WIEDERHOLUNG (BIS ZU BLATT 7)

JULIA SAUTER

Wir wiederholen, welche Aufgabentypen bis zu diesem Zeitpunkt behandelt worden sind. Auf der nächsten Seite können Sie sich selber testen. Dies ist ein Trainingszettel für die Probeklausur (= Übungsblatt 8).

(1) Teilen mit Rest in den ganzen Zahlen.
(2) Umrechnen zwischen Ziffernsystemen.
(3) Addition, Subtraktion und Multiplikation in anderen Ziffernsystemen.
(4) Erweiterter euklidischer Algorithmus.
(5) Lösen einer linearen diophantischen Gleichung der Form

$$ax + by = c$$

mit explizit gegebenen $a, b, c \in \mathbb{Z}$.
(das heißt: Finden Sie alle $(x, y) \in \mathbb{Z}^2$, die die Gleichung erfüllen.)
(6) Berechnung des ggT zweier ganzer Zahlen mit Hilfe der Primfaktorzerlegung.
(7) Invertieren von primen Restklassen. Gegeben $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ mit $\mathrm{ggT}(a, n) = 1$, dann findet man mit dem erweiterten euklidischen Algorithmus $k, m \in \mathbb{Z}$ mit

$$ka + mn = 1.$$

Reduzieren wir modulo n, d.h. für die Restklassen modulo n erhalten wir

$$[k]_n[a]_n = [1]_n.$$

Damit haben wir $[k]_n$ als das Inverse von $[a]_n$ ausgerechnet.
Anmerkung: Sie können auch die Potenzen von $[a]_n$ berechnen, um das Inverse zu finden, das dauert nur häufig länger.
(8) Potenzieren von Restklassen.
(9) Lösen einer Gleichung

$$ax \equiv c \pmod{n}$$

mit $a, c \in \mathbb{Z}$ in den Restklassen modulo n. Hier gilt es zu verstehen, dass man stattdessen die Lösungen als die Restklassen $[x]_n$ findet, so dass es $(x, y) \in \mathbb{Z}^2$ gibt mit

$$ax + ny = c.$$

(10) Caesar-Verschlüsselung
(11) Zeigen, dass eine diophantische Gleichung keine Lösung in den ganzen Zahlen hat: Durch Reduktion modulo n (für ein glücklich gewähltes n).
(Warnung: Es ist oft nicht klar, welches n man nehmen soll. Wenn die diophantische Gleichung doch Lösungen in $\mathbb{Z}$ hat, kann man sich lange vergeblich bemühen.)
(12) Lösen simultaner Kongruenzen.
(13) Lösen von diophantischen Gleichungen modulo n insbesondere auch mit
   a) dem chinesischen Restsatz.
   b) dem Satz von Hensel, wenn er anwendbar ist.

Trainingszettel

(1) Teilen Sie:
   (a) 4321 durch 5 mit Rest.
   (b) 1480 durch 7 mit Rest.

(2) Schreiben Sie
   (a) 4321_{10} im 5-er System.
   (b) 1480_{10} im 7-er System.

(3) (a) Subtrahieren Sie 1221_3 von 10010_3 im 3-er System.
   (b) Multiplizieren Sie 2301_4 mit 32_4 im 4-er System.

(4) Finden Sie den größten gemeinsamen Teiler von 31 und 75 und schreiben Sie ihn als Linearkombination von 31 und 75.

(5) Finden Sie alle Lösungen $(x, y) \in \mathbb{Z}^2$ der diophantischen Gleichungen

$$62x + 150y = 4.$$

(6) Berechnen Sie: $\mathrm{ggT}(3072, 1452)$ mit Hilfe der Primfaktorzerlegung in $\mathbb{Z}$.

(7) Invertieren Sie $[31]_{75}$ und $[75]_{31}$.

(8) (a) Berechnen Sie alle Potenzen von $[6]_{25}$ bis eine Wiederholung eintritt.
   (b) Berechnen Sie alle Potenzen von $[6]_{11}$ bis eine Wiederholung eintritt.

(9) Lösen Sie die Gleichung

$$62x \equiv 4 \pmod{150}$$

in den Restklassen modulo 150.

(10) Wir ordnen den Buchstaben $A, B, C, \ldots$ die Zahlen $0, 1, 2, \ldots$ zu. Verschlüsseln Sie *Hello World* mit der Caesar Verschlüsselung $y \equiv 5x + 1 \pmod{26}$ und berechnen Sie die Entschlüsselungsvorschrift.

(11) Zeigen Sie, dass

$$x^{13} - 13y - x + 1 = 0$$

keine Lösungen in $\mathbb{Z}$ hat. Hinweis: Hier kann der kleine Satz von Fermat benutzt werden.

(12) Finden Sie alle $x \in \mathbb{Z}$, die die folgenden Kongruenzen erfüllen.

$$x \equiv 10 \pmod{15}, \quad x \equiv 10 \pmod{25}, \quad x \equiv 0 \pmod{5}.$$

(13) (a) Finden Sie **alle** Lösungen von

$$x^2 + 3 \equiv 0 \pmod{91}$$

in den Restklassen modulo 91. Beachten Sie $91 = 7 \cdot 13$.

   (b) Finden Sie **eine** Lösung von

$$x^2 + 5 \equiv 0 \pmod{49}.$$

in den Restklassen modulo 49.

Lösungen vom Trainingszettel 1

(1) Teilen Sie:
   (a) 4321 durch 5 mit Rest.
   $4321 = 864 \cdot 5 + 1$.
   (b) 1480 durch 7 mit Rest.
   $1480 = 211 \cdot 7 + 3$.

(2) Schreiben Sie
   (a) 4321_{10} im 5-er System.
   $4321_{10} = 114241_5$.
   (b) 1480_{10} im 7-er System.
   $1480_{10} = 4213_7$.

(3) (a) Subtrahieren Sie 1221_3 von 10010_3 im 3-er System.
   1012_3
   (b) Multiplizieren Sie 2301_4 mit 32_4 im 4-er System.
   212232_4

(4) Finden Sie den größten gemeinsamen Teiler von 31 und 75 und schreiben Sie ihn als Linearkombination von 31 und 75. $1 = 12 \cdot 75 - 29 \cdot 31$.

(5) Finden Sie alle Lösungen $(x, y) \in \mathbb{Z}^2$ der diophantischen Gleichungen

$$62x + 150y = 4.$$

Teile durch $ggT(62, 150) = 2$, und erhalte $31x+75y = 2$. Multipliziere $31(-29)+12\cdot 75 = 1$ mit 2, und erhalte

$$31(-58) + 75 \cdot 24 = 2$$

Allgemeine Lsg: $x = -58 + 75k, y = 24 - 31k$ mit $k \in \mathbb{Z}$.

(6) Berechnen Sie: $\mathrm{ggT}(3072, 1452)$ mit Hilfe der Primfaktorzerlegung in $\mathbb{Z}$.
$3072 = 3 \cdot 2^{10}, 1452 = 3 \cdot 2^2 \cdot 11^2$ also $ggT = 3 \cdot 2^2 = 12$.

(7) Invertieren Sie $[31]_{75}$ und $[75]_{31}$.
Folgt direkt aus (4): $[31]_{75}^{-1} = [-29]_{75}, [75]_{31}^{-1} = [12]_{31}$

(8) (a) Berechnen Sie alle Potenzen von $[6]_{25}$ bis eine Wiederholung eintritt.
   $6^6 \equiv 6 \pmod{25}$ ist die erste Wiederholung.
   (b) Berechnen Sie alle Potenzen von $[6]_{11}$ bis eine Wiederholung eintritt.
   Diese Frage ist äquivalent zur Berechnung der Ordnung von 6 modulo 11, 6 is eine Primitivwurzel modulo 11 , hier gilt $6^{11} \equiv 6 \pmod{11}$ ist die erste Wiederholung.

(9) Lösen Sie die Gleichung

$$62x \equiv 4 \pmod{150}$$

in den Restklassen modulo 150.

Wir wissen schon, dass die Gleichung $62x + 150y = 4$ Lösungen mit den folgenden x-Anteil hat:

$$x = -58 + 75k,$$

wir müssen nur noch bestimmen zu welchen $2(= ggT(62, 150))$ Restklassen modulo 150 diese x gehören:

$$[-58]_{150}, [17]_{150}$$

hier ist einfach $17 = -58 + 75$ ausgerechnet worden.

(10) Wir ordnen den Buchstaben $A, B, C, \ldots$ die Zahlen $0, 1, 2, \ldots$ zu. Verschlüsseln Sie *Hello World* mit der Caesar Verschlüsselung $y \equiv 5x + 1 \pmod{26}$ und berechnen Sie die Entschlüsselungsvorschrift.

$$10, 21, 4, 4, 19 \quad 7, 19, 8, 4, 16$$

Die Entschlüsselungsvorschrift ist $x \equiv -5y + 5 \pmod{26}$.

(11) Zeigen Sie, dass

$$x^{13} - 13y - x + 1 = 0$$

keine Lösungen in $\mathbb{Z}$ hat. Hinweis: Hier kann der kleine Satz von Fermat benutzt werden. Rechne modulo 13. Kleiner Fermat: $x^{13} \equiv x \pmod{13}$. Also gilt:

$$x - 0 \cdot y - x + 1 \equiv 1 \pmod{13}$$

und dies ist ungleich $0 \pmod{13}$, also gibt es keine Lösungen modulo 13 und damit keine Lösungen in $\mathbb{Z}$.

(12) Finden Sie alle $x \in \mathbb{Z}$, die die folgenden Kongruenzen erfüllen.

$$x \equiv 10 \pmod{15}, \quad x \equiv 10 \pmod{25}, \quad x \equiv 0 \pmod{5}.$$

Die letzte Kongruenz ist impliziert bei den ersten beiden, also können wir uns auf die simultane Kongruenz

$$x \equiv 10 \pmod{15}, \quad x \equiv 10 \pmod{25}$$

einschränken. $ggT(15, 25) = 5$, $kgV(15, 25) = 75$. Wegen $10 - 10 \equiv 0 \pmod{5}$ ist der chinesische Restsatz anwendbar, in diesem Fall ist die Lösung trivial, da $a = b = 10$:

$$x \equiv 10 \pmod{75}.$$

(13) (a) Finden Sie **alle** Lösungen von

$$x^2 + 3 \equiv 0 \pmod{91}$$

in den Restklassen modulo 91. Beachten Sie $91 = 7 \cdot 13$.
Berechne Lsg mod 7:

$$x^2 \equiv -3 \equiv 4 \pmod{7}$$

hat die Lösungen $x \equiv \pm 2 \pmod{7}$.
Berechne Lsg mod 13:

$$x^2 \equiv -3 \equiv 10 \pmod{13}$$

hat die Lösungen $x \equiv \pm 6 \pmod{13}$.
Viermaliges Anwenden des chinesischen RS gibt nun alle Lösungen modulo 91:
Die simultane Kongruenz $x \equiv a \pmod{7}, x \equiv b \pmod{13}$ wird gelöst, indem man von $1 = 2 \cdot 7 - 13$ ausgehend das folgende ansetzt $x \equiv b \cdot 14 - a \cdot 13 \pmod{91}$. Wir erhalten

1. für $a = 2, b = 6$: $x \equiv 58 \pmod{91}$
2. für $a = -2, b = 6$: $x \equiv 19 \pmod{91}$
3. für $a = -2, b = -6$: $x \equiv -58 \pmod{91}$
4. für $a = 2, b = -6$: $x \equiv -19 \pmod{91}$

(b) Finden Sie **eine** Lösung von

$$x^2 + 5 \equiv 0 \pmod{49}.$$

in den Restklassen modulo 49.

Eine Lösung mod 7 von

$$x^2 \equiv -5 \equiv 2 \pmod{7}$$

ist $c = 3$. Sei $f(x) = x^2 + 5$ Wir betrachten

$$\frac{f(c)}{7} + kf'(c) \equiv 2 + k6 \equiv 0 \pmod{7}$$

das impliziert $6k \equiv 5 \pmod 7$ und dies impliziert $k \equiv 2 \pmod 7$. Wir wählen $k = 2$ als Repräsentanten dieser Restklasse modulo 7 und setzen

$$c_1 := c + k \cdot 7 = 3 + 2 \cdot 7 = 17$$

Nach dem Satz von Hensel ist 17 eine Lösung von $x^2 + 5 = 0$ modulo 49.