

UNIVERSIDAD DE GRANADA

Ejercicios resueltos Álgebra I

Doble Grado de Informática y Matemáticas

Curso 2016/17

1. Ejercicio 1 de la relación 3 - Comprobar si dos números son congruentes.

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.

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

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.

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

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

Esto implica que $7^{40} \equiv 1 \pmod{100}$

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

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

- $7 \equiv_{40} 7$
- $7^2 \equiv 49 \pmod{40}$
- $7^3 \equiv 13 \pmod{40}$
- ...
- $7^5 \equiv_{40} 7$

Luego $7^{35} \equiv_{40} 7^3 \equiv_{40} 13$, pues ya habíamos obtenido ese 13 como resultado de hacer las congruencias de las potencias sucesivas de 7.

4) $3 \cdot 5^{2n+1} + 2^{3n+1}$ 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:

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

Y seguimos desarrollando.

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

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

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

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. Ejercicio 6 de la relación 3.

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:

- $J \equiv 21 \pmod{25}$
- $A \equiv 3 \pmod{7} \equiv 3J$
- $P \equiv 11 \pmod{16} \equiv 5J$

Por lo que el sistema resultante es

$$\left. \begin{array}{l} x \equiv 21 \pmod{25} \\ 3x \equiv 3 \pmod{7} \\ 5x \equiv 11 \pmod{16} \end{array} \right\}$$

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:

$$\left. \begin{array}{l} x \equiv 21 \pmod{25} \\ 3x \equiv 3 \pmod{7} \\ 5x \equiv 11 \pmod{16} \end{array} \right\} \implies \left\{ \begin{array}{l} x \equiv 21 \pmod{25} \\ x \equiv 1 \pmod{7} \\ x \equiv 15 \pmod{16} \end{array} \right.$$

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 que nos lleva a la congruencia: $21 + y * 25 \equiv 1 \pmod{7} \implies 4y \equiv 1 \pmod{7} \implies y \equiv 2 \pmod{7}$ 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 $x \equiv 71 \pmod{175}$.

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

$$\begin{cases} x \equiv 71 \pmod{175} \\ x \equiv 15 \pmod{16} \end{cases}$$

3. Ejercicio 1 de la relación 4.

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:

$$12x \equiv 8 \pmod{20} \implies 3x \equiv 2 \pmod{5} \implies x \equiv 4 \pmod{5}$$

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 recursiva utilizando el mismo método. Al dividir 19 entre 12 tenemos que:

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

Podríamos decir, como $1 = 50(8) + 19(-21)$ tenemos que $19(-21) \equiv 1 \pmod{50}$ luego solo tendríamos que multiplicar por 42 y tendríamos que $19(-21 * 42) \equiv 42 \pmod{50}$. 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:

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

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

4) $5^{30} \mathbf{x} = \mathbf{2}$ 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 $x = 2$

4. Ejercicio 2 de la relación 4

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

1) \mathbb{Z}_{125}

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

2) \mathbb{Z}_{1000}

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

5. Ejercicio 2 (parte 2) de la relación 4

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.