Lösung der Sonderaufgabe vom 21.10.2004
Studiengang Network Computing
WS 2004/2005

Martin Grandrath (Matr. Nr.: 46375)

12. Dezember 2004

Inhaltsverzeichnis

1 Behauptung

Gegeben seien die Zahlen a, b, x, y, n mit $a, b, n \in \mathbb{N}^+$, $b > a > 1$ und $x, y \in \mathbb{N}_0$. Ferner sei der größte gemeinsame Teiler (ggT) von a und b 1. Dann soll gelten:

$$\exists x \; \exists y \; (ax + by = n, \text{ für } n \geq n_0) \tag{1}$$

Gesucht wird p, d. h. die größte natürliche Zahl, die sich *nicht* in der o.g. Form darstellen lässt. ($\Rightarrow p = n_0 - 1$)

2 Vermutung

$$p = ab - (a + b)$$

3 Prüfen, ob p existiert

Nach dem Euklidischen Algorithmus lässt sich der größte gemeinsame Teiler T zweier Zahlen $a, b \in \mathbb{N}$ in der Form $T = aw + bz$ mit $w, z \in \mathbb{Z}$ darstellen.

Das heißt, dass im konkreten Fall gilt

$$aw + bz = 1 \qquad \text{mit } w, z \in \mathbb{Z} \tag{2}$$

und somit auch

$$amw + bmz = m \qquad \text{mit } m \in \mathbb{N} \tag{3}$$

Da $b > a > 1$ ist, folgt, dass entweder $w < 0 < z$ oder $w > 0 > z$ ist. OBdA untersuchen von $w < 0 < z$:

$$\underbrace{-a(a-1)w}_{>0} + b \cdot 0z = n$$

Addieren von (3) ergibt:

$$\begin{aligned} -a(a-1)w + amw + b \cdot 0z + bmz &= n + m \\ -a(a-1-m)w + b(0+m)z &= n + m \\ a(m-a+1)w + bmz &= n + m \end{aligned}$$

Einsetzen der Werte $m = 0, \; m = 1, \; \ldots, \; m = a - 1$ und Substituieren von $(m - a + 1)w$ durch x_{m+1} bzw. mz durch y_{m+1} ergibt die für den Induktionsanfang benötigten Gleichungen.

4 Beweis

4.1 Vollständige Induktion

4.1.1 Induktionsanfänge

$$\begin{aligned} ax_1 + by_1 &= n \\ ax_2 + by_2 &= n+1 \\ ax_3 + by_3 &= n+2 \\ &\vdots \\ ax_a + by_a &= n+a-1 \end{aligned}$$

4.1.2 Induktionsschluss

$$\begin{aligned} ax + by &= n + a \\ ax - a + by &= n \\ a(x-1) + by &= n \end{aligned}$$

4.2 Bestimmen von x_a

$$\begin{aligned} ax_a + by_a &= n + a - 1 \\ ax_a - a + by_a &= n - 1 \\ a(x_a - 1) + by_a &= p \end{aligned}$$

Aus diesem Widerspruch zur Behauptung folgt:

$$\begin{aligned} &\Rightarrow x_a - 1 \notin \mathbb{N}_0 \\ &\Rightarrow x_a = 0 \end{aligned}$$

4.3 Bestimmen von y_a

4.3.1 y_a nach oben abschätzen

Annahme

$$\begin{aligned} y_a &> a-1 \\ y_a &\geq a \\ y_a &= a+\delta \qquad (\delta \in \mathbb{N}_0) \end{aligned}$$

Gegenbeweis

$$\begin{aligned} by_a &= n+a-1 \\ b(a+\delta) &= n+a-1 \\ ba+b\delta &= n+a-1 \\ ba-a+b\delta &= n-1 \\ a\,(b-1)+b\delta &= p \end{aligned}$$

Diese Aussage steht im Widerspruch zur Behauptung und muss folglich falsch sein.

$$\Rightarrow y_a \leq a-1$$

4.3.2 y_a nach unten abschätzen

Aus

$$n < n+1 < n+2 < \ldots < n+a-1$$

ergibt sich

$$ax_1+by_1 < ax_2+by_2 < ax_3+by_3 < \ldots < by_a$$

daraus folgt

$$\Rightarrow y_a > y_k \qquad (k \in [1, a-1])$$

4.3.3 Untersuchen von y_k

Behauptung

Alle y_k mit $k \in [1, a]$ sind paarweise verschieden.

Beweis
Angenommen,

$$\begin{aligned} ax_n + by_n &= ax_m + by_n + q \qquad (q \in [1, a-1]) \\ ax_n &= ax_m + q \\ q &= ax_n - ax_m \\ q &= a(x_n - x_m) \end{aligned}$$

Hier liegt ein Widerspruch vor, da q innerhalb des Intervalls $[1, a-1]$ liegen muss und daher kein Vielfaches von a darstellen kann.

4.3.4 Zusammenfassung

Für y_a gilt also

- $y_a \leq a - 1$
- $y_a > y_k \geq 0$
- Alle a Faktoren y_k sind paarweise verschieden

$$\Rightarrow y_a = a - 1$$

4.4 Bestimmen von p

$$\begin{aligned} ax_a + by_a &= n + a - 1 \qquad x_a = 0,\ y_a = a - 1 \\ b(a-1) &= n + a - 1 \\ n &= ab - b - a + 1 \\ n &= ab - (a + b) + 1 \\ p &= n - 1 \\ p &= ab - (a + b) \end{aligned}$$