Elliptische Kurven & Kryptologie Serie 8

Kongruente Zahlen Abgabe: 28. April

Eine positive natürliche Zahl n heisst ***kongruente Zahl*** falls es positive rationale Zahlen X, Y, Z gibt für die gilt:

$$X^2 + Y^2 = Z^2 \quad \text{und} \quad \tfrac{1}{2}XY = n$$

Mit anderen Worten, n ist eine kongruente Zahl falls n der Flächeninhalt eines rechtwinkligen Dreiecks mit rationalen Seiten ist.

1. Zeige, dass 6 eine kongruente Zahl ist und finde mit der Formel für pythagoräische Tripel zwei weitere kongruente Zahlen.

2. Sei $n > 0$ eine natürliche Zahl und seien X, Y, Z, x rationale Zahlen mit $X < Y < Z$. Zeige, dass die folgende Abbildung $(X, Y, Z) \leftrightarrow x$ eine Bijektion definiert zwischen den rechtwinkligen Dreiecken mit Seitenlängen X, Y, Z und Flächeninhalt n, und den rationalen Zahlen x, so dass $x, x+n, x-n$ alles quadrate rationaler Zahlen sind:

$$(X, Y, Z) \;\mapsto\; x = \left(\frac{Z}{2}\right)^2$$

$$x \;\mapsto\; X = \sqrt{x+n} - \sqrt{x-n}\,, \quad Y = \sqrt{x+n} + \sqrt{x-n}\,, \quad Z = 2\sqrt{x}$$

3. Sei n eine positive natürliche Zahl. Definiere:

$$K_n := \{(X, Y, Z) \in \mathbb{Q}^3 \mid X, Y, Z > 0,\ X^2 + Y^2 = Z^2,\ \tfrac{1}{2}XY = n\}$$

Des weiteren soll die Kurve C_n wie folgt definiert sein:

$$C_n : y^2 = x^3 - n^2 x$$

Es sei V_n die Menge aller rationalen Punkte auf C_n im ersten Quadranten von $\mathbb{Q}^2$:

$$V_n := C_n(\mathbb{Q}) \cap \{(x, y) \in \mathbb{Q}^2 \mid x, y > 0\}$$

(a) Zeige, dass die folgenden Zuordnungen eine Bijektion zwischen den Mengen K_n und V_n realisieren:

$$(X, Y, Z) \;\mapsto\; (x, y) = \left(\frac{n(X+Z)}{Y},\ \frac{2n^2(X+Z)}{Y^2}\right)$$

$$(x, y) \;\mapsto\; (X, Y, Z) = \left(\frac{x^2 - n^2}{y},\ \frac{2nx}{y},\ \frac{x^2 + n^2}{y}\right)$$

(b) Folgere: n ist genau dann eine kongruente Zahl wenn $V_n \neq \varnothing$ gilt.

(c) Sei n eine quadratfreie kongruente Zahl und sei $(X, Y, Z) \in K_n$, so dass (kX, kY, kZ) ein primitives pythagoräisches Zahlentripel ist, wobei k das kgV der Nenner von X, Y und Z bezeichnet. Leite aus den Gleichungen $(X \pm Y)^2 = Z^2 \pm 4n$ die folgende Gleichung her:

$$\left(\frac{X^2 - Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 - n^2$$

Beweise mit Hilfe dieser Gleichung, dass ein Punkt $(x, y) \in V_n$ existiert, welcher

$$x = \left(\frac{p}{2q}\right)^2$$

erfüllt, das heisst, x ist das Quadrat einer rationalen Zahl mit geradem Nenner. *Hinweis*: Benutze die Aufgabe 2.

4. (a) Ist $P = (x, y) \in V_n$, so tritt für $2P = (x', y')$ genau einer der folgenden Fälle ein:

$$2P \in V_n, \qquad -2P \in V_n, \qquad y' = 0$$

Hinweis: Die Menge V_n wird in Aufgabe 3 definiert.

(b) Finde zu einer kongruenten Zahl n (*z.B.* $n = 6$ oder $n = 7$ (Maple)) mindestens zwei rechtwinklige Dreiecke mit rationalen Seiten der Fläche n.