Mathematisches Institut
der Universität München
Prof. Dr. O. Forster

SS 2017
5. Juli 2017

Einführung in die Zahlentheorie

Übungsblatt 10

Aufgabe 37

Sei p eine ungerade Primzahl und $D \in \mathbb{Z}$ mit $\left(\frac{D}{p}\right) = -1$.
Man beweise durch vollständige Induktion über $k \geqslant 1$: Die Gruppe

$$\mathrm{Pell}(\mathbb{Z}/p^k, D) = \left\{A = \begin{pmatrix} x & yD \\ y & x \end{pmatrix} \in \mathrm{M}(2 \times 2, \mathbb{Z}/p^k) : \det A = 1\right\}$$

ist zyklisch.

Aufgabe 38

Man zeige: Eine ungerade Zahl $N \geqslant 3$ ist genau dann prim, wenn folgende beiden Bedingungen erfüllt sind:

i) Für alle zu N teilerfremden Zahlen a gilt

$$a^{(N-1)/2} \equiv \pm 1 \bmod N.$$

ii) Es gibt mindestens eine ganze Zahl a mit

$$a^{(N-1)/2} \equiv -1 \bmod N.$$

Aufgabe 39

Sei $N \geqslant 3$ eine ganze Zahl. Es gebe eine Primzahl $q > \sqrt{N}$ und eine ganze Zahl a, so dass

$$a^q \equiv 1 \bmod N \quad \text{und} \quad \gcd(a-1, N) = 1.$$

Man beweise, dass N prim ist.

Aufgabe 40

Sei q eine ungerade Primzahl, so dass $p := 2q - 1$ ebenfalls prim ist und $N := pq$.
Man zeige: Die Untergruppe

$$G := \left\{a \in (\mathbb{Z}/N)^* : a^{(N-1)/2} = \left(\frac{a}{N}\right)\right\} \subset (\mathbb{Z}/N)^*$$

hat genau $\varphi(N)/4$ Elemente.