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.

Lösung:

a) Additionstabelle für $\mathbb{Z}_6^+$

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

b) Multiplikationstabelle für $\mathbb{Z}_6^*$

$\times_6$	1	5
1	1	5
5	5	1

Da laut Vorlesung für Multiplikative Gruppe modulo n gilt: $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \text{ggT}(a,n) = 1\}$ und dies für $a = 0, 2, 3, 4, 6$ nicht zu trifft.

2 Primfaktorzerlegung

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

Lösung:

i	$(x_{i-1}^2 - 1)$	x_i	y	k	(d)
1	-	6	6	2	(-)
2	35	35	35	4	(1)
3	1224	102	35	4	(1)
4	10403	118	118	8	(1)
5	13923	85	118	8	(11)