

Teoría para el problema 5

Valoraciones p-ádicas:

La valoración p-ádica de un número entero m es el exponente de la mayor potencia de un primo p que divide a m . Se denota por $v_p(m)$, con $v_p: \mathbb{Z} \rightarrow \mathbb{N}_0 \cup \{\infty\}$. Por ejemplo, $v_2(24)=3$ porque 2^3 es la máxima potencia de 2 que divide a 24, $v_3(24)=1$ porque 3^1 es la máxima potencia de 3 que divide a 24, y $v_7(24)=0$ porque 7^0 es la máxima potencia de 7 que divide a 24. Es fácil ver que se cumplen las siguientes propiedades:

1. $v_p(a \cdot b) = v_p(a) + v_p(b)$ para cualesquiera a, b enteros y p primo.
2. $v_p(a^n) = n \cdot v_p(a)$ para cualesquiera $a \in \mathbb{Z}, n \in \mathbb{N}^+$, y p primo.
3. $v_p(0) = \infty$ para cualquier p primo.
4. $v_p(n) \leq \log_p n$ siendo n un entero positivo y p primo.
5. $v_p(a + b) = \min\{v_p(a), v_p(b)\}$ si p es un primo y a y b son enteros tales que $v_p(a) \neq v_p(b)$.

LTE (Lifting the exponents):

El lema de lifting the exponents (LTE) establece que:

- Si p es un primo impar:
 - $v_p(a^n - b^n) = v_p(a - b) + v_p(n)$ para cualesquiera a y b enteros tales que $p \nmid a, p \nmid b$ y $p \mid (a-b)$; con n un entero positivo.
 - $v_p(a^n + b^n) = v_p(a + b) + v_p(n)$ para cualesquiera a y b enteros tales que $p \nmid a, p \nmid b$ y $p \mid (a+b)$; con n un entero positivo.
- Con valoraciones 2-ádicas:
 - $v_2(a^n - b^n) = v_2(a - b)$ para cualesquiera a y b enteros impares, siendo n un entero positivo **impar**.
 - $v_2(a^n - b^n) = v_2(a - b) + v_2(a + b) + v_2(n) - 1$ para cualesquiera a y b enteros impares, siendo n un entero positivo **par**.

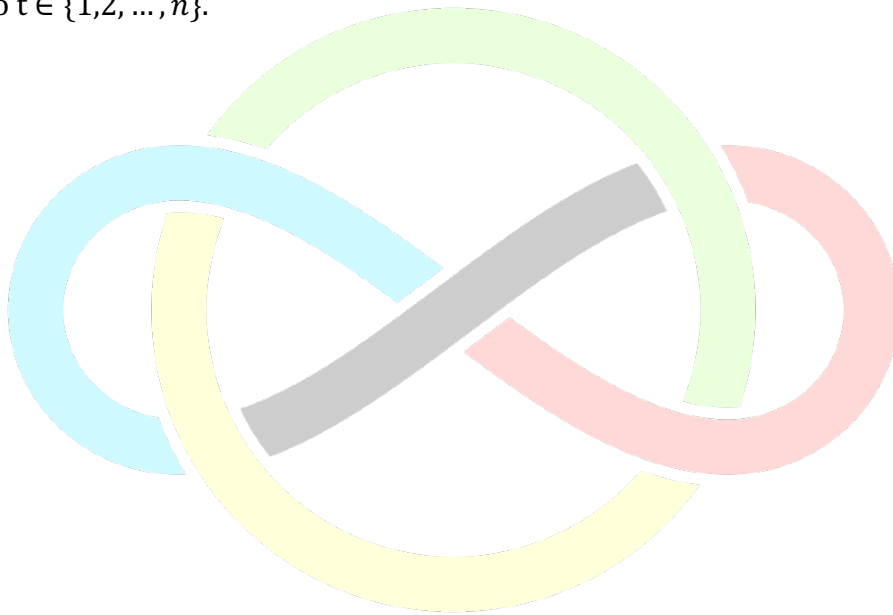
Teoría para el problema 3

Teorema de Lagrange para congruencias polinómicas: Dado un primo p , para todo polinomio $f(x) = c_0 + c_1x + \dots + c_nx^n$ de grado n con coeficientes enteros tal que $p \nmid c_n$, se cumple que la congruencia polinómica $f(x) \equiv 0 \pmod{p}$ tiene, a lo sumo, n soluciones.

Fórmulas de Cardano-Vieta: Si $r_1, r_2, \dots, r_n \in \mathbb{C}$ son las raíces de un polinomio de grado n (escribiéndose las múltiples tantas veces como sea su multiplicidad), $p(x) \in \mathbb{C}[x]$, de la forma $a_0 + a_1x + \dots + a_nx^n$ ($a_n \neq 0$), entonces se tiene que:

$$(-1)^t \frac{a_{n-t}}{a_n} = \sum_{1 \leq i_1 < i_2 < \dots < i_t \leq n} r_{i_1} r_{i_2} \dots r_{i_t}$$

Para todo $t \in \{1, 2, \dots, n\}$.



Nota: \mathbb{N}_0 denota el conjunto de los números naturales incluyendo el 0 (es decir, $\{0, 1, 2, \dots\}$), y \mathbb{N}^+ el de los enteros positivos.