Bestimmung des modularen multiplikativen Inversen

Eine Zahl d ist das multiplikative Inverse zu einer Zahl a (mod n), wenn gilt: $e \cdot d \equiv 1 \pmod n$

Bsp.: Gesucht ist d mit $4 \cdot d \equiv 1 \pmod 7$, d.h. e = 4 ; n = 7.

$4 \cdot d \equiv 1 \pmod 7 \quad \Leftrightarrow \quad 4 \cdot d - k \cdot 7 = 1$ mit einer beliebigen Zahl $k \in \mathbb{Z}$.

unser Ziel muss also eine Lösung (d ; k) dieser Gleichung sein, von der wir nur d benötigen.

Eine systematische Lösung – **der Erweiterte Euklidische Algorithmus**

Aus Klasse 8/9 kennst du bereits den *Euklidischen Algorithmus* zur Bestimmung des ggT zweier Zahlen. Auf diesem Algorithmus werden wir aufbauen.

Wiederhole die Vorgehensweise bei diesem Algorithmus. Recherchiere dazu im Internet.

Berechne damit:

ggT(330;78) ; ggT(504; 154) ; ggT(286; 630) ; ggT(6141, 3243)

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) *Unsere Gleichung $4 \cdot d - k \cdot 7 = 1$ mit $d, k \in \mathbb{Z}$ ist eine Gleichung diesen Typs.*

b) *Welche Bestandteile in unserer Gleichung entsprechen a, b, x und y in der allgemeinen?*

c) *Bespreche deine Erkenntnisse mit deinem Nachbarn/deiner Nachbarin.*

Prinzipielles Vorgehen: Zunächst wird mit dem bekannten Euklidischen Algorithmus der ggT(a;b) bestimmt. Dann werden die Gleichungen „zurückgerechnet“, um eine Darstellung des ggT(a;b) in der Form $a \cdot x + b \cdot y$ zu bekommen.

An unserem Beispiel $4 \cdot d - k \cdot 7 = 1$ durchgeführt:

1) Euklid: bestimme den ggT(4;7) → Benennung der Gleichungen

$7 = 1 \cdot 4 + 3$ → I

$4 = 1 \cdot 3 + 1$ → II

$3 = 3 \cdot 1 + 0$

2) Jetzt rechnen wir zurück.

ZIEL: drücke die *1* *(den ggT)* *durch 4 und 7* aus!

aus II: $1 = 4 - 1 \cdot 3$ → III „*4 ist schon GUT! 3 nicht. → 3 durch 4 und 7 darstellen!*“

aus I in III: $3 = 7 - 1 \cdot 4$ „*Darstellung der 3 ersetzen in Gleichung II.*“

Dann folgt mittels Ausmultiplizieren und Zusammenfassen die Lösung:

$$1 = 4 - 1 \cdot (7 - 1 \cdot 4) = 4 - 1 \cdot 7 + 1 \cdot 4 = 2 \cdot 4 - 1 \cdot 7 = 4 \cdot 2 - 1 \cdot 7, \text{ also:}$$

$$1 = 4 \cdot 2 - 1 \cdot 7$$

Damit hat die Gleichung $4 \cdot d - k \cdot 7 = 1$ die Lösung $d = 2$ (und $k = 1$). *(→ Probe!)*

Von dieser Lösung benötigen wir nur einen Teil: Unser ursprüngliches Problem (s.o.) war die Lösung der Gleichung $4 \cdot d = 1 \pmod 7$, d.h. wir benötigen nur den Wert für d.

Es gilt: $(4 \cdot 2) = 8 = 1 \pmod 7$. Damit ist $d = 2$ das (multpl.) Inverse zu $e = 4$ bezüglich mod 7.

Übung:

1. *Berechne die Inversen von AB „03b.0_mgk_Verschlüsseln_durch_modulare_Mult.“ (S.5) mit dem Erweiterten Euklidischen Algorithmus. Vergleiche den Aufwand...*

Bem: Erinnere dich an die Regel $(a + z \cdot n) \bmod n = a \pmod n$ *für* $z \in \mathbb{Z}$.

2. *Bestimme das modulare Inverse d zu e bezüglich mod n, also die Zahl e mit der Eigenschaft* $e \cdot d \equiv 1 \pmod n$. *Führe eine Probe durch!*

e	n	d	Probe
14	45	29	$14 \cdot 29 = 406 \equiv 1 \pmod{45}$, da $45 \cdot 9 = 405$
17	390		
70	143		
3	101		
56	225		
99	455		

3. *Erstelle selbst eine Aufgabe des selben Typs wie oben und gib sie zur Lösung weiter.*
4. * *Zusatz für Programmierer: Setze den Algorithmus in einer Tabellenkalkulation oder in Scratch um: In zwei Eingabefeldern werden e und n angegeben, die Ausgabe liefert d.*