Universität Tübingen
Mathematisches Institut Tübingen, den 8.01.2008

Übungen zur Elementaren Zahlentheorie (11)

(41) Sei p eine ungerade Primzahl. Ist q die kleinste natürliche Zahl mit $(\frac{q}{p}) = -1$, so ist q eine Primzahl und $q < 1 + \sqrt{p}$.

(42) Sei p eine Primzahl mit $p \equiv 5 \,(\mathrm{mod}\, 8)$. Man zeige, dass es eine *ungerade* Primzahl $q < \sqrt{2p}$ gibt mit $(\frac{q}{p}) = -1$. (Bekanntlich gilt $p = a^2 + b^2$ mit $a, b \in \mathbb{N}$, und $a^2 - b^2$ ist ungerade mit $(\frac{a^2-b^2}{p}) = -1$.)

(43) Ist p eine Primzahl mit $p \equiv 7 \,(\mathrm{mod}\, 8)$, so gibt es eine natürliche Zahl a mit $a^2 < p < (a+1)^2$. Ist a gerade, so hat $p - a^2$ einen Primteiler $q \equiv 3 \,(\mathrm{mod}\, 4)$, und für diesen gilt $(\frac{q}{p}) = -1$ und $q < 2\sqrt{p} - 1$. Ist a ungerade, so hat $(p - a^2)/2$ einen Primteiler $q \equiv 3 \,(\mathrm{mod}\, 4)$, und für diesen gilt $(\frac{q}{p}) = -1$ und $q < \sqrt{p} - \frac{1}{2}$.

Anmerkung: Gauß hat (mit 19 Jahren) gezeigt, dass es zu einer Primzahl $p \equiv 1 \,(\mathrm{mod}\, 8)$ immer eine ungerade Primzahl $q < \sqrt{p}$ gibt mit $(\frac{q}{p}) = -1$ (*Disquisitiones arithmeticae*). Für $p \equiv 3 \,(\mathrm{mod}\, 8)$ gibt es solches $q < 1 + 2\sqrt{p}$, wie Nagell 1923 gezeigt hat.

(44) Ist $p \equiv 1 \,(\mathrm{mod}\, 4)$ eine Primzahl mit $p > 17$, so gibt es eine *ungerade* Primzahl $q < \sqrt{p}$ mit $(\frac{q}{p}) = 1$. (Man schreibe $p = a^2 + 4b^2$ mit $a, b \in \mathbb{N}$ und a ungerade und unterscheide die Fälle $a = 1$ und $a > 1$, b keine Potenz von 2, sowie $a > 1$, b ist Potenz von 2 (d.h., p ist Fermat-Primzahl).