

Série de Colares
Divisão Eucl

Problema 11.20

Ache uma nova prova, por indução da segunda de Fermat

Demonstração

Pelo Soma de Colares,

$$\text{Logo } (a+1)^p \equiv a^p + 1 \pmod{p}$$

$$\text{Logo } (a+1)^p \equiv a^p + 1 \pmod{p}$$

Subtraindo $(a+1)$ em ambos os lados

$$\text{temos que } (a+1)^p - (a+1) \equiv a^p + 1 - (a+1) \pmod{p}$$

$$\text{Logo } (a+1)^p - (a+1) \equiv a^p - a \pmod{p}$$

A13

Por indução

$$\text{Base: } [p | a^p - a] \quad [p | 0^p - 0]$$

$$0^p - 0 = 0$$

$$\text{Logo } p \cdot 0 = 0$$

P.I Suponha $[p | a^p - a]$ H.I

Procuramos prova que $p | (a+1)^p - (a+1)$

Mas pela A13 se $(a+1)^p - (a+1) \equiv a^p - a \pmod{p}$

$$\text{Logo } p | ((a+1)^p - (a+1))$$

$$\text{Logo } a^p \equiv a \pmod{p}$$

$$(\forall p \text{ primo } \forall a \in \mathbb{Z}) \quad [a^p \equiv a \pmod{p}]$$

¶6.22 Sejam p, q primos distintos $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$

Demonstração

Pelo pequeno teorema de Fermat
temos que $p^{q-1} \equiv 1 \pmod{q}$

e que $q^{p-1} \equiv 1 \pmod{p}$

logo $p^{q-1} + q^{p-1} \equiv 1 \pmod{q}$

e $p^{q-1} + q^{p-1} \equiv 1 \pmod{p}$

mas como $pq \mid p^{q-1} + q^{p-1} - 1$

logo $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$



(p, q primos $p \neq q$) $\left[p^{q-1} + q^{p-1} \equiv 1 \pmod{pq} \right]$