

(1706)

Autistralia

Titus

Considera el producto

$$f(x) = \underbrace{\left(x + \frac{1}{x} + 1\right) \cdots \left(x + \frac{1}{x} + 1\right)}_{p-1 \text{ vegades}} = \left(x + \frac{1}{x} + 1\right)^{p-1}$$

~~*Representa de~~

Al expandir això, un terme x^i conta una equeta amb i més SI's que NO's (x vol dir SI, $\frac{1}{x}$ vol dir NO, 1 vol dir NO HO SE). Per tant, volem el terme independent de $f(x) \bmod p$.

Per això usem el factor de que si $x \in \mathbb{Z}_p^*$ llavors

$$1^x + 2^x + \cdots + (p-1)^x = \begin{cases} -1 & \text{si } p-1 \mid x \\ 0 & \text{si no} \end{cases} \pmod{p}.$$

Això és e.z., agafant g avel primitiva mod p ;

llavors fent servir $\{1, 2, \dots, p-1\} = \{g^0, g^1, \dots, g^{p-2}\}$ i fent una geometria en g^x . No s'oc el teu pare com per estar demostrant-te well-known facts, fill in the blanks yourself si no et conveng.

Ara, temos que

$$f(x) = x^{p-1} + a_{p-2}x^{p-2} + \dots + a_1x + a_0 + a_{-1}\frac{1}{x} + \dots + a_{-(p-2)}\frac{1}{x^{p-2}} + \frac{1}{x^{p-1}}.$$

Somem em $x=1, 2, \dots, p-1$. Temos

$$f(1) + f(2) + \dots + f(p-1) =$$

$$= 1^{p-1} + \dots + (p-1)^{p-1} +$$

$$+ a_{p-2} \left(1^{p-2} + \dots + (p-1)^{p-2} \right) +$$

$\vdots$

$$+ a_1 \left(1 + \dots + (p-1) \right) +$$

$$+ a_0 \cdot (p-1) +$$

$$+ a_{-1} \left(1^{-1} + \dots + (p-1)^{-1} \right) +$$

$\vdots$

$$+ a_{-(p-2)} \left(1^{-(p-2)} + \dots + (p-1)^{-(p-2)} \right) +$$

$$+ 1^{-(p-1)} + \dots + (p-1)^{-(p-1)}$$

$$= -1 - a_0 - 1 = -a_0 - 2 \pmod{p}.$$

Ara, $f(i) = \left(i + \frac{1}{i} + 1\right)^{p-1}$. Si $i + \frac{1}{i} + 1 = 0 \Rightarrow f(i) = 0$.

Si $i + \frac{1}{i} + 1 \neq 0 \Rightarrow f(i) = 1$.

Ara $i + \frac{1}{i} + 1 = 0 \Leftrightarrow i^2 + i + 1 = 0 \Leftrightarrow i^3 = 1$ (p no ser $p=3$,
 $i \neq 1$ (lavors es $i=1$)).

Escrivint $i = g^k$, on g és una primitiva mod p , tenim
 que $i^3 = 1$ ($i \neq 1$) passa si $i = g^{\frac{p-1}{3}}$ o $i = g^{\frac{2(p-1)}{3}}$.

Lavors, si $p=1$ (3 hi ha 2 valors de $1, \dots, p-1$
 que donen $f(i)=0$. Si $p \neq 1$ (3 n'hi ha 0.

Lavors

Si $p=1$ (3.

$$-2 - a_0 = f(1) + \dots + f(p-1) = p-1 - 2 = p-3 \Rightarrow a_0 = 1(p).$$

Si $p \neq 1$ (3, $p \neq 3$.

$$-2 - a_0 = f(1) + \dots + f(p-1) = p-1 = -1 \Rightarrow a_0 = -1(p).$$

Si $p=3$.

Fas $\left(x + \frac{1}{x} + 1\right)^2$ i el terme independent surt $0 \bmod 3$.