Elliptische Kurven und Kryptographie

Serie 7

Rechnen auf elliptischen Kurven — Musterlösungen

---

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

Lösung:

(a) Da es sich um eine Kurve in WNF handelt, können wir die Formel aus der Vorlesung verwenden. Wir berechnen die Parameter der Gerade $y = \lambda x + \nu$ durch $-P$ und Q:

$$\lambda = \frac{5 - (-2)}{2 - (-2)} = \frac{8}{4} = 2, \quad 5 = 2 \cdot 2 + \nu \implies \nu = 1.$$

Dann erhalten wir

$$-P + Q = (\lambda^2 - (a + x_0 + x_1), -(\lambda x_2 + \nu)) = (4 - (0 - 2 + 2), -2x_2 - 1) = (4, -9).$$

Analog erhalten wir für die Gerade $y = \lambda x + \nu$ durch Q und R, dass $\lambda = \frac{1}{3}$ und $\nu = \frac{13}{3}$ sowie

$$Q + R = \left(\frac{1}{9} - 2 + 1, -\frac{1}{3}x_2 - \frac{13}{3}\right) = \left(-\frac{8}{9}, -\frac{109}{27}\right).$$

(b) Wir erhalten $\lambda = -\frac{13}{5}$ und $\nu = \frac{7}{5}$ sowie

$$(-P + Q) + R = \left(\frac{169}{25} - 4 + 1, -\frac{13}{5}x_2 + \frac{7}{5}\right) = \left(\frac{94}{25}, -\frac{1047}{125}\right),$$

bzw. $\lambda = -\frac{14}{15}$ und $\nu = -\frac{73}{15}$ sowie

$$-P + (Q + R) = \left(\frac{196}{225} + 2 + \frac{8}{9}, -\frac{14}{15}x_2 - \frac{73}{15}\right) = \left(\frac{94}{25}, -\frac{1047}{125}\right).$$

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

Lösung:

Wir berechnen $(1,12) \# (9,10)$. Die beiden Punkte liegen auf der Geraden $x = 49 - 4y$. Eingesetzt in die Kurvengleichung erhalten wir

$$-63y^3 + 2352y^2 - 28\,812y + 115\,920 = 0.$$

Weiter wissen wir, dass das linke Polynom durch $(y-12)$ und $(y-10)$ teilbar ist. Das Resultat nach Polynomdivision ist ausserdem durch -21 teilbar und wir erhalten $3y - 46 = 0$, was uns $y = \frac{46}{3}$ und $x = -\frac{37}{3}$ liefert.

25. Die elliptische Kurve $y^2 = x^3 - 49x$ besitzt den ganzzahligen Punkt $P = (25, 120)$.

Finde zwei rationale pythagoräische Tripel $(a, b, c) \in \mathbb{Q}^3$ mit $0 < a < b < c$, so dass gilt

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

Lösung:

Der Punkt $P = (x_0, y_0) = (25, 120)$ liefert folgendes pythagoräische Tripel:

$$a = \frac{2\,n\,x}{y} = \frac{35}{12}\,, \quad b = \frac{(x^2 - n^2)}{y} = \frac{24}{5} \quad \text{und} \quad c = \frac{(x^2 + n^2)}{y} = \frac{337}{60}\,.$$

Addiert man einen der Punkte $(\pm 7, 0)$ oder $(0, 0)$ zu P, so erhält man bloss äquivalente Tripel. Wir berechnen also $2P$.

Die Tangente an C in P ist von der Form $\alpha x + \beta y + \gamma = 0$ mit $\alpha = 3x_0^2 - 49 = 1826$ und $\beta = -2y_0 = -240$. Somit ist die Steigung λ und den y-Achsen-Abschnitt ν:

$$\lambda = -\frac{\alpha}{\beta} = \frac{1826}{240} = \frac{913}{120}, \quad \nu = y_0 - \lambda x_0 = -\frac{1685}{24}\,.$$

Damit erhalten wir

$$2Q = (\lambda^2 - (a + 2x_0), -(\lambda x_0 + \nu)) = \left(\frac{113\,569}{120^2}, -\frac{17\,631\,503}{120^3}\right)$$

und schliesslich

$$a = \frac{52\,319}{40\,440}, \quad b = \frac{566\,160}{52\,319}\,.$$

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

(a) Zeige: Die Kurve

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

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

$$C_4 \colon y^2 = x^3 + ax^2 + bx$$

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

(c) Zeige: Die Kurve

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

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

Beweis:

(a) Wir verdoppeln (mit der üblichen Methode) den Punkt und erhalten $P \# P = P$ bzw. $P + P = (x_0, -y_0) = -P$. Somit wissen wir, dass P von der Ordnung 3 ist.

(b) Wir verdoppeln P und erhalten $(0, 0)$, was die Ordnung 2 besitzt. Somit ist P selbst ein Punkt der Ordnung 4.

(c) Wir verdoppeln P und erhalten $2P = (4u^2, -4u^3)$. Danach können wir entweder $2P$ noch einmal verdoppeln oder $P + 2P$ berechnen. Im ersten Fall erhalten wir $4P = (0, -4u^3) = -P$, im zweiten $3P = (4u^2, 4u^3) = -2P$.