Resumão de Álgebra A

Vinícius Claudino Ferraz

$$\varphi(p) = p - 1 \tag{1}$$

$$\varphi(p^n) = p^{n-1}(p-1) \tag{2}$$

$$m = p_1^{n_1} \cdots p_r^{n_r} \Rightarrow \varphi(m) = p_1^{n_1-1} \cdots p_r^{n_r-1}(p_1-1)\cdots(p_r-1) \tag{3}$$

$$(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \mod m \tag{4}$$

$$(a,p) = 1 \Rightarrow a^{p-1} \equiv 1 \mod p \tag{5}$$

$$a^p \equiv a \mod p \tag{6}$$

$$ax \equiv b \mod m, (a,m) = 1 \Rightarrow x \equiv ba^{\varphi(m)-1} \mod m \tag{7}$$

$$(p-1)! + 1 \equiv 0 \mod p \tag{8}$$

$$(n-1)! + 1 \equiv 0 \mod n \Rightarrow n \text{ é primo.} \tag{9}$$

$$(m_i, m_j) = 1, X \equiv a_i \mod m_i \Rightarrow M = \Pi m_i, M_i = \frac{M}{m_i}, M_i x_i \equiv 1 \mod m_i, \exists! X \equiv \Sigma m_i x_i a_i \mod M \tag{10}$$

$$C \equiv aP + b \mod 26 \tag{11}$$

$$P \equiv a^{-1}(C - b) \mod 26 \tag{12}$$

$$C_i \equiv P_i + k_i \mod 26 \tag{13}$$

$$C \equiv AP \mod 26 \tag{14}$$

$$P \equiv A^{-1}C \mod 26 \tag{15}$$

$$C \equiv P^e \mod p \tag{16}$$

$$de \equiv 1 \mod (p-1) \tag{17}$$

$$(e, p-1) = 1 \tag{18}$$

$$C^d \equiv P \mod p \tag{19}$$

$$n = p_1 p_2 \tag{20}$$

$$(e, \varphi(n)) = 1 \tag{21}$$

$$C \equiv P^e \mod n \tag{22}$$

$$de \equiv 1 \mod \varphi(n) \tag{23}$$

$$C^d \equiv P \mod n \tag{24}$$