

Examen parcial de Matemática Discreta 2

IMERL/FIng/UdelaR

26 de abril de 2018

1. (a)
 - i. Definir número primo.
 - ii. Enunciar el teorema fundamental de la aritmética.
 - iii. Expresar la cantidad de divisores positivos de un número natural en función de su descomposición en factores primos.
- (b) Probar que x es un cuadrado perfecto si y sólo si en la descomposición en factores primos de x , todos sus factores primos aparecen con exponente par.
- (c) Hallar todos los enteros que admiten exactamente 27 divisores positivos y son menores o iguales a 7000. ¿Cuáles de estos son cuadrados perfectos?

- (a) Sea $p \in \mathbb{N}$. p es primo si y sólo si $p \geq 2$ y los únicos divisores positivos de p son 1 y p . El teorema fundamental de la aritmética establece que todo natural $x \geq 2$ se descompone en forma única como producto de primos. Más precisamente:

$$\forall n \in \mathbb{N} \quad n \geq 2 \Rightarrow \exists! k \in \mathbb{N}^* \exists! \alpha_1, \dots, \alpha_k \in \mathbb{N}^*$$

$$\exists! p_1, \dots, p_k \text{ primos } x = \prod_{i=1}^k p_i^{\alpha_i}$$

Observar que los primos y sus exponentes son únicos a menos de permutaciones en el orden, ya que el producto es conmutativo.

Si la descomposición en factores primos de x es $\prod_{i=1}^k p_i^{\alpha_i}$, la cantidad de divisores positivos de x es $\prod_{i=1}^k (\alpha_i + 1)$. Este resultado se probó en el curso (la prueba no se pedía).

- (b) Sea $x = y^2 = y \cdot y$. Sea $y = \prod_{i=1}^k p_i^{\alpha_i}$ la descomposición en factores primos de y . Entonces $x = y^2 = \left(\prod_{i=1}^k p_i^{\alpha_i} \right)^2 = \prod_{i=1}^k p_i^{2\alpha_i}$ y esta última es la descomposición en factores primos de x por la unicidad de la descomposición en producto de primos (teorema fundamental de la aritmética, enunciado en la parte anterior). Esto prueba que si x es un cuadrado perfecto, sus factores primos aparecen con exponente par (los $2\alpha_i$ son todos pares). El recíproco es inmediato: Si $\prod_{i=1}^k p_i^{2\alpha_i}$ es la descomposición en factores primos de x , entonces $x = \left(\prod_{i=1}^k p_i^{\alpha_i} \right)^2$, que es un cuadrado perfecto.

(c) Si $x = \prod_{i=1}^k p_i^{\alpha_i}$, entonces tiene $\prod_{i=1}^k (\alpha_i + 1)$ divisores positivos (enunciado en la parte a). Si este producto es $27 = 3^3$, entonces las posibilidades son:

- i. x tiene tres factores primos, todos ellos con exponente 2 (expresando $27 = 3 \times 3 \times 3 = (\alpha_1 + 1) \times (\alpha_2 + 1) \times (\alpha_3 + 1)$).
- ii. x tiene dos factores primos, uno con exponente 8 y el otro con exponente 2 (expresando $27 = 3 \times 9 = (\alpha_1 + 1) \times (\alpha_2 + 1)$).
- iii. x tiene un sólo factor primo de exponente 26 (expresando $27 = \alpha_1 + 1$).

En todo lo que sigue, usaremos la monotonía del producto para decidir cuáles son las posibles soluciones.

- i. Veamos el caso de los que admiten 3 factores primos $p < q < r$ de exponente 2. Los que admiten factor 2 ($p = 2$) aparecen en

$2^2 \times q^2 \times r^2$	resultado
$2^2 \times 3^2 \times 5^2$	900
$2^2 \times 3^2 \times 7^2$	1764
$2^2 \times 3^2 \times 11^2$	4356
$2^2 \times 3^2 \times 13^2$	6084
$2^2 \times 5^2 \times 7^2$	4900

la siguiente tabla:

Dado que $2^2 \times 3^2 \times 17^2 = 10404$, no hay más números de la forma $2^2 \times 3^2 \times r^2$ en el rango pedido. Dado que $2^2 \times 5^2 \times 11^2 = 12100$, tampoco hay más números de la forma $2^2 \times 5^2 \times r^2$ en el rango pedido. Similarmente, no hay números de la forma $2^2 \times 7^2 \times r^2$ en el rango pedido, ya que el menor de ellos es $2^2 \times 7^2 \times 11^2 = 23716 > 7000$.

El menor de los números de la forma $p^2 \times q^2 \times r^2$ que no admite el factor 2 es $3^2 \times 5^2 \times 7^2 = 11025 > 7000$.

Concluimos que en el rango pedido, los números con 27 divisores que admiten 3 factores primos distintos admiten necesariamente el factor 2 y son los que aparecen en la tabla.

- ii. Ahora estudiaremos en caso de los que admiten dos factores primos $p < q$. Estos números pueden ser $p^8 \times q^2$ o $p^2 \times q^8$. Tenemos la siguiente tabla con los que admiten factor 2 ($p = 2$):

$2^8 \times p^2$	resultado
$2^8 \times 3^2$	2304
$2^8 \times 5^2$	6400

Como $2^8 \times 7^2 = 12544$, no hay más números de la forma $2^8 \times q^2$ en el rango pedido.

Además, el menor número de la forma $2^2 \times q^8$ es $2^2 \times 3^8 = 26244 > 7000$, de modo que no hay números de la forma $2^2 \times q^8$ en el rango pedido.

El menor de los números de la forma $p^8 \times q^2$ que no admite factor 2 es $3^8 \times 5^2 = 164025 > 7000$.

Concluimos que en el rango pedido, los números con 27 divisores que admiten dos factores primos distintos admiten el factor 2 y son los que aparecen en la tabla.

- iii. Como $2^{26} = 67108864 > 7000$ y 2 es el menor primo, es claro que en el rango pedido no hay números de la forma p^{26} con p primo.

En definitiva, los números pedidos son los que aparecen en las tablas:

$$\{900, 1764, 2304, 4356, 4900, 6084, 6400\}$$

Son todos cuadrados perfectos puesto que sus factores primos aparecen una cantidad par de veces en su descomposición en factores primos (resultado enunciado en la pregunta de la parte b).

2. (a) Definir \mathbb{Z}_n , el conjunto de los enteros módulo n . Definir las operaciones de suma y producto en \mathbb{Z}_n . ¿Para qué números naturales n los elementos no nulos de \mathbb{Z}_n son todos invertibles (resp. al producto)?
- (b) Hallar el inverso de 10 en \mathbb{Z}_7 . Probar que $\forall x, y \in \mathbb{Z}$ $10x + y$ es múltiplo de 7 si y sólo si $x - 2y$ es múltiplo de 7.
- (c) Probar usando (b) que el número cuya representación en base 10 es $\underbrace{22 \dots 2}_n 3$ con $n \in \mathbb{N}$ no es múltiplo de 7 para ningún n (**Sug:** razonar por inducción completa).

- (a) Para cada natural n se define la relación de equivalencia (en \mathbb{Z}) $x \equiv_n y \iff n|(x - y)$. Esta relación determina un conjunto cociente que es $\mathbb{Z}_n := \mathbb{Z} / \equiv_n$, esto es: $\mathbb{Z}_n = \{\bar{i} \mid i \in \mathbb{Z}\}$ donde $\bar{i} = \{n \in \mathbb{Z} \mid n \equiv_n i\} = i + n\mathbb{Z}$ (es decir, \bar{i} es la clase de equivalencia de i).

Se definen: $\bar{x} + \bar{y} := \overline{x + y}$ y $\bar{x} \cdot \bar{y} := \overline{x \cdot y}$. Se probó en el curso que estas definiciones son compatibles con la relación \equiv_n y por lo tanto son correctas en \mathbb{Z}_n (no se pide probar esto). Esto significa:

- Para todo x, x', y, y' si $x \equiv_n x'$ e $y \equiv_n y'$, entonces $x + y \equiv_n x' + y'$.
- Para todo x, x', y, y' si $x \equiv_n x'$ e $y \equiv_n y'$, entonces $x \cdot y \equiv_n x' \cdot y'$.

La condición necesaria y suficiente para que todos los elementos de $\mathbb{Z}_n \setminus \{\bar{0}\}$ sean invertibles es que n sea primo. No se pedía probar este resultado del curso.

- (b) Invertir 10 en \mathbb{Z}_7 es equivalente a invertir 3, puesto que ambos son equivalentes módulo 7. Como $5 \times 3 = 15 \equiv_7 1$, concluimos que 5 es el inverso de 10.

Por la definición de la relación \equiv_7 , $10x + y$ es múltiplo de 7 si y sólo si $10x + y \equiv_7 0$. Además tenemos que 5 es el inverso de 10 módulo 7. Entonces:

$$\begin{aligned}
10x + y &\equiv_7 0 && \Longleftrightarrow \\
5 \times (10x + y) &\equiv_7 5 \times 0 && \Longleftrightarrow \\
x + 5y &\equiv_7 0 && \Longleftrightarrow \\
x - 2y &\equiv_7 0
\end{aligned}$$

Siendo la última línea consecuencia de que $-2 \equiv_7 5^1$.

- (c) Lo probamos por inducción completa en n . Para $n = 0$ es inmediato ya que 3 no es múltiplo de 7.

Sea $x = \underbrace{22 \dots 2}_{n+1} 3$ y supongamos que $\underbrace{22 \dots 2}_n 3$ no es múltiplo de 7.

A x lo podemos escribir como $10 \times \underbrace{22 \dots 2}_{n+1} + 3$, de modo que por el criterio de la parte b, x es múltiplo de 7 si y sólo si $\underbrace{22 \dots 2}_{n+1} - 6$ es múltiplo de 7. Como $-6 \equiv_7 1$, entonces $\underbrace{22 \dots 2}_{n+1} - 6 \equiv_7 \underbrace{22 \dots 2}_{n+1} + 1 = \underbrace{22 \dots 2}_n 3$ y por hipótesis de inducción, este número no es múltiplo de 7.

Esta parte se puede formular con 9 en lugar de 2 o tomando n dígitos del conjunto $\{2, 9\}$, ya que $2 \equiv_7 9$.

3. (a) Definir la función de Euler. Enunciar el Teorema de Euler.
(b) Probar que para todo $m, n \in \mathbb{N}$:

$$m, n > 1 \text{ y coprimos} \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$$

- (c) Calcular 6397^{6397} módulo 360.

- (a) La función de Euler se define como $\varphi : \mathbb{N}^* \rightarrow \mathbb{N}$
 $\varphi(n) := \#\{x \in \mathbb{N}^* \mid x < n \text{ y } \gcd(x, n) = 1\}$. Equivalentemente, $\varphi(n) = \#\mathbb{Z}_n^*$, es decir, $\varphi(n)$ es el orden del grupo multiplicativo de \mathbb{Z}_n .

El teorema de Euler dice que, si $\gcd(a, n) = 1$ ($a \in \mathbb{Z}$ y $n \in \mathbb{N}^*$), entonces $a^{\varphi(n)} \equiv_n 1$.

- (b) Sea m, n coprimos. Lo que se nos pide probar es que $\#\mathbb{Z}_{mn}^* = \#\mathbb{Z}_m^* \#\mathbb{Z}_n^*$. Como el producto de cardinales es el cardinal del producto cartesiano, el resultado equivale a probar:

$$\#\mathbb{Z}_{mn}^* = \#(\mathbb{Z}_m^* \times \mathbb{Z}_n^*)$$

Para esto, consideramos para cada natural m a $\pi_m : \mathbb{Z} \rightarrow \mathbb{Z}_m$ definida como $\pi_m(x) := \bar{x} = x + m\mathbb{Z}$ ($\pi_m(x)$ es la clase de equivalencia de x módulo m).

¹La partes b de este ejercicio pide lo mismo que las partes a y b del ejercicio 16 del práctico

Observamos que si $x \equiv_{mn} y$, entonces $x \equiv_m y$ y $x \equiv_n y$. Esto prueba que la función $\Psi : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ definida como $\Psi(\bar{x}) := (\pi_m(x), \pi_n(x))$ está bien definida². Probaremos que si restringimos Ψ a los invertibles de \mathbb{Z}_{mn} , obtenemos una biyección

$$\widehat{\Psi} : \mathbb{Z}_{mn}^* \rightarrow \mathbb{Z}_m^* \times \mathbb{Z}_n^*$$

Sea $(\bar{a}, \bar{b}) = (a + m\mathbb{Z}, b + n\mathbb{Z}) \in \mathbb{Z}_m^* \times \mathbb{Z}_n^*$. Como m, n son coprimos, por el teorema chino del resto sabemos que

$$\begin{cases} x \equiv_m a \\ x \equiv_n b \end{cases} \iff x \equiv_{mn} x_0$$

donde x_0 es una solución particular del sistema. Dicho de otro modo, el teorema afirma que la solución existe y es única módulo mn .

La solución x_0 es entonces invertible módulo m (ya que $x_0 \equiv_m a \in \mathbb{Z}_m^*$) e invertible módulo n (ya que $x_0 \equiv_n b \in \mathbb{Z}_n^*$). Entonces $\gcd(x_0, m) = \gcd(x_0, n) = 1$ y concluimos que $\gcd(x_0, mn) = 1$, de donde $\bar{x}_0 \in \mathbb{Z}_{mn}^*$.

La existencia de x_0 afirma entonces que Ψ es sobreyectiva y la unicidad módulo mn afirma que Ψ es inyectiva³.

- (c) Primero reducimos 6397 módulo 360, obteniendo 277. Como $360 = 2^3 \times 3^2 \times 5$ y 277 no es divisible entre ninguno de los factores 2, 3 y 5, entonces 277 y 360 son coprimos. Por otra parte $\varphi(360) = \varphi(2^3)\varphi(3^2)\varphi(5) = 4 \times 6 \times 4 = 96$, usando la fórmula que se probó en la parte b y que $\varphi(p^k) = p^k - p^{k-1}$ cuando p es primo. Reduciendo el exponente módulo 96 obtenemos 61. Entonces, tenemos que calcular 277^{61} módulo 360.

$61 = 2^5 + 2^4 + 2^3 + 2^2 + 1$ (61 en base 2 es 111101), de modo que

$$277^{61} = 277^{2^5} \times 277^{2^4} \times 277^{2^3} \times 277^{2^2} \times 277$$

(método de exponenciación rápida, visto en el curso).

La siguiente tabla recoge módulo 360 los sucesivos valores de 277^{2^i} con $i = 0, 1, 2, 3, 4$ y 5 (recordar la fórmula recursiva $a^{2^{i+1}} = (a^{2^i})^2$):

i	277^{2^i}
0	277
1	$76729 \equiv_{360} 49$
2	$2401 \equiv_{360} 241$
3	$58081 \equiv_{360} 121$
4	$14641 \equiv_{360} 241$
5	$58081 \equiv_{360} 121$

²Es decir: que no depende del representante x elegido

³La demostración de este resultado visto en el curso la pueden leer también en las notas (Teorema 2.6.3)

Entonces $277^{61} \equiv_{360} 121 \times 241 \times 121 \times 241 \times 277 \equiv_{360} 277$ ya que $121 \times 241 \equiv_{360} 1$.

Una alternativa es plantear que $x \equiv_{360} 6397^{6397}$ si y sólo si:

$$\begin{cases} x \equiv_8 6397^{6397} \\ x \equiv_9 6397^{6397} \\ x \equiv_5 6397^{6397} \end{cases} \quad \begin{cases} x \equiv_8 5 \\ x \equiv_9 7 \\ x \equiv_5 2 \end{cases} \quad . \text{ Esta reducción se hace aplicando Eu-}$$

ler en cada exponente y reduciendo las bases en los respectivos módulos. Aplicando las técnicas vistas en el curso se puede resolver este sistema en congruencias, reduciéndolo a $x \equiv_{360} 277$.