Bew (16.5)

Sei $i > s$.

1. Fall: k_i ungerade $\Rightarrow \nu_2(p_i - 1) > \nu$ (nach Def. von ν)
$\Rightarrow 2^{\nu+1} \mid p_i - 1 \overset{(2)}{\Rightarrow} \underline{2^{\nu+1} \mid p_i^{k_i} - 1}$

2. Fall: k_i gerade
Nach Def. von ν gilt $2^\nu \mid p_i - 1$
k_i gerade $\Rightarrow p_i^{k_i - 1} + \ldots + p_i + 1$ gerade $\Rightarrow 2 \mid p_i^{k_i - 1} + \ldots + 1$ $\Big\}$ $\overset{(2)}{\Rightarrow}$
$2^{\nu+1} \mid p_i^{k_i} - 1$

Also (5) $\underline{2^{\nu+1} \mid p_i^{k_i} - 1 \quad \forall i > s}$

$$\Rightarrow \quad p_i^{k_i} \equiv 1 \pmod{2^{\nu+1}} \quad \forall i > s$$

$i \le s \overset{(4)}{\Rightarrow} 2^\nu \mid p_i^{k_i} - 1, \; 2^{\nu+1} \nmid p_i^{k_i} - 1$

$\rightarrow \; p_i^{k_i} - 1 = 2^\nu \cdot t_i$ mit t_i ungerade.

Einsetzen in (1) ergibt

$$n - 1 = \sum_{i=1}^{s} 2^\nu t_i \pi_i + \sum_{j=s+1}^{r} \underbrace{(p_i^{k_i} - 1)}_{\equiv 0 \pmod{2^{\nu+1}} \text{ nach (5)}} \pi_i$$

$$\equiv \sum_{i=1}^{s} 2^\nu t_i \pmod{2^{\nu+1}}$$

denn: $2^\nu t_i \underbrace{(\pi_i - 1)}_{\text{gerade}} \equiv 0 \pmod{2^{\nu+1}} \Rightarrow 2^\nu t_i \pi_i \equiv 2^\nu t_i \pmod{2^{\nu+1}}$

Folglich (6) $\quad n - 1 \equiv (t_1 + t_2 + \ldots + t_s) \cdot 2^\nu \pmod{2^{\nu+1}}$

Aus (6) folgt $\quad e = \nu \Leftrightarrow t_1 + \ldots + t_s$ ungerade $\Leftrightarrow s$ ungerade
$\uparrow$
alle t_i sind ungerade.

Genauer: „$\Rightarrow$" $\quad e = \nu \Rightarrow 2^{\nu+1} \nmid n - 1$

Annahme: $t_1 + \ldots + t_s = t = 2t'$ gerade.

$\Rightarrow \quad n - 1 \equiv t \cdot 2^\nu = t' \cdot 2^{\nu+1} \equiv 0 \pmod{2^{\nu+1}} \Rightarrow 2^{\nu+1} \mid n - 1$ ↯.

„$\Leftarrow$" Ann: $e > \nu \Rightarrow 2^{\nu+1} \mid n - 1 \overset{(6)}{\Rightarrow} 2^{\nu+1} \mid t \cdot 2^\nu \Rightarrow 2 \mid t$

$\rightarrow t = t_1 + \ldots + t_s$ gerade ↯. □