Algunos ejercicios de la teoría de números elemental

Alexey Beshenov (cadadr@gmail.com)

21 de septiembre de 2021

Los ejercicios de esta hoja usan los siguientes conceptos de la teoría de números elemental: divisibilidad, mcd, identidad de Bézout, factorización en números primos, congruencias $\text{mód } n$, función ϕ de Euler.

Para las soluciones, véase
`https://cadadr.org/teoria-de-numeros-basica/guia-1-soluciones.pdf`

Ejercicios para hacer en vivo

Problema 0.

a) Encuentre el mínimo número positivo n de la forma $30\,a + 105\,b$ para $a, b \in \mathbb{Z}$.
¿Cuáles son los a y b correspondientes? ¿Son únicos?

b) Calcule $5^{2021} \pmod{13}$.

c) Para $N = 105$, ¿cuántos números $0 \le x < N$ son invertibles módulo N?

d) Para $n = 2, 3, 4, 5, 6$, ¿cuántos números $0 \le x < 13$ satisfacen $x \equiv y^n \pmod{13}$ para algún $y \in \mathbb{Z}$?

Problema 1. Si $\operatorname{mcd}(a, b) = \operatorname{mcd}(c, d) = 1$ y $\frac{a}{b} + \frac{c}{d}$ es un número entero, demuestre que necesariamente $b = \pm d$.

Problema 2. El teorema de Wilson afirma que $(p-1)! \equiv -1 \pmod{p}$ para p primo. Demuestre que $(n-1)! \equiv 0 \pmod{n}$ si $n \ge 6$ es compuesto.

Problema 3.

a) Demuestre que $\operatorname{mcd}(a, a+b) \mid b$.

b) Si $\operatorname{mcd}(a, b) = 1$, demuestre que $\operatorname{mcd}(a+b, a-b) = 1$ o 2.
En particular, calcule $\operatorname{mcd}(a+1, a-1)$.

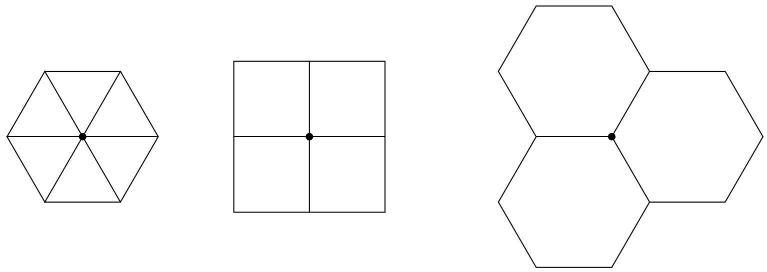
Problema 4 (IWYMIC 2019 Individual contest)**.** Encuentre el mínimo n tal que $x = 55n^3$ que tiene 55 divisores $1 \le d \le x$, $d \mid x$.

Problema 5 (IWYMIC 2019 Team contest)**.** p_1, p_2, p_3 son primos tales que

$$p_1 p_2 p_3 = p_1 + p_2 + p_3 + 1007.$$

Encuentre p_1, p_2, p_3.

Problema 6. Se fija un punto en el plano y se consideran unas copias de n-ágono regular, tratando de colocarlas alrededor del punto. Demuestre que esto es posible solamente con 6 triángulos, o 3 cuadrados, o 6 hexágonos, como en el dibujo de abajo:



Sugerencia: si N es el número de n-ágonos, entonces $N \cdot (n-2)\,\frac{\pi}{n} = 2\pi$. (¿Por qué?)

Problema 7. Demuestre que si $a^n - 1$ es primo, entonces $a = 2$ y n es primo.

Comentario. Los primos de la forma $2^p - 1$ se conocen como los **primos de Mersenne**; su infinitud es una conjetura abierta. Muchos de los números $2^p - 1$ son compuestos, el primero siendo $2^{11} - 1 = 23 \cdot 89$.

$$
\begin{array}{ll}
2^2 - 1: & \text{primo} = 3 \\
2^3 - 1: & \text{primo} = 7 \\
2^5 - 1: & \text{primo} = 31 \\
2^7 - 1: & \text{primo} = 127 \\
2^{11} - 1: & \text{compuesto} = 23 \cdot 89 \\
2^{13} - 1: & \text{primo} = 8191 \\
2^{17} - 1: & \text{primo} = 131071 \\
2^{19} - 1: & \text{primo} = 524287 \\
2^{23} - 1: & \text{compuesto} = 47 \cdot 178481 \\
2^{29} - 1: & \text{compuesto} = 233 \cdot 1103 \cdot 2089 \\
2^{31} - 1: & \text{primo} = 2147483647 \\
2^{37} - 1: & \text{compuesto} = 223 \cdot 616318177 \\
2^{41} - 1: & \text{compuesto} = 13367 \cdot 164511353 \\
 & \ldots \\
2^{61} - 1: & \text{primo} = 2305843009213693951 \\
2^{67} - 1: & \text{compuesto} = 193707721 \cdot 761838257287 \\
 & \ldots
\end{array}
$$

Problema 8. Demuestre que si $a^n + 1$ es primo, entonces a es par y $n = 2^k$ es una potencia de 2.

Comentario. Los primos de la forma $2^{2^k} + 1$ se conocen como los **primos de Fermat**. Su finitud es una conjetura abierta. El primer número compuesto de esta forma es $2^{2^5} + 1 = 641 \cdot 6700417$ (dos factores primos). Note que estos números crecen muy rápido con k.

$$
\begin{array}{ll}
2^{2^0} + 1: & \text{primo} = 3 \\
2^{2^1} + 1: & \text{primo} = 5 \\
2^{2^2} + 1: & \text{primo} = 17 \\
2^{2^3} + 1: & \text{primo} = 257 \\
2^{2^4} + 1: & \text{primo} = 65537 \\
2^{2^5} + 1: & \text{compuesto} = 641 \cdot 6700417 \\
2^{2^6} + 1: & \text{compuesto} = 274177 \cdot 67280421310721 \\
2^{2^7} + 1: & \text{compuesto} = 59649589127497217 \cdot 5704689200685129054721
\end{array}
$$

Fermat conjeturó (demasiado optimísticamente) que los números de la forma $2^{2^k} + 1$ son primos, pero Euler descubrió que $641 \mid (2^{2^5} + 1)$. De hecho, parece que para todo $k \ge 5$ los números $2^{2^k} + 1$ son compuestos.

Problema 9.

a) Para $a \neq 0$ y $m \neq n$ calcule $\operatorname{mcd}(a^{2^m}+1, a^{2^n}+1)$.

b) Concluya que los números 2^2+1, $2^{2^2}+1$, $2^{2^3}+1$, $\ldots$ son coprimos por pares.

Ejercicios para hacer en casa

Problema 10.

a) Demuestre que si n es impar, entonces $8 \mid (n^2-1)$. Además, si $3 \nmid n$, entonces $6 \mid (n^2-1)$.

b) Demuestre que para todo n, se tiene $30 \mid (n^5-n)$ y $42 \mid (n^7-n)$.

Problema 11. Sean a, b, c números enteros.

a) Demuestre que la ecuación
$$ax+by=c$$
tiene una solución entera (x, y) si y solamente si $\operatorname{mcd}(a,b) \mid c$.

b) (*) Si (x_0, y_0) es una solución, demuestre que todas las soluciones tienen forma
$$x = x_0 + t\,\frac{b}{d}, \quad y = y_0 - t\,\frac{a}{d},$$
para $d = \operatorname{mcd}(a,b)$ y $t \in \mathbb{Z}$.

Problema 12. Para un entero n y un parámetro natural $k = 0, 1, 2, \ldots$, definamos
$$\sigma_k(n) = \sum_{\substack{1 \le d \le n \\ d \mid n}} d^k.$$

a) Demuestre que $\sigma_k(mn) = \sigma_k(m)\,\sigma_k(n)$ para $\operatorname{mcd}(m,n) = 1$.

b) Para $n = p_1^{e_1} \cdots p_s^{e_s}$, deduzca una fórmula para $\sigma_k(n)$.

Problema 13. Como un caso particular del ejercicio anterior, consideremos el número de divisores
$$d(n) = \sigma_0(n) = \#\{1 \le d \le n \mid d \mid n\}.$$

Encuentre los números tales que $d(n) = n/3$ y $n = d(n)^2$.

Problema 14 (IWYMIC 2019 Individual contest)**.** Encuentre todas las soluciones enteras (m,n) de la ecuación
$$\frac{m^2+mn+n^2}{m+2n} = \frac{13}{3}.$$

Problema 15 (IWYMIC 2019 Team contest)**.** Encontrar todos los posibles dígitos (a,b) (es decir, $0 \le a, b \le 9$) tales que el número $2a1b9$ cumple la congruencia
$$2a1b9^{2019} \equiv 1 \pmod{13}.$$

Problema 16. Encontrar soluciones enteras $x, y > 0$ de la ecuación
$$\frac{1}{\sqrt{x}} + \frac{1}{\sqrt{y}} = \frac{1}{\sqrt{20}}.$$