Zahlentheorie

Übung, LVA 405.031
C. Fuchs, I. Vukusic

10. Übungsblatt, SS 2022

03.06.2022

1. Zwei Zahnräder mit $m = 21$ beziehungsweise $n = 52$ Zähnen greifen ineinander.
   a) Wie viele Umdrehungen muss das große Zahnrad machen, bis wieder - wie zu Beginn - der gleiche Zahn des einen Rades in die gleiche Lücke des anderen greift?
   b) Wir nummerieren die Zähne von 0 bis 20 bzw. die Lücken von 0 bis 51 jeweils im Drehsinn. Zu Beginn treffen Zahn und Lücke mit den Nummern 0 aufeinander. Wie viele Umdrehungen müssen die beiden Räder machen, bis der Zahn mit der Nummer 17 (vom kleineren Rad) und die Lücke mit der Nummer 11 (vom größeren Rad) ineinandergreifen? Kann jede beliebige Zahlenkombination auftreten?
   c) Bei einem zweiten Räderwerk hat das größere Zahnrad 54 Zähne, das kleinere wieder 21. Welche Nummern können jetzt ineinandergreifen, wenn zu Beginn wieder die Nullen aufeinandertreffen?

2. Zerlege $\mathbb{Z}_{221}$ gemäß 3.2.3 in ein Produkt von Restklassenringen und gib dabei den Isomorphismus sowie die dazugehörige inverse Abbildung explizit an.

3. Beweise den Zusatz in 4.1.1: Die Lösungsmenge der Gleichung $ax = b$ in $\mathbb{Z}_n$ ist gegeben durch $\{x_0, x_0 + n', x_0 + 2n', \ldots, x_0 + (d-1)n'\}$, wobei $d = \mathrm{ggT}(a, n)$ ein Teiler von b und x_0 die kleinste Lösung von $ax = b$ in $\mathbb{Z}_n$ ist und wobei $n' = n/d$ gesetzt wird.

4. Das Caesar-Verschlüsselungsverfahren vom 8. Übungsblatt kann leicht verallgemeinert werden, indem wir gemäß $x \mapsto ax + b \bmod 41$ verschlüsseln. Verschlüssele die Wörter MATHEMATIK und ZAHLENTHEORIE mit a) $a = 1, b = 10$, b) $a = 10, b = 1$ und c) $a = b = 11$. Berechne die zugehörigen Entschlüsselungsformeln.

5. Löse in $\mathbb{Z}_{23}$ das lineare Gleichungssystem $14x + 21y = 22, 10x + 18y = 5$. Verwende dabei in jedem Schritt die Operationen des Restklassenrings und begründe, dass die Umformung erlaubt ist.