

Solucionario¹ del examen de Álgebra I, primero de Ingeniería Informática
3 de septiembre de 2002

1. (2 puntos)

(a) Sea $A = \{1, 2, \dots, 10\}$ y consideremos $X = A \times A$. Se define la relación \mathcal{R} en X dada por

$$(a, b) \mathcal{R} (c, d) \iff a + b = c + d.$$

Probar que es de equivalencia.

Solución. Para decidir si un elemento de X , digamos (a, b) , está relacionado o no con otro, (c, d) , sólo hay que comprobar si la suma de las coordenadas del primero, $a + b$, coincide o no con la suma de las del segundo, $c + d$. La comprobación de las tres propiedades habituales es casi inmediata:

- Reflexiva: si $(a, b) \in X$, es claro que $(a, b) \mathcal{R} (a, b)$, porque $a + b = a + b$.
- Simétrica: si $(a, b) \mathcal{R} (c, d)$, entonces se tiene que $a + b = c + d$. Pues ya está: si queremos, cambiemos el orden en que escribimos esta identidad, $c + d = a + b$, para que quede más visual, y ya tenemos que $(c, d) \mathcal{R} (a, b)$.
- Transitiva: suponemos que $(a, b) \mathcal{R} (c, d)$ y que $(c, d) \mathcal{R} (e, f)$, y tenemos que comprobar si, en estas condiciones, se tiene que $(a, b) \mathcal{R} (e, f)$. Las dos primeras condiciones nos dicen que

$$a + b = c + d \quad \text{y} \quad c + d = e + f,$$

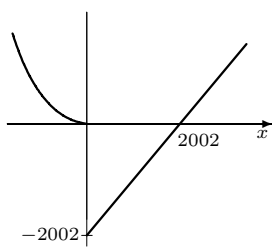
de donde se deduce que $a + b = e + f$. Y esto supone que $(a, b) \mathcal{R} (e, f)$.

(b) Sea $f : \mathbb{R} \rightarrow \mathbb{R}$ dada por

$$f(x) = \begin{cases} x^2 & \text{si } x < 0; \\ x - 2002 & \text{si } x \geq 0. \end{cases}$$

Comprobar si f es inyectiva y/o sobreyectiva.

Solución. Dibujemos un esbozo de la gráfica de $f(x)$, para hacernos una idea.



Por supuesto, el dibujo no está hecho a escala, pero nos sirve para darnos cuenta de que la función no va a ser ni inyectiva (por ejemplo, el valor $f(x) = 2$ se toma para dos valores distintos de x) ni sobreyectiva (la función no toma valores por debajo de -2002). Estas observaciones, escritas con un poco más de cuidado, sirven ya de respuesta (nótese que basta con exhibir contraejemplos). Por ejemplo, encontramos x_1 y x_2 distintos tales que $f(x_1) = f(x_2) = 2$ resolviendo

$$\begin{aligned} x_1^2 = 2 &\Rightarrow x_1 = \pm\sqrt{2} \quad \text{y nos quedamos con la raíz negativa, claro;} \\ x_2 - 2002 = 2 &\Rightarrow x_2 = 2004. \end{aligned}$$

Así que $f(-\sqrt{2}) = f(2004) = 2$, luego $f(x)$ no es inyectiva.

Para la sobreyectividad, basta observar que $f(x)$ no puede tomar el valor, digamos, -3000 , para ningún x . Porque si x es negativo, $f(x) = x^2$, una cantidad positiva. Y si $x \geq 0$, entonces $f(x) = x - 2002$, y para que esto fuera igual a -3000 tendría que ser $x = -998$ (que no es un número positivo).

¹Es una solucionario que contiene, por supuesto, las soluciones de los ejercicios. Pero que también incluye comentarios e indicaciones diversas que, aunque no se exigían en el examen, pueden ser de interés.

2. (2 puntos)

(a) ¿Es cierto que $3^{24} \equiv 1 \pmod{39}$?

Solución. La primera tentación es aplicar el teorema de Fermat-Euler, porque $\phi(39) = 24$. ¡Ah!, pero es que 3 no es primo con el módulo, 39, así que no podemos aplicar el citado teorema^a.

Hay que calcular 3^{24} módulo 39 y ver qué sale. Desde luego, no tiene sentido calcular 3^{24} y luego dividir por 39 para obtener el resto; hay que aprovechar que estamos en \mathbb{Z}_{39} . Podríamos hacerlo con el algoritmo de exponenciación rápida (que exige calcular los valores de 3^{2^n} módulo 39, para $n = 1, 2, 3, 4$), pero en este caso, podemos hacerlo de una manera más sencilla. Y es que basta observar que

$$\begin{aligned} 3^1 &\equiv 3 \pmod{39}, \\ 3^2 &\equiv 9 \pmod{39}, \\ 3^3 &\equiv 27 \pmod{39}, \\ 3^4 &= 81 = 2 \times 39 + 3 \equiv 3 \pmod{39}, \end{aligned}$$

A partir de aquí, la serie se repite periódicamente: por ejemplo (módulo 39), $3^5 \equiv 9$, $3^6 \equiv 27$, $3^7 \equiv 3$, etc. Observemos que, en las potencias n que sean múltiplos de 3, $3^n \equiv 27$. Ése es el caso, en particular, de $n = 24$, así que ya tenemos la respuesta:

$$3^{24} \equiv 27 \pmod{39}.$$

^aNo podemos aplicar el teorema, es cierto, pero, si pensamos un poco, la respuesta es bastante sencilla: sólo hay que convencerse de que no es posible que $3^n \equiv 1$ módulo 39, sea cual sea el $n \geq 1$ que tomemos, ya que 3^n es divisible por 3 y cualquier $m \equiv 1 \pmod{39}$ no es divisible por 3.

(b) Hallar todos los enteros x tales que $x \equiv 7 \pmod{12}$ y $x \equiv 4 \pmod{15}$.

Solución. Es un sistema de dos ecuaciones, pero los módulo, 12 y 15, no son primos entre sí. Pese a eso, intentemos resolver el sistema^a, de la manera habitual: primero, pasamos a un módulo común, el $mcm(12, 15) = 60$,

$$\begin{cases} x \equiv 7 \pmod{12} \\ x \equiv 4 \pmod{15} \end{cases} \implies \begin{cases} 5x \equiv 35 \pmod{60} \\ 4x \equiv 16 \pmod{60} \end{cases}$$

Llegados aquí, basta restar ambas ecuaciones para obtener la solución:

$$x \equiv 19 \pmod{60}.$$

Esto es, todos los enteros de la forma $x = 19 + 60k$, donde k es cualquier entero.

^aLo que hace que vayamos a obtener solución es que $mcd(12, 15) = 3$ divide a la diferencia $7 - 4 = 3$. Además, la solución es única módulo $mcm(12, 15) = 60$, pero eso tampoco era necesario hacerlo explícito.

3. (2 puntos)

- (a) Escribir como composición de ciclos disjuntos la siguiente permutación de S_8 :

$$\sigma = (1234) \circ (3456) \circ (5678),$$

y calcular su orden.

Solución. Sólo hay que componer las permutaciones, en el orden adecuado (primero, la que escribimos en último lugar). Démosles nombres (con subíndices que recuerdan el orden en que las vamos a ir componiendo): $\sigma = \sigma_3 \circ \sigma_2 \circ \sigma_1$. Por cuestiones de espacio, empleamos la siguiente notación para describir las sucesivas composiciones:

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \sigma_1 \\ 1 & 2 & 3 & 4 & 6 & 7 & 8 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \sigma_2 \\ 1 & 2 & 4 & 5 & 3 & 7 & 8 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \sigma_3 \\ 2 & 3 & 1 & 5 & 4 & 7 & 8 & 6 \end{array}$$

Ya tenemos la permutación σ (léase la última línea), que es fácil de descomponer en ciclos disjuntos:

$$\sigma = \left(\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 5 & 4 & 7 & 8 & 6 \end{array} \right) = (1\ 2\ 3) \circ (4\ 5) \circ (6\ 7\ 8).$$

Escrita así, calcular su orden es sencillo, pues basta obtener el mínimo común múltiplo de los órdenes de los ciclos que la componen: $mcm(3, 2, 3) = 6$.

- (b) Sea $(G, *)$ un grupo. Probar que dados $a, b \in G$, el inverso de $a * b$ es $b^{-1} * a^{-1}$.

Solución. Probablemente, el ejercicio más sencillo del examen (¡siempre que no tengamos miedo a escribir y manipular símbolos!). Tenemos un grupo G , cuya operación es $*$; y sólo podemos aplicar que la operación es cerrada y asociativa, que existe elemento neutro e y que todo elemento de G tiene inverso.

Para comprobar si $b^{-1} * a^{-1}$ es el inverso de $a * b$... ¡solo hay que “multiplicarlos”!: si sale e , ya está. Pues vamos con ello:

$$(b^{-1} * a^{-1}) * (a * b) = b^{-1} * a^{-1} * a * b = b^{-1} * e * b = b^{-1} * b = e.$$

En la primera igualdad, para “quitar” los paréntesis, utilizamos la propiedad asociativa; en la segunda, la definición de inverso (de a , en este caso). En la tercera, que e es el elemento neutro. Y, por último, la cuarta igualdad se sigue de la definición de inverso (de b).

En realidad habría que comprobar que $(a * b) * (b^{-1} * a^{-1}) = e$ (¿o quizás no?, piénsese). Pero nótese que en ningún momento hemos intercambiado el orden en que multiplicamos: ¡nadie nos ha dicho si el grupo es abeliano (conmutativo) o no! Solo en el caso de que G fuera abeliano se tendría que el inverso de $a * b$ es $a^{-1} * b^{-1}$.

4. (2 puntos) Sea $p(x) = x^3 + 3x + 111$. Determinar los **grados** de los factores irreducibles de $p(x)$ en

(a) $\mathbb{Q}[x]$ (indicación: comprobar que si $n \in \mathbb{Z}$ entonces $n^3 + 3n$ es par);

Solución. Se trata de un polinomio de grado 3, cuyos coeficientes son enteros (esto es importante). Las posibilidades que tenemos son: que el polinomio sea irreducible, que se factorice en un producto de un polinomio de grado 2 por uno de grado 1, o que sea el producto de tres de grado 1.

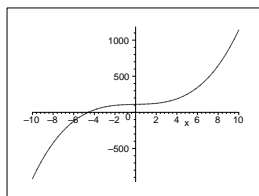
En este primer apartado, en que consideramos el polinomio en $\mathbb{Q}[x]$, hay varias formas de abordar el problema. La primera es muy directa y sencilla: consiste en aplicar el criterio de Eisenstein. Encontramos un primo $p = 3$ que divide a todos los coeficientes (menos al de x^3) y tal que $p^2 = 9$ no divide al término independiente. Así que el polinomio es irreducible en $\mathbb{Q}[x]$.

Otro posible enfoque consiste en buscar raíces (rationales) del polinomio. Los candidatos p/q a ser raíces deben cumplir que $p|111$ y $q|1$. Así que, de haber raíces racionales, deberían ser números enteros, y las únicas posibilidades son $\pm 1, \pm 3, \pm 37$ ó ± 111 (los divisores positivos y negativos de 111).

Se podría comprobar, uno a uno, si estos números son realmente raíces del polinomio (y se vería que no). Pero es más sencillo utilizar la indicación del enunciado. Primero comprobamos que $n^3 + 3n$ es, para cualquier $n \in \mathbb{Z}$, un número par: si n es par, es obvio. Y si n es impar, n^3 y $3n$ son impares, luego su suma, $n^3 + 3n$, es par. De manera que, al sumarle 111 a $x^3 + 3x$ (si x es un número entero), nunca obtendremos 0. No hay raíces enteras, así que el polinomio es irreducible.

(b) $\mathbb{R}[x]$ (indicación: dibujar la gráfica);

Solución. Dibujamos, como nos sugiere el enunciado, la gráfica de $p(x)$:



Y observamos que hay un punto de corte con el eje real (en torno a $x = -5$): ésa es una raíz real del polinomio. ¿Cómo asegurar que no hay más? Si calculamos la derivada, $p'(x) = 3x^2 + 3$, vemos que es una función positiva (de hecho, $p'(x) \geq 3$ para cualquier $x \in \mathbb{R}$), así que la función $p(x)$ es creciente, de manera que no puede haber más raíces^a. En conclusión, el polinomio $p(x)$ es el producto de un polinomio de grado 1 y uno (irreducible) de grado 2.

^aSi queremos ponernos más finos, el que $p(x) \rightarrow +\infty$ cuando $x \rightarrow \infty$ y $p(x) \rightarrow -\infty$ cuando $x \rightarrow -\infty$, junto con el hecho de que $p(x)$ sea una función continua, es lo que hace que podamos asegurar que tiene, al menos, una raíz real. Y el que la función sea creciente nos asegura que no puede haber más de una.

(c) $\mathbb{C}[x]$.

Solución. No hay mucho que decir aquí: el Teorema Fundamental del Álgebra nos asegura que el polinomio, que es de grado 3, tiene tres raíces complejas. Así que se puede escribir como el producto de tres polinomios de grado 1.

5. (2 puntos)

- (a) Hallar todas las soluciones de la ecuación diofántica $307x + 1524y = 1$.

Solución. Aplicamos primero el algoritmo de Euclides:

$$\begin{aligned} 1524 &= 4 \times 307 + 296 \\ 307 &= 1 \times 296 + 11 \\ 296 &= 26 \times 11 + 10 \\ 11 &= 1 \times 10 + 1 \\ 10 &= 10 \times 1 + 0 \end{aligned}$$

Comprobamos así que $\text{mcd}(1524, 307) = 1$, y por eso vamos a encontrar soluciones de la ecuación.

Para hallar una particular, digamos (x_0, y_0) , de la ecuación, utilizamos los cálculos anteriores: a partir de la penúltima línea, escribimos 1 como combinación lineal (con coeficiente enteros) de los sucesivos pares de números involucrados: 11 y 10, 11 y 296, 296 y 307; y, por último, de 307 y 1524.

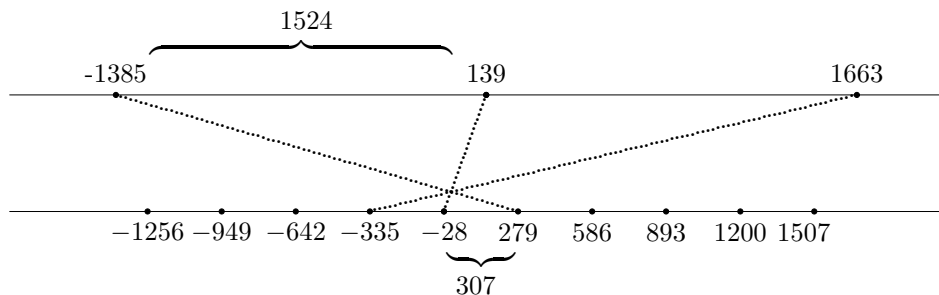
$$\begin{aligned} 1 &= 11 - 1 \times 10 \\ &= -1 \times 296 + 27 \times 11 && \text{ya que } 10 = 296 - 26 \times 11 \\ &= 27 \times 307 - 28 \times 296 && \text{ya que } 11 = 307 - 1 \times 296 \\ &= \underbrace{139}_{=x_0} \times 307 - \underbrace{28}_{=y_0} \times 1524 && \text{ya que } 296 = 1524 - 4 \times 307 \end{aligned}$$

Así que una solución de la ecuación es el par $(139, -28)$. Escribir la solución general es ahora sencillo:

$$\begin{cases} x &= 139 + 1524k \\ y &= -28 - 307k \end{cases} \quad \text{donde } k \text{ es cualquier entero.}$$

- (b) De entre las soluciones (x, y) de la ecuación anterior, ¿hay alguna con $1524000 \leq x \leq 1524500$?

Solución. Las soluciones del apartado anterior forman un par de progresiones aritméticas, que representamos en la figura (arriba, los valores de x , abajo los de y ; en línea discontinua, cómo se emparejan):



Pero en este segundo apartado sólo nos piden fijarnos en la progresión aritmética de la línea de arriba. ¿Habrá algún valor en el intervalo $[1524000, 1524500]$? Dado que los “saltos” arriba son de longitud 1524, no son necesarias muchas cuentas: para $k = 1000$ tenemos el valor 1524139 en el intervalo (y no hay ningún otro).

6. (Este ejercicio supone 1 punto extra sobre el 10).

(a) Calcular 2^n módulo 6, para $n = 1, 2, 3, \dots$

Solución. Calculamos los primeros casos:

$$2^1 \equiv 2 \pmod{6}$$

$$2^2 \equiv 4 \pmod{6}$$

$$2^3 \equiv 2 \pmod{6}$$

$$2^4 \equiv 4 \pmod{6}$$

No hay que seguir: vemos que el patrón se va a repetir periódicamente (algo que se puede probar, más formalmente, por inducción). Así que, módulo 6,

$$2^n \equiv \begin{cases} 4 & \text{si } n \text{ es par;} \\ 2 & \text{si } n \text{ es impar.} \end{cases}$$

(b) Usar lo anterior para calcular a_{13} módulo 7, donde $a_1 = 2$ y $a_{k+1} = 2^{a_k}$, para cada $k \geq 1$.

Solución. Los primeros términos de la sucesión $\{a_j\}$ son

$$a_1 = 2, \quad a_2 = 2^{a_1} = 2^2 = 4, \quad a_3 = 2^{a_2} = 2^4 = 16 \dots$$

Es claro que son todos números pares (en realidad, potencias de 2). Por lo tanto,

$$a_{12} = 2^{a_{11}} \equiv 4 \pmod{6},$$

por el apartado anterior (y el hecho de que a_{11} es par). Podremos escribir, entonces, a_{12} como

$$a_{12} = 6k + 4, \quad \text{donde } k \text{ es cierto entero.}$$

Nos piden calcular a_{13} módulo 7. Con lo que tenemos hasta aquí, podemos escribir que

$$a_{13} = 2^{a_{12}} = 2^{6k+4} = (2^6)^k 2^4.$$

¡Ah!, pero en \mathbb{Z}_7 resulta que $2^6 \equiv 1$ (por el teorema de Fermat). Así que el cálculo es bien sencillo:

$$a_{13} = (2^6)^k 2^4 \equiv 2^4 = 16 \equiv 2 \pmod{7}.$$