**Seja p $\geq$ 2 um inteiro, prove que, se $f(x) = x^2 + x + p$ é primo para $0 \leq x \leq \sqrt{\frac{p}{3}}$, f é primo para todo 0 $\leq$ x $\leq$ p – 2.**

Suponha que exista um divisor próprio de f(x) para algum valor de x, com $\sqrt{\frac{p}{3}} < x \leq p - 2$.

Tome q como o menor primo que é um desses divisores próprios, não é muito difícil ver que q > 2, basta verificar que { p, p+2, …, p + k(k+1) } = { p } em $Z_2$ e p $\neq$ 0.

*Lema 1:* Se

$$f(k) \equiv a(\mathrm{mod}\, m),\ f(k+m) = f(k) + m(m+1+2k) \Rightarrow f(k+m) \equiv a(\mathrm{mod}\, m)$$

Considere f(x) $\in$ $Z_q$[X], podemos estabelecer o seguinte lema:

*Lema 2. f(x) = f(y) em $Z_q$[X] $\Leftrightarrow$ x = y ou x = -y – 1*

Dem.

$f(x) = f(y) \Leftrightarrow x^2 + x = y^2 + y \Leftrightarrow x^2 - y^2 = (x+y)(x-y) = y - x$

se x $\neq$ y, como $Z_q$ é corpo, podemos aplicar a lei do cancelamento de fatores, logo:

$(x+y)(x-y) = y - x, x \neq y \Leftrightarrow x + y = -1 \Leftrightarrow x = -y - 1$

Dos lemas 1 e 2, temos: $f(0) = f(q-1), f(1) = f(q-2), \ldots, f(k) = f(q-k-1), k \leq \frac{q-1}{2}$

e, se q divide algum valor de x no intervalo acima, o conjunto

$S = \left\{ f(0), f(1), \ldots, f\left(\frac{q+1}{2}\right) \right\} \subset Z_q$ deve conter um único zero.

Para isso ser possível temos necessariamente que $\frac{q+1}{2} > \sqrt{\frac{p}{3}}$.

A seguinte desigualdade pode ser inferida já que o menor fator primo de um número composto não pode exceder sua raiz quadrada e f é uma função crescente para os naturais:

$$q \leq \sqrt{f\left(\frac{q+1}{2}\right)} = \sqrt{\left(\frac{q+1}{2}\right)\left(\frac{q+3}{2}\right) + p} < \sqrt{\left(\frac{q+2}{2}\right)^2 + p} < \left(\frac{q+2}{2}\right) + \sqrt{\frac{p}{3}} \Rightarrow q < 2 + 2\sqrt{\frac{p}{3}}$$

Notamos então que $\sqrt{\frac{p}{3}} < \frac{q+1}{2} < \frac{3}{2} + \sqrt{\frac{p}{3}}$. Este intervalo tem comprimento 3/2, logo o número de inteiros que ele possui é sempre menor ou igual a dois, logo os possíveis 0 de S são $f\left(\frac{q-1}{2}\right), f\left(\frac{q+1}{2}\right)$, vamos agora provar que nenhum deles é 0 módulo q.

*Lema 3.* $f(k+1)-f(k)=(k+1)[(k+2)-k]=2(k+1)$

....., $f\left(\frac{q-3}{2}\right)$, $f\left(\frac{q-1}{2}\right)$, $f\left(\frac{q+1}{2}\right)$

Se o penúltimo termo for um 0 em S, temos, pelo lema 3, que o termo anterior é 1 e o próximo termo também é 1, mas isso contraria o lema 2, que nos garante que todos os elementos de S são distintos.

Sobrou então provar que $f\left(\frac{q+1}{2}\right)=\frac{q^2+4q+4p+3}{4}$ não é um 0 em S.

Primeiramente vamos notar que se o último elemento é 0 o penúltimo é -1, o antepenúltimo é -2, de modo geral, para m $\geq$ 0, $f\left(\frac{q-3}{2}-m\right)=-m^2-2m-2$.

Sendo assim, $f(0)=-\left(\frac{q-3}{2}\right)\left(\frac{q+1}{2}\right)-2=-\frac{q^2-2q+5}{4}=p\Rightarrow 4p=2q-q^2-5$

Substituindo 4p no último elemento:

$f\left(\frac{q+1}{2}\right)=\frac{q^2+4q+2q-q^2-5+3}{4}=\frac{6q-2}{4}=\frac{3q-1}{2}$, logo $q<f\left(\frac{q+1}{2}\right)<2q$, e assim provamos que não há nenhum 0 em S e, chegamos a conclusão de que o enunciado é válido.