Universidad de Granada

Ejercicios resueltos Álgebra I

Doble Grado de Informática y Matemáticas

Curso 2016/17

1. Relación 1

1.1. Ejercicio 3

¿Cuál de los siguientes conjuntos son subanillos de los anillos indicados?

1. $a \in \mathbb{Q} | 3a \in \mathbb{Z} \subseteq \mathbb{Q}$,
2. $m + 2n\sqrt{3} |\ m, n \in \mathbb{Z} \subseteq \mathbb{R}$,
3. $f(x) = \sum a_i x^i \in \mathbb{Z}[x] | a_1$es múltiplo de$2 \subseteq \mathbb{Z}[x]$,
4. $f(x) = \sum a_i x^1 \in \mathbb{Z}[x] | 2/a_2 \subseteq \mathbb{Z}[x]$.

Comenzamos diciendo que para que un subconjunto B sea un subanillo de un anillo A se tiene que cumplir que:

- $1, -1 \in B$ (contienen al elemento neutro para el producto y su opuesto).
- B es cerrado para la suma y el producto.

Pasemos ahora a analizar los casos descritos arriba.

i. $a \in \mathbb{Q} | 3a \in \mathbb{Z} \subseteq \mathbb{Q}$

Este este subconjunto no es un anillo ya que $1, -1 \in \mathbb{Q}$ no están en él, ya que no son múltiplos de 3.

ii. $m + 2n\sqrt{3} |\ m, n \in \mathbb{Z} \subseteq \mathbb{R}$

Con $n = 0$ y $m = 1, -1$ tenemos 1 y -1 de $\mathbb{R}$. Además, sean cuales sean n, m de $\mathbb{Z}$ este subconjunto es cerrado para la suma y el producto, dado que la suma de enteros es siempre un entero y lo mismo ocurre con el producto.

iii. $f(x) = \sum a_i x^i \in \mathbb{Z}[x] | a_1$es múltiplo de$2 \subseteq \mathbb{Z}[x]$

Con $a_0 = 1, -1$ y $a_i = 0, i > 0$ tenemos el elemento neutro del producto y su opuesto. Además, sean cuales sean los a_i este subconjunto es cerrado para la suma y el producto ya que para los $a_i, i \neq 1$ la suma y producto de números enteros es siempre un número entero y en el caso del a_1, la suma y producto de múltiplos de 2 es siempre un múltiplo de 2.

iv. $f(x) = \sum a_i x^1 \in \mathbb{Z}[x] | 2/a_2 \subseteq \mathbb{Z}[x]$

Este subconjunto no es un anillo ya que $1, -1 \in \mathbb{Z}[x]$ no están en él ya que todos sus elementos son monomios de la forma $a_i x^1$.

2. Relación 2

2.1. Ejercicio 1

Calcular las soluciones enteras positivas de la ecuación diofántica $138x + 30y = 12150$**.**

Tenemos la siguiente ecuación:

$$138x + 30y = 12150$$

Para resolverla deberemos calcular los coeficientes de Bezout, para ello realizamos la siguiente tabla:

138	1	0
30	0	1

Ésta es nuestra tabla inicial: ¿cómo la hemos hecho?
Bien, tenemos una ecuación con 2 incógnitas y por tanto 2 coeficientes asociados a cada incógnita. En la tabla inicial ponemos el primer coeficiente con mayor norma (en este caso, con los enteros, es el que tiene mayor valor absoluto - el 138 en este ejercicio), y el menor en la segunda fila. A continuación ponemos como podemos ver en la tabla, en la primera fila (1 0) y en la segunda (0 1). Esto siempre es fijo.

Vamos ahora con el siguiente paso: tenemos que dividir el primer coeficiente entre el segundo y el resto lo pondremos debajo de los coeficientes, es decir:

$138 = 30 \cdot 4 + 18$
El resto es 18 por lo que la tabla sería:

138	1	0
30	0	1
18		

Ahora, ¿qué ponemos en los huecos a la derecha? Muy fácil, solo tenemos que coger el cociente de la división, negarlo, multiplicarlo por el número que tiene encima y sumarlo al número que tiene dos huecos por encima. Es decir, en este caso, tenemos el -4 (el cociente 4 negado):

- Para el primero: $-4 \cdot 0 + 1 = 0 + 1 = 1$
- Para el segundo: $-4 \cdot 1 + 0 = -4$

Por lo que nos queda la siguiente tabla:

138	1	0
30	0	1
18	1	-4

El proceso se ha de repetir hasta que obtengamos en las sucesivas divisiones resto 0. Ahora hacemos la división de 30 entre 18:

$30 = 18 \cdot 1 + 12$

Con coeficientes:
- Primero: $-1 \cdot 1 + 0 = -1 + 0 = -1$
- Segundo: $-1 \cdot -4 + 1 = 4 + 1 = 5$

La tabla ahora sería:

138	1	0
30	0	1
18	1	-4
12	-1	5

Repetimos:

$18 = 12 \cdot 1 + 6$

Con coeficientes:
- Primero: $-1 \cdot -1 + 1 = 1 + 1 = 2$
- Segundo: $-1 \cdot 5 + -4 = -5 + -4 = -9$

La tabla ahora es:

138	1	0
30	0	1
18	1	-4
12	-1	5
6	2	-9

Seguimos dividiendo:

$12 = 6 \cdot 2$

Hemos llegado al resto 0, entonces paramos (no hace falta calcular aquí los coeficientes), por lo que nuestra tabla final es la siguiente:

138	1	0
30	0	1
18	1	-4
12	-1	5
6	2	-9
0		

Nota: los dos últimos coeficientes son los llamados coeficientes de Bezout (2 y -9)

El siguiente paso que debemos tomar a continuación es ver si la ecuación tiene soluciones, ¿cómo lo sabemos? Pues cogemos el número anterior del 0, en nuestro caso es el 6 (qué es el máximo común divisor de los coeficientes originales de nuestra ecuación) y si divide al término independiente también, entonces la ecuación tiene soluciones enteras.

Dividimos todo entre 6:

$$23x + 5y = 2025$$

Podemos ver que 2025 sigue siendo entero, luego la ecuación tiene soluciones enteras. Ahora veamos como obtener todas las soluciones posibles.

Siempre se utiliza el siguiente esquema, primero va la incógnita con el primer coeficiente que se ha puesto en la tabla, nosotros hemos puesto el 138, luego va primero la "x". Entonces:

$$x = c' \cdot u + b' \cdot k$$

Donde c' es el término independiente una vez se haya dividido por el mcd, en este caso (2025), u es el último coeficiente correspondiente (izquierda para el primero, derecha para el segundo), en este caso (2), b es el coeficiente de la otra incógnita una vez dividida ya por el mcd, es decir, tiene que ser el coeficiente de la y (5); finalmente, la k es un parámetro que puede ser cualquier valor del anillo (en este caso entero).

Para el segundo coeficiente se hace lo mismo solo que con una ligera variación:

$$y = c' \cdot v - a' \cdot k$$

Se hace lo mismo pero en vez de sumar con el coeficiente contrario, resta, es la única diferencia y hay que tener cuidado con no confundirnos en esto.

Dicho esto, obtenemos nuestras ecuaciones generales:

$$x = 2025 \cdot 2 + 5 \cdot k = 4050 + 5k$$
$$y = 2025 \cdot -9 - 23 \cdot k = -18225 - 23k$$

Ahora bien, aun no hemos acabado: nos piden las soluciones enteras POSITIVAS. Luego x e y tienen que ser mayor que 0, simplemente veamos las inecuaciones:

$$x > 0 \implies 4050 + 5k > 0 \implies -810 < k$$
$$y > 0 \implies -18225 - 23k > 0 \implies -792,391... > k \implies -792 > k$$

Entonces tenemos que las soluciones enteras positivas de la ecuación que nos daban son:

$$x = 2025 \cdot 2 + 5 \cdot k = 4050 + 5k$$
$$y = 2025 \cdot -9 - 23 \cdot k = -18225 - 23k$$
$$k \in \{t \in \mathbb{Z} : -810 < t < -792\}$$

2.2. Ejercicio 2

"Cuarenta y seis náufragos cansados arribaron a una bella isla. Allí encontraron ciento veintiséis montones de cocos, de no más de cincuenta cada uno, y catorce cocos sueltos, y se los repartieron equitativamente..." (cuento del año 850 a.c.). ¿Cuántos cocos había en cada montón?

Tenemos la siguiente información:
- Hay 46 náufragos.
- Hay 126 montones de cocos (en cada montón no hay mas de 50 cocos).
- Hay 14 cocos sueltos.

Denotamos:
- x ≡ "nº de cocos que hay en cada montón"
- y ≡ "nº de cocos que le tocan a cada náufrago"

Sabemos que se repartieron equitaviamente, luego el número total de cocos que haya dividido entre el número de náufragos debe ser exacto. Esto es, el nº total de cocos (x · 126 + 14) entre el número de náufragos (46) debe dar exacto (y). La ecuación sería:

$$126x + 14 = 46y \implies 126x - 46y = -14$$

Como el ejercicio 1, procedemos a calcular el mcd y los coeficientes de Bezout:

126	1	0
-46	0	1
34	1	2
-12	1	3
10	3	8
-2	4	11
0		

Divisiones hechas:
$126 = -46 \cdot -2 + 34$
$-46 = 34 \cdot -1 + -12$
$34 = -12 \cdot -2 + 10$
$-12 = 10 \cdot -1 + -2$

Veamos facilmente que -14 es divisible entre -2, luego la ecuación tiene soluciones, veamos que tenemos:

$$-63x + 23y = 7$$

Y las siguientes ecuaciones generales:

$$x = 28 + 23k$$

$$y = 77 + 63k$$

$$k \in \mathbb{Z}$$

Ahora acotamos las soluciones, ambas incógnitas deben ser positivas y además x no puede ser más de 50:

$$x > 0 \implies 0 < 28 + 23k \implies k > -1,21... \implies k \geq -1$$

$$x \leq 50 \implies 50 \geq 28 + 23k \implies 0,95... > k \implies k \leq 0$$

$$y > 0 \implies 77 + 63k > 0 \implies -1,2... < k \implies k \geq -1$$

Podemos ver facilmente que o bien k vale 0; o bien, -1. Luego las soluciones son:

Primera solucion:
x = 28 (cocos por montón)
y = 77 (cocos a cada náufrago)

Segunda solución:
x = 5 (cocos por montón)
y = 14 (cocos a cada náufrago)

2.3. Ejercicio 3

Disponemos de 15 euros para comprar 40 sellos de correos, de 10, 40, y 60 céntimos y, al menos, necesitamos 2 de cada tipo ¿Cuántos sellos de cada clase podremos comprar?

Nombramos las siguientes variables:
- x ≡ "nº de sellos de 10 cent. comprados"
- y ≡ "nº de sellos de 40 cent. comprados"
- z ≡ "nº de sellos de 60 cent. comprados"

Disponemos de 15 euros (1500 cent.) para comprar estos 3 tipos de sellos, y además tenemos que comprar 40 sellos en total. Tenemos entocnes:

$$1500 = 10x + 40y + 60z$$

$$40 = x + y + z$$

Primero deberemos despejar una incógnita con la segunda ecuación (por ejemplo la z), quedando:

$$5x + 2y = 90$$

Hacemos la tabla:

5	1	0
2	0	1
1	1	-2
0		

Nota: siempre que nos salga mcd = 1, entonces la ecuación tiene solución.

División: $5 = 2 \cdot 2 + 1$

Ahora hacemos las ecuaciones generales (para obtener z basta sustituir x e y en la ecuación del principio):

$$x = 90 + 2k$$
$$y = -180 - 5k$$
$$z = 130 + 3k$$
$$k \in \mathbb{Z}$$

Además sabemos que cada variable mínimo debe ser 2 y como máximo 36, luego:

$$x \geq 2 \implies k \geq -44$$
$$x \leq 36 \implies k \leq -27$$
$$y \geq 2 \implies -36,4 \geq k \implies k \leq -37$$
$$y \leq 36 \implies -43,2 \leq k \implies k \geq -43$$
$$z \geq 2 \implies -42,6... \leq k \implies k \geq -42$$
$$z \leq 36 \implies -31,3.. \geq k \implies k \leq -32$$

Luego k estará acotado así:

$$k \in \{t \in \mathbb{Z} : -42 \leq t \leq -37\}$$

2.4. Ejercicio 4

Llueve y, en un mercadillo improvisado en Moscú, un paraguas nos cuesta 190 rublos. Disponemos solo de billetes de 3 rublos, y el vendedor solo de 5 rublos ¿Podremos hacer la compra-venta? ¿Cómo?

Asignamos las siguientes variables:
- x ≡ "nº de billetes de 3 rublos (pagados)"
- y ≡ "nº de billetes de 5 rublos (devueltos)"

Sabemos que 190 no es un múltiplo de 3, luego no podremos pagar exacto. Entonces sabemos claramente que tendremos que pagar más de 190 y además que nos dará una vuelta, luego la ecuacion será:

$$3x - 190 = 5y \implies 3x - 5y = 190$$

Hacemos la tabla (ojo, esta vez la y tiene mayor norma):

-5	1	0
3	0	1
-2	1	-2
1	1	2
0		

Divisiones:
- $-5 = 3 \cdot -1 + -2$
- $3 = -2 \cdot -1 + 1$

Y las ecuaciones generales:

$$y = 190 + 3k$$

$$x = 380 + 5k$$

$$k \in \mathbb{Z}$$

Acotamos k, sabiendo que tenemos que poner como mínimo el valor del paraguas (64 billetes) y que al menos tienen que devolver un billete:

$$x \geq 64 \implies -63,2 \leq k \implies k \geq -63$$

$$y \geq 1 \implies k \geq -63$$

Luego k estará acotado por:

$$k \in \{t \in \mathbb{Z} : t \geq -63\}$$

En particular podremos hacer la compra-venta con k = -63, luego las soluciones más pequeñas serían:
- x = 65 (billetes de 3 rublos entregados)
- y = 1 (billetes de 5 rublos devueltos)

2.5. Ejercicio 5

En una torre eléctrica, se nos ha roto una pata de 4 m de altura. Para equilibrarlo provisionalmente, disponemos de 7 discos de madera de 50 cm de grosor y de otros 12 de 30 cm. ¿Cuál de las siguientes afirmaciones es verdadera?
- No podremos equilibrar la torre.
- Podremos equilibrar la torre, y de una única manera.
- Podremos equilibrar la torre, y de dos únicas maneras.
- Podremos equilibrar la torre, y de más de 2 maneras distintas.

Nombramos las variables:
- x ≡ "nº de discos de 50cm"
- y ≡ "nº de discos de 30cm"

Y obtenemos la ecuación:

$$50x + 30y = 400 \implies 5x + 3y = 40$$

Hacemos la tabla:

5	1	0
3	0	1
2	1	-1
1	-1	2
0		

Divisiones hechas:
- $5 = 3 \cdot 1 + 2$
- $3 = 2 \cdot 1 + 1$

Y obtenemos las ecuaciones generales:

$$x = -40 + 3k$$

$$y = 80 - 5k$$

$$k \in \mathbb{Z}$$

Acotamos la k, sabiendo que x e y deben ser positivos o 0; y además solo podemos usar 7 discos de 50cm y 12 de 30cm como máximo:

$$x \geq 0 \implies k \geq 13,3... \implies k \geq 14$$

$$x \leq 7 \implies 15,66... \geq k \implies k \leq 15$$

$$y \geq 0 \implies k \leq 16$$

$$y \leq 12 \implies 13,6 \leq k \implies k \geq 14$$

Luego tenemos que k puede ser 14 o 15, por tanto tenemos dos soluciones:

Primera solución:
- x = 2 (discos de 50cm)
- y = 10 (discos de 30cm)

Segunda solución: - x = 5 (discos de 50cm)
- y = 5 (discos de 30cm)

2.6. Ejercicio 6

En el mes pasado, hemos gastado 13 euros y 20 céntimos en 12 llamadas telefónicas a Alemania y Francia, y solo nos cobran el establecimiento de llamada. En las llamadas a Alemania nos cobran 15 céntimos más que a las de Francia. Recordamos que han sido más las llamadas a Francia que a Alemania, pero ¿cuántas llamadas hemos hecho a cada sitio y qué nos han cobrado por cada una?

Nombramos las variables:
- x ≡ "nº de llamadas hechas a Francia"
- y ≡ "nº de llamadas hechas a Alemania"
- z ≡ "coste de una llamada a Francia"
- z + 15 ≡ "coste de una llamada a Alemania"

Tenemos las siguientes ecuaciones:

$$1320 = (z + 15)y + xz$$

$$12 = x + y$$

Despejamos x, y sustituimos, obteniendo:

$$1320 = 15y + 12z$$

Hacemos la tabla:

15	1	0
12	0	1
3	1	-1
0		

Divisiones hechas: $15 = 12 \cdot 1 + 3$

Ecuación final:

$$5y + 4z = 440$$

Ecuaciones generales, x se obtiene sustituyendo x:

$$y = 440 + 4k$$

$$z = -440 - 5k$$

$$x = -428 - 4k$$

$$k \in \mathbb{Z}$$

Ahora acotamos la k, sabiendo que el coste de llamada debe ser mayor que 0, que las llamadas deben ser positivas y menor que 12. En concreto sabemos que debe haber más

llamadas a Francia que a Alemania, luego el nº máximo de llamadas de Alemania debe ser 5, y el nº de llamadas mínimas de Francia 6:

$$z < 0 \implies k < -88$$

$$y \geq 1 \implies -109,75 \leq k \implies k \geq -109$$

$$y \leq 5 \implies -108,... \geq k \implies k \leq -109$$

$$x \geq 6 \implies -108,... \geq k \implies k \leq -109$$

$$x \leq 11 \implies -109,... \leq k \implies k \geq -109$$

Luego tenemos una única solución, k = -109, que nos da:
- x = 8 (llamadas a Francia)
- y = 4 (llamadas a Alemania)
- z = 105 (cent. cuesta una llamada a Francia)
- z + 15 = 120 (cent. cuesta una llamada a Alemania)

2.7. Ejercicio 7

Una persona va al supermercado y compra 12 cajas de vino, unas de blanco y otras de tinto, por 1200 euros. Si el blanco vale 30 euros más por caja que el tinto, y ha comprado el mínimo posible de tinto ¿Cuántas cajas habrá comprado de cada uno?

Nombramos las variables:
- x ≡ "nº de cajas de vino blanco"
- y ≡ "nº de cajas de vino tinto"
- z ≡ "precio por una caja de vinto tinto"
- z + 30 ≡ "precio por una caja de vino blanco"

Tenemos de esta manera dos ecuaciones:

$$1200 = (z + 30)x + yz$$

$$12 = x + y$$

Despejando la y de la segunda ecuación y sustituyendo en la primera tenemos:

$$30x + 12z = 1200$$

Hacemos la tabla:

30	1	0
12	0	1
6	1	-2
0		

Divisiones hechas: $30 = 12 \cdot 2 + 6$

La ecuación dividida sería:

$$5x + 2z = 200$$

Y las ecuaciones generales (y se obtiene sustituyendo por x):

$$x = 200 + 12k$$

$$z = -400 - 30k$$

$$y = -188 - 12k$$

$$k \in \mathbb{Z}$$

Acotando la k de manera que el precio de una caja debe ser positivo, al igual que el nº de cajas compradas (y menor que 12 - al menos debemos comprar una caja de cada tipo, y comprar 12 en total):

$$z > 0 \implies -13,33... > k \implies k \leq -14$$

$$x \geq 1 \implies -16,... \leq k \implies k \geq -16$$

$$x \leq 11 \implies -15,75 \geq k \implies k \leq -16$$

$$y \geq 1 \implies -15,75 \geq k \implies k \leq -16$$

$$y \leq 11 \implies -16,6 \leq k \implies k \geq -16$$

En concreto, tenemos que hay una única solución, k vale -16, luego las soluciones serían:
- x = 8 (cajas de vino blanco compradas)
- y = 4 (cajas de vino tinto compradas)
- z = 80 (euros vale cada caja de vino tinto)
- z + 30 = 110 (euros vale cada caja de vino blanco)

2.8. Ejercicio 8

Un vendedor en el mercado tiene un cesto de manzanas de (muy poco) más de mil. Haciendo grupos de 30 sobran 20 y haciendo grupos de 40 sobran 30. Hallar el número de manzanas que hay en el cesto.

Nombramos las siguientes variables:
- x ≡ "nº de grupos de 30 manzanas"
- y ≡ "nº de grupos de 40 manzanas"
- z ≡ "nº de manzanas totales"

Tenemos las siguientes ecuaciones:

$$z = 30x + 20$$

$$z = 40y + 30$$

Luego igualando las ecuaciones tenemos:

$$3x - 4y = 1$$

Hacemos la tabla:

-4	1	0
3	0	1
-1	1	1
0		

Divisiones hechas: $-4 = 3 \cdot -1 + -1$

La ecuación final sería:

$$-3x + 4y = -1$$

Y las ecuaciones generales (sustituyendo luego z, por alguna):

$$y = -1 - 3k$$

$$x = -1 - 4k$$

$$z = -10 - 120k$$

$$k \in \mathbb{Z}$$

Acotamos x e y (los grupos deben ser positivos y al menos 1), y las manzanas totales (z) más de 1000:

$$x \geq 1 \implies -0,5 \geq k \implies k \leq -1$$

$$y \geq 1 \implies -0,33... \geq k \implies k \leq -1$$

$$z > 1000 \implies k < -8,41 \implies k \leq -9$$

Luego k será:

$$k \in \{t \in \mathbb{Z} : t \leq -9\}$$

En concreto, la solución mínima k = -9, tenemos:
- z = 1070 (manzanas en total)
- x = 35 (grupos de 30 manzanas)
- y = 26 (grupos de 40 manzanas)

2.9. Ejercicio 10 - 2 en K[x]

2. Calcular el máximo común divisor y el mínimo común múltiplo, en el anillo Z_3[x], de los polinomios x^4+x^3-x-1 y x^5+x^4-x-1. Encontrar todos los polinomios f (x) y g(x) en Z_3[x], con grado de g(x) igual a 7, tales que (x^4+x^3-x-1) f(x)+(x^5+x^4-x-1) g(x) = x^4+x^2+1

Máximo común divisor

$$\begin{array}{r|ll} x^5+x^4-x-1 & 1 & 0 \\ x^4+x^3-x-1 & 0 & 1 \\ x^2-1 & 1 & \text{-x} \\ 0 & & \end{array}$$

Las divisiones realizadas han sido :

- $(x^5+x^4-x-1)/(x^4+x^3-x-1)$

Cociente: x
Resto: x^2-1

- $(x^4+x^3-x-1)/(x^2-1)$

Cociente: x^2+x+1
Resto: 0

Así, el máximo común divisor es x^2-1

Mínimo común múltiplo

Usamos que [a,b]=$\frac{ab}{(a,b)}$

$(x^5+x^4-x-1)(x^4+x^3-x-1) = x^9+2x^8+x^7-x^6-x^3+x^2+2x+1$

$(x^9+2x^8+x^7-x^6-x^3+x^2+2x+1)/(x^2-1) = x^7-x^6-x^5+x^4-x^3+x^2+x-1$

Por lo tanto, el mínimo común múltiplo es $x^7-x^6-x^5+x^4-x^3+x^2+x-1$

Ecuación diofántica

Dividiendo por el máximo común divisor la ecuación para obtener al reducida (vemos que tiene solución) queda:

$(x^2 + x + 1)$ f(x)+$(x^3 + x^2 + x + 1)$ g(x) $= x^2 + 2$

Aplicando la igualdad de Bezout (a partir de los cálculos del máximo común divisor):

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

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

Obtenemos como solución particular:

f_0(x) $= -x^3 - 2x$

g_0(x) $= x^2 + 2$

La solución general quedaría:

f(x) $= -x^3 - 2x + k(x)(x^3 + x^2 + x + 1)$

g(x) $= x^2 + 2 - k(x)(x^2 + x + 1)$

Para cumplir la condición g(x) igual a 7 observamos que el grado de k(x) tiene que ser igual a 5. De este modo, todas soluciones pedidas son las que se obtienen a partir de la general para todos los k(x) de Z_3[x] tal que gr(k(x)) = 5.

2.10. Ejercicio 15 - 1 en $\mathbb{Z}[\sqrt{n}]$

En el anillo $\mathbb{Z}[\sqrt{n}]$ calcular
a) mcd$(2 - 3\sqrt{-2}, 1 + \sqrt{-2})$, mcm$(2 - 3\sqrt{-2}, 1 + \sqrt{-2})$.
b) En $\mathbb{Z}[\sqrt{n}]$, calcula mcd$(3 + \sqrt{3}, 2)$ y mcm$(3 + \sqrt{3}, 2)$.

a) Calcularemos primero el mcd, para ello usaremos el método de la tabla que venimos haciendo desde siempre (ver ejercicio 1 de esta relación). Sin embargo, para calcular la norma tendremos que multiplicar el número por su conjugado, en general:

$N(a + b\sqrt{n}) = (a + b\sqrt{n}) \cdot (a - b\sqrt{n}) = x^2 - b^2 n$

Bien, ahora veamos quien tiene mayor norma:
$N(2-3\sqrt{-2}) = 4 - 9 \cdot (-2) = 4 + 18 = 22$
$N(1+\sqrt{-2}) = 1 - 1 \cdot (-2) = 3$

Y hacemos la tabla, pero ¿cómo sacamos el resto y el cociente en $\mathbb{Z}[\sqrt{n}]$? Usemos de ejemplo la división que vamos a tener que hacer:

$$\frac{2-3\sqrt{-2}}{1+\sqrt{-2}}$$

Lo que tenemos que hacer es multiplicar por el conjugado del denominador:

$$\frac{(2-3\sqrt{-2})(1-\sqrt{-2})}{(1+\sqrt{-2})(1-\sqrt{-2})} = \frac{-4-5\sqrt{-2}}{3}$$

Hemos llegado a un número del tipo $a+b\sqrt{n}$, ahora tenemos que sacar el cociente. Para hacerlo solo debemos sacar la parte entera redondeando, es decir:
$\frac{-4}{3} = -1,333 \implies a = -1$
$\frac{-5}{3} = -1,666 \implies b = -2$
Luego el cociente será: $q = -1 - 2\sqrt{-2}$
Ahora para calcular el resto, sabemos que es el dividendo menos el divisor por el cociente, luego:

$$r = 2 - 3\sqrt{-2} + (1+\sqrt{-2})(-1-2\sqrt{-2}) = -1$$

Hemos acabado, la tabla sería:

$2-3\sqrt{-2}$	1	0
$1+\sqrt{-2}$	0	1
-1	1	$1+2\sqrt{-2}$
0		

Concluimos que el mcd$(2-3\sqrt{-2}, 1+\sqrt{-2})$ = -1, ahora para hallar el mcm simplemente tenemos que: $mcm(a,b) = \frac{ab}{mdc(a,b)}$. Luego:

$$[2-3\sqrt{-2}, 1+\sqrt{-2}] = \frac{(2-3\sqrt{-2})(1+\sqrt{-2})}{-1} = -8+\sqrt{-2}$$

b) Realizamos el mismo proceso que en a). Calculamos las normas:
$N(3+\sqrt{3}) = 9 - 3 = 6$
$N(2) = 4$

La tabla quedaría:

$3+\sqrt{3}$	1	0
2	0	1
$-1-\sqrt{3}$	1	$-2-\sqrt{3}$
0		

La primera división sería:

$$\frac{3+\sqrt{3}}{2} \implies q = 2+\sqrt{3}, r = -1-\sqrt{3}$$

Y la segunda:

$$\frac{2}{-1-\sqrt{3}} = 1-\sqrt{3} \implies q = 1-\sqrt{3}, r = 0$$

Luego $mcd(3+\sqrt{3}, 2) = 1-\sqrt{3}$, y entonces:

$$mcm(3+\sqrt{3}, 2) = \frac{(3+\sqrt{3})(2)}{1-\sqrt{3}} = -2\sqrt{3}$$

2.11. Ejercicio 16 - 2 en $\mathbb{Z}[\sqrt{n}]$

Probar que en el anillo $\mathbb{Z}[\sqrt{2}]$ el entero cuadrático $2+\sqrt{2}$ y su conjugado $2-\sqrt{2}$ son asociados. ¿Quiénes son su máximo común divisor y su mínimo común múltiplo?

Bien, sabemos que dos elementos de un anillo son asociados si uno se divide al otro; es decir, x y y son asociados si x divide a y, e y divide a x.

Veamos la norma de ambos elementos:
- $N(2+\sqrt{2}) = 4-2 = 2$
- $N(2-\sqrt{2}) = 4-2 = 2$

Da igual cual dividamos entre cual, como vemos:

$$\sqrt{2+\sqrt{2}}2 - \sqrt{2} = 3+2\sqrt{2}$$

$$\sqrt{2-\sqrt{2}}2 + \sqrt{2} = 3-2\sqrt{2}$$

Vemos que efectivamente son asociados, ya que uno se divide al otro. En este caso el máximo común divisor puede cogerse como cualquiera de los dos, y el mínimo común múltiplo sería el contrario al que hemos elegido.

2.12. Ejercicio 17 - 3 en $\mathbb{Z}[\sqrt{n}]$

a) Determinar un entero de Gauss $\alpha \in \mathbb{Z}[i]$, tal que al dividirlo por 3 da resto i, mientras su resto al dividirlo 3 + 2i es 1 + i.

a) Simplemente realizamos las siguientes ecuaciones:

$$\alpha = 3x + i$$

$$\alpha = (3+2i)y + (1+i)$$

E igualando:

$$3x + (-3 - 2i)y = 1$$

Sacamos la norma:
- $N(-3 - 2i) = 9 + 4 = 13$
- $N(3) = 9$

Hacemos la tabla:

-2-2i	1	0
3	0	1
i	1	1+i
0		

Divisiones hechas: 3-2i = (1-i)3 + i

La ecuación final sería:

$$(-3i)x + (-2 + 3i)y = -i$$

Como nos pide un entero de Gauss, basta que saquemos una solución particular, obteniendo:

$$y = -i$$

$$x = 1 - i$$

$$\alpha = 3 - 2i$$

b)

3. Relación 3

3.1. Ejercicio 1

Discutir, usando congruencias, la validez de las siguientes afirmaciones:

1) 320^{207} y 2^{42} dan el mismo resto al dividirlos por 13.

Tenemos que reducir ambos números, hacemos las bases.

$320^{207} \equiv 8^{207} mod(13) \equiv (2^3)^{207} mod(13) \equiv 2^{621}$

Ahora, calculamos los restos de las potencias de 2, hasta ver cuándo se repite uno de los restos:

- $2^1 \equiv_{13} 2$
- $2^2 \equiv_{13} 4$
- ...
- $2^{13} \equiv_{13} 2$

Ahora, como nos ha salido que la potencia es 13, aplicamos la función φ de Euler a 13 para ver con qué número tienen que ser las potencias congruentes.

$$\varphi(13) = 12$$

Por último, como tenemos los dos números en la misma base, tenemos que ver si los exponentes son congruentes módulo 12.

$$621 \equiv_{12} 42 \implies 9 \equiv_{12} 6$$

Por lo que no son congruentes módulo 12, luego los dos números iniciales no dan el mismo resto al dividirlos por 13.

2) $5^{2n+1} + 2^{2n+1}$ es divisible por 7 cualquiera que sea el entero $n \geq 1$

Tenemos que ver si $5^{2n+1} + 2^{2n+1} \equiv_7 0$ para $n \geq 1$. Pero $5 \equiv_7 -2$, luego:

$$5^{2n+1} + 2^{2n+1} \equiv_7 -(2)^{2n+1} + 2^{2n+1} \equiv_7 0$$

Luego siempre es divisible por 7 para cualquier entero.

4)Las dos últimas cifras del número 7^{355} son 4 y 3.

Para esto, bastaría ver si $7^{355} \equiv 43 mod(100)$. Para ello, vamos a facilitar el cálculo usando la función φ de Euler. $\varphi(100) = 100 * 1/2 * 4/5 = 40$.

Esto implica que $7^{40} \equiv 1 mod(100)$

Vamos a reducir el 7^{355} con módulo 40. Si dividimos 355 entre 40 nos queda un resto de 35, luego $7^{355} \equiv 7^{35} mod(100)$.

Ahora, vamos a calcular las potencias de 7 para ver cuándo se repite el resto al ir añadiendo exponentes.

- $7 \equiv_{100} 7$
- $7^2 \equiv 29 mod(100)$
- $7^3 \equiv 43 mod(100)$
- ...
- $7^5 \equiv_{100} 7$

Luego $7^{35} \equiv_{100} 7^3 \equiv_{100} 43$, pues ya habíamos obtenido ese 43 como resultado de hacer las congruencias de las potencias sucesivas de 7.

4) $3 * 5^{2n+1} + 2^{3n+1}$ es divisible por 17 cualquiera que sea el entero $n \geq 1$

Tenemos que volver a ver en este caso, si el número es congruente con 0 módulo 17. Ahora, quitando el n+1 en el 5:

$$3 * 5^{2n+1} + 2^{3n+1} \equiv_{17} 0 \implies 15 * 5^{2n} + 2^{3n+1}$$

Y seguimos desarrollando.

$$15*5^{2n}+2^{3n+1} \equiv \implies -2^{2n}+2^{3n+1} \equiv_{17} -2*8^n+2^{3n+1} = -2*2^{3n} = -(2)^{3n+1}+2^{3n+1} = 0$$

6) Un número es divisible por 4 si y solo si el número formado por sus dos últimas cifras es múltiplo de 4.

Vamos ver si : $a_n a_{n-1} ... a_1 a_0 \iff a_1 a_0 \equiv_4 0$.

El número vendrá dado: $a_n * 10^n + a_{n-1} * 10^{n-1} + ... + a_1 * 10 + a_0$.

Pero, tomando todas la demás cifras menos las dos últimas, su suma es congruente con 0 módulo 4, luego basta ver si los dos últimos es congruente con 0 módulo 4, pero eso es el enunciado, luego queda probado.

3.2. Ejercicio 4

Una banda de 13 piratas se reparten N monedas de oro, pero le sobran 8. Dos mueren, las vuelven a repartir y sobran 3. Luego se ahogan 3 y sobran 5. ¿Cuál es la mínima cantidad posible N de monedas?

$$\begin{cases} \text{N} \equiv 8 \text{ mod}(13) \\ \text{N} \equiv 3 \text{ mod}(11) \\ \text{N} \equiv 5 \text{ mod}(8) \end{cases}$$

Resolvemos el sistema formado por la primera y la tercera ecuación:

$\text{N} \equiv 8 \text{ mod}(13) \rightarrow \text{N} = 8 + 13 \cdot \text{x}$

Sustituimos en la tercera ecuación

$8 + 13 \cdot \text{x} \equiv 5 \text{ mod}(8) \rightarrow 5 \cdot \text{x} \equiv 5 \text{ mod}(8) \Rightarrow \text{x} \equiv 1 \text{ mod}(8)$ (Podemos simplificar el 5 porque (5,8) = 1)

$x_0 = 1 \Rightarrow N_0\ 8 + 13 \cdot 1 = 21$ (Solución óptima)

$\text{N} \equiv 21 \text{ mod}(8 \cdot 13) = 21 \text{ mod}(104)$

Ahora, resolvemos el sistema con la ecuación anterior y la segunda del sistema inicial

$\text{N} \equiv 21 \text{ mod}(104) \rightarrow 21 + 104 \cdot \text{x}$

$21 + 104 \cdot \text{x} \equiv 3 \text{ mod}(11) \Rightarrow 10 + 5 \cdot \text{x} \equiv 3 \text{ mod}(11) \Rightarrow 5 \cdot \text{x} \equiv -7 \text{ mod}(11) \Rightarrow 5 \cdot \text{x} \equiv 4 \text{ mod}(11)$

Figura 1: mcd

11	1	0
5	0	1
1	1	-2
0		

$1 = 1 \cdot 11 + 5 \cdot (-2) \rightarrow 5 \cdot (-2) \equiv 1 \text{ mod}(11)$

Multiplicamos por 4 y así obtendremos una solución particular

$5 \cdot (-8) \equiv 4 \text{ mod}(11) \Rightarrow x_0 = -8$

Sustituimos y nos queda $N_0 = -811$

$\text{N} \equiv -811 \text{ mod}(1144) = 333 \text{ mod}(1144)$ (donde 1144 = [11,104])

$\text{N} = 333 + 1144 \cdot \text{k}$

Solución: La cantidad mínima de monedas sería cuando k vale 0. Entonces el número de monedas es 333

3.3. Ejercicio 6

Antonio, Pepe y Juan son tres campesinos que principalmente se dedican al cultivo de la aceituna. Este año la producción de los olivos de Antonio fue tres veces la de los de Juan y la de Pepe cinco veces la de los de Juan. Los molinos a los que estos campesinos llevan la aceituna, usan recipientes de 25 litros el de Juan, 7 litros el de Antonio y 16 litros el de Pepe. Al envasar el aceite producido por los olivos de Juan sobraron 21 litros, al envasar el producido por Antonio sobraron 3 litros y al envasar el producido por Pepe sobraron 11 litros. Sabiendo que la producción de Juan está entre 1000 y 2000 litros ¿cual fue la producción de cada uno de ellos?.

Vamos a plantear primero el problema. Llamamos:

1. A = 3J; P = 5J
2. La capacidad es: J = 25, A = 7 y P = 16.
3. Sobran: J = 21, A = 3, y P = 11.

Así, el sistema a plantear es:

- $J \equiv 21 mod(25)$
- $A \equiv 3 mod(7) \equiv 3J$
- $P \equiv 11 mod(16) \equiv 5J$

Por lo que el sistema resultante es

$$\left.\begin{array}{r} x \equiv 21 mod(25) \\ 3x \equiv 3 mod(7) \\ 5x \equiv 11 mod(16) \end{array}\right\}$$

Tenemos que hacer transformaciones hasta llegar a dejar la x sola en cada una de las ecuaciones en congruencia. Si las hacemos, la transformación es:

$$\left.\begin{array}{r} x \equiv 21 mod(25) \\ 3x \equiv 3 mod(7) \\ 5x \equiv 11 mod(16) \end{array}\right\} \implies \begin{cases} x \equiv 21 mod(25) \\ x \equiv 1 mod(7) \\ x \equiv 15 mod(16) \end{cases}$$

Y este es el sistema final a resolver. Para ello, resolvemos dos primero y luego resolvemos esos dos con el siguiente. Resolvemos el de las dos primeras:

Vemos que la primera ecuación es : $x = 21 + y * 25$ lo quenos lleva a la congruencia: $21 + y * 25 \equiv 1 mod(7) \implies 4y \equiv 1 mod(7) \implies y \equiv 2 mod(7)$ por tanto la solución óptima es $y_0 = 2$ y ahora si $y = 2$, eso implica que (volviendo a la x que habíamos despejado) $x_0 = 21 + 50 = 71$ y si volvemos a expresarlo como congruencias nos queda $x \equiv 71 mod(175)$.

Hemos reducido una ecuación, ahora tendríamos que volver a resolver el sistema

$$\begin{cases} x \equiv 71 mod(175) \\ x \equiv 15 mod(16) \end{cases}$$

3.4. Ejercicio 11 - 1 parte K[x] y $\mathbb{Z}\sqrt{n}$

(1). Probar el teorema de Ruffini: *si $f(x) \in A[x]$, entonces $f(a)$ es igual al resto de dividir $f(x)$ entre $x - a$.*

Demostración.
Si A es un Dominio Euclídeo y $f(x) \in A[x]$, entonces $\exists q, r \in A$ tales que
$f(x) = q(x - a) + r$, donde r es el resto al dividir $f(x)$ por $x - a$. Entonces, evaluamos f en a, y tenemos que $f(a) = (a - a)q + r = r$, como queríamos demostrar. □

Nota. La tesis del teorema también puede expresarse como la siguiente congruencia: $f(x) \equiv f(a)\ mod\ (x - a)$.

(2). Encontrar un polinomio $f(x) \in \mathbb{Q}[x]$ de grado 3 tal que:

- $f(0) = 6$
- $f(1) = 12$
- $f(x) \equiv (3x + 3)\ mod\ (x^2 + x + 1)$

Solución. Primero, reescribimos las condiciones del enunciado en términos de congruencias, usando el teorema de Ruffini:

- $f(x) \equiv 6\ mod\ (x)$
- $f(x) \equiv 12\ mod\ (x - 1)$
- $f(x) \equiv (3x + 3)\ mod\ (x^2 + x + 1)$

Para resolver este sistema de tres congruencias, lo reducimos en primer lugar a un sistema de dos congruencias, tomando las dos primeras.

Nos centramos en la ecuación $f(x) \equiv 6\ mod\ (x)$, que ya está resuelta: su solución general es $f(x) = 6 + g(x) \cdot x$, con $g(x) \in \mathbb{Q}[x]$. Sustituyendo en la segunda ecuación, nos quedaría $6 + g(x) \cdot x \equiv 12\ mod\ (x - 1)$. Resolvamos ahora esta congruencia:

Primero simplificamos la expresión, llegando a $g(x) \cdot x \equiv 6\ mod\ (x - 1)$. Calculemos ahora el mcd $(x, x - 1)$, calculando además los coeficientes de Bezout:

r	u	v
x	1	0
$x - 1$	0	1
1	1	-1

Vemos que $(x, x-1) = 1$, y haciendo uso de la identidad de Bezout, nos queda que $1 = \mathbf{1} \cdot x + \mathbf{(-1)} \cdot (x-1)$. Como esta forma es la de las soluciones de una ecuación en congruencia, deducimos que $1 \cdot x \equiv 1 \ mod \ (x-1)$, y multiplicando por 6 tenemos que $6 \cdot x \equiv 6 \ mod \ (x-1)$. Si comparamos esta expresión con la ecuación original, es evidente que $g_0(x) = 6$ es una solución particular. Entonces, $f_0(x) = 6 + 6x$ es una solución particular del sistema, y la solución general será:

$$f(x) \equiv f_0(x) \ mod \ ([x, x+1]) \Rightarrow f(x) \equiv 6 + 6x \ mod \ (x^2 - x) \tag{1}$$

Pasamos ahora a resolver, del mismo modo, el sistema formado por la tercera ecuación original, y la ecuación (1).

La solución general de (1) es $f(x) = (6+6x) + h(x) \cdot (x^2 - x)$, con $h(x) \in \mathbb{Q}[x]$. Sustituyendo en la tercera ecuación y simplificando, nos quedaría $h(x) \cdot (x^2 - x) \equiv -3 - 3x \ mod \ (x^2 + x + 1)$. Resolvamos ahora esta congruencia, calculando para ello $(x^2 - x, x^2 + x + 1)$, y los coeficientes de Bezout:

r	**u**	**v**
$x^2 - x$	1	0
$x^2 + x + 1$	0	1
$-2x - 1$	1	-1
$\frac{3}{4}$	$\frac{1}{2}x + \frac{1}{4}$	$\frac{-1}{2}x + \frac{3}{4}$

Vemos que $(x^2 - x, x^2 + x + 1) = \frac{3}{4}$, y haciendo uso de la identidad de Bezout, nos queda lo siguiente:

$$\frac{3}{4} = \mathbf{(\frac{1}{2}x + \frac{1}{4})} \cdot (x^2 - x) + \mathbf{(-\frac{1}{2}x + \frac{3}{4})} \cdot (x^2 + x + 1)$$

Dividimos ahora la ecuación por $\frac{3}{4}$, y tenemos que:

$$1 = \left(\frac{2}{3}x + \frac{1}{3}\right) \cdot (x^2 - x) + \left(-\frac{2}{3}x + 1\right) \cdot (x^2 + x + 1)$$

Como esta forma es la de las soluciones de una ecuación en congruencia, deducimos que:

$$\left(\frac{2}{3}x + \frac{1}{3}\right) \cdot (x^2 - x) \equiv 1 \ mod \ (x^2 + x + 1)$$

y ahora multiplicamos por $-3x - 3$:

$$(-3x - 3) \cdot \left(\frac{2}{3}x + \frac{1}{3}\right) \cdot (x^2 - x) \equiv -3x - 3 \ mod \ (x^2 + x + 1)$$

Si comparamos esta expresión con la ecuación original, es evidente que una solución particular es $g_0(x) = (-3x - 3) \cdot (\frac{2}{3}x + \frac{1}{3}) = -2x^2 - 3x - 1$. Podemos calcular una solución partícular óptima, ya que esta no lo es, sin más que calcular su resto al dividirla por $x^2 + x + 1$, que es $1 - x$. Entonces, $f_0(x) = 6 + 6x + (1 - x)(x^2 - x) = -x^3 + 2x^2 + 5x + 6$ es una solución particular del sistema, y la solución general será:

$$f(x) \equiv f_0(x) \ mod \ ([x^2 - x, x^2 + x + 1]) \Rightarrow f(x) \equiv -x^3 + 2x^2 + 5x + 6 \ mod \ (x^4 - x)$$

Entonces, el polinomio pedido sería justamente $f(x) = -x^3 + 2x^2 + 5x + 6$, y podemos comprobar que, efectivamente, se cumplen las condiciones del enunciado.

3.5. Ejercicio 13 - 3 parte K[x] y $\mathbb{Z}\sqrt{n}$

Determinar los polinomios $f(x) \in \mathbb{Q}[x]$ de grado menor o igual que tres que satisfacen el sistema de congruencias

$$\left.\begin{array}{r} f(x) \equiv x-1 \ mod(x^2+1) \\ f(x) \equiv x+1 \ mod(x^2+x+1) \end{array}\right\}$$

En primer lugar, reescribimos la primera ecuación para sustituirla en la segunda.

$$f(x) \equiv x-1 \ mod(x^2+1) \implies f(x) = x-1+(x^2+1)g(x)^{\circledast}$$

Reemplazando lo obtenido, tenemos:

$$x-1+(x^2+1)g(x) \equiv x+1 \ mod(x^2+x+1)$$

Pasamos el x-1 restando:

$$(x^2+1)g(x) \equiv 2 \ mod(x^2+x+1)$$

Resolvemos esta ecuación, que tendrá solución si, y solo si, $(x^2+1,\ x^2+x+1)/2$. Así, hallamos el mcd a través de la tablita correspondiente:

x^2+x+1	1	0
x^2+1	0	1
x	1	-1
1	$-x$	$x+1$
0		

Obtenemos de esta forma que $(x^2+1,\ x^2+x+1) = 1$, que divide a 2, por tanto, habrá solución. Partiendo de la identidad de Bezout: $1 = (x^2+x+1)(-x)+(x^2+1)(x+1)$, la transformamos en una ecuación en congruencia (si vemos la ecuación como $(x^2+x+1)(x) = (x^2+1)(x+1)-1$, por la definición de congruencia) $(x^2+1)(x+1) \equiv 1 \ mod(x^2+x+1)$, multiplicando por 2, encontramos la g(x) buscada: $(x^2+1)(2x+2) \equiv 2 \ mod(x^2+x+1)$. $g(x) = 2x+2$.

Sustituyendo en $^{\circledast}$ el polinomio g(x) recién encontrado llegaremos a f_0(x), solución parcial del sistema.

$$f_0(x) = x-1+(x^2+1)g(x) = x-1+(x^2+1)(2x+2) = 2x^3+2x^2+3x+1$$

La solución general será

$$f(x) \equiv f_0(x) mod[x^2+1,\ x^2+x+1]$$

Calculamos el mcm:

$$[x^2+1,\ x^2+x+1] = \frac{(x^2+x+1)(x^2+1)}{1} = x^4+x^3+2x^2+x+1$$

Como el ejercicio pide aquellos polinomios de grado menor o igual que tres, nos basta con la solución parcial, ya que otras soluciones eran polinomios de grado superior al buscado.

Solución: $f_0(x) = 2x^3 + 2x^2 + 3x + 1$

3.6. Ejercicio 15 - 5 parte K[x] y $\mathbb{Z}\sqrt{n}$

En el anillo $Z[\sqrt{3}]$, resolver la congruencia.

$$(1+\sqrt{3})x \equiv 9 - 4\sqrt{3} \ mod(2\sqrt{3})$$

Primero calculamos el máximo común divisor de $(1+\sqrt{3})$ y $(2\sqrt{3})$.

$$N(1+\sqrt{3}) = \sqrt{1+(\sqrt{3})^2} = \sqrt{1+3} = 2$$
$$N(2\sqrt{3}) = \sqrt{(2\sqrt{3})^2} = 2\sqrt{3}$$

Como $N(1+\sqrt{3}) < N(2\sqrt{3})$ pondremos primero $2\sqrt{3}$

$$\begin{array}{l|ll} 2\sqrt{3} & 1 & 0 \\ 1+\sqrt{3} & 0 & 1 \\ 0 & & \end{array}$$

Sabemos que el resto es 0 puesto que:

$$\frac{2\sqrt{3}}{1+\sqrt{3}} = \frac{(2\sqrt{3})(1-\sqrt{3})}{(1+\sqrt{3})(1-\sqrt{3})} = \frac{2\sqrt{3}-6}{1-3} = \frac{2\sqrt{3}-6}{-2} = 3-\sqrt{3}$$

Por lo tanto, el cociente de esta división es $3-\sqrt{3}$ y de resto cero. Quedando el mcd de $(1+\sqrt{3})$ y $(2\sqrt{3})$ es $(1+\sqrt{3})$. Veamos si $(1+\sqrt{3})$ divide $9-4\sqrt{3}$.

$$\frac{9-4\sqrt{3}}{1+\sqrt{3}} = \frac{(9-4\sqrt{3})(1-\sqrt{3})}{(1+\sqrt{3})(1-\sqrt{3})} = \frac{9-9\sqrt{3}-4\sqrt{4}+4(\sqrt{3})^2}{1-(\sqrt{3})^2} = \frac{21-13\sqrt{3}}{-2} = \frac{13\sqrt{3}-21}{2} = \frac{13}{2}\sqrt{3}-\frac{21}{2}$$

El cociente la division es $q = 6$ y el resto es:

$$r = (9-4\sqrt{3}) - 6\cdot(1+\sqrt{3}) = 9-4\sqrt{3}-6-6\sqrt{3} = 3-10\sqrt{3} \neq 0$$

Como $(1+\sqrt{3})$ no divide $9-4\sqrt{3}$. Esta ecuación no tiene solución.

4. Ejercicio 16 - 6 parte K[x] y $\mathbb{Z}\sqrt{n}$

En el anillo $\mathbb{Z}$[i], resolver el siguiente sistema de congruencias:

$$\begin{cases} x \equiv i & mod\ (3) \\ x \equiv 1+i & mod\ (3+2i) \\ x \equiv 3+2i & mod\ (4+i) \end{cases}$$

Resolución.

Empezaremos resolviendo el sistema:

$$\begin{cases} x \equiv i & mod\ (3) \\ x \equiv 1+i & mod\ (3+2i) \end{cases}$$

Para ello hallaremos la solución particular de $x \equiv i\ mod\ (3)$. Como i es una unidad del anillo, entonces $\forall a \in \mathbb{Z}[i] \Rightarrow (a, i) = i$. Los coeficientes de Bezout son $0 * 3 + 1 * i = 1$ de manera trivial. Entonces la solución general de la primera ecuación sería $x = i + 3 * k$.

Ahora sustituimos x en la segunda ecuación, y nos queda la ecuación $i+3k \equiv 1+i\ mod(3+2i)$ de manera equivalente $3k \equiv 1\ mod\ (3+2i)$. Ahora sacaremos los coeficientes de Bezout de 3 y 3+2i.

	3+2i	3
3+2i	1	0
3	0	1
-i	1	-1-i

Por ello, sabemos que $3 * (-1 - i) \equiv -i\ mod(3 + 2i)$. Una solución particular será $k = (-1-i)*-i = (i-1)$. La solución general para k será por lo tanto $k = (i-1)+(3+2i)*k'$.

Sustituimos la particular de k en la primera resolución y hallaríamos $M = [3, 3 + 2i]$ para ver cada cuanto debemos hacer la repetición. Para calcular el mcm recordaremos que $(a, b) * [a, b] = ab \Rightarrow \frac{ab}{(a,b)} = [a, b]$. Entonces para nuestro caso particular $[3, 3 + 2i] = \frac{9+6i}{-i} = 9i - 6$. Así pues la solución será:

$$x = i + 3(i - 1) + k''(9i - 6) = 4i - 3 + k''(9i - 6)$$

Ahora cogemos el sistema:

$$\begin{cases} x \equiv 4i-3 & mod\ (9i-6) \\ x \equiv 3+2i & mod\ (4+i) \end{cases}$$

Para resolverlo y hallar (por fin) la solución final haremos lo mismo: hallar la solución general de la primera ecuación (ya resuelta) y sustituir en la segunda, mcm de los módulos y terminamos.

Solución primera ecuación: $4i - 3 + k''(9i - 6)$.

Sustituimos segunda: $4i-3+k''(9i-6) \equiv 3+2i \ \ mod\,(4+i) \rightarrow (9i-6)k'' \equiv 6-2i \ \ mod\,(4+i)$

Hallamos coeficientes de bezout y mcd:

	9i-6	4+i
9i-6	1	0
4+i	0	1
2i	1	1-2i
i	-2	4i-1

Enunciamos solución particular y un indicio de la general: Como $(9i-6)(-2) \equiv i \ mod\,(4i-1) \Rightarrow (9i-6)(-2)(-6i-2) \equiv i(-6i-2) \ mod\,(4i-1) \Rightarrow (9i-6)(12i+4) \equiv (6-2i) \ mod\,(4i-1) \Rightarrow k'' = (12i+4) + [9i-6, 4+i]k'''$

Calculamos [9i-6,4+i]: $\frac{30i-33}{i} = 30 - 33i$

Solución general: $(12i + 4) + (30 - 33i)k'''$

5. Relación 4

5.1. Ejercicio 1

Resuelve las ecuaciones siguientes en los anillos que se indican:

1) 12x = 8 en el anillo $\mathbb{Z}_{20}$.

Lo primero es comprobar si tiene solución. Para ello, tenemos que ver si $(20, 12) = 4(5, 3) = 4$ divide a 8, que sabemos que sí.

Ahora, planteamos la ecuación en congruencias:

$$12x \equiv 8 mod(20) \implies 3x \equiv 2 mod(5) \implies x \equiv 4 mod(5)$$

Luego una solución particular de nuestro problema es 4. Además, es la óptima pues $R_{20}(4) = 4$.

Ahora, las soluciones vendrán dadas por $4 + k * 5$ en $\mathbb{Z}_{20}$, luego son $\{4, 9, 14, 19\}$.

2) 19x = 42 en el anillo $\mathbb{Z}_{50}$.

Para empezar, tiene solución si, y solo si, $(19, 50) = 1$ divide a 42, como resulta evidente a simple vista y lo que nos indica también que nuestro problema tiene exactamente una solución. Como de buenas a primeras no se ve ningún método de simplificación factible para llegar hasta nuestra solución y como estamos en un Dominio de Ideales Principales(DIP) podemos usar la Identidad de Bezout hallada a partir del Algoritmo de Euclides.

r	u	v
50	1	0
19	0	1
12	1	-2
7	-1	3
5	2	-5
2	-3	8
1	8	-21

Explicaremos en este caso como se obtienen los coeficientes de Bezout para el resto 7 dejando claro que los demás restos se sacarán de forma recusirva utilizando el mismo método. Al dividir 19 entre 12 tenemos que:

$$19 = 12(+1) + 7 \implies 7 = 19(+1) + 12(-1) \implies 7 = 19(+1) + (50(+1) + 19(-2))(-1) \implies$$
$$\implies 7 = 50(-1) + 19(+3)$$

A continuación, como $1 = 50(8) + 19(-21)$ tenemos que $19(-21) \equiv 1 mod(50)$ luego solo tendríamos que multiplicar por 42 y tendríamos que $19(-21 * 42) \equiv 42 mod(50)$.

Luego, la conclusión es que $x = -21 * 42 \equiv_{50} 29 * 42 = 1218 \equiv_{50} 18$.

4) 5^{30} x = 2 en $\mathbb{Z}_7$

Podemos despejar un poco la ecuación viendo que:

$$5^{30} \equiv_7 -2^{30} = 2^{30}$$

Ahora, como 2 y 7 son primos entre sí, usamos la función φ de Euler y vemos: $2^{\varphi(7)} = 2^6 \equiv_7 1$

Luego resulta que $2^{30} \equiv_7 2^6 \equiv_7 1$

Por lo que $x_0 = 2$ y la solución es $x = 2$

5.2. Ejercicio 2

Determina cuántas unidades y cuántos divisores de cero tienen los anillos:

Antes de empezar hemos de tener en cuenta que en estos anillos todos los elementos son o unidades o divisores de cero sólo tenemos que restarle al cardinal del anillo el número de unidades para obtener el número de divisores de cero.

1) $\mathbb{Z}_{125}$

Para ello, basta calcular $|U(\mathbb{Z}_{125})| = \varphi(125) = 125 \cdot (1 - \frac{1}{5}) = 100$, luego como tiene **100 unidades**, tiene **25 divisores de cero**.

2) $\mathbb{Z}_{72}$

Calculamos $\varphi(72) = 72 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) = 36 \cdot \frac{2}{3} = 24$, hay un total de **24 unidades y 48 divisores de cero**.

3) $\mathbb{Z}_{88}$

Siguiendo el proceso de antes calculamos la función φ de Euler, la cual nos permitirá obtener el número de unidades de este anillo.

Así pues calculamos:

$\varphi(88) = 88 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{11}) = 40$, es decir, $|U(\mathbb{Z}_{88})| =$ **40 unidades** y por tanto hay $88 - 40 =$ **48 divisores de cero**.

Recordaremos que los valores de λ en $\varphi(\alpha)$ del tipo $(1-\frac{1}{\lambda})$ son los divisores irreducibles de α

4) $\mathbb{Z}_{1000}$

Volvemos a hacer lo mismo, $\varphi(1000) = 1000 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{5}) =$**400 unidades** y por tanto hay **600 divisores de cero**.

5.3. Ejercicio 3

Determina si la igualdad a = b es cierta en los siguientes casos:

Como la interpretación de los paréntesis puede dar lugar a malinterpretaciones consideraremos en los dos primeros apartados la base como un número elevado a otro, y en los dos siguientes consideraremos una base que está elevada a un exponente el cual es base de otra potencia.

1) $\mathbf{a = (9^{55})^9}$ y $\mathbf{b = (7^{70})^{55}}$ en el anillo $\mathbb{Z}_{21}$

Partiremos de que $9^{55^9} = 9^{495}$, pero (como 9 y 21 son primos relativos) podemos calcular la función φ de Euler para saber cuantas unidades hay en el anillo y ver "con qué frecuencia se repiten los valores de las potencias"

Entonces: $\varphi(21) = 21 \cdot \frac{2}{3} \cdot \frac{6}{7} = 12$

Y esto quiere decir que $9^{495} \equiv_{21} 9^{R_{12}(495)} \equiv_{21} 9^3$

Calculamos este valor:

$9^1 \equiv_{21} 9 \quad ; \quad 9^2 \equiv_{21} 18 \quad ; \quad \mathbf{9^3 \equiv_{21} 15 = a}$

Y ahora hacemos lo propio para $b = 7^{70^{55}}$
b es congruente con $7^{10^{55}}$ (usamos $\varphi(21)$ para esto) y $7^{10^{55}} \equiv_{21} 7^{550} \equiv_{21} 7^{R_{12}(550)} \equiv_{21} 7^{16}$

Pero $7^1 \equiv_{21} 7^2 \equiv_{21} ... \equiv_{21} \mathbf{7^{16} \equiv_{21} 7 = b} \Rightarrow \mathbf{a \neq b}$

2) $\mathbf{a = (2^5)^{70}}$ y $\mathbf{b = (5^{70})^2}$ en el anillo $\mathbb{Z}_{21}$

Podemos hacer uso de la función φ del ejercicio anterior, pues estamos en el mismo anillo, así sólo tenemos que repetir el mismo proceso

$2^{350} \equiv_{21} 2^{R_{12}(350)} \equiv_{21} \mathbf{2^2 \equiv_{21} 4 = a}$

Y por su parte para b:

$5^{70^2} \equiv_{21} 5^{140} \equiv_{21} 5^{R_{12}(140)} \equiv_{21} \mathbf{5^5 \equiv_{21} 17 = b}$

Luego: $\mathbf{a \neq b}$

3) $\mathbf{a = 12^{55^{70}}}$ y $\mathbf{b = 10^{70^{55}}}$ en el anillo $\mathbb{Z}_{22}$

Empezaremos calculando la función $\varphi(22)$ que nos será de utilidad en los siguientes ejercicios:

$\varphi(22) = 22 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{11}) = 10$

$a = 12^{55^{70}} = (3 \cdot 4)^{55^{70}} = 3^{55^{70}} \cdot 4^{55^{70}}$

Calculamos por separado cuánto vale cada uno de estos:

$3^{55^{70}} \rightarrow$ Como 3 es primo relativo con 22 podemos hacer uso de la función $\varphi(22)$, por lo que con el teorema de Euler obtenemos que:

$3^{\varphi(22)} \equiv 1 mod(22)$

Y de esto deducimos que:

$3^{55^{70}} \equiv_{22} 3^{R_{\varphi(22)}(55^{70})}$

Aquí entonces tenemos que hallar cuál es la solución de $R_{10}(55^{70}) = R_{10}(5^{70})$. Pero rápidamente observamos que $5^1 \equiv_{10} ... \equiv_{10} 5^n \equiv_{10} 5$ y por tanto $R_{10}(5^{70}) = 5$

En este momento ya podemos calcular cuánto vale $3^{55^{70}}$, que es congruente con 3^5

$$3^1 \equiv_{22} 3 \quad ; \quad 3^2 \equiv_{22} 9 \quad ; \quad 3^3 \equiv_{22} 5 \quad ; \quad 3^4 \equiv_{22} 15 \quad ; \quad \mathbf{3^5 \equiv_{22} 1}$$

Y hacemos lo propio con $4^{50^{70}}$:

No podemos proceder como en lo anterior haciendo uso de la función φ de Euler, pues 4 y 22 no son primos relativos. En su lugar hay que operar de una manera más "rudimentaria", hallando con qué frecuencia se repiten las potencias de 4 en este anillo.

$$4^1 \equiv_{22} 4 \quad ; \quad 4^2 \equiv_{22} 16 \quad ; \quad 4^3 \equiv_{22} 20 \quad ; \quad 4^4 \equiv_{22} 14 \quad ; \quad \mathbf{4^5 \equiv_{22} 12} \quad ; \quad 4^6 \equiv_{22} 4$$

De esto sacamos que se repiten cada 5, o visto de otra manera, esto quiere decir que $4^{55^{70}} \equiv_{22} 4^{R_5(55^{70})}$, pero como $R_5(55) = 0 \Rightarrow 4^{55^{70}} \equiv_{22} 4^5$

Uniendo ambos resultados vemos que el producto de esto nos queda $1 \cdot 12 = \mathbf{12} = \mathbf{a}$

Y ahora calculamos b:

$10^{70^{55}} = 5^{70^{55}} \cdot 2^{70^{55}}$

Repetimos el mismo o procedimiento, calculamos por separado el valor de cada uno de los términos y luego multiplicamos. Siguiendo el criterio de "si son primos relativos con 22 podemos usar la función φ de Euler y si no tendremos que estudiar las repeticiones en las potencias".

De este modo obtenemos:

$2^{70^{55}} \equiv_{22} 2^{R_{10}(70^{50})} \Rightarrow \equiv_{22} \mathbf{2^{10} \equiv_{22} 12}$ *(Mediante repeticiones en las potencias)*

$5^{70^{55}} \equiv_{22} 5^{R_{\varphi(22)}(70^{55})} \equiv_{22} \mathbf{5^{10} \equiv_{22} 1}$ *(Mediante la función φ de Euler)*

Con lo que concluimos que el producto es:

$$12 \cdot 1 = \mathbf{12} = \mathbf{b}$$

Afirmando en este caso que **a y b son iguales**

4) $\mathbf{a = 5^{5^{70}} \cdot 11^{5^{70}}}$ y $\mathbf{b = 10^{70^{22}}}$ en el anillo $\mathbb{Z}_{22}$

Volvemos a hacer lo mismo que antes. Calculamos primero el valor de a:

$5^{5^{70}} \equiv_{22} 5^{R_{\varphi(22)}(5^{70})} \equiv_{22} 5^5$; (*Observamos que* $R_{\varphi(22)}(5^{70}) = 5$)

Luego $5^5 \equiv_{22} 1$

$11^{5^{70}} \equiv_{22} ? \rightarrow$ No podemos usar $\varphi(22)$ pues 11 y 22 no son primos relativos, pero rápidamente apreciamos que:

$11^x \equiv_{22} 11 \ \forall \ x \in \mathbb{N}$

Obteniendo como resultado $\mathbf{a = 11 \cdot 1 = 11}$

Para b calculamos el producto de:

$2^{70^{22}} \equiv_{22} 2^{R_{10}(70^{22})} \equiv_{22} 2^{10} \equiv_{22} 12$

(Como 2 y 22 son primos estudiamos las repeticiones de las potencias de 2 en $\mathbb{Z}_{22}$*)*

$5^{70^{22}} \equiv_{22} 5^{R_{10}(70^{22})} \equiv_{22} 1$

Con lo que nos queda $\mathbf{1 \cdot 12 = 12 = b}$

Y finalizamos concluyendo que $\mathbf{a \neq b}$

5.4. Ejercicio 5 - 2 en anillos de restos de K[x]

Sea $\mathcal{F}_9 = \mathbb{Z}_3[x]_{x^2+1}$ el anillo de restos del anillo $\mathbb{Z}_3[x]$ módulo $x^2 + 1$.

Vamos primero a describir los polinomios que hay:

$$\mathcal{F}_9 = \mathbb{Z}_3[x]_{x^2+1} = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$$

Por tanto, este anillo tiene 9 polinomios:

1) Argumentar que $\mathcal{F}_9$ es un cuerpo

Para ello, tenemos que ver si x^2+1 es un irreducible en $\mathbb{Z}_3[x]$. Vemos si tiene raíces, dándole los valores 0, 1 y 2 y vemos que en ningún caso el resultado es cero, por tanto es irreducible por la afirmación: Si $f(x)$ no es irreducible $\exists x - a : x - a / f \implies f(a) = 0$

Entonces, $\mathcal{F}_9$ es un cuerpo.