SOLUÇÃO

5.

a) Supondo $(a,p)=1$ mostre que $a^{p-1} \equiv 1(mod\ p)$.

Solução

Como $(a,p)=1$, então $\overline{a} \in \mathbb{Z}_p^*$ por outro lado lembremos que $|\mathbb{Z}_p^*| = p-1$, logo:

$$\overline{a^{p-1}} = \overline{a}^{p-1} = \overline{1}$$

por tanto $a^{p-1} \equiv 1(mod\ p)$.

$\square$

b) $a^p + (p-1)!a \equiv 0\ (mod\ p)$.

Solução

Caso 1: $a \equiv 0\ (mod\ p)$.

Neste primer caso como $a \equiv 0\ (mod\ p)$, então $a = kp$ para algum $k \in \mathbb{Z}$, logo $a^p = k^p p^p$ assim $a^p + (p-1)!a = k^p\ p^p + (p-1)!\ k\ p = p[k^{p-1}\ p^p + (p-1)!\ k]$ ou seja

$$a^p + (p-1)!a \equiv 0\ (mod\ p).$$

Caso 2: $a \not\equiv 0\ (mod\ p)$, em outras palavras $(a,p)=1$.

Pelo item a) temos que $\overline{a}^{p-1} = \overline{1}$ em $\mathbb{Z}_p^*$, então $\overline{a}^p = \overline{a}$ em $\mathbb{Z}_p^*$, daqui

$$a^p - a = mp \qquad (I)$$

para algum $m \in \mathbb{Z}$

Agora pelo Teorema de Wilson, $(p-1)! \equiv -1\ (mod\ p)$, ou seja $(p-1)! + 1 = np$, para algum $n \in \mathbb{Z}$, logo

$$(p-1)!\ a = npa - a \qquad (II)$$

Agora somando (I) e (II) temos:

$$a^p + (p-1)!\ a = mp + npa = p(m+na)$$

em outras palavras $a^p + (p-1)!\ a \equiv 0\ (mod\ p)$.

$\square$

c) Sejam $m, n \in \mathbb{N}$ primos relativos, $(G, \cdot)$ um grupo e $g \in G$ tal que $g^m = e$ e $g^n = e$ mostre que $g = e$.

Solução

Como $(m,n)=1$ existem $r, s \in \mathbb{Z}$ talque $rm + sn = 1$, assim:

$$g = g^1 = g^{rm+sn} = g^{rm} \cdot g^{sn} = (g^m)^r \cdot (g^n)^s = e^r \cdot e^s = e \cdot e = e$$