Elliptische Kurven und Kryptographie

Serie 9

der Rang von $y^2 = x^3 - (klmn)^2 \cdot x$ Besprechung am 28. November

---

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.