Aufgabe 31. Sei G eine Gruppe und $H \subseteq G$ eine Untergruppe. Zeige, daß durch

$$x \equiv_H y \iff x^{-1}y \in H$$

eine Äquivalenzrelation auf G definiert ist. Die Äquivalenzklassen heißen *Linksnebenklassen*.

Aufgabe 32. Wir betrachten die ganzen Zahlen als Gruppe $(\mathbb{Z}, +)$. Seien $m, n \in \mathbb{Z}$. Zeige, daß die kleinste Untergruppe $H \subseteq \mathbb{Z}$, die sowohl m als auch n enthält, gegeben ist durch $H = k\mathbb{Z}$, wobei $k = \mathrm{ggT}(m, n)$.

Aufgabe 33. Berechne die letzten zwei Ziffern in der Dezimaldarstellung der Zahl

$$a = 27^{202104}.$$

Vorgangsweise: Berechne Zahlen r_1 und r_2 sodaß

$$a \equiv r_1 \mod 4 \quad \text{und} \quad a \equiv r_2 \mod 25$$

und bestimme dann $a \mod 100$ mit dem chinesischen Restsatz.

Aufgabe 34 (Asmuth-Bloom-Verfahren)**.** Der chinesische Restsatz kann verwendet werden, um ein Geheimnis auf n Personen so aufzuteilen, daß mindestens k Personen nötig sind, um es zu lösen. Hier ist $n = 3$ und $k = 2$.

- Wähle teilerfremde Zahlen $m_0 < m_1 < m_2 < m_3$, sodaß $m_0 m_3 < m_1 m_2$.
- Das Geheimnis ist eine Zahl $0 \leq r < m_0$. Wähle eine zufällige Zahl $0 \leq t < \frac{m_1 m_2}{m_0}$ und setze $a = r + t m_0$ (dadurch ist sichergestellt, daß $a < m_1 m_2$).
- Berechne $c_i = a \mod m_i$ für $i = 1, 2, 3$.
- Die Zahl m_0 ist öffentlich bekannt, das Geheimnis wird wie folgt aufgeteilt: Alice erhält (c_1, m_1), Bob erhält (c_2, m_2) und Charly erhält (c_3, m_3).
- Um die geheime Zahl s wiederherzustellen, müssen mindestens zwei, zum Beispiel Alice und Bob, gemeinsam das Gleichungssystem

$$\begin{aligned} x &\equiv c_1 \mod m_1 \\ x &\equiv c_2 \mod m_2 \end{aligned}$$

lösen und können dann $s = x \mod m_0$ berechnen.

(a) Begründe, warum am Ende $s = r$ ist. Worauf ist dabei zu achten?
(b) Seien konkret $m_0 = 5$, $m_1 = 7$, $m_2 = 9$, $m_3 = 11$. Angenommen, Alice erhält das Paar $(4, 7)$ und Bob erhält das Paar $(8, 9)$. Wie lautet das Geheimnis r? Kann t rekonstruiert werden? Welches Paar (c_3, m_3) hat Charly erhalten?
(c) Angenommen, Charly erhält das Paar $(8, 11)$ und die Information, daß $0 \leq t \leq 5$ ist (er kennt m_1 und m_2 nicht). Welche möglichen Werte hat r?

Aufgabe 35. (a) Beschreibe und berechne einen Diffie-Hellman-Schlüsselaustausch mit den Parametern $p = 31$, $g = 5$, $a = 13$, $b = 11$. Was fällt auf? Welchen Parameter sollte man ändern?
(b) Zu einem Diffie-Hellman-Schlüsselaustausch seien folgende Daten bekannt:

$$g = 8 \qquad p = 29$$
$$m = 22 \qquad n = 2$$

Bestimme die geheimen Parameter a, b und den Schlüssel r!