

Mathe 1 Tutorium Blatt 7

Alex B.

Dezember 2024

1 Lösen von linearen diophantischen Gleichungen

- Man kann mithilfe des erweiterten Euklidischen Algorithmus einfach sämtliche Möglichkeiten für die Lösung von linearen diophantischen Gleichungen bestimmen. Hierfür muss man nur folgende Schritte befolgen:
 - Ermittle den $\text{ggT}(a,b) = d$ mithilfe des Algorithmus von Euklid
 - Ermittle eine mögliche Lösung der Gleichung mithilfe des erweiterten Algorithmus von Euklid
 - Bestimmen aller Lösungen durch Erweitern von x_0 und y_0 mit $\frac{b}{d} * k$ und $-\frac{a}{d} * k$, wobei $k \in \mathbf{Z}$

2 Aufgaben

- Bestimme alle möglichen Lösungen der folgenden diophantischen Gleichungen
 - a) $a = 225, b = 79, c = 23$
 - b) $a = 625, b = 105, c = 20$
 - c) $a = 1111, b = 729, c = 4$

3 Modulare Arithmetik

- Rechnen in Restklassen: Zwei Zahlen, die dasselbe Ergebnis modulo einer anderen Zahl ergeben, heißen kongruent. Die Kongruenzen einer Zahl entsprechen dann ihrer jeweiligen Restdarstellung und man kann mit ihnen nach den bekannten Rechenregeln rechnen. Ein Inverses der Multiplikation (die Division) ist allerdings nur möglich, wenn die Zahl und das Modul 1 als ggT besitzen.

- Der Chinesische Restesatz: Man kann große Module leichter lösen, indem man sie in mehrere (teilerfremde) Module aufteilt und später durch ein System an simultanen Kongruenzen auf die ursprüngliche Modulgröße zurückrechnet.

4 Aufgaben

- Berechne (falls möglich) die Ergebnisse der folgenden Aufgaben in den Restklassen
 - a) Was ist das additive Inverse von $17 \bmod 20$
 - b) Was ist $x \equiv 4^{-1} \bmod 61$
- Löse folgende Aufgaben mithilfe des chinesischen Restesatzes:
 - a) $111 + 23 * 4^{-1} \bmod 143$
 - b) $41 + 12 * 7^{-1} \bmod 407$
 - c) $5 \bmod 7, 8 \bmod 11$ und $\bmod 13$
 - d) $12 \bmod 17, 56 \bmod 101$ und $42 \bmod 107$
 - e) $3 \bmod 4, 5 \bmod 8$ und $7 \bmod 16$
 - f) $2 \bmod 7, 20 \bmod 8$ und $3 \bmod 15$
 - g) $2 \bmod 3, 4 \bmod 5, 10 \bmod 13$ und $9 \bmod 17$