# Elementare Zahlentheorie (Version 2): Übung 5

1. Sei $p \geq 3$ eine ungerade Primzahl. Wir wissen, daß alle Zahlen $1 \leq m \leq p-1$ Einheiten in $\mathbb{Z}_p$ sind. Sie bilden eine Gruppe unter Multiplikation. Es wird in der Vorlesung gezeigt, daß eine Primitivwurzel $g \in U(\mathbb{Z}_p)$ existiert: d.h.

   $$\{g, g^2, \ldots, g^{p-2}, g^{p-1} = 1\} = \{1, 2, \ldots, p-1\}.$$

   Können Sie zeigen, daß höchstens $\frac{p-1}{2}$ von diesen Zahlen Primitivwurzeln modulo $p$ sein können?

2. Sei $a \in \mathbb{N}$ eine Quadratzahl. D.h. $\exists b \in \mathbb{N}$ mit $b^2 = a$. Zeigen Sie, daß keine Primzahlen $p > a$ existieren, mit $a$ eine Primitivwurzel modulo $p$.

3. Fermat's kleiner Satz lautet: Sei $p \in \mathcal{P}$ eine Primzahl. Dann gilt

   $$a^{p-1} \equiv 1 \bmod p,$$

   für alle $a \in \mathbb{Z}_p \setminus \{0\}$. Andererseits ist dann eine Zahl $n \in \mathbb{N}$ sicherlich <u>nicht</u> prim, falls ein $1 < a < n$ existiert mit $a^{n-1} \not\equiv 1 \bmod n$.

   Nun, die sogenannten 'Fermatzahlen' sind die Zahlen der Art $f_m = 2^{2^m} + 1$, für alle $m \in \mathbb{N}$. Irrtümlicherweise behauptete Fermat, daß $f_m$ prim sei, für alle $m \in \mathbb{N}$. Was war sein Fehler? Vielleicht ist es ihm gelungen, zu zeigen, daß $2^{f_m - 1} \equiv 1 \bmod f_m$ für alle $m$. Können Sie die Richtigkeit dieser Gleichung auch bestätigen?

   Es gibt allerdings viele Fermatzahlen, die nicht prim sind.[1] Z.B.

   $$f_5 = 2^{2^5} + 1 = 4294967297 = 641 \times 6700417$$

   ist nicht prim, da $3^{f_5 - 1} \not\equiv 1 \bmod f_5$. Als 'freiwillige' Übung für diejenigen, die Lust am Rechnen haben: (ein Computer wäre sicherlich hilfreich hier)

   Was ist eigentlich die Zahl $3^{f_5 - 1} \bmod f_5$?

[1] Tatsächlich kennt niemand eine einzige prim Fermatzahl, die größer als $f_4$ ist!