ggT und Euklidischer Algorithmus

RG, 14.11.2006

Satz: Es gibt $x,y \in Z$ s.d. $ax+by=n \Leftrightarrow ggT(a,b)|n$
(Insbesondere gibt es $ax+by=n$ zum $ggT=n$; und für teilerfremde Zahlen a, b mit $1=n$)

Beweis:
„$\Rightarrow$“
Es gebe x und y s.d. $ax+by=n$ und g sei = ggT(a,b)
$\Rightarrow a=ga_1$ und $b=gb_1$ sowie $ga_1x+gb_1y=n$
$\Rightarrow g(a_1x+b_1y)=n$
$\Rightarrow g|n$, da (a_1x+b_1y) ganzzahlig ist.
„$\Leftarrow$“
Euklidischer Algorithmus
$b=ax_1+R_1$ mit $R_1<a$ (sonst x_1 um 1 erhöhen)
$a=R_1x_2+R_2$ mit $R_2<R_1$ (sonst x_2 um 1 erhöhen)
$R_1=R_2x_3+R_3$ mit $R_3<R_2$ (sonst x_3 um 1 erhöhen)
...
$R_{n-2}=R_{n-1}x_n+R_n$ mit $R_n<R_{n-1}$ (sonst x_2 um 1 erhöhen)
$R_{n-1}=R_nx_{n+1}+R_{n+1}$ mit $R_{n+1}=0$
Behauptung: $R_n=ggT(a,b)$.
Begründung:
Erstens: R_n teilt R_{n-1}, also auch R_{n-2}, also auch… R_1, a und b.
R_n teilt a und b und damit auch ggT(a,b).
Zweitens: Zeile $R_{n-2}=R_{n-1}x_n+R_n$ als $R_n=R_{n-2}-R_{n-1}x_n$ nach oben hin auflösen bis zur Zeile a=… und b=…, so dass nur noch Summanden mit den Faktoren a oder b enthalten sind.
Diese dann zur Gleichung $ax+by=R_n$ zusammenfassen:
$R_n = R_{n-2}-R_{n-1}x_n$ und $R_{n-1} = R_{n-3}-R_{n-2}x_{n-1} \Rightarrow R_n = R_{n-2}-(R_{n-3}-R_{n-2}x_{n-1})x_n$ (Gln *)
Weiterhin $R_{n-2} = R_{n-4}-R_{n-3}x_{n-2}$ und $R_{n-3} = R_{n-5}-R_{n-4}x_{n-3}$ in Gln (*) einsetzen und so weiter, bis nur noch Summanden mit Faktoren a und b vorhanden sind. Diese zusammenfassen zur Gleichung $ax+by=R_n$. Nach „$\Rightarrow$“ gilt nun, dass $ggT(a,b)|R_n$.
Zusammengenommen: R_n teilt ggT(a,b) („erstens“) und $ggT(a,b)|R_n$ („zweitens“). Also muss gelten $ggT(a,b)=R_n$. *Ende der Begründung*.
Damit gibt es zu ggT(a,b) immer x und y so dass $ax+by=ggT(a,b)$. *A forteriori* gibt es solche x und y auch zu jedem Vielfachen des ggT(a,b).
q.e.d.

Satz: Für alle teilerfremden $a,b \in Z$ gilt die Kürzungsregel in Z_n:
$av \equiv aw \pmod b \Rightarrow v \equiv w \pmod b$
Beweis:
Nach dem Satz oben gibt es zum ggT(a,b)=1 ganze Zahlen x und y so dass $ax+by=1$. Das bedeutet, dass es ein Inverses x (mod b) zu a gibt: $ax \equiv 1 \pmod b$.
Zu beiden Seiten der Äquivalenz $av \equiv aw \pmod b$ werde dieses x (mod b) multipliziert, und es ergibt sich $av \equiv aw \pmod b \Rightarrow xav \equiv xaw \pmod b \Rightarrow 1 \cdot v \equiv 1 \cdot w \pmod b \Rightarrow v \equiv w \pmod b$. *q.e.d.*

Satz: Für *nicht* teilerfremden $a,b \in Z$ gilt die Kürzungsregel in Z_n *nicht*!
Gegenbeispiele: $12 \cdot \equiv 21 \ (\equiv 3) \pmod 9$ aber *keineswegs* $12/3 \equiv 21/3 \pmod 9$!
Ebenso gibt es Nullteiler: $6 \cdot 3 = 18 \equiv 0 \pmod 9$, aber weder 6, noch 3 sind Nullen in Z_9.