Public Key Cryptography

We want to prove that

$$\gcd\left(a^{j!}-1, N\right) = N \implies \gcd\left(a^{(j+1)!}-1, N\right) = N.$$

Proof. Note that

Definition. Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>1}$. Then

$$a \equiv b \pmod{n} \overset{\text{def.}}{\iff} n \mid a - b.$$

Let $\gcd\left(a^{j!}-1, N\right) = N$ then

$$\begin{aligned} \gcd\left(a^{j!}-1, N\right) = N &\implies N \mid a^{j!} - 1 \quad \because d = \gcd(a,b) \Rightarrow d \mid a \wedge d \mid b \\ &\implies a^{j!} \equiv 1 \pmod{N}, \end{aligned}$$

and so

$$a^{(j+1)!} = \left(a^{j!}\right)^{(j+1)} \equiv 1^{j+1} = 1 \pmod{N}.$$

Thus

$$\begin{aligned} a^{(j+1)!} \equiv 1 \pmod{N} &\implies N \mid a^{(j+1)!} - 1 \\ &\implies \exists k \in \mathbb{Z} : a^{(j+1)!} - 1 = Nk. \end{aligned}$$

Hence we have

$$\gcd\left(a^{(j+1)!}-1, N\right) = \gcd(Nk, N) = N.$$

□

Department of Information Security, Cryptography and Mathematics
Kookmin University