Innermathematische Beziehungen
Zahlentheorie (Übung)

Prof. Dr. Markus Vogel
Fabian Grünig

Sommersemester 2018
Mittwoch, 14:00 Uhr, H009

Aufgabe 9 *(Geometrische Summenformel)*
Zeige mit vollständiger Induktion folgende Identität: Für alle Zahlen $q \in \mathbb{Q}$ mit $q \neq 0$ und $q \neq 1$ gilt

$$\sum_{k=0}^{n-1} q^k = \frac{q^n - 1}{q - 1}$$

Aufgabe 10 *(Mersenne-Primzahlen)*
Zur Erinnerung: Eine Primzahl $p \in \mathbb{N}$ heißt eine *Mersenne-Primzahl*, wenn sie die Gestalt

$$p = 2^n - 1,$$

für eine geeignete natürliche Zahl $n \in \mathbb{N}$ hat. Beispiele für Mersenne-Primzahlen sind

$$3 = 2^2 - 1, \quad 7 = 2^3 - 1, \quad 31 = 2^5 - 1, \quad 131071 = 2^{17} - 1.$$

Wir zeigen in dieser Übung, dass Mersenne-Zahlen zur Basis 2 die einzigen Kandidaten für Primzahlen dieser Gestalt liefern. Außerdem entwickeln wir notwendige Voraussetzungen für den Exponenten n von Mersenne-Primzahlen.

(i) Es sei $k \in \mathbb{N}$ eine natürliche Zahl $k \neq 0$ und $k \neq 1$. Zeige, dass die Zahl der Gestalt $2^{2k} - 1$ keine Primzahl ist.
Tipp: Verwende eine binomische Formel, um diese Zahl als Produkt zu schreiben.

(ii) Es seien $a \in \mathbb{Z}$ eine ganze Zahl und $n \in \mathbb{N}$ eine natürliche Zahl. Zeige, dass

$$(a^n - 1) = (a - 1) \cdot (a^{n-1} + a^{n-2} + \cdots + a^2 + a + 1).$$

(iii) Es seien $a \in \mathbb{Z}$ eine ganze Zahl und $n, k \in \mathbb{N}$ natürliche Zahlen. Zeige, dass

$$(a^{kn} - 1) = (a^k - 1) \cdot (a^{k(n-1)} + a^{k(n-2)} + \cdots + a^{2k} + a^k + 1).$$

(iv) Es seien $a \in \mathbb{N}$ und $n \in \mathbb{N}$, sodass $a^n - 1$ eine Primzahl ist. Zeige, dass dann notwendig auch n eine Primzahl sein muss.
Tipp: Zeige dies indirekt oder verwende ein Widerspruchsargument.

(v) Es sei $p \in \mathbb{N}$ eine Primzahl und $a \in \mathbb{N}$, sodass $a^p - 1$ eine Primzahl ist. Zeige, dass dann notwendig $a = 2$ gelten muss.

Wir haben insgesamt gezeigt, dass eine natürliche Zahl der Form $a^n - 1$ nur dann eine Primzahl sein kann, wenn sie *Mersenne*-Gestalt $2^p - 1$ hat, also $a = 2$ und p prim.