Hoja 4: Teorema de Lagrange sobre polinomios mód p

Alexey Beshenov (cadadr@gmail.com)

23 de septiembre de 2021

Un resultado importante que me gustaría presentar a continuación es el siguiente teorema, descubierto por Lagrange.

> Sea p un número primo. Consideremos un polinomio con coeficientes enteros
>
> $$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$
>
> donde $p \nmid a_n$. Entonces, la congruencia $f(x) \equiv 0 \pmod{p}$ tiene $\leq n$ soluciones.

Recuerde que un polinomio de grado n siempre tiene $\leq n$ raíces reales o complejas. El resultado de arriba nos dice que lo mismo sucede con congruencias polinomiales mód p. El argumento es bastante sutil, así que lo voy a dar por completo, sin convertirlo en otro problema más.

Demostración del teorema de Lagrange. Se procede por inducción sobre n. El caso base es $n = 1$, cuando el polinomio en cuestión es lineal.

Para el paso inductivo, supongamos que el resultado se cumple para los grados $< n$. Ahora si $f(x) \equiv 0 \pmod{p}$ no tiene soluciones, no hay que probar nada. Sino, sea $a \in \mathbb{Z}$ una solución, así que $f(a) \equiv 0 \pmod{p}$. Podemos dividir $f(x)$ por el polinomio mónico lineal $x - a$. Nos quedará

$$f(x) = (x - a)\, g(x) + r,$$

donde

$$g(x) = b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + \cdots + b_1 x + b_0,$$

y $p \nmid b_{n-1} = a_n$. Sustituyendo $x = a$, notamos que $r = f(a)$. Entonces, módulo p se tiene

$$f(x) \equiv (x - a)\, g(x) \pmod{p}.$$

Ahora dado que p es primo (!), tenemos

$$f(x) \equiv 0 \iff x \equiv a \text{ o } g(x) \equiv 0 \pmod{p}.$$

Por la hipótesis de inducción, $g(x) \equiv 0 \pmod{p}$ tiene $\leq n - 1$ soluciones. □

Ejemplo. El teorema de Lagrange implica que la congruencia $x^n \equiv 1 \pmod{p}$ no puede tener más de n soluciones mód p. En particular, $x^2 \equiv 1 \pmod{p}$ tiene solamente las soluciones obvias $x \equiv \pm 1$. Sin embargo, hay 4 soluciones mód 8:

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod{8}.$$

Esto sucede porque 8 es un número compuesto.

Problema 4.1 (Teorema de Wilson-2)**.** Consideremos la congruencia $x^{p-1} \equiv 1 \pmod{p}$.

a) Combine el pequeño teorema de Fermat con nuestra prueba del teorema de Lagrange para establecer la congruencia de polinomios

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod{p}.$$

b) Deduzca de a) el teorema de Wilson: $(p-1)! \equiv -1 \pmod{p}$.

Problema 4.2. Use el teorema de Lagrange para probar que si $d \mid (p-1)$, entonces la congruencia $x^d \equiv 1 \pmod{p}$ tiene precisamente d soluciones.

Sugerencia: factorice $x^{p-1} - 1 = (x^d - 1)(\cdots)$, y recuerde el pequeño teorema de Fermat.

Problema 4.3. Demuestre que $x^{p-2} + x^{p-1} + \cdots + x + 1 \equiv 0 \pmod{p}$ tiene exactamente $p-2$ soluciones. ¿Cuáles son?