Lösbarkeit von Kongruenzen der Form $ax \equiv b \bmod m$

In der letzten Übung kamen die Kongruenzen ein bisschen zu kurz. Hier eine kleine Wiederholung. Es ist übrigens durchaus erlaubt, beim Test alle Werte durchzuprobieren um so auf eine Lösung von $ax \equiv b \bmod m$ zu kommen. Für alle, die es genauer wissen wollen hier ein kleiner Text mit Beispielen am Ende.

Wir haben eine Kongruenz der Form $ax \equiv b \bmod m$.

Beispiele dafür wären z.B. die Kongruenzen aus der Übung: $8x \equiv 4 \bmod 16$ oder $8x \equiv 4 \bmod 15$.
Ein sehr hilfreicher Satz ist der folgende:

> $ax \equiv b \bmod m$ ist lösbar genau dann wenn $ggT(a, m)$ teilt b.

Wie gehe ich das Problem jetzt an:

1. Schritt: Überprüfe ob $ggT(a, m)$ die Zahl b teilt

Wenn nein sind wir hier fertig und können sagen: Es gibt keine Lösung!
Wenn ja: weiter zum nächsten Schritt

2. Schritt: Dividieren durch den $ggT(a, m)$

Ich nenne den $ggT(a, m)$ jetzt d. Ich kann nun die ganze Gleichung durch d dividieren. Dann erhalte ich aus $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ und $m' = \frac{m}{d}$ eine neue Kongruenz der Form:

$$a'x \equiv b' \bmod m'$$

Hier gilt $ggT(a', m') = 1$, das heißt es gibt ein Inverses modulo m', also ein c mit $a'c \equiv 1 \bmod m'$ oder anders ausgedrückt: Es gibt c und e mit $1 = a'c + m'e$. Diese beiden Werte berechne ich mir mit dem Euklidischen Algorithmus. (Siehe Beispiel)

3. Schritt: Multiplizieren mit c

Ich kann nun die ganze Kongruenz mit c multiplizieren. Daraus ergibt sich:

$$\begin{aligned} ca'x &\equiv cb' \bmod m' \text{ also (weil } ca' \equiv 1 \bmod m) \\ x &\equiv cb' \bmod m' \end{aligned}$$

Die Lösung ist also $\{..., cb' - 2m, cb' - m, cb', cb' + m, cb' + 2m, ...\}$ oder anders gesagt $cb' + jm$, $j \in \mathbb{Z}$.

Beispiele

Bsp 1: $8x \equiv 4 \bmod 16$

1. Schritt:
$ggT(8, 16) = 8$, aber 8 teilt nicht 4, das heißt wir sind fertig und es gibt keine Lösung.

Bsp 2: $8x \equiv 4 \bmod 15$

1. Schritt:
$ggT(8, 15) = 1$, 1 teilt 4, das heißt es gibt eine Lösung.

2. Schritt:
Wir dividieren die Gleichung durch 1, dadurch ändert sie sich aber nicht. Jetzt müssen wir $ggT(8, 15)$ mit dem Euklidischen Algorithmus anders darstellen um an das Inverse c zu gelangen.

$$\begin{aligned} 15 &= 8 * 1 + 7 \\ 8 &= 7 * 1 + 1 \\ 7 &= 1 * 7 + 0 \end{aligned}$$

Das heißt, wir können jetzt den $ggT(8, 15)$ darstellen durch

$$1 = 8 - 7 * 1 = 8 - (15 - 8 * 1) * 1 = 2 * 8 - 15$$

Das Inverse c ergibt sich also als 2 mod 15, also können wir alle Zahlen nehmen, die kongruent 2 modulo 15 sind. Wir setzen $c = 2$.

3. Schritt:
Wir Multiplizieren die Gleichung mit $c = 2$. Daraus ergibt sich:

$$\begin{aligned} x &\equiv 2 * 4 \bmod 15 \\ x &\equiv 8 \bmod 15 \end{aligned}$$

Das heißt die Lösungen sind $\{\dots, -2 * 15 + 8, -15 + 8, 8, 8 + 15, 8 + 2 * 15, \dots\} = \{\dots, -24, -7, 8, 23, 38, \dots\}$ oder schöner $8 + j * 15$, $j \in \mathbb{Z}$.

Bsp 3: $3x \equiv 9 \bmod 12$

1. Schritt:
$ggT(3, 12) = 3$, 3 teilt 9, das heißt es gibt eine Lösung.

2. Schritt:
Dividiere die Kongruenz durch 3, es ergibt sich die neue Kongruenz

$$x \equiv 3 \bmod 4$$

Die Lösungen sind direkt ablesbar, sie sind $\{\dots, -5, -1, 3, 7, 11, \dots\}$ oder schöner $3+j*4$, $j \in \mathbb{Z}$.

Bsp 4: $15x \equiv 10 \bmod 25$

1. Schritt:
$ggT(15, 25) = 5$, 5 teilt 10, das heißt es gibt eine Lösung.

2. Schritt:
Dividiere durch den $ggT(15, 25)$. Man erhält

$$3x \equiv 2 \bmod 5$$

$ggT(3, 5) = 1$, also gibt es ein c mit $3 * c \equiv 1 \bmod 5$. Wir berechnen dieses c wieder mit dem Euklidischen Algorithmus:

$$\begin{aligned} 5 &= 3 * 1 + 2 \\ 3 &= 2 * 1 + 1 \\ 2 &= 1 * 2 + 0 \end{aligned}$$

Also können wir den $ggT(3, 5)$ wieder anders darstellen.

$$1 = 3 - 2 * 1 = 3 - (5 - 3 * 1) * 1 = 2 * 3 - 5$$

Wir erhalten also als Inverses $c = 2$.

3. Schritt:
Multiplizieren mit $c = 2$ liefert

$$\begin{aligned} x &= 2 * 2 \bmod 5 \\ x &= 4 \bmod 5 \end{aligned}$$

Die Lösungen sind also $\{\dots, -6, -1, 4, 9, 14, \dots\}$ oder anders angeschrieben $4 + j * 5$, $j \in \mathbb{Z}$.