TEORÍA DE NÚMEROS **Hoja de Problemas** **nº 1**

(1) Demostrar que hay infinitos primos tales que:

(a) $p \equiv 3 \mod 4$,

(b) $p \equiv 1 \mod 4$,

(c) $p \equiv 5 \mod 6$.

Estos son casos particulares del siguiente resultado:
Teorema De Dirichlet de los Primos en Progresiones Aritméticas:
Sean $a, m \in \mathbb{Z}$ tales que $(a, m) = 1$. Entonces existen infinitos primos p tales que $p \equiv a \mod m$.

(2) Sea p un primo. Demostrar

(a) $\begin{pmatrix} p \\ k \end{pmatrix} \equiv 0 \mod p \quad 1 \leq k < p$.

(b) $2^{p-1} \equiv 1 \mod p$ si p es un primo impar.

(c) **Pequeño Teorema de Fermat:** Si $a, p \in \mathbb{Z}$ con p un primo tal que $p \not| a$ entonces $a^{p-1} \equiv 1 \mod p$.

(3) Para un entero n se define $\phi(n)$ como el número de enteros menores a n y coprimos con n. A esta función se le llama la función ϕ de Euler. Demostrar la **Fórmula de Euler:** Sean $a, n \in \mathbb{Z}$ tales que $(a, n) = 1$, entonces $a^{\phi(n)} \equiv 1 \mod n$.

Sea $\pi(x) = \#\{p \text{ primo} : p \leq x\}$, el **Teorema del Número Primo** dice:

$$\pi(x) \sim \frac{x}{\log x}$$

cuando $x \to \infty$. Este resultado fue probado en 1896, independientemente por J. Hadamard y Ch. de la Valle Poussin.
Los siguientes ejecicios no pretenden demostrar este teorema, pero si dar estimaciones de $\pi(x)$.

(4) Sea p_k el primo k-esimo. Demostrar

(a) $p_{k+1} \leq p_1\, p_2 \ldots p_k + 1$.

(b) $p_k < 2^{2^k}$.

(c) $\pi(x) \geq \log(\log x)$.

(5) **(a)** Demostrar $\begin{pmatrix} 2\,n \\ n \end{pmatrix} \leq 2^{2\,n}$.

(b) Sea $\theta(n) = \sum_{p \leq n} \log p$. Demostrar que $\theta(2n) - \theta(n) \leq 2\,n \log 2$.

(Ayuda: $\prod_{n < p \leq 2\,n} p$ divide a $\begin{pmatrix} 2\,n \\ n \end{pmatrix}$).

(c) Demostrar $\theta(2^n) \leq 2^{n+1} \log 2$ para todo $n \geq 0$.

(d) Demostrar $\pi(x) - \pi(\sqrt{x}) \leq \dfrac{8\,x \log 2}{\log x}$.
(Ayuda: Para $x \geq 2$ elegir n tal que $2^n \leq x < 2^{n+1}$).

(e) Demostrar que $\pi(x) \leq \dfrac{9\,x \log 2}{\log x}$

(Ayuda: Demostrar $\sqrt{x} \leq \dfrac{x \log 2}{\log x}$ para $x \geq 16$).

Ahora vamos a ver los números de Fermat que se definen como $F_n = 2^{2^n} + 1$. Fermat hizo la conjetura de que estos números eran todos primos. De hecho, $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ son primos, pero desafortunadamente, F_5 es divisible por 641. Se desconoce si hay infinitos números primos de la forma F_n, pero si que se sabe que hay un número infinito de ellos que son compuestos.

(6) Demostrar que si $p = 2^n + 1$ es primo, entonces $n = 2^m$ para algún entero m, es decir $p = F_m$.

(7) Demostrar que F_n divide a $F_m - 2$ si $n < m$ y de aquí deducir que $(F_n, F_m) = 1$ si $n \neq m$.

Dado un número natural n, sea $n = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ su factorización única como producto de potencias de primos. Se define el radical de n, denotado por $\mathrm{rad}(n)$, al producto $p_1 \dots p_n$.
En 1980, Masser y Oesterlé formularon la siguiente conjetura:
Conjetura ABC: Sean A, B, C tres enteros coprimos entre sí tal que $A + B = C$. Para cualquier $\varepsilon > 0$, existe $k(\varepsilon)$ tal que

$$\max(|A|, |B|, |C|) \leq k(\varepsilon)(\mathrm{rad}(A\,B\,C))^{1+\varepsilon}.$$

(8) Asumiendo la Conjetura ABC, demostrar que si $x\,y\,z \neq 0$ y $x^n + y^n = z^n$ para tres enteros x, y, z coprimos entre sí entonces n está acotado.

(9) Para todo $k \geq 1$ existen k números compuestos consecutivos.

(10) Si $n > 1$ y $a^n - 1$ es primo, probar que $a = 2$ y n es primo. A estos primos se les conoce con el nombre de Primos de Mersenne.

(11) Un entero se llama perfecto si es la suma de sus divisores. Demostrar que si $2^n - 1$ es primo, entonces $2^{n-1}(2^n - 1)$ es perfecto.

(12) Demostrar que si p es un primo impar, cualquier divisor de $2^p - 1$ es de la forma $2\,k\,p + 1$, para algn entero positivo k.

(13) Demostrar el siguiente resultado:

Teorema de Wilson: n es primo si y solo si $n|(n-1)! + 1$.