Prof. Dr. R. Bieri WS 2004/2005

Frankfurt/M., den 13.12.2004

Mathematik I (Zahlbereiche)
Ausgewählte Musterlösungen[1]
Lösung von Aufgabe 4 aus Serie 4

Für $a, m, n \in \mathbb{N}, a > 1, m \geq n$ zeige man:

(a) $\text{ggT}(m, n) = \text{ggT}(n, m-n)$

(b) $\text{ggT}\ (a^m - 1, a^n - 1) = \text{ggT}(a^n - 1, a^{m-n} - 1)$

(c) $\text{ggT}\ (a^m - 1, a^n - 1) = a^{\text{ggT}(m,n)} - 1$

Lösung:

Allgemein gilt : 1.) $d = \text{ggT}(a, b) \Leftrightarrow$ $(i)\ d \mid a$, $(ii)\ d \mid b$, $(iii)\ e \mid a \wedge e \mid b \Rightarrow e \mid d$

2.) $a \mid b \wedge a \mid c \Rightarrow a \mid (xb + ya)$ für alle $x, y \in \mathbb{Z}$

(a) Sei $d := \text{ggT}(m, n)$ und $g := \text{ggT}\ (n, m-n)$

- $d \mid m \wedge d \mid n \overset{2.)}{\Rightarrow} d \mid m - n \wedge d \mid n \overset{1.)(iii)}{\Rightarrow} d \mid g$
- $g \mid n \wedge g \mid m - n \overset{2.)}{\Rightarrow} g \mid n \wedge g \mid (m-n) + n \Rightarrow g \mid n \wedge g \mid m \overset{1.)(ii)}{\Rightarrow} g \mid d$
- $d \mid g \wedge g \mid d \Rightarrow g = d$

(b) Sei $e : \text{ggT}(a^m - 1, a^n - 1)$ und $f := \text{ggT}(a^n - 1, a^{m-n} - 1)$

- Es gilt: $(a^{m-n} - 1) = \underbrace{(a^m - 1) - (a^{m-n} - 1)(a^n - 1) - (a^n - 1)}_{(*)}$

  Da $e \mid a^m - 1 \wedge e \mid a^{m-n} - 1 \overset{2.)}{\Rightarrow} e \mid (*) \Rightarrow e \mid a^{m-n} - 1$
  $e \mid a^{m-n} - 1 \wedge e \mid a^n - 1 \overset{1.)(iii)}{\Rightarrow} e \mid f$
- Da $(a^m - 1) = (a^{m-n} - 1) + (a^{m-n} - 1)(a^n - 1) + (a^n - 1)$ gilt, kann man analog erkennen, dass $f \mid e$ gilt.

[1] *auch als pdf-Datei im Internet unter:* http://www.math.uni-frankfurt.de/~bieri/

- $e \mid f \wedge f \mid e \Rightarrow e = f$

(c) Sei wieder $d := \mathrm{ggT}(m,n)$ und $e := \mathrm{ggT}(a^m - 1, a^n - 1)$
Z.Z.: $e = a^d - 1$. Es gilt: $e = a^d - 1 \Leftrightarrow \underbrace{a^d - 1 \mid e}_{(i)} \wedge \underbrace{e \mid a^d - 1}_{(ii)}$

(i): $d \mid m \wedge d \mid n \Rightarrow m = x \cdot d \wedge n = y \cdot d$ mit $x, y \in \mathbb{N}$.

$$\Rightarrow\ a^m - 1 = (a^d - 1)(1 + a^d + a^{2d} + \cdots + a^{(x-1)d}) \quad \text{sowie}$$
$$a^n - 1 = (a^d - 1)(1 + a^d + a^{2d} + \cdots + a^{(y-1)d}$$
$$\Rightarrow\ a^d - 1 \mid a^n - 1 \wedge a^d - 1 \mid a^n - 1 \overset{1.)(iii)}{\Rightarrow} a^d - 1 \mid e.$$

(ii): Da $d = \mathrm{ggT}(m,n)$, gibt es nach Bezout ganze Zahlen u, v' mit $d = m \cdot u + n \cdot v'$.
Wir wählen $v = -v'$ und erhalten $d = m \cdot u - n \cdot v$.
$a^m - 1 \mid a^{m \cdot n} - 1$, weil $a^{m \cdot n} - 1 = (a^m - 1)(1 + a^m + a^{2m} + \cdots + a^{(n-1)\cdot m)})$.
Analog gilt $a^n - 1 \mid a^{n \cdot v} - 1$.
$e \mid a^m - 1, e \mid a^n - 1 \wedge a^n - 1 \mid a^{m \cdot u} - 1, a^n - 1 \mid a^{n \cdot v} - 1 \Rightarrow$
$e \mid a^{m \cdot u} - 1 \wedge e \mid a^{n \cdot v} - 1 \overset{2.)}{\Rightarrow} e \mid (a^{m \cdot u} - 1) - (a^{n \cdot v} - 1) \Rightarrow$
$e \mid a^{m \cdot u} - a^{n \cdot v} \Rightarrow e \mid a^{nv} \cdot (a^{m \cdot u - n \cdot v} - 1) \overset{s.o.}{\Rightarrow} e \mid a^{nv} \cdot (a^d - 1)$.

Da zwei aufeinanderfolgende Zahlen teilerfremd sind und $e \mid a^n - 1$ gilt, folgt ggT $(e, a^n) = 1$ und somit ggT $(e, a^{n \cdot v}) = 1$.
Da aber e Teiler von $a^{n \cdot v} \cdot (a^d - 1)$ ist, kann also nur $e \mid a^d - 1$ gelten.

(i),(ii): $a^d - 1 \mid e \wedge e \mid a^d - 1 \Rightarrow e = a^d - 1$.