Bestimmung des modularen multiplikativen Inversen

ggT(330;78) = 6 ; ggT(504; 154) = 14 ; ggT(286; 630) = 2 ; ggT(6141, 3243) = 69

Der „Erweiterte Euklidischer Algorithmus (EEA)“

Allgemein:

Der EEA liefert für eine Gleichung der Form $a \cdot x + b \cdot y = ggT(a;b)$ mit $a, b \in \mathbb{N}$ (neben dem ggT(a;b) als Zwischenergebnis) die Lösungen $x, y \in \mathbb{Z}$.

Begründe mündlich:

a) + b) a= 4, b= 7, ggT(4 ; 7) = 1 → Definition ist erfüllt.

k, d : Variable mit d= x und k= -y.

Übung:

1. *Vergleiche den Aufwand von Probierlösung vs. Algorithmus* Sobald die Zahlen größer/unhandlicher werden, ist der Algorithmus effektiver.

2. *Bestimme das modulare Inverse d zu e:*

e	n	d	Probe
14	45	29	14 ·29 = 406 ≡ 1 (mod 45), da 45 · 9 = 405
17	390	23	17 ·23 = 391 ≡ 1 (mod 390)
70	143	47	70 ·47 = 3290 ≡ 1 (mod 143), da 23 ·143 = 3289
3	101	34	3 ·34 = 102 ≡ 1 (mod 101)
56	225	-4 bzw 221	56 ·(-4) = -1224 ≡ 1 (mod 225), da (-4) ·225 = -1125 56 ·221 = 12.376 ≡ 1 (mod 225), da 55 ·225 = 12.375
99	455	239	99·239 = 23.661 ≡ 1 (mod 455), da 52 ·455 = 23.660