

Q 11.

$$n! = 1 \times 2 \times 3 \times \dots \times n, \quad n \in \mathbb{N}$$

To show $\rightarrow a^{n!} \equiv 1 \pmod{n}$ s.t. $\gcd(a, n) = 1$.

1) $\gcd(a, n) = 1$

$\gcd(a, n) = 1$

$\gcd(a^2, n) = 1$

$\gcd(a^3, n) = 1$

\vdots

$\gcd(a^n, n) = 1$

$a \nmid n$

by Lemma 48 of

$\gcd(a, b) = 1$ and $\gcd(a, c) = 1$

$\rightarrow \gcd(a, bc) = 1$

by Thm 83,

$a^{n!} \equiv 1 \pmod{n} \quad (\gcd(a, n) = 1)$

$(a^2)^{n!} \equiv 1 \pmod{n} \quad (\gcd(a^2, n) = 1)$

$(a^3)^{n!} \equiv 1 \pmod{n} \quad (\gcd(a^3, n) = 1)$

\vdots

$(a^n)^{n!} \equiv 1 \pmod{n} \quad (\gcd(a^n, n) = 1)$

$\rightarrow a^{n! + 2n! + 3n! + \dots + nn!} \equiv 1 \pmod{n}$

$a^{n! \frac{n(n+1)}{2}} \equiv 1 \pmod{n}$

$n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n > \left(\frac{n}{2}\right)^{\frac{n}{2}}$