Aufgabe 13.1. (KV)
Sei x, y, z ein primitives pythagoräisches Tripel. Zeige

(a) Genau eine der Zahlen x, y ist durch 3 teilbar. Genau eine der Zahlen x, y, z ist durch 5 teilbar.

Beweis: Die quadratischen Reste modulo 3 sind $\bar{0}$ und $\bar{1}$. Es muss $z \equiv 1$ sein, ansonsten wäre $x \equiv y \equiv 0$, was im Widerspruch zu $(x, y) = 1$ steht. Dann ist aber $x^2 \equiv 0$, $y^2 \equiv 1$, d.h. $x \equiv 0$ und $y \in \{\bar{1}, \bar{2}\}$ mod 3. Der andere Fall verläuft analog.
Die quadratischen Reste modulo 5 sind $\bar{0}$, $\bar{1}$ und $\bar{4}$. Ist $z \equiv 0$, so muss $x^2 \equiv 1$, $y^2 \equiv 4$ (bzw. umgekehrt) sein. In diesem Fall sind x und y nicht durch 5 teilbar. Für $x \equiv 0$ mod 5 folgt $y^2 \equiv z^2 \equiv 1$ oder $y^2 \equiv z^2 \equiv 4$, also sind y und z nicht durch 5 teilbar. Für $y \equiv 0$ mod 5 folgen analoge Überlegungen.

(b) Für jeden Primteiler p von z gilt $p \equiv 1$ mod 4

Beweis: Nach Satz 6.1.1(5) ist jeder Primteiler p von $n = x^2 + y^2$ mit $(x, y) = 1$, entweder gleich 2 oder $\equiv 1$ mod 4. Jetzt ist $n = z^2$ und wir haben $2^2 = 4 \,|\, z^2$ für $p = 2$. Daraus folgt, dass z^2 eine gerade Quadratzahl ist. Dies kann nicht stimmen. Also kann nur $p \equiv 1$ mod 4 gelten.

(c) Es ist $z \equiv 1$ mod 12 oder $z \equiv 5$ mod 12.

Beweis: Nach (a) wähle oBdA $x \equiv 0$ mod 3. Dann gilt $3 \nmid y$ und $\bar{y} \in \mathbb{N}_{12} \setminus \{3, 6, 9\}$. Hieraus ergibt sich schnell, dass $\bar{x}^2 \in \{0, 9\}$ und $\bar{y}^2 \in \{1, 4\}$. Folglich ist die Summe $\bar{x}^2 + \bar{y}^2$ in $\{1, 4, 10\}$.
Angenommen $\bar{z}^2 \equiv 4$, so folgt $\bar{z} \in \{2, 4, 8, 10\}$, d.h. z ist gerade. Aber dann muss entweder x und y gerade oder ungerade sein. Ersteres steht im Widerspruch zu $(x, y) = 1$ und letzteres würde zu $\bar{x}, \bar{y} \in \{1, 3\}$ und $\bar{z}^2 \equiv 2$ mod 4 führen. Gerade Quadratzahlen sind aber durch 4 teilbar! Analog zeigt man, dass $\bar{z}^2 \equiv 10$ nicht sein kann. Demnach gilt $\bar{z}^2 \equiv 1$ und $\bar{z} \in \{1, 5, 7, 11\}$. Für $\bar{7}$ und $\bar{11}$ erhält man mod 4 den Rest 3, d.h. z besitzt einen Primteiler p mit $p \equiv 3$ mod 4. Dies steht aber im Widerspruch zu Aufgabenteil (b).

(d) Ist x gerade, so sind $z - x$ und $\frac{1}{2}(z - y)$ Quadrate.

Beweis: x ist eine gerade Zahl und das gegebene Tripel $[x, y, z]$ ein Element der Menge

$$\{(x, y, z) \in \mathbb{N}^3 \mid z^2 = x^2 + y^2,\ (x, y) = 1,\ x \equiv 0 \bmod 2\}.$$

Wir gewinnen das Urbild $\eta^{-1}([x, y, z]) = [a, b] \in \mathbb{N}^2$ und haben somit ganze Zahlen a, b mit $x = 2ab$, $y = b^2 - a^2$ und $z = a^2 + b^2$. Damit lassen sich schnell die folgenden Rechnungen durchführen:

$$\tfrac{1}{2}(z - y) = \tfrac{1}{2}((a^2 + b^2) - (b^2 - a^2)) = a^2 \qquad z - x = (a^2 + b^2) - 2ab = (a - b)^2.$$

Aufgabe 13.2. (DH)
Zunächst zeigen wir die beiden Identitäten. Sei $g \in \mathbb{N}$ gerade, so gilt

$$g^2 + \left(\frac{g^2}{4} - 1\right)^2 = g^2 + \left(\frac{g^2}{4}\right)^2 - \frac{1}{2}g^2 + 1 = \left(\frac{g^2}{4}\right)^2 + \frac{1}{2}g^2 + 1 = \underbrace{\left(\frac{g^2}{4} + 1\right)^2}_{\in \mathbb{N}}$$

und ist $u \in \mathbb{N}$ ungerade, so gilt

$$u^2 + \left(\frac{u^2 - 1}{2}\right)^2 = u^2 + \left(\frac{u^2}{2}\right)^2 - \frac{1}{2}u^2 + \left(\frac{1}{2}\right)^2 = \left(\frac{u^2}{2}\right)^2 + \frac{1}{2}u^2 + \left(\frac{1}{2}\right)^2 = \underbrace{\left(\frac{u^2 + 1}{2}\right)^2}_{\in \mathbb{N}}.$$

Damit erhalten wir also durch entsprechende Wahl von g bzw. u pythagoräische Tripel. Allerdings erhält man auf diese Weise nicht alle pythagoräischen Tripel, denn es gelten

$$\left(\frac{u^2 + 1}{2}\right) - \left(\frac{u^2 - 1}{2}\right) = 1$$
$$\left(\frac{g^2}{4} + 1\right) - \left(\frac{g^2}{4} - 1\right) = 2$$

und somit erhält man nur Lösungen für $a^2 + b^2 = c^2$ mit $c = b + 1$ bzw. $c = b + 2$. Lösungen, die nicht von dieser Form sind, sind zum Beispiel $(20, 21, 29)$ und $(28, 45, 53)$.

Aufgabe 13.3. (AB)

(a) Ist p Primzahl mit $p \equiv 3 \,(\mathrm{mod}\, 4)$, so gibt es kein Paar $x, y \in \mathbb{Z}^2$ mit $x^2 - py^2 = -1$.

Beweis: Sei also p Primzahl mit $p \equiv 3 \,(\mathrm{mod}\, 4)$. Es gilt $x^2 - py^2 = -1 \Leftrightarrow x^2 + 1 = py^2$ und für alle $y \in \mathbb{Z}$ ist $\omega_p(py^2) = 2\omega_p(y) + 1$ ungerade. Wegen $p \equiv 3 \,(\mathrm{mod}\, 4)$ kann py^2 also nicht als Summer zweier Quadrate ganzer Zahlen geschrieben werden, insbesondere nicht in der Form $py^2 = x^2 + 1$ mit $x \in \mathbb{Z}$.

(b) Sei $p > 2$ Primzahl. Zeige: Die kleinste natürliche Zahl q mit $\left(\frac{q}{p}\right) = -1$ ist eine Primzahl.

Beweis: Sei also $p > 2$ Primzahl und sei q die kleinste natürliche Zahl mit $\left(\frac{q}{p}\right) = -1$. Offensichlich gilt dann $q > 1$, denn 1 ist immer quadratischer Rest. Also besitzt q eine Primfaktorzerlegung $q = p_1^{e_1} \cdot \dots \cdot p_t^{e_t}$ mit $t \geq 1$. Weiterhin gilt $\left(\frac{q}{p}\right) = \left(\frac{p_1}{p}\right)^{e_1} \cdot \dots \cdot \left(\frac{p_t}{p}\right)^{e_t} = -1$, d.h. für mindestens ein $i \in \{1, \dots, t\}$ gilt $\left(\frac{p_i}{p}\right) = -1$. Da q aber die kleinste natürliche Zahl mit $\left(\frac{q}{p}\right) = -1$ ist, muss $q = p_i$ gelten.

Aufgabe 13.3. Ford'sche Kreise. (AB)
Ist $\frac{p}{q}$ ein gekürzter Bruch, so sei $K\left(\frac{p}{q}\right)$ der Kreis in der Ebene $\mathbb{R}^2$ mit Mittelpunkt $\left[\frac{p}{q}, \frac{1}{2q^2}\right]$ und Radius $\frac{1}{2q^2}$.

(a) Zeige: Sind $0 \leq \frac{a}{b} < \frac{c}{d} \leq 1$ gekürzte Brüche, so haben die Kreise $K\left(\frac{a}{b}\right)$ und $K\left(\frac{c}{d}\right)$ nie innere Punkte gemeinsam. Sie berühren sich genau dann, wenn $cb - ad = 1$ gilt.

Beweis: Die Mittelpunkte der beiden Kreise haben Abstand $d = \sqrt{(\frac{c}{d} - \frac{a}{b})^2 + (\frac{1}{2d^2} - \frac{1}{2b^2})^2}$ und die Summe ihrer Radien beträgt $s = \frac{1}{2d^2} + \frac{1}{2b^2}$. Es können drei Fälle auftreten:

(1) $d > s$: Die Kreise haben keine gemeinsamen Punkte.
(2) $d = s$: Die Kreise berühren sich und haben genau einen gemeinsamen Punkt.
(3) $d < s$: Die Kreise haben gemeinsame innere Punkte.

Wegen $(\frac{c}{d} - \frac{a}{b})^2 + (\frac{1}{2d^2} - \frac{1}{2b^2})^2 \geq 0$ genügt es, d^2 und s^2 zu vergleichen, betrachte also $d^2 - s^2$:

$$\begin{aligned} d^2 - s^2 &= \left(\frac{c}{d} - \frac{a}{b}\right)^2 + \left(\frac{1}{2d^2} - \frac{1}{2b^2}\right)^2 - \left(\frac{1}{2d^2} + \frac{1}{2b^2}\right)^2 \\ &= \left(\frac{bc - ad}{bd}\right)^2 + \left(\frac{b^2 - d^2}{2b^2d^2}\right)^2 - \left(\frac{b^2 + d^2}{2b^2d^2}\right)^2 \\ &= \left(\frac{bc - ad}{bd}\right)^2 - \frac{4b^2d^2}{4b^4d^4} \qquad \left(\begin{array}{l}\text{die quadratischen Terme der letzten} \\ \text{beiden Summanden heben sich weg}\end{array}\right) \\ &= \frac{(bc - ad)^2 - 1}{b^2d^2} \end{aligned}$$

Da $a, c \in \mathbb{Z}$ und $b, d \in \mathbb{N}$ gilt wegen $\frac{a}{b} < \frac{c}{d}$ auch $ad < bc$ und damit $bc - ad \geq 1$. Fall (3) tritt also nie auf und Fall (2) genau dann, wenn $bc - ad = 1$ gilt.

(b) Interpretiere die folgende Skizze und zeichne die Ford'schen Kreise für alle gekürzten Brüche $\frac{p}{q}$ mit $0 \leq p \leq q \leq 5$.

Interpretation: Gilt für die gekürzten Brüche $\frac{a}{b} < \frac{c}{d}$ die Bedingung $bc - ad = 1$, sind $\frac{a}{b} < \frac{c}{d}$ also Farey-Nachbarn, dann gilt dies ebenso für $\frac{a}{b} < \frac{a+c}{b+d}$ und $\frac{a+c}{b+d} < \frac{c}{d}$. Weiterhin ist die Zahl $\frac{a+c}{b+d}$ die einzige, die diese beiden Bedingungen erfüllt.

Skizze: