ALG Ü5

165) (a) $k \in \mathbb{N}$ bel. zz: $(ggT(k,n)=1) \Leftrightarrow (\forall l \in k+n\mathbb{Z}: ggT(l,n)=1) \Leftrightarrow (\exists l \in k+n\mathbb{Z}: ggT(l,n)=1)$

Angenommen $ggT(k,n)=1$, das heißt $\forall m \geq 2: \neg(m|k \wedge m|n)$. Sei $m \geq 2$ bel.

1. Fall $\neg m|n \Rightarrow m \neq ggT(l,n)$

2. Fall $m|n \Rightarrow l = k+nj$ $\quad m|l \Leftrightarrow \exists x \in \mathbb{Z}: mx = l = k+nj$

Da $m|n$ gilt $\exists y \in \mathbb{Z}: my = n$ Wir wollen einen Widerspruch zu $m|k$ herleiten.

$mx = k+nj = k+myj \Leftrightarrow m\underbrace{(x-yj)}_{\in \mathbb{Z}} = k \Rightarrow m|k$ ↯ da $ggT(k,n)=1$

($m|n$ und $m|k$ darf für $m \geq 2$ nicht gelten)

Gezeigt (bzw. klar) ist $(ggT(k,n)=1) \Rightarrow (\forall l \in k+n\mathbb{Z}: ggT(l,n)=1) \Rightarrow (\exists l \in k+n\mathbb{Z}: ggT(l,n)=1)$

zz: $(\exists l \in k+n\mathbb{Z}: ggT(l,n)=1) \Rightarrow (ggT(k,n)=1)$

Sei $j \in \mathbb{Z}$: $l = k+nj$. Es gilt $\forall m \geq 2: \neg(m|l \wedge m|n)$, da $ggT(l,n)=1$.

Sei $m \geq 2$ bel. 1. Fall $\neg m|n \Rightarrow m \neq ggT(k,n)$

2. Fall $m|n$ Angenommen $m|k$ also $\exists x \in \mathbb{Z}: mx = k$ zz: $m|l$ also Widerspruch

Da $m|n$ gilt $\exists y \in \mathbb{Z}: my = n$. $l = k+nj = mx + myj = m\underbrace{(x+yj)}_{\in \mathbb{Z}} \Rightarrow m|l$ ↯

$\Rightarrow ggT(k,n)=1$

b) $A := \{k+n\mathbb{Z} \mid k \in \mathbb{Z}, ggT(n,k)=1\}$ $\quad B := \{k+n\mathbb{Z} \mid k \in \{0,\dots,n-1\} \wedge ggT(n,k)=1\}$

$C := \{k \mid k \in \{0,\dots,n-1\} \wedge ggT(n,k)=1\}$

zz: $|A| = |B| = |C|$

$B \subseteq A$ gilt nach Definition. $\Rightarrow |B| \leq |A|$

Wir wollen zeigen $|C| \leq |B|$. Sei $k \in C$ bel. $\Rightarrow ggT(n,k)=1 \Rightarrow k+n\mathbb{Z} \in B$

Für $k_1, k_2 \in \{0,\dots,n-1\}$, $k_1 \neq k_2$ gilt $k_1+n\mathbb{Z} \neq k_2+n\mathbb{Z}$ $\Rightarrow |C| \leq |B|$

Nun müssen wir noch zeigen $|A| \leq |C|$.

$\forall k \in \mathbb{Z}: k+n\mathbb{Z} = (k-n)+n\mathbb{Z} \Rightarrow \forall k \in \mathbb{Z}\ \exists k' \in \{0,\dots,n-1\}: k+n\mathbb{Z} = k'+n\mathbb{Z}$

Sei $k+n\mathbb{Z} \in A$ bel. Sei $k'+n\mathbb{Z} = k+n\mathbb{Z}$ mit $k' \in \{0,\dots,n-1\}$. zz: $k' \in C$

Da $k'+n\mathbb{Z} \in A \Rightarrow ggT(n,k')=1$ also $k' \in C$. $\Rightarrow |A| \leq |C|$

$\Rightarrow |A| \leq |C| \leq |B| \leq |A| \Rightarrow |A| = |B| = |C|$ □