Lösungen zu Übungsblatt 8.

Aufgabe 1 (8 Punkte)**.** Berechnen Sie

(i) $\bar{a}^6$ und $\bar{a}^7$ für alle $\bar{a} \in \mathbb{Z}/7\mathbb{Z}$,

(ii) $\bar{a}^8$ und $\bar{a}^9$ für alle $\bar{a} \in \mathbb{Z}/8\mathbb{Z}$.

Anmerkung: Beachten Sie, dass die Notation für die Äquivalenzklasse modulo n, $[a]_n$ und $\bar{a}$ genau das Gleiche bedeuten. Das heißt $[a]_n = \bar{a} = \{a + k \cdot n,\ k \in \mathbb{Z}\} = a + n\mathbb{Z}$.

Lösung zu Aufgabe 1. Zu i) (4 Punkte): Aus dem kleinen Satz von Fermat (1 Punkt), wissen wir dass

$$a^{\varphi(p)} = a^{p-1} \equiv 1 \mod p$$

mit $p \not| a$. Beachte das $\varphi(p) = p - 1$ und $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ genau dann, wenn $p \not| a$. Dies lässt sich auch formulieren als

$$a^p \equiv a \mod p$$

für alle $a \in \mathbb{Z}$ (für a mit $p|a$ ist dies trivialerweise richtig). Da 7 eine Primzahl ist, gilt also $\bar{a}^7 = \bar{a}$ für alle $a \in \mathbb{Z}/7\mathbb{Z}$. Während $\bar{a}^6 = 1$ für $a \in (\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$ gilt und $\bar{0}^6 = \bar{0}$. Zu ii) (4 Punkte): Hier ist $n = 2^3$ und $\varphi(2^3) = 2^2(2-1) = 4$. D.h. wir wissen aus dem kleinen Satz von Fermat, dass $\bar{a}^8 = (\bar{a}^4)^2 = \bar{1}$, sowie $\bar{a}^9 = \bar{a}$, für a mit $2 \not| a$. Für $a = 2, a = 4, a = 6$ gilt stets $8|a^8, a^9$ und damit $\bar{a}^8 = \bar{a}^9 = \bar{0}$.

Aufgabe 2 (10 Punkte)**.** Sei φ die eulersche Phi-Funktion.

(i) Berechnen Sie $\varphi(1)$, $\varphi(2025)$, $\varphi(121)$ und $\varphi(120)$.

(ii) Zeigen Sie, dass $\varphi(n)$ genau dann ungerade ist, wenn $n \in 1, 2$.

Lösung zu Aufgabe 2. Lösung zu i) (5 Punkte): Für $\varphi(1)$ müssen wir die Elemente in $\mathbb{Z}/1\mathbb{Z} = \{\bar{1}\}$ anschauen, hier gibt es nur $\bar{1}$. Da $\bar{1} \cdot \bar{1} = \bar{1}$ ist dieses Element eine Einheit und somit ist $\varphi(1) = 1$.

Für $\varphi(121)$ berechnen wir mithilfe der Primfaktorzerlegung und der Formel

$$\varphi(121) = \varphi(11^2) = 11^{2-1}(11-1) = 11 \cdot 10 = 110.$$

Für $\varphi(2025)$ ebenso:

$$\varphi(2025) = \varphi(5 \cdot 405) = \varphi(5 \cdot 5 \cdot 81) = \varphi(3^4 \cdot 5^2) = (3^{4-1}(3-1)) \cdot (5^{2-1}(5-1)) = 3^3 \cdot 2 \cdot 5 \cdot 4 = 1080.$$

Und für $\varphi(120)$:

$$\varphi(120) = \varphi(2^3 \cdot 3 \cdot 5) = (2^{3-1}(2-1))(3^{1-1}(3-1)) \cdot (5^{1-1}(5-1)) = 2^2 \cdot 2 \cdot 4 = 32.$$

Lösung zu ii) (5 Punkte): Ist $n = p_1^{n_1} \cdots p_m^{n_m}$ die Primfaktorzerlegung mit für Primzahlen $p_1, p_2, \cdots, p_m$ und $n_1, n_2, \cdots, n_m \in \mathbb{N} \setminus \{0\}$ (2 Punkte), so folgt aus der expliziten Formel für die Eulersche Phi-Funktion

$$\varphi(n) = \varphi(p_1^{n_1} \cdots p_m^{n_m}) = (p_1^{n_1-1}(p_1-1)) \cdots (p_m^{n_m-1}(p_m-1)).$$

Da jede Primzahl außer 2 ungerade ist, ist dieses Produkt gerade, sobald n einen Primfaktor $p \neq 2$ hat (durch den Faktor $p1$).

Wenn kein Primfaktor $p \neq 2$ auftritt, muss $n = 2^k$ für ein $k \in \mathbb{N}$ sein. Für $k \geq 2$ ist dann

$$\varphi(2^k) = 2^{k-1}(2-1) = 2^{k-1},$$

wobei $k - 1 \geq 1$ ist, somit ist $\varphi(2k)$ hier gerade.

Damit bleiben $n = 1$ und $n = 2$ zu prüfen. Wir wissen bereits $\varphi(1) = 1$ und für $\varphi(2) = 2^{1-1}(2-1) = 1$.

Insgesamt haben wir also gesehen, dass $\varphi(1) = \varphi(2) = 1$ und für alle anderen n ist $\varphi(n)$ gerade.

Aufgabe 3 (12 Punkte)**.** Beweisen Sie für die eulersche Phi-Funktion:

(i) Ist $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = p_1^{e_1} \cdots p_r^{e_r}$, dann gilt

$$\varphi(n) = n \cdot \prod_{i=1}^{r} (1 - \frac{1}{p_i}).$$

(ii) Für alle $a, b \in \mathbb{N} \setminus \{0\}$ gilt

$$\varphi(ab) = \varphi(a) \cdot \varphi(b) \cdot \frac{\mathrm{ggT(a,b)}}{\varphi(\mathrm{ggT(a,b)})}.$$

Lösung zu Aufgabe 3. Lösung zu i) (6 Punkte): Wir wissen, dass φ multiplikativ ist (2 Punkte) und $\varphi(p^k) = p^{k1}(p1)$ für Primzahlen p und $k \geq 1$. Hieraus folgt

$$\varphi(n) = \varphi(p_1^{e_1}) \cdot \varphi(p_r^{e_r}) = \prod_{i=1}^{r} (p_i - 1) p_i^{e_i - 1}.$$

Wegen $n = p_1^{e_1} \cdots p_r^{e_r}$ finden weiter

$$\varphi(n) = n \prod_{i=1}^{r} (p_i - 1) p_i^{-1} = n \prod_{i=1}^{r} (1 - \frac{1}{p_i}).$$

Zu ii) (6 Punkte): Wir schreiben

$$a = \varphi(p_1^{e_1}) \cdot \varphi(p_r^{e_r}) \varphi(q_1^{h_1}) \cdot \varphi(q_u^{h_u}),$$
$$b = \varphi(p_1^{f_1}) \cdot \varphi(p_r^{f_r}) \varphi(w_1^{t_1}) \cdot \varphi(w_v^{t_v}),$$

mit verschiedenen Primzahlen $p_1, \cdots, p_r, q_1, \cdots, q_u, w_1, \cdots, w_v$, und $e_i, f_i, h_i, t_i \geq 1$. Dann gilt

$$\mathrm{ggT(a,b)} = \mathrm{p_1^{\min\{e_1,f_1\}} \cdots p_r^{\min\{e_r,f_r\}}}$$

und nach i)

$$\varphi(ab)\varphi(\mathrm{ggT(a,b)}) = (\mathrm{ab} \prod_{\mathrm{i=1}}^{\mathrm{r}} (1 - \mathrm{p_i^{-1}}) \prod_{\mathrm{i=1}}^{\mathrm{u}} (1 - \mathrm{q_i^{-1}}) \prod_{\mathrm{i=1}}^{\mathrm{v}} (1 - \mathrm{w_i^{-1}}))(\mathrm{ggT(a,b)} \prod_{\mathrm{i=1}}^{\mathrm{r}} (1 - \mathrm{p_i^{-1}})).$$

Andererseits

$$\varphi(a)\varphi(b) = (a \prod_{i=1}^{r} (1 - p_i^{-1}) \prod_{i=1}^{u} (1 - q_i^{-1}))(b \prod_{i=1}^{r} (1 - p_i^{-1}) \prod_{i=1}^{v} (1 - w_i^{-1})).$$

Dies zeigt die Behauptung!

Aufgabe 4 (10 Punkte)**.** Beweisen Sie, dass für $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ die Multiplikation

$$\begin{aligned} m_a : \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z} \\ \bar{x} &\mapsto \overline{ax} \end{aligned}$$

ein Isomorphismus (von Gruppen) ist.

Lösung zu Aufgabe 4. Wir wissen, dass die Multiplikation mittels Repräsentanten wohldefiniert ist (2 Punkte). Daher ist auch die Abbildung m_a wohldefiniert (2 Punkte). Außerdem gilt für a, b

$$m_a \circ m_b(\bar{x}) = m_a(\overline{bx}) = \overline{abx} = m_{ab}(\bar{x}),$$

und, wegen $a^1 a = aa^1 = e$, daher $m_a \circ m_{a^1} = m_{a^1} \circ m_a = Id$. D.h. m_a ist bijektiv. Wir haben auch

$$m_a(\bar{x} + \bar{y}) = m_a(\overline{x+y}) = \overline{a(x+y)} = \overline{ax} + \overline{ay} = m_a(\bar{x}) + m_a(\bar{y}),$$

d.h. m_a ist ein Homomorphismus der additiven Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ (6 Punkte).

Zusatzaufgabe 5. Seien $a, b \in \mathbb{Z}$ teilerfremd und sei $c \in \mathbb{Z}$ beliebig. Beweisen Sie $\mathrm{ggT(a,c)} = \mathrm{ggT(a, c \cdot b)}$.

Zusatzaufgabe 6. (i) Berechnen Sie die kleinste natürliche Zahl n mit $\bar{4}^7 = \bar{n}$ in $\mathbb{Z}/13\mathbb{Z}$.

(ii) Berechnen Sie die kleinste natürliche Zahl n mit $\bar{6}^{21} = \bar{n}$ in $\mathbb{Z}/39\mathbb{Z}$.