universität wien

Fakultät für Mathematik

Arman Sadeghi Rad
Matrikelnummer 12223560
Einführung in das mathematische Arbeiten
Wintersemester 2022/2023

Übungsblatt 5B

Aufgabe 1. Der größte gemeinsame Teiler von a und m ist $\mathrm{ggT}(a, m)$. Daher ist auch die Aussage

$$\mathrm{ggT}\left(\frac{a}{\mathrm{ggT}(a,m)}, \frac{m}{\mathrm{ggT}(a,m)}\right) = 1$$

richtig. Nach einem Satz von der Vorlesung gibt es $p, q \in \mathbb{Z}$, sodass

$$\frac{a}{\mathrm{ggT}(a,m)}p + \frac{m}{\mathrm{ggT}(a,m)}q = 1. \tag{1}$$

Nach einer Multiplikation mit b wird hergeleitet, dass

$$abp\frac{1}{\mathrm{ggT}(a,m)} + mbq\frac{1}{\mathrm{ggT}(a,m)} = b$$

und in der Resklasse von m

$$abp\frac{1}{\mathrm{ggT}(a,m)} \equiv b \mod m. \tag{2}$$

Für die Gleichungen 1 und 2 in der Restklasse von m, gelten auch $p + km$ wenn $k \in \mathbb{Z}$. aber wenn $k = \mathrm{ggT}(a, m)$ dann gilt

$$ab(p+m\mathrm{ggT}(a,m))\frac{1}{\mathrm{ggT}(a,m)} = abp\frac{1}{\mathrm{ggT}(a,m)} + m\frac{\mathrm{ggT}(a,m)}{\mathrm{ggT}(a,m)} \equiv abp\frac{1}{\mathrm{ggT}(a,m)} \equiv b \mod m.$$

Daher gibt es nur $\mathrm{ggT}(a, m)$ Lösungen die mod m inkongruent sind.

Aufgabe 2. Wir müssen die Elementen bestimmen die Einheite sind. Dafür sollte man die Elementen wie x auswählen, die wenn $R = \mathbb{Z}_n$, $\mathrm{ggT}(x, n) = 1$.

$$\begin{array}{l}
\mathbb{Z}_4 : \{\bar{1}, \bar{3}\} \\
\mathbb{Z}_7 : \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\} \\
\mathbb{Z}_8 : \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \\
\mathbb{Z}_9 : \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}
\end{array}$$

Aufgabe 3. $p_1 = 5, a_1 = 4$, $p_2 = 7, a_2 = 6$, $p_3 = 9, a_3 = 8$. Daher $p_1p_2p_3 = 315$.

$$\begin{array}{lrl}
\mathrm{ggT}(\frac{p_1p_2p_3}{p_1} = 63, p_1 = 5) = 1 & 2 \cdot 63 - 25 \cdot 5 = 1 & \Rightarrow a_1M_1N_1 = 504 \\
\mathrm{ggT}(\frac{p_1p_2p_3}{p_2} = 45, p_2 = 7) = 1 & -2 \cdot 45 + 13 \cdot 7 = 1 & \Rightarrow a_2M_2N_2 = -540 \\
\mathrm{ggT}(\frac{p_1p_2p_3}{p_3} = 35, p_3 = 9) = 1 & -1 \cdot 35 + 4 \cdot 9 = 1 & \Rightarrow a_3M_3N_3 = -280
\end{array}$$

Daher ist die Lösung $x = -316 \equiv -1 \mod 315$. Aber die Besonderheit der Reste ist die Tatsache, dass alle der Kongruenzen, den Rest -1 haben. Daher das System von Kongruenzen könnte durch $x \equiv -1 \mod 5 \cdot 7 \cdot 9$ abgekürzt werden. Durch die Lösung auch wird dieselbe Zahl ergibt. $x \equiv -1 \equiv -316 \mod 315$

Aufgabe 4.

$$\begin{aligned}
7x &\equiv 8 \equiv 28 &&\mod 20 &&\Rightarrow & x &\equiv 4 &&\mod 20\\
5x &\equiv 6 \equiv -15 &&\mod 21 &&\Rightarrow & x &\equiv -3 &&\mod 21\\
9x &\equiv 13 \equiv 36 &&\mod 23 &&\Rightarrow & x &\equiv 4 &&\mod 23
\end{aligned}$$

Es ist genügend, nur das System für $x \equiv -3 \mod 21$ und $x \equiv 4 \mod 460$ zu lösen.

$$10 \cdot 460 - 219 \cdot 21 = 1 \Rightarrow x = -3 \cdot 10 \cdot 460 - 4 \cdot 219 \cdot 21 = -31196 \equiv 7444 \mod 20 \cdot 20 \cdot 23$$

Aufgabe 5. **mod** 2:

$$n \equiv b_0 + (b_1 + b_2 + \cdots + b_k) \cdot \bar{1} \mod 2$$

mod 7: Hierfür sollte man erstens b_i Zahlen in 6-Gruppen einteilen und die Zahlen davon paarweise wie $(b_i - b_{i+3}) + (b_{i+1} - b_{i+4}) + (b_{i+2} - b_{i+5})$ umformulieren. Weil

$$\begin{array}{ccccccccccccc}
1 & \xRightarrow{\times 3} & 3 & \xRightarrow{\times 3} & 2 & \xRightarrow{\times 3} & -1 & \xRightarrow{\times 3} & -3 & \xRightarrow{\times 3} & -2 & & \mod 7\\
b_1 & & b_2 3 & & b_3 3^2 & & b_4 3^3 & & b_5 3^4 & & b_6 3^5 & &
\end{array}$$

Wenn die Summe nach dem Einteilen und der Rest von der triadischen Entwicklung durch 7 teilbar ist, dann wird auch die Zahl durch 7 teilbar.
mod 9:

$$n \equiv b_0 + b_1 3 \mod 9$$

Weil die andere Sätze schon durch 9 teilbar sind.