

PRIMER PARCIAL - 6 MAYO 2024 - DURACIÓN: 3 HORAS.

Número de parcial	Cédula	Nombre y Apellido

Las respuestas deben estar correctamente argumentadas. Se debe incluir el razonamiento utilizado para obtener cada resultado.

- Enunciar el teorema fundamental de la aritmética (no se pide probarlo).
 - Enunciar y probar una expresión para la cantidad de divisores positivos de un número natural, en función de su descomposición en factores primos.
 - Probar que $x \in \mathbb{N}$ es un cuadrado perfecto, si y sólo si, en la descomposición en factores primos de x , todos sus factores primos aparecen con exponente par.
 - Hallar todos los naturales menores o iguales a 400 que admiten exactamente 9 divisores positivos. ¿Cuáles de estos naturales son cuadrados perfectos?
- Enunciar el Teorema Chino del Resto (en el caso general de $k \geq 2$ ecuaciones).
 - Demostrar el Teorema Chino del Resto para el caso de 2 ecuaciones.
 - Investigar si el siguiente sistema tiene solución, y en caso afirmativo hallar todas sus soluciones.
$$\begin{cases} x \equiv 17 \pmod{88} \\ x \equiv 83 \pmod{143} \end{cases}.$$
- Definir la función φ de Euler y enunciar el teorema de Euler.
 - Enunciar y probar una expresión para calcular $\varphi(p^n)$, siendo p primo y $n \in \mathbb{Z}^+$.
 - Hallar un entero $0 \leq m < 297$, tal que $m \equiv 30^{132} \pmod{297}$.

Solución

Ejercicio 1

1. Enunciar el teorema fundamental de la aritmética (no se pide probarlo).

Ver Teorema 1.7.1 de las notas del curso, y la Observación 1.7.4. Ambos enunciados son equivalentes.

2. Enunciar y probar una expresión para la cantidad de divisores positivos de un número natural, en función de su descomposición en factores primos.

Ver Corolario 1.7.6 de las notas del curso, ítem 2.

3. Probar que $x \in \mathbb{N}$ es un cuadrado perfecto, si y sólo si, en la descomposición en factores primos de x , todos sus factores primos aparecen con exponente par.

Ver Corolario 1.7.6 de las notas del curso, ítem 3.

4. Hallar todos los naturales menores o iguales a 400 que admiten exactamente 9 divisores positivos. ¿Cuáles de estos naturales son cuadrados perfectos?

Fijemos $n \in \mathbb{N}$ arbitrario. Por el Teorema fundamental de la aritmética, existen primos distintos p_i , y exponentes enteros $n_i \geq 0$, tales que: $n = p_1^{n_1} \dots p_r^{n_r}$. Usando la Parte (b) de este ejercicio, podemos expresar la cantidad de divisores positivos de n como: $Div_+(n) = (n_1 + 1) \dots (n_r + 1)$. Por lo tanto, buscamos n que cumpla:

$$Div_+(n) = (n_1 + 1) \dots (n_r + 1) = 9 = 3 \times 3.$$

Como 3 es primo, hay solamente dos formas en que se puede cumplir lo anterior:

- (a) **Caso 1:** existe un índice i para el cual $n_i + 1 = 9$; y los restantes índices cumplen: $n_j + 1 = 1$. Es decir: $n_i = 8$, y $n_j = 0$, para todo $j \neq i$. En este caso $n = p_i^8$, con p_i primo. La condición $n \leq 400$ equivale a: $p_i^8 \leq 400$. El único primo que cumple esto es: $p_i = 2$. Por lo tanto, este caso aporta únicamente el natural $n = 2^8 = 256$.
- (b) **Caso 2:** existen dos índices distintos i y k , tales que: $n_i + 1 = 3$, $n_k + 1 = 3$; y los restantes índices cumplen: $n_j + 1 = 1$. Es decir: $n_i = n_k = 2$, y $n_j = 0$, para todo $j \notin \{i, k\}$. En este caso $n = p_i^2 p_k^2$, con p_i y p_k primos distintos. La condición $n \leq 400$ equivale a: $p_i^2 p_k^2 \leq 400$. Las parejas de primos distintos que cumplen esta condición, son: $(p_i, p_k) \in \{(2, 3), (2, 5), (2, 7), (3, 5)\}$. Los naturales asociados son:

$$n = p_i^2 p_k^2 \in \{2^2 3^2, 2^2 5^2, 2^2 7^2, 3^2 5^2\} = \{36, 100, 196, 225\}.$$

Por lo tanto, el conjunto de números naturales que cumplen lo pedido, es:

$$\{2^8, 2^2 3^2, 2^2 5^2, 2^2 7^2, 3^2 5^2\} = \{256, 36, 100, 196, 225\}.$$

Usando la Parte (c) de este ejercicio, es inmediato ver que todos son cuadrados perfectos.

Ejercicio 2

1. Enunciar el Teorema Chino del Resto (en el caso general de $k \geq 2$ ecuaciones).

Ver Teorema 2.5.1 de las notas del curso.

2. Demostrar el Teorema Chino del Resto para el caso de 2 ecuaciones.

Ver la prueba del Teorema 2.5.1 de las notas del curso. Lo que se pide probar equivale al paso base $k = 2$ de dicha prueba.

3. Investigar si el siguiente sistema tiene solución, y en caso afirmativo hallar todas sus soluciones.

$$\begin{cases} x \equiv 17 \pmod{88} \\ x \equiv 83 \pmod{143} \end{cases}.$$

Veamos primero si los módulos son coprimos, para intentar aplicar el TCR al sistema. La factorización en primos del primer módulo es: $88 = 2^3 \times 11$. El segundo módulo no es divisible entre 2, pero sí es divisible entre 11, pues: $143 = 11 \times 13$. Por lo tanto: $\text{mcd}(88, 143) = 11$. Como los módulos no son coprimos, no podemos aplicar el TCR al sistema. Sin embargo, sí podemos aplicar el TCR a cada ecuación por separado. Esto permite afirmar que el sistema original equivale a:

$$\begin{cases} x \equiv 17 \pmod{8 \times 11} \\ x \equiv 83 \pmod{11 \times 13} \end{cases} \Leftrightarrow \begin{cases} x \equiv 17 \pmod{2^3} \\ x \equiv 17 \pmod{11} \\ x \equiv 83 \pmod{11} \\ x \equiv 83 \pmod{13} \end{cases}.$$

Antes de continuar reducimos respecto a cada módulo. En particular, haciendo esto vemos que la segunda y tercera ecuación del nuevo sistema son equivalentes:

$$\begin{cases} x \equiv 17 \pmod{2^3} \\ x \equiv 17 \pmod{11} \\ x \equiv 83 \pmod{11} \\ x \equiv 83 \pmod{13} \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \pmod{8} \\ x \equiv 6 \pmod{11} \\ x \equiv 5 \pmod{13} \end{cases}.$$

Obtenemos entonces un sistema equivalente al original, pero con la ventaja de que sus

módulos son coprimos. Por lo tanto, por el TCR, podemos afirmar que el sistema tiene solución, y que esta es única módulo el producto de los módulos: $8 \times 11 \times 13 = 1144$.

Veamos ahora cuáles son las soluciones del sistema. De la primera ecuación se obtiene: $x = 1 + 8k$, con $k \in \mathbb{Z}$. Reemplazando en la segunda ecuación:

$$(1 + 8k) \equiv 6 \pmod{11} \Leftrightarrow 8k \equiv 5 \pmod{11}.$$

Para “despejar” k , vamos a calcular el inverso de 8 módulo 11. Es decir, buscamos $z \in \mathbb{Z}$, tal que: $8z \equiv 1 \pmod{11}$. Por definición de congruencia, esto equivale a la ecuación diofántica: $8z - 11l = 1$, con variables $z, l \in \mathbb{Z}$. Usando el algoritmo de Euclides extendido, podemos ver que una solución particular es: $z = -4$, $l = -3$. Por lo tanto, el inverso buscado es: $z \equiv -4 \pmod{11}$. Reemplazando esta inversa en la ecuación anterior, se obtiene:

$$8k \equiv 5 \pmod{11} \Leftrightarrow k \equiv -20 \pmod{11} \equiv 2 \pmod{11}.$$

Es decir: $k = 2 + 11m$, con $m \in \mathbb{Z}$. Reemplazando, se obtiene la solución de las primeras dos ecuaciones del sistema:

$$x = 1 + 8k = 1 + 8(2 + 11m) = 17 + 88m \equiv 17 \pmod{88}.$$

Por lo tanto, el sistema a resolver es ahora:

$$\begin{cases} x \equiv 17 \pmod{88} \\ x \equiv 5 \pmod{13} \end{cases}.$$

De la primera ecuación: $x = 17 + 88k$, con $k \in \mathbb{Z}$. Reemplazando en la segunda ecuación:

$$(17 + 88k) \equiv 5 \pmod{13} \Leftrightarrow 88k \equiv -12 \pmod{13} \Leftrightarrow 10k \equiv 1 \pmod{13}.$$

Es decir: k es el inverso de 10 módulo 13. Por lo tanto, para hallar k , podemos resolver la siguiente diofántica: $10k = 13l + 1$. Si probamos con algunos valores positivos de l , vemos que se cumple: $13(3) + 1 = 40$; por lo que una solución particular es: $k = 4$, $l = 3$. Por lo tanto: $k \equiv 4 \pmod{13}$. Es decir: $k = 4 + 13m$, con $m \in \mathbb{Z}$. Reemplazando, se obtiene la solución del sistema:

$$x = 17 + 88k = 17 + 88(4 + 13m) = 369 + 88 \times 13m \equiv 369 \pmod{8 \times 11 \times 13}.$$

Ejercicio 3

1. Definir la función φ de Euler y enunciar el teorema de Euler.

Ver la Definición 2.6.1 de las notas del curso.

2. Enunciar y probar una expresión para calcular $\varphi(p^n)$, siendo p primo y $n \in \mathbb{Z}^+$.

Ver el Ejemplo 2.6.2. de las notas del curso, ítem 4.

3. Hallar un entero $0 \leq m < 297$, tal que $m \equiv 30^{132} \pmod{297}$.

Veamos primero si podemos usar el Teorema de Euler para calcular la potencia pedida. La factorización de la base es: $30 = 2 \times 3 \times 5$, y la del módulo es: $297 = 3 \times 99 = 3^3 \times 11$. Por lo tanto: $\text{mcd}(30, 297) = 3$. Como la base y el módulo no son coprimos, no podemos usar el Teorema de Euler para calcular la potencia pedida. Sin embargo, usando el TCR, podemos afirmar que el problema inicial es equivalente al siguiente sistema de congruencias:

$$m \equiv 30^{132} \pmod{3^3 \times 11} \Leftrightarrow \begin{cases} m \equiv 30^{132} \pmod{3^3} \\ m \equiv 30^{132} \pmod{11} \end{cases}.$$

Ahora vamos a tratar de simplificar cada ecuación por separado, para obtener un sistema de congruencias más sencillo. Para simplificar la primera ecuación, podemos argumentar de la siguiente forma:

$$30 = 3 \times 10 \Rightarrow 30^{132} = 3^{132} 10^{132} = 3^3 3^{129} 10^{132} \equiv 0 \pmod{3^3}.$$

Por lo tanto, por transitiva, la primera ecuación equivale a: $m \equiv 0 \pmod{3^3}$.

Para simplificar la segunda ecuación, intentemos usar el Teorema de Euler. En este caso el módulo y la base sí son coprimos: $\text{mcd}(30, 11) = 1$. Por lo tanto, por el Teorema de Euler: $30^{\varphi(11)} = 30^{10} \equiv 1 \pmod{11}$. Por otro lado: $132 = 13 \times 10 + 2$. Por lo tanto:

$$30^{132} = (30^{10})^{13} 30^2 \equiv 30^2 \pmod{11} \equiv 900 \pmod{11} \equiv 9 \pmod{11}.$$

El sistema es entonces:

$$m \equiv 30^{132} \pmod{3^3 \times 11} \Leftrightarrow \begin{cases} m \equiv 0 \pmod{3^3} \\ m \equiv 9 \pmod{11} \end{cases}.$$

De la primera ecuación: $m = 27k$, con $k \in \mathbb{Z}$. Reemplazando en la segunda y simplificando:

$$27k \equiv 9 \pmod{11} \Leftrightarrow 5k \equiv 9 \pmod{11}.$$

Es sencillo ver que $k = 4$ es solución particular de esta ecuación. Por lo tanto: $k = 4 + 11l$, con $l \in \mathbb{Z}$. Reemplazando:

$$m = 27k = 27(4 + 11l) \equiv 27 \times 4 \pmod{27 \times 11} \equiv 108 \pmod{27 \times 11}.$$