Elementare Zahlentheorie (VU) – Sommersemester 2022

Endklausur – 28.6.2022

- Lösen Sie jede Aufgabe auf einem separaten Blatt (die erste Aufgabe können Sie am Deckblatt lösen).
- Schreiben Sie auf jedes Blatt Ihren Namen und Ihren Gruppenleiter!

Name: **Matrikelnr.:**

Gruppe: ☐ **1 (Smertnig, früh)** ☐ **2 (Fripertinger)** ☐ **3 (Smertnig, spät)** ☐ **4 (Fadinger)**

Pro Aufgabe sind **2 Punkte** zu erreichen. Viel Erfolg!

Aufgabe 1 (Kurzfragen) (a) (**1 P.**) Kreuzen Sie diejenigen Aussagen an, die für alle a, b, $c \in \mathbb{Z}$ gelten. (Ohne Beweis)

- ☐ $\mathrm{ggT}(a,b,c) = \mathrm{ggT}(a, \mathrm{ggT}(b,c))$.
- ☐ Aus $\mathrm{ggT}(a,b,c) = 1$ folgt $\mathrm{ggT}(a,b) = 1$.
- ☐ Aus $\mathrm{ggT}(a,b) = 1$ folgt $\mathrm{ggT}(a,b,c) = 1$.
- ☐ $\mathrm{ggT}(a,b)\,\mathrm{kgV}(a,b) = |ab|$.
- ☐ Ist $d = \mathrm{ggT}(a,b)$, so gilt $a \mid bc$ genau dann, wenn $a \mid dc$.

(*Ohne Beweis*)

(b) (**1 P.**) Bestimmen Sie

$$(\mathbb{Z}/15\mathbb{Z})^\times = \{\overline{1}, \qquad\qquad\qquad\qquad \}.$$

Aufgabe 2 (2 P.)
Bestimmen Sie die kleinste natürliche Zahl x, welche folgende Kongruenzen (gleichzeitig) erfüllt

$$x \equiv 2 \mod 10, \qquad x \equiv 3 \mod 13, \qquad x \equiv 1 \mod 17.$$

Aufgabe 3 (2 P.)
Seien $n \in \mathbb{N}$ und $p \in \mathbb{P}$ mit $n < p < 2n$. Beweisen Sie

$$\binom{2n}{n} \equiv 0 \mod p.$$

Für welche Primzahlen p gilt $\binom{2p}{p} \equiv 0 \mod p$?

Aufgabe 4 (2 P.)
Formulieren (**1 P.**) und beweisen (**1 P.**) Sie **einen** der folgenden beiden Sätze:

- Satz von Euler (definieren Sie dabei auch die Eulersche φ-Funktion);
- Lösbarkeit und Lösungsanzahl der linearen Kongruenz $aX \equiv b \mod m$ (mit a, $b \in \mathbb{Z}$, $m \in \mathbb{N}$).