Universidad de Granada

Ejercicios resueltos Álgebra I

Doble Grado de Informática y Matemáticas

Curso 2016/17

1. Relación 2

1.1. 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 izquierda? Muy facil, 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:

$$23x + 5y = 20250$$

Podemos ver que 20250 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 (20250), 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:

$$x = 20250 \cdot 2 + 5 \cdot k = 40500 + 5k$$
$$y = 20250 \cdot -9 - 23 \cdot k = -182250 - 23k$$

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:

$$x > 0 \implies 40500 + 5k > 0 \implies -8100 < k$$
$$y > 0 \implies -182250 - 23k > 0 \implies -7923,91... > k \implies -7923 > k$$

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

$$x = 20250 \cdot 2 + 5 \cdot k = 40500 + 5k$$
$$y = 20250 \cdot -9 - 23 \cdot k = -182250 - 23k$$
$$k \in \{t \in \mathbb{Z} : -8100 < t < 7923\}$$

2. Relación 3

2.1. Ejercicio 1

Enunciado: 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.

$300^{207} \equiv 8^{207} mod(13) \equiv (2^3)^{207} mod(13) \equiv 2^{621}$

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 exmponentes son congruentes módulo 12.

$$621 \equiv_{12} 42 \implies 9 \equiv_{12} 8$$

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.

2.2. Ejercicio 5

Enunciado: 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 $N(1+\sqrt{3}) < N(2\sqrt{3})$ pondrémos 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. Por lo tanto el m.c.d. de $(1+\sqrt{3})$ y $(2\sqrt{3})$ es $(1+\sqrt{3})$. Veamos si $(1+\sqrt{3})$ divide $9-4\sqrt{3}$.

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

Por lo tanto el cociente la division es $q=6$ y el resto es:

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

Por lo tanto como $(1+\sqrt{3})$ no divide $9-4\sqrt{3}$ esta ecuación no tiene solución.

2.3. Ejercicio 6

Enunciado: 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: Vamos a llamar:

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

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

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:

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

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. Relación 4

3.1. Ejercicio 1

Enunciado: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:

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

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 halllada apartir 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:

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

Podríamos decir, como $1 = 50(8) + 18(-21)$ tenemos que $19(-21) \equiv 1mod(50)$ luego solo tendríamos que multiplicar por 42 y tendríamos que $19(-21 * 42) \equiv 42mod(50)$. Sin embargo, este argumento es inválido puesto que $(42, 50) = 2(21, 50) = 2 \neq 1$. En este caso,

por suerte, la congruencia de $(42, 50) = 2$ es una de los restos hallados con el Algoritmo de Euclides por lo que sí podemos hacer el siguiente argumento:

$$2 = 50(-3) + 19(8) \implies 19(8) \equiv 2 mod(50) \overset{(21,50)=1}{\implies} 19(8+21) \equiv 42 mod(50)$$

Luego, la conclusión es que $x = 8 * 21 = 168 \equiv_{50} 18$.

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 $x = 2$

3.2. Ejercicio 2

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

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. Y teniendo 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.

Así pues calculamos:

$\varphi(88) = 88 \cdot (1 - \frac{1}{2}) = 44$, es decir, $|U(\mathbb{Z}_{88}) =$ **44 unidades** y por tanto hay $88 - 44 =$ **44 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**.

3.3. Ejercicio 2(segunda parte de la relacion)

Enunciado: 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.