Für die Beweisrichtung b) ⇒ a) des Satzes (16.4) benötigen wir den Hilfssatz (16.5), der hier bewiesen wird.

Bew.: Setze $\pi_i := \prod_{k=i+1}^{r} p_k^{e_k}$ $(i=1..r)$. Dann ist $\pi_r = 1$.

Dann gilt

$$\sum_{i=1}^{r} (p_i^{e_i}-1)\pi_i = (p_1^{e_1}-1)\pi_1 + \ldots + (p_{r-1}^{e_{r-1}}-1)\pi_{r-1} + (p_r^{e_r}-1)$$

$$= \underbrace{(p_1^{e_1}\pi_1)}_{=n} - \pi_1 + p_2^{e_2}\pi_2 - \pi_2 + \ldots + p_{r-1}^{e_{r-1}}\pi_{r-1} - \pi_{r-1} + \underbrace{p_r^{e_r}}_{=\pi_{r-1}} - 1$$

$$= n-1$$

(1) $$n-1 = \sum_{i=1}^{r} (p_i^{e_i}-1)\pi_i$$

(2) $$p_i^{e_i}-1 = (p_i-1)(p_i^{e_i-1}+\ldots+p_i+1)$$

(3) $$n-1 = \sum_{i=1}^{r} (p_i-1)\sigma_i \quad \text{mit } \sigma_i = (p_i^{e_i-1}+\ldots+p_i+1)\pi_i \in \mathbb{N}$$

Nachweis von a) Nach Def von ν gilt $2^\nu \mid p_i-1 \ \forall i=1..r$

$\overset{(3)}{\Rightarrow}$ $2^\nu \mid n-1$ $\Rightarrow$ $\underline{\nu \le e = \nu_2(n-1)}$

Nachweis von b) Seien $1,2,\ldots,s$ die Indizes $i \in \{1,2,\ldots,r\}$, für die e_i ungerade und $\nu_2(p_i-1)=\nu$ gilt (notfalls Umnummerierung der Primzahlen $p_1 \ldots p_r$)

Sei $\underline{i \le s}$ $\nu_2(p_i-1)=\nu \Rightarrow 2^\nu \mid p_i-1$ und $2^{\nu+1} \nmid p_i-1$

Annahme: $2^{\nu+1} \mid p_i^{e_i}-1 \overset{(2)}{\Rightarrow} 2^{\nu+1}\cdot a = p_i^{e_i}-1 = (p_i-1)(p_i^{e_i-1}+\ldots+p_i+1)$

$$= 2^\nu \cdot b \,(p_i^{e_i-1}+\ldots+p_i+1)$$

($\nu_2(p_i-1)=\nu$)

$\Rightarrow 2a = p_i^{e_i-1}+\ldots+p_i+1 \Rightarrow p_i^{e_i-1}+\ldots+p_i+1$ gerade.

Diese Summe ungerade Zahlen hat e_i Summanden $\Rightarrow$ e_i gerade ↯.

Also (4) $\underline{2^{\nu+1} \nmid p_i^{e_i}-1 \ \forall i \le s}$