica de la función multivariable $6x^2+7y=3$ resultan

$$x_1 = 2+7t,\ \ x_2 = 5+7t \text{ e } y_1 = 3+24t+42t^2,\ \ y_2 = 4+60t+42t^2$$

ver http://hojamat.es/parra/raizprim.pdf.

Para los valores de las variables:

$$x = 6(2+7t)^2 = 294t^2+168t+24$$
$$y = 7(3+24t+42t^2) = 294t^2+168t+21$$
$$z = (294t^2+168t+24)-(294t^2+168t+21) = 24-21 = 3$$

y la función multiplicativa vendrá determina por

$$f(3+7t) = f(6(2+7t)^2) + f(7(-(3+24t+42t)))$$

Dejamos al lector la comprobación de las doce soluciones restantes de este sistema.

4.3 Resolver $8x^2+9y \equiv 11(mód.17)$.

Algunas de las soluciones de este sistema son:

x	$\equiv$	0	1	2	3	4	5	6	7	8	9	... $(mód.17)$
y	$\equiv$	5	6	9	14	4	13	7	3	1	1	... $(mód.17)$

$$x_1 = 4+9t,\ \ y_1 = 13+64t+72t^2$$
$$x_2 = 5+9t,\ \ y_1 = 21+80t+72t^2$$

Para $x = 3+17t$ e $y = 14+17t$, tenemos:

$$x = 3+17t = 8(3+17t)^2 \equiv 4(mód.17)$$
$$y = 14+17t = 9(14+17t) \equiv 7(mód.17)$$
$$z = 11+17t = 4+7 \equiv 11(mód.17)$$

de donde la función multiplicativa viene determinada por

$$f(11(mód17)) = f(4(mód.17)) + f(7(mód.17))$$

Para $x_1 = 4+9t$ e $y_1 = 13+64t+72t^2$, tenemos:

$$x = 4+9t = 8(4+9t)^2 \equiv 2(mód.9)$$
$$y = 13+64t+72t^2 = 9(13+64t+72t^2) \equiv 0(mód.9)$$
$$z = 11+9t = 2+0 \equiv 2(mód.9)$$

y la función multiplicativa la expresamos como

$$f(2(mód.9)) = f(2(mód.9)) + f(0(mód.9))$$

4.4 **Resolver** $7x^2 + 10y \equiv 438(mód.31)$.

El sistema planteado es equivalente a $7x^2 + 10y \equiv 4(mód.31)$, que tendrá solución algebraica si y sólo si, 4 es resto cuadrático respecto al módulo 10. Y es cierto, ya que dicho sistema viene determinado por el grupo $\{1,4,9,6,5,6,9,4,1\}$, donde uno de los elementos es el 4. La solución algebraica es, por tanto:

$$x_1 = 2 + 10t \text{ e } y_1 = 41 + 28t + 70t^2$$
$$x_2 = 8 + 10t \text{ e } y_2 = 1 + 112t + 70t^2$$

Los valores de las variables son:

$$x = 2 + 10t = 7(2 + 10t)^2 \equiv 8(mód.10)$$
$$y = 41 + 28t + 70t^2 = 10(41 + 28t + 70t^2) \equiv 0(mód.0)$$
$$z = 438 + 10t = 8 + 0 \equiv 8(mód.10)$$

y la función multiplicativa:

$$f(8(mód.10)) = f(8(mód.10)) + f(0(mód.10))$$

Observen que el valor de y se produce por sustitución, por tanto su valor modular es cero, ya que es producto del propio módulo.

En cuanto a la solución modular, si tenemos en cuenta que los valores de x recorren todo el sistema completo de restos respectos al módulo 31, obtendremos 31 soluciones probables. Por ejemplo, la última $x = 30 + 31t$ e $y = 9 + 31t$ nos proporciona:

$$x = 30 + 31t = 7(30 + 31t)^2 \equiv 7(mód.31)$$
$$y = 9 + 31t = 10(9 + 31t) \equiv 28(mód.31)$$
$$z = 438 + 31t = 7 + 28 \equiv 4(mód.31)$$

y la función multiplicativa:

$$f(4(mód.31)) = f(7(mód.31)) + f(28(mód.31))$$

4.5 **Resolver** $5x^2 + 17y \equiv 31(mód.77)$.

Este sistema tendrá solución si y sólo si lo tiene con los módulos 7 y 11. Y dado que la tiene en ambos casos, el sistema tiene 76 soluciones para x, que recorren todo el sistema completo de restos respecto al módulo 77, esto es $\{0,1,2,3,...,73,74,75,77-1\}$.

Para $x = 23+77t$ e $y = 41+77t,$ obtenemos los siguientes valores de las variables:

$$x = 23+77t = 5(23+77t)^2 \equiv 27(mód.77)$$
$$y = 41+77t = 17(41+77t) \equiv 4(mód.77)$$
$$z = 31+77t = 27+4 \equiv 31(mód.77)$$

y la función multiplicativa:

$$f(31(mód.77)) = f(27(mód.77)) + f(4(mód.77))$$

Si tenemos en cuenta que $x = 23+77t$ es equivalente a $x_1 = 2+7t,\ x_2 = 1+11t$ e $y = 41+77t$ es equivalente a $y_1 = 6+7t,\ y_2 = 8+11t,$ tenemos:

$$x = 23+7t = 5(2+7t)^2 \equiv 6(mód.7)$$
$$y = 41+7t = 17(6+7t) \equiv 4(mód.7)$$
$$z = 31+7t = 6+4 \equiv 3(mód.7)$$

y la función multiplicativa:

$$f(3(mód.7)) = f(6(mód.7)) + f(4(mód.7))$$

Dejamos en manos del lector la búsqueda de nuevas soluciones en los distintos niveles de este sistema multivariable.

16.5. Grupos Multidimensionales Modulares

5.1 Transformación de una cuadrática multidimensional

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 si, y sólo si, c es resto cuadrático de ax^2 respecto al *módulo b*.

Supongamos $x^2 + 5x = 2,$ que 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 si, y sólo si, 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.

5.2 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 $x = \dfrac{-11 \pm \sqrt{11^2 - 4 \cdot 5(-3)}}{2 \cdot 5} = \dfrac{-11 \pm \sqrt{181}}{10},$ dos raíces reales.

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

Para la ecuación $5x^2+11x=3$. Transformamos a una modular $5x^2+11x\equiv 3(mód.11)$ que simplificada podemos escribir como $x^2\equiv 5(mód.11)$. 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 $5x^2+11x\equiv 3(mód.11)$ se transforma en un sistema con infinitas soluciones mediante la modificación de los parámetros e y t que podemos escribir como:

$$f(x)=5x^{e_1}+11x^{e_2}\equiv 3(mód.11)\ \begin{cases} x_1=4+11t & \begin{cases} e_1=2+10s \\ e_2=1+10s \end{cases} \\ x_2=7+11t & \end{cases}$$

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

Despejamos **x** en función de **y**:

Sea $5x^2+11y=3$ que escribimos como $5x^2\equiv 3(mód.11)$. Simplificada resulta $x^2\equiv 5(mód.11)$ que sabemos tiene como solución $x_1=4+11t\ y\ x_2=7+11t$.

Despejamos **y** en función de **x**:

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:

$$f(x,y)=5x^{e_1}+11y^{e_2}\equiv 3(mód.11)\ \begin{cases} x_1=4+11t\ \ y_1=\ 7+40t+55t^2 & \begin{cases} e_1=2+10s \\ e_2=1+10s \end{cases} \\ x_2=7+11t\ \ y_2=22+70t+55t^2 & \end{cases}$$

Las soluciones paramétricas de las variables para este sistema podemos representarlas como:

$$f(x,y)=5(4+11t)^2+11(-(7+40t+55t^2))=3$$
$$f(x,y)=5(7+11t)^2+11(-(22+70t+55t^2))=3$$

que serán tantas como valores se le asignen a t.

Las soluciones paramétricas exponenciales podemos representarlas como:

$$f(x,y)=5x^{e_1}+11y^{e_2}\equiv 3(mód.11)$$

que serán tantas como valores se le asignen a e_1 y a e_2, indistintamente. Por ejemplo, el sistema $5x^{22}+11y^{31}\equiv 3(mód.11)$ es equivalente a $5x^2+11y\equiv 3(mód.11)$. En ambos casos la solución es $x_1=4+11t$ *y* $x_2=7+11t$ para x.

5.3 **A partir de la ecuación $4x^2+17y+12=0$, crear, si es posible, un sistema multidimensional sobre el anillo $\mathbb{Z}_{23}$.**

La ecuación $4x^2+17y+12=0$ es equivalente a $4x^2+17y\equiv 11(mód.23)$ sobre el anillo $\mathbb{Z}_{23}$.

La solución de esta ecuación no plantea ningún tipo de dificultad, ya que los valores de x serán todos aquellos que conformen el sistema completo de restos, desde el 0 hasta el 22. En cuanto a los valores de y, en función de los de x se pueden obtener fácilmente.

Supongamos que $x=13+23t$ e $y=15+23t$ es una de las soluciones del sistema. Los valores de las variables vendrán determinados por:

$$x=13+23t=4(13+23t)^2\equiv 9(mód.23)$$
$$y=15+23t=17(15+23t)\equiv 2(mód.23)$$
$$z=11+23t=9+2\equiv 11(mód.23)$$

y la función multiplicativa:

$$f(11(mód.23))=f(9(mód.23))+f(2(mód.23))$$

Por la *función Euler* $\varphi(23)=23-1=22$, se modifican los exponentes de x e y, respectivamente, en $e_1=2+22s$ *y* $e_2=1+22s$. Por tanto, la función multidimensional generada podemos representarla como :

$$f(x,y)=4x^{e_1}+17y^{e_2}\equiv 11(mód.23)\ \begin{cases} x=13+23t & \begin{cases} e_1=2+22s \\ e_2=1+22s \end{cases} \\ y=15+23t & \end{cases}$$

así, $4x^{46}+17y^{67}\equiv 11(mód.23)$ tiene las mismas soluciones que $4x^2+17y\equiv 11(mód.23)$.

$$x=13+23t=4(13+23t)^{46}\equiv 9(mód.23)$$
$$y=15+23t=17(15+23t)^{67}\equiv 2(mód.23)$$
$$z=11+23t=9+2\equiv 11(mód.23)$$

5.4 **A partir de la ecuación $6x^{66}+7y^{33}=13$ crear, si es posible, un sistema multidimensional sobre el anillo $\mathbb{Z}_{51}$.**

La *función de Euler* $\varphi(51)=51\big((2/3)(16/17)\big)=32$ por lo que los exponentes de x e y vendrán determinados por $e_1=2+32s$ *y* $e_2=1+32s$, respectivamente. Así, los exponentes indicados se forman como $e_1=2+32\cdot 2=66$ *y* $e_2=1+32\cdot 1=33$.

Una de las muchas soluciones es $x=37+51t$ e $y=16+51t$ que generan los siguientes valores para las variables:

$$x = 37 + 51t = 6(37 + 51t)^{66} \equiv 3(mód.51)$$
$$y = 16 + 51t = 7(16 + 51t)^{33} \equiv 10(mód.51)$$
$$z = 13 + 51t = 2 + 10 \equiv 13(mód.51)$$

Pero el módulo se factoriza como $51 = 3 \cdot 17,$ luego la solución anterior podemos escribirla como $x = 1 + 3t,\ x = 3 + 17t$ e $y = 1 + 3t,\ y = 16 + 17t.$

Calculamos los valores de las variables:

$$x = 3 + 17t = 6(3 + 17t)^2 \equiv 3(mód.17)$$
$$y = 16 + 17t = 7(16 + 17t) \equiv 10(mód.17)$$
$$z = 13 + 17t = 3 + 10 \equiv 13(mód.17)$$

En este caso, los exponentes parametrizados serían $e_1 = 2 + 16s\ y\ \mathrm{e}_2 = 1 + 16s.$

5.5 A partir de la ecuación $11x^3 + 12y^2 = 19$ crear, si es posible, un sistema multidimensional sobre el anillo $\mathbb{Z}_{23^2}$.

Escribimos la ecuación como $11x^3 + 12y^2 \equiv 19(mód.23^2)$ y tomamos la última solución que resulta ser $x = 523 + 23^2 t$ e $y = 288 + 23^2 t.$ Ahora calculamos los valores de las variables:

$$x = 523 + 23^2 t = 11(523 + 23^2 t)^3 \equiv 269(mód.23^2)$$
$$y = 288 + 23^2 t = 12(288 + 23^2 t)^2 \equiv 279(mód.23^2)$$
$$z = 19 + 23^2 t = 269 + 279 \equiv 19(mód.23^2)$$

que genera la siguiente función multiplicativa:

$$f(19(mód.23^2)) = f(269(mód.23^2)) + f(279(mód.23^2))$$

Por la función de Euler $\varphi(23^2) = 23(23-1) = 506,$ lo que nos permite paremetrizar los exponentes como $e_1 = 3 + 506s\ y\ \mathrm{e}_2 = 2 + 506s$ y obtener los sistemas multidimensionales:

$$f(x,y) = 11x^{e_1} + 12y^{e_2} \equiv 19(mód.23) \begin{cases} x = 17 + 23t \\ y = 12 + 23t \end{cases} \begin{cases} e_1 = 3 + 22s \\ e_2 = 2 + 22s \end{cases}$$

$$f(x,y) = 11x^{e_1} + 12y^{e_2} \equiv 19(mód.23^2) \begin{cases} x = 523 + 23^2 t \\ y = 288 + 23^2 t \end{cases} \begin{cases} e_1 = 3 + 506s \\ e_2 = 2 + 506s \end{cases}$$

Dejamos en manos del lector buscar algunas de las muchas soluciones que plantean estos sistemas.

BIBLIOGRAFÍA

AIGNER y ZIEGLER, El Libro de las Demostraciones, ISBN: 84-95599-95-3
ALACA and KENNETH, Introductory Algebraic Number Theory, ISBN: 0-521-54011-9
APOSTOL, Tom M., Introducción a la Teoría Analítica de Números, ISBN: 84-291-5006-4
AYRES, Frank Jr., Álgebra Moderna, ISBN: 968-422-917-8
BOLKER, Ethan D., Elementary Number Theory, ISBN: 0-486-45807-5
COHN, Harvey, Advanced Number Theory, ISBN: 0-486-64023-X
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
STOPPLE, Jeffrey, A Primer of Analytic Number Theory, ISBN: 0-521-01253-8
TATTERSALL, James T., Elementary Number Theory in Nine Chapters, ISBN: 0-521-61524-0
ZALDÍVAR, Felipe, Introducción a la Teoría de Grupos, ISBN: 968-36-3591-1

AYUDA INTERNET

http://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n
http://es.wikipedia.org/wiki/Ley_de_reciprocidad_cuadr%C3%A1tica
http://es.wikipedia.org/wiki/Residuo_cuadr%C3%A1tico
http://Hojamat.es
http://lombok.demon.co.uk/mathToolkit/group/multiplicative (Orden multiplicativo de un grupo)
http://mathworld.wolfram.com/ (Todo el saber sobre Matemáticas (en inglés))
http://maxima.programas-gratis.net/ (Programa de Matemáticas gratis, que puedes descargar e instalar)
http://www.akiti.ca/Mathfxns.html (Solución de ecuaciones)
http://www.branchingnature.org/Teoria_Grupos_Anillos_Dario_Sanchez_2004.pdf (Trabajo del profesor José Darío Sánchez Hernández, que recomendamos)
http://www.numbertheory.org/php/php.html#quadratic_residues (Programa teoría de números)
http://www.vadenumeros.es/actividades/division-por-ruffini.htm (Soluciones Ruffini)
http://www.wolframalpha.com/examples/ (Soluciones algebraicas)