Elliptische Kurven und Kryptographie

Serie 8

27. Seien k, l, m, n positive ganze Zahlen, so dass gilt

$$m^2 = n^2 + nl + l^2 \quad \text{und} \quad k = n + l\,.$$

Zeige, dass dann folgende Aussagen gelten:

(a) $m^2 = n^2 - kn + k^2$

(b) $\big(2mn, m^2 - n^2, m^2 + n^2\big)$, $\big(2ml, m^2 - l^2, m^2 + l^2\big)$, $\big(2km, k^2 - m^2, k^2 + m^2\big)$ sind ganzzahlige pythagoräische Tripel.

(c) $A := klmn$ ist eine kongruente Zahl.

(d) Die Kurve $y^2 = x^3 - A^2x$ besitzt drei ganzzahlige Punkte (x, y) mit $y > 0$ die auf einer Geraden liegen.

Beweis:

(a) Es gilt $n^2 - kn + k^2 = n^2 - (n + l)n + n^2 + 2nl + l^2 = n^2 + nl + l^2 = m^2$.

(b) Die Einträge sind offensichtlich alle ganzzahlig. Ausserdem gilt $(m^2 - n^2)^2 + (mn)^2 = (m^2 + n^2)^2$ und analog für die anderen beiden Tripel.

(c) Bei $A := klmn$ handelt es sich gerade um die Fläche der Dreiecke in (b), denn $m^2 - n^2 = nl + l^2 = kl$ und analog für die anderen beiden Tripel.

(d) Wir ordnen einem Tripel (a, b, c) den Punkt mit den folgenden Koordinaten zu:

$$x = \frac{A(b + c)}{a} = \frac{b(b + c)}{2}, \quad y = \frac{2A^2(b + c)}{a^2} = \frac{b^2(b + c)}{2}\,.$$

Somit erhalten wir $P_{mn} = (x_{mn}, y_{mn}) = \big((m^2 - n^2)m^2, (m^2 - n^2)^2 m^2\big)$ und analog für $P_{ml} = (x_{ml}, y_{ml})$ sowie $P_{km} = (x_{km}, y_{km})$. Nun lässt sich zeigen, dass

$$\frac{y_{mn} - y_{ml}}{x_{mn} - x_{ml}} = 2m^2 - l^2 - n^2 = n^2 + 2nl + l^2 = k^2 \quad \text{und} \quad \frac{y_{km} - y_{ml}}{x_{km} - x_{ml}} - k^2 = \ldots = 0\,.$$

Daraus folgt, dass die Punkte auf einer Gerade liegen.

28. Finde drei ganzzahlige Punkte (x, y) mit $y > 0$ auf der Kurve $y^2 = x^3 - 840^2x$ die auf einer Geraden liegen.

Hinweis: $m = 7$

Lösung:

Mit dem Hinweis und durch Ausprobieren findet man $l = 3$ sowie $n = 5$ und somit $k = 8$. Wie gewünscht gilt dann auch $klmn = 840$.

Wir erhalten also die Punkte

$$P_{mn} = (1176, 28\,224), \quad P_{ml} = (1960, 78\,400) \quad \text{und} \quad P_{km} = (960, 14\,400).$$