AUSGEWÄHLTE KAPITEL DER ZAHLENTHEORIE
10. ÜBUNGSBLATT

PROF. DR. HENNING KRAUSE
DR. JULIA SAUTER

Aufgabe 1. Es sei $m \in \mathbb{N}$. Finde für die folgenden Wahlen von m jeweils (mindestens) eine Restklasse $[x]_m$ mit $x^2 \equiv 2 \pmod{m}$.

$$(1)\ m = 7, \quad (2)\ m = 17, \quad (3)\ m = 7 \cdot 17, \quad (4)\ m = 7 \cdot 7$$

Hinweis: Bei (3) chin. Restsatz, bei (4) Satz von Hensel mit $f(x) = x^2 - 2$.

Aufgabe 2.

(1) Man sagt, dass es eine Primitivwurzel modulo m gibt, falls es einen primen Rest modulo m der Ordung $\varphi(m)$ gibt. Zeige, dass es keine Primitivwurzel modulo 12 gibt.
(2) Es sei p eine Primzahl und g eine Primitivwurzel modulo p. Zeige, dass
$$[g]_p, [g]_p^2, \ldots, [g]_p^{p-1}$$
paarweise verschieden sind. Folgere, dass dies alle primen Reste modulo p sind.

Aufgabe 3. Es sei p eine ungerade Primzahl. Zeige, dass kein quadratischer Rest modulo p eine Primitivwurzel modulo p ist.

Aufgabe 4.

(1) Finde die **2** verschiedenen quadratischen Reste modulo 15 mit dem chinesischen Restsatz. Überlege mit dem chinesichen Restsatz, dass es für $m = pq$ mit $p \neq q$ prim genau
$$(\frac{\mathbf{p-1}}{\mathbf{2}})(\frac{\mathbf{q-1}}{\mathbf{2}})$$
quadratische Reste modulo m gibt.

(2) Es seien $x, a, b \in \mathbb{Z}$. Zeige: Wenn
$$x \equiv a \pmod{3} \quad \text{und} \quad x \equiv b \pmod{5}$$
gilt, dann ist $\mathrm{ord}_{15}(x) = \mathrm{kgV}(\mathrm{ord}_3(a), \mathrm{ord}_5(b))$.
Folgere, dass es keine Primitivwurzeln modulo 15 gibt.

Abgabe: Freitag, 24. Juni 2016, bis 10.15 Uhr in der Vorlesung. Für jede Aufgabe gibt es 4 Punkte.