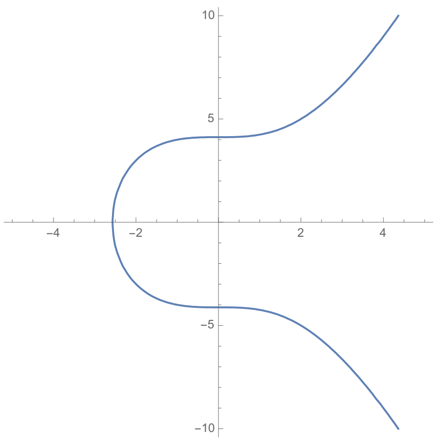
Elliptische Kurven und Kryptographie

Serie 7

Rechnen auf elliptischen Kurven | Besprechung am 14. November

---

23. Gegeben sei die elliptische Kurve $y^2 = x^3 + 17$



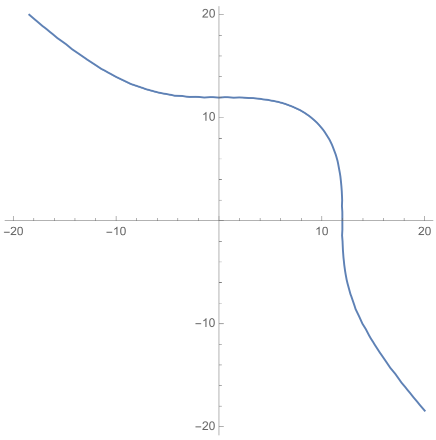
mit den ganzzahligen Punkten $\pm P = (-2, \pm 3)$, $\pm Q = (2, \pm 5)$, $\pm R = (-1, \pm 4)$.

(a) Berechne $-P + Q$ und $Q + R$.

(b) Verifiziere $(-P + Q) + R = -P + (Q + R)$.

24. Die sogenannte *Taxicab*-Kurve, mit den ganzzahligen Punkten $(1, 12)$ und $(9, 10)$, ist gegeben durch

$$x^3 + y^3 = 1729\,.$$



Finde zwei rationale Zahlen $x, y \in \mathbb{Q} \setminus \mathbb{Z}$, so dass gilt $x^3 + y^3 = 1729$.

25. Die elliptische Kurve $y^2 = x^3 - 49x$ besitzt den ganzzahligen Punkt $(25, 120)$. Finde zwei rationale pythagoräische Tripel $(a, b, c) \in \mathbb{Q}^3$ mit $a < b$, so dass gilt

$$a^2 + b^2 = c^2 \quad \text{und} \quad \frac{ab}{2} = 7\,.$$

26. *Beispiele für Kurven mit Punkten endlicher Ordnung.*

(a) Zeige: Die Kurve

$$C_3 : y^2 = x^3 + (m^2 - 3x_0)x^2 + (2md + 3x_0^2)x + (d^2 - x_0^3)$$

hat bei $(x_0, mx_0 + d)$ einen Punkt der Ordnung 3.

(b) Zeige: Für $m^2 = 2x_0 + a$ und $b = x_0^2$, wobei $x_0 > 0$, hat die Kurve

$$C_4 : y^2 = x^3 + ax^2 + bx$$

bei (x_0, mx_0) einen Punkt der Ordnung 4.

(c) Zeige: Die Kurve

$$C_5 : y^2 = x^3 - 4u^2x^2 + (4u^3)^2$$

hat bei $(0, 4u^3)$ einen Punkt der Ordnung 5.