Problem 6.4 - Orders Modulo a Prime

Seja n um inteiro positivo e $p > n+1$ um primo. Prove que p divide

$$1^n + 2^n + \dots + (p-1)^n$$

Seja g a raiz primitiva $(\text{mod } p)$. $[n < p-1]$

Logo $S \equiv 1^n + 2^n + \dots + (p-1)^n \equiv \quad (\text{mod } p)$

$\equiv g^n + g^{2n} + g^{3n} + \dots + g^{(p-1)n} \quad (\text{mod } p)$

$\equiv a + a^2 + \dots + a^{(p-1)} \quad (\text{mod } p), \quad a = g^n \not\equiv 1$

$\equiv \dfrac{a^p - a}{a-1} \equiv a\underbrace{(a^{p-1} - 1)}_{\equiv 0}\underbrace{(a-1)^{-1}}_{\not\equiv 0} \quad (\text{mod } p)$

$\equiv 0$

$\square$

Problem 6.5 - Orders Modulo a Prime

Ache todos os inteiros positivos a e n t.q:

$$\frac{(a+1)^n - a^n}{n}$$

é inteiro.

Vamos tentar resolver o caso $\underline{a=1}$.

$n \mid 2^n - 1$. Seja p o menor divisor primo de n.

$\Rightarrow p \mid 2^n - 1$ e $p \mid 2^{p-1} - 1$. $\Rightarrow p \mid 2^1 - 1 = 1$. Abs!

Seja p o menor divisor primo de n.

Se $a \equiv 0 \pmod p \Rightarrow (a+1) \equiv 1 \pmod p \Rightarrow (a+1)^n - a^n \equiv 1 \pmod p$ Abs!

Se $a \equiv -1 \pmod p \Rightarrow (a+1) \equiv 0 \pmod p \Rightarrow (a+1)^n - a^n \equiv \pm 1 \pmod p$ Abs!

Se $a \not\equiv 0$ e $a \not\equiv -1$:

$$\left.\begin{array}{l} (a+1)^n \equiv a^n \pmod p \Rightarrow ((a+1)a^{-1})^n \equiv 1 \pmod p \\ \text{Mas, } \quad ((a+1)a^{-1})^{p-1} \equiv 1 \pmod p \end{array}\right\} \Rightarrow$$

$$\Rightarrow (a+1)a^{-1} \equiv 1 \pmod p \Rightarrow a+1 \equiv a \pmod p \text{ Abs!}$$

Logo, n não possui divisor primo $\Rightarrow n=1$. (Sempre funciona!)