

Universität Leipzig Institut für Informatik Bioinformatik/IZBI	Algorithmen und Datenstrukturen II SoSe 2024 – Freiwillige Serie 12		
P.F. Stadler, T. Gatter	Ausgabe am 18.06.2024	Lösung am 25.06.2024	Seite 1/1

Algorithmen und Datenstrukturen II

SoSe 2024 – Serie 12

1 Modulo-Arithmetik

Geben Sie die Tabellen an, die die Operationen in folgenden zwei Gruppen beschreiben. Die Gruppen sind auf Folie 9 der Vorlesung 11 definiert; geben Sie Tabellen entsprechend zu den Beispielen auf Folie 10 an.

- a) (2 Punkte) Additionstabelle für Gruppe $(\mathbb{Z}_6, +_6)$
- b) (4 Punkte) Multiplikationstabelle für Gruppe $(\mathbb{Z}_6^*, \times_6)$

Hinweis: überlegen sie jeweils (insbesondere für die multiplikativen Gruppen) zuerst, welche Zahlen überhaupt Elemente der Gruppe sind und somit überhaupt in der jeweiligen Tabelle vorkommen.

2 Primfaktorzerlegung

Finden Sie einen Primfaktor von $n = \mathbf{187}$ mit Hilfe von Pollards Rho-Algorithmus. Geben Sie den Programmablauf tabellarisch wieder. Für $i = 1, 2, \dots$, geben Sie in jeder Tabellenzeile jeweils die Werte von i , $(x_{i-1}^2 - 1)$, x_i , y , k und $d = \text{ggT}(x_i - y, n)$ an bis zur ersten Zeile mit $d > 1$. x_1 werde mit 6 initialisiert (d.h. nicht als irgendeine andere Zufallszahl).