AUSGEWÄHLTE KAPITEL DER ZAHLENTHEORIE
PROBEKLAUSUR 2

PROF. DR. HENNING KRAUSE
DR. JULIA SAUTER

Bitte benutzen Sie keinen Taschenrechner. Die Probeklausur ist auf 90 Minuten angelegt. Jede Aufgabe zählt 4 Punkte.

Aufgabe 1. Überprüfe, ob die folgenden Zahlen als Summe von zwei Quadraten geschrieben werden können und schreibe sie gegebenenfalls als Summe zweier Quadrate:
$16 \cdot 13, \quad 17 \cdot 18 \cdot 19.$

Aufgabe 2. Es sei $m = pq \in \mathbb{Z}$ mit p und q verschiedene Primzahlen. Zeige für jedes $a \in \mathbb{Z}$ mit Hilfe des chinesischen Restsatzes

$$\mathrm{ord}_m(a) = \mathrm{kgV}(\mathrm{ord}_p(a), \mathrm{ord}_q(a)).$$

Aufgabe 3. Ein Kollege möchte seine monatliches Gehalt geheim halten, deswegen wendet er die RSA-Verschlüsselung mit $m = 15$ und $d = 3$ auf die Zahlen $0, 1, \ldots, 10$ gesehen als Reste modulo 15 an.
Mit welcher Zahl muss man die Reste modulo 15 potenzieren, um zu entschlüsseln?
Sein Gehalt ist verschlüsselt als $8, 2, 1, 0$, wieviel verdient er?

Aufgabe 4. Überprüfe, ob die folgenden Zahlen als Summe von zwei Quadraten geschrieben werden können und schreibe sie gegebenenfalls als Summe zweier Quadrate:
$16 \cdot 13, \quad 17 \cdot 18 \cdot 19.$

Aufgabe 5. Berechne die folgenden Legendre-Symbole:
$\left(\frac{16}{101}\right), \quad \left(\frac{300}{277}\right)$

Aufgabe 6.

(1) Berechne $[20]_{17}^{100}$.
(2) Berechne $\mathrm{ord}_{13}(4)$. Ist 4 eine Primitivwurzel modulo 13?

Diese Probeklausur ist zur Wiederholung von Blatt 9-12 gedacht - relevant für die Klausur ist aber das gesamte bis dahin behandelte Material.