

## Introducción a la Teoría de Números

### 1. Números primos – entrega 3/9

1. Usar la criba de Eratóstenes para hacer una lista de todos los primos hasta 100.
2. Probar que hay infinitos primos de la forma  $6x - 1$ .
3. Usar el Teorema de los Números Primos ( $\pi(x) \sim x/\log x$ ) para deducir que

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x} = 0.$$

4. ★ Sea  $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$  un polinomio cuadrático con coeficientes enteros y  $a > 0$ , e.g.  $f(x) = x^2 + x + 6$ . Formular una conjetura sobre cuándo el conjunto

$$\{f(n) : n \in \mathbb{Z} \text{ y } f(n) \text{ es primo}\}$$

es infinito.

5. Si  $p$  es un entero positivo tal que  $p$  y  $p^2 + 2$  son primos entonces  $p = 3$ .
6. Si  $a^n - 1$  es primo, con  $n \geq 2$ , mostrar que  $a = 2$  y que  $n$  es primo. Los primos de la forma  $2^p - 1$  se llaman primos de Mersenne, por ejemplo  $2^3 - 1 = 7$  y  $2^5 - 1 = 31$ . El número primo más grande conocido a la fecha es el primo de Mersenne  $2^{32.582.657} - 1$ . No se sabe si hay infinitos primos de Mersenne (se conocen 44 a la fecha).
7. Si  $a^n + 1$  es primo, con  $n \geq 2$ , mostrar que  $a$  es par y que  $n$  es una potencia de 2. Primos de la forma  $2^{2^t} + 1$  se llaman primos de Fermat. Por ejemplo,  $2^{2^1} + 1 = 5$  y  $2^{2^2} + 1 = 31$ . No se sabe si hay infinitos primos de Fermat.
8. ★ Mostrar que  $\sum' 1/n$ , la suma sobre los enteros libres de cuadrados, diverge. Deducir que  $\prod_p (1 + 1/p)$  diverge. Como  $e^x > 1 + x$ , concluir que  $\sum_p 1/p$  diverge.
9. Calcular el máximo común divisor  $\gcd(455, 1235)$  a mano.
10. Encontrar  $x, y \in \mathbb{Z}$  tales que  $2261x + 1275y = 17$ .
11. Sean  $a, b, c \in \mathbb{Z}$ . Mostrar que la ecuación  $ax + by = c$  tiene solución en enteros si  $\gcd(a, b) \mid c$ .
12. Sea  $d = \gcd(a, b)$ . Mostrar que uno puede usar el algoritmo de Euclides para encontrar enteros  $m$  y  $n$  tales que  $am + bn = d$ . Sugerencia: escribir cada resto sucesivo como combinación lineal de  $a$  y  $b$  (e.g.  $r = a - bq$  en el primer paso).
13. Para todo impar  $n$ , mostrar que  $8 \mid n^2 - 1$ . Si  $3 \nmid n$ , entonces  $6 \mid n^2 - 1$ .
14. Para todo  $n$  mostrar que  $30 \mid n^5 - n$  y que  $42 \mid n^7 - n$ .