Einführung in die Zahlentheorie
Blatt 10

hhu Düsseldorf
WiSe 2021/22

Abgabe: bis Mittwoch 22.12.2021

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~khalupczok/EZ/`
Die folgenden Aufgaben sind schriftlich zu bearbeiten und abzugeben. Wie üblich sind dabei alle Behauptungen zu beweisen. Resultate aus der Vorlesung dürfen verwendet werden, die zugehörigen Referenznummern können Sie zur Klarstellung dann mit angeben.

Aufgabe 1 (3 Punkte):

(1) Es gibt unendlich viele Primzahlen p, so dass 10 quadratischer Rest mod p ist.

Hinweis: $N = (p_1 \cdots p_k A)^2 - 10$.

(2) Es gibt unendlich viele Primzahlen p, so dass die Periodenlänge der Dezimalbruchentwicklung von $\frac{1}{p}$ höchstens $\frac{p-1}{2}$ beträgt.

Aufgabe 2 (2 Punkte):

Ist g eine Primitivwurzel mod m, so gelten für den diskreten Logarithmus bezüglich g die folgenden Logarithmusgesetze. Seien $a, b \in \mathbb{Z}$, $(ab, m) = 1$, $k \in \mathbb{Z}$. Dann gilt

(1) $\operatorname{dlog}_g(ab) \equiv \operatorname{dlog}_g(a) + \operatorname{dlog}_g(b) \quad (\varphi(m))$,

(2) $\operatorname{dlog}_g(a^k) \equiv k \operatorname{dlog}_g(a) \quad (\varphi(m))$,

Aufgabe 3 (3 Punkte):

Sei $n \in \mathbb{N}$, $n > 2$ und seien $q_1 = 2 < q_2 < ... < q_k$ alle Primzahlen $\leq n$ und p eine Primzahl mit $p \equiv 1 \bmod 8q_2 \cdots q_k$. Dann ist jedes $a \leq n$ ein quadratischer Rest mod p.

Aufgabe 4 (5 Punkte):

Sei a quadratischer Rest mod p.

(1) Ist $p \equiv 3 \bmod 4$, so hat die Kongruenz $x^2 \equiv a \bmod p$ eine Lösung der Gestalt $x = a^n$. (Welche noch?)

(2) Ist $p \equiv 5 \bmod 8$, so hat die Kongruenz $x^2 \equiv a \bmod p$ eine Lösung der Gestalt $x = a^n$ oder $x = 2^m a^n$.

Aufgabe 5 (4 Punkte):

Für welche Primzahlen p ist 13 quadratischer Rest mod p?
(Man suche nach einer völlig korrekten und doch konzisen Form der Antwort.)

Aufgabe 6 (3 Punkte):

Für jede ungerade Primzahl p gilt $\displaystyle\sum_{k=1}^{p-2} \Big(\frac{k(k+1)}{p}\Big) = -1$.