Elliptische Kurven und Kryptographie

Serie 9

29. Seien k, l, m, n paarweise teilerfremde positive ganze Zahlen mit m quadratfrei, so dass gilt

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

Zeige: Der Rang der elliptischen Kurve $y^2 = x^3 - (klmn)^2 \cdot x$ ist mindestens zwei.

Hinweis: Es gilt der folgende zahlentheoretische Satz:

Sind u, v, w positive natürliche Zahlen und ist $w^2 = u^4 \pm u^2v^2 + v^4$, so ist $w^2 = 1$.

Daraus folgt, dass höchstens eine der Zahlen k, l, n eine Quadratzahl ist.

Beweis:

Wir bezeichnen $A := klmn$, $C_A\colon y^2 = x^3 - A^2 \cdot x$, $\Gamma := C_A(\mathbb{Q})$ und gehen wie folgt vor: Es genügt zu zeigen, dass $\#\alpha(\Gamma) > 8$, denn aus

$$2^r = \frac{\#\alpha(\Gamma)\,\#\overline{\alpha}(\overline{\Gamma})}{4}$$

folgt dann $r > 1$, also $r \geq 2$. In Kapitel 7 haben wir α wie folgt definiert:

$$\alpha\colon \Gamma \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2,\quad \left.\begin{array}{rcl} \mathscr{O} & \mapsto & 1 \\ (0,0) & \mapsto & -A \\ (x,y) & \mapsto & x \end{array}\right\} \mod (\mathbb{Q}^\times)^2$$

Wir betrachten nun ganzzahlige Pythagoräische Zahlentripel, die zugehörigen Punkte auf Γ und deren Bilder unter α. Wir beginnen mit $\big(a_1, b_1, c_1\big) = \big(2mn, m^2 - n^2, m^2 + n^2\big)$ und erhalten

$$x_1 = x_{mn} = (m^2 - n^2)m^2 = klm^2 \equiv kl \in \alpha[\Gamma]$$

sowie analog $x_2 := x_{ml} \equiv kn$ und $x_3 := x_{km} \equiv ln$. Definiere ausserdem $\big(a_4, b_4, c_4\big) = \big(b_1, a_1, c_1\big)$ usw. und erhalte $x_4 = m(m+n)^2n \equiv mn$, $x_5 \equiv lm$ und $x_6 \equiv km$. Für $j = 1, \ldots, 6$ seien schliesslich $\big(a_{j+6}, b_{j+6}, c_{j+6}\big) = \big(a_j, b_j, -c_j\big)$, was uns $x_{j+6} \equiv -x_j$ liefert.

Da nun schlimmstenfalls eine der Zahlen k, l, n eine Quadratzahl ist, sei (ohne Einschränkung) $k \in (\mathbb{Q}^\times)^2$. Dann gilt $\{\pm l, \pm lm, \pm ln, \pm m, \pm mn, \pm n\} \subseteq \alpha[\Gamma]$, also $\#\alpha[\Gamma] \geq 12 > 8$, was zu zeigen war.