Aufgaben

Aufgabe 1. Es sei $n \in \mathbb{N}$ und $F_n = 2^{2^n} + 1$ (F_n heißt eine Fermat-Zahl).

a. Zeigen Sie, dass F_2, F_3 und F_4 Primzahlen sind, aber dass F_5 zerlegbar ist.

b. Zeigen Sie : Ist F_n eine Primzahl, dann gilt $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

c. Es sei jetzt $q \neq 3$ ein Primfaktor von F_n. Es sei d die Ordnung von 3 in $\mathbb{F}_q^\times$. Zeigen Sie : Gilt $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$, dann gilt $d = 2^{2^n}$.

d. Zeigen Sie, dass F_n genau dann eine Primzahl ist, wenn $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ ist (Pépin-Test).

Aufgabe 2. Eine natürliche Zahl n heißt a-Carmichael ($a \in \mathbb{N},\ a \geq 2$) wenn n keine Primzahl ist und $a^{n-1} \equiv 1 \pmod{n}$ ist. Es sei $p \neq 2$ eine Primzahl mit $p \nmid a(a^2-1)$, und es sei $n = (a^{2p}-1)/(a^2-1)$.
Zeigen Sie :

a. n ist keine Primzahl,

b. $a^{2p} \equiv 1 \pmod{n}$,

c. n ist a-Carmichael,

d. für jedes $a \geq 2$ existieren unendlich viele a-Carmichael Zahlen.

Aufgabe 3. Es sei n keine Primzahl und keine Carmichael-Zahl. Ein $a \in \mathbb{Z}$ heißt Fermat-Zeuge von n, wenn $a^{n-1} \not\equiv 1 \pmod{n}$ ist. Es sei :

$$F_n := \{\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times | a \text{ ist Fermat} - \text{Zeuge von } n\}.$$

Zeigen Sie :

$$|F_n| \geq \frac{1}{2}|(\mathbb{Z}/n\mathbb{Z})^\times|.$$

Aufgabe 4. Es sei $p \equiv 1 \bmod 4$ eine Primzahl. Machen Sie aus folgendem Argument (Zagier, 1990) einen ausführlichen Beweis des Satzes 10.3 der Vorlesung.
Die auf der endlichen Menge $S = \{(x,y,z) \in \mathbb{N}^3 | x^2 + 4yz = p\}$ durch

$$(x,y,z) \mapsto \begin{cases} (x+2z, z, y-x-z) \text{ falls } x < y-z \\ (2y-x, y, x-y+z) \text{ falls } y-z < x < 2y \\ (x-2y, x-y+z, y) \text{ falls } x > 2y \end{cases}$$

definierte Involution hat genau einen Fixpunkt, so dass $|S|$ ungerade ist ; daher hat aber auch die Involution $(x,y,z) \mapsto (x,z,y)$ einen Fixpunkt.

Die Blätter sollen bis Donnerstag, den 11.12. um 14.15 Uhr in die dafür vorgesehenen Einwurfkästen im Foyer des Mathematischen Instituts abgegeben werden.