Cryptologie 3

Aufgabenblatt 3, 2017-05-15

Aufgabe 1 [8 PUNKTE]

(a) [2 PUNKTE] Welche der beiden folgenden gegebenen Gleichungen beschreibt eine elliptische Kurve über den rationalen Zahlen $\boldsymbol{Q}$? Begründen Sie ihre Antwort!

$$y^2 = x^3 - 43x + 166 \qquad y^2 = x^3 - 3x + 2$$

(b) [2 PUNKTE] Gegeben ist der Punkt $P_1 = (3, 8)$, der auf einer der beiden Kurven aus (a) liegt. Bestimmen Sie einen weiteren Punkt P_2 der Kurve als Schnittpunkt der Tangente in P_1 mit der Kurve.

(c) [2 PUNKTE] Bestimmen Sie die Summen $P_1 + P_2$ und $P_1 - P_2$ in $E(\boldsymbol{Q})$.

(d) [2 PUNKTE] Beweisen Sie, dass ein Polynom $x^3 + ax + b$ keine mehrfache Nullstelle besitzt, falls die Diskriminante $\Delta = 4a^3 + 27b^2 \neq 0$ ist.

Lösungsvorschlag:

(a) Nachzuprüfen ist, ob der Wert der Diskriminante von 0 verschieden ist:

$$\Delta_0 = 4(-43)^3 + 27(166)^2 = 425984 \neq 0 \quad \text{und} \quad \Delta_1 = 4(-3^3) + 27(2^2) = 0$$

Damit beschreibt die erste Gleichung eine elliptische Kurve, die zweite hingegen nicht.

(b) $P_1 = (3, 8)$ erfüllt die erste Gleichung. Wegen $y_1 = 8 \neq 0$ ist die Kurvengleichung nach x zu differenzieren:

$$2yy' = 3x^2 - 43$$

Einsetzen von P_1 liefert

$$16y' = 27 - 43 = -16 \quad \text{also} \quad y' = -1$$

Mit dieser Steigung ergibt sich die Tangente im Punkt P_1 zu

$$y = -x + 11$$

Einsetzen in die Kurvengleichung liefert

$$0 = x^3 - 43x + 166 - (-x + 11)^2 = x^3 - x^2 - 21x + 45 = (x - 3)^2(x + 5)$$

woraus man den Schnittpunkt der Tangente in P_1 mit der Kurve als $P_2 = (-5, 16)$ bestimmt.

(c) Für die beiden Punkte P_1 und P_2 der Tangentenmethode gilt in $\boldsymbol{E}(K)$

$$P_1 + P_1 + P_2 = O \quad \text{bzw.} \quad P_1 + P_2 = -P_1 = (3, -8)$$

Um $P_1 - P_2 = (3, 8) + (-5, -16)$ zu bestimmen, verwenden wir die Sekantenmethode: wegen $x_1 \neq x_2$ erhalten wir die Sekantengleichung

$$y = \frac{8+16}{3+5}(x+5) - 16 = 3x - 1$$

Einsetzen in die Kurvengleichung liefert

$$0 = x^3 - 43x + 166 - (3x-1)^2 = x^3 - 9x^2 - 37x + 165 = (x-3)(x+5)(x-11)$$

Damit haben wir als Schnittpunkt der Sekante mit der Kurve den Punkt $P_3 = (11, 32)$ gefunden, woraus $P_1 - P_2 = -P_3 = (11, -32)$ folgt.

(d) Wir argumentieren indirekt: Aus

$$(x-u)^2(x-v) = x^3 - (2u+v)x^2 + (u^2 + 2uv)x - u^2 v = x^3 + ax + b$$

folgt unmittelbar

$$v = -2u \quad , \quad a = -3u^2 \quad \text{und} \quad b = 2u^3$$

Dann erhält man die Diskriminante $\Delta = 4a^3 + 27b^2 = -108u^6 + 108u^6 = 0$. Ist dagegen die Diskriminante von 0 verschieden, kann die Kurve keine doppelte Nullstelle haben.

Aufgabe 2 [10 PUNKTE]

Betrachten Sie den Ring $\boldsymbol{G}$ der ganzen Gauß'schen Zahlen.

(a) [4 PUNKTE] Berechnen Sie $\text{ggT}\,(18 - 4i, 3 + 15i)$.

(b) [6 PUNKTE] Analog zu $\mathbb{Z}_n$ als Menge der Restklassen modulo einer natürlichen Zahl n lässt sich die Menge $\boldsymbol{G}_c$ der Restklassen modulo einer ganzen Gauß'schen Zahl $c = a + bi$ definieren.

Beweisen Sie: Falls $|\,\text{ggT}(x + yi, c)| = 1$ dann existiert ein Inverses von $x + yi$ modulo c .

Berechnen Sie das Inverse von $2 + 5i$ modulo $5 + 5i$.

Lösungsvorschlag:

(a) Statt $a + ib$ schreiben wir $\langle a, b \rangle$.

Algorithmus 13.1 liefert

$$\begin{aligned}
g_0 &= \langle 18, -4 \rangle \\
g_1 &= \langle 3, 15 \rangle \\
g_2 &= \langle 18, -4 \rangle - \langle 3, 15 \rangle \langle 0, -1 \rangle = \langle 3, -1 \rangle \\
g_3 &= \langle 3, 15 \rangle - \langle 3, -1 \rangle \langle -1, 5 \rangle = \langle 1, -1 \rangle \\
g_4 &= \langle 3, -1 \rangle - \langle 1, -1 \rangle \langle 2, 1 \rangle = 0
\end{aligned}$$

Folglich gilt $\text{ggT}(\langle 18, -4 \rangle, \langle 3, 15 \rangle) = \langle 1, -1 \rangle$.

Wir können das Verfahren aber auch in derselbem Schema aufschreiben, das uns vom Euklidischen Algorithmus her bekannt ist:

$$\begin{array}{rcrcrcr}
\langle 18, -4 \rangle & = & \langle 0, -1 \rangle & \cdot & \langle 3, 15 \rangle & + & \langle 3, -1 \rangle \\
\langle 3, 15 \rangle & = & \langle -1, 5 \rangle & \cdot & \langle 3, -1 \rangle & + & \langle 1, -1 \rangle \\
\langle 3, -1 \rangle & = & \langle 2, 1 \rangle & \cdot & \langle 1, -1 \rangle & + & \langle 0, 0 \rangle
\end{array}$$

(b) Vorüberlegung: Für $c = \langle a, b\rangle \in G$ erhält man eine kanonische Menge K_c von Repräsentanten für G_c, indem man das von $\langle |a|, -|b|\rangle$ und $i \cdot \langle |a|, -|b|\rangle = \langle |b|, |a|\rangle$ aufgespannte Quadrat betrachtet, wobei die Randpunkte zwischen $\langle |a|, -|b|\rangle$ bzw. $\langle |b|, |a|\rangle$ und der Summe dieser Punkte einschließlich zu entfernen sind. Ganz G läßt sich mit Parallelverschiebungen dieses Quadrats überdecken ("pflastern").

Die Abbildung $G \xrightarrow{\bmod \langle a,b\rangle} K$ bildet nun Elemente von G auf die entsprechenden Punkte in K_c gemäß dieser Pflasterung ab. Man beachte, dass für vier sich nur um ± 1 bzw. $\pm i$ unterscheidende Punkte dasselbe K verwendet wird, damit die Einheiten $\langle 0, 0\rangle$ sowie $\langle 1, 0\rangle$ bzgl. Addition und Multiplikation in G in der Repräsentantenmenge K enthalten sind (andernfalls hätte man ungewöhnliche multiplikative Einheiten in der Repräsentantenmenge).

In jedem *Hauptidealring*, d.h., in jedem kommutativen nullteilerfreien Ring, in dem Jedes Ideal ein Hauptideal ist, läßt sich der ggT immer als Linearkombination der Argumente darstellen (Lemma von Bezout).

Ist der Ring sogar *Euklidisch*, d.h., läßt sich eine *Division mit Rest* definieren, so kann man diese zur Bestimmung des ggT verwenden, mittels des *Euklidischen Algorithmus*.

Gemäß Algorithmus 13.1 erhalten wir $g := \mathrm{ggT}(\langle x, y\rangle, \langle a, b\rangle)$ als Linearkombination der Gauß'schen Zahlen $\langle x, y\rangle$ und $\langle a, b\rangle$, etwa

$$g = \langle u, v\rangle\langle x, y\rangle + \langle e, d\rangle\langle a, b\rangle$$

mit $\langle u, v\rangle, \langle e, d\rangle \in \boldsymbol{G}$. Wegen $|g| = 1$ läßt sich also auch 1 als Linearkombination derselben Gauß'schen Zahlen darstellen:

$$1 = \frac{\langle u, v\rangle}{g}\langle x, y\rangle + \frac{\langle e, d\rangle}{g}\langle a, b\rangle$$

Modulo $\langle a, b\rangle$ stimmen also 1 und $\frac{\langle u,v\rangle}{g}\langle x, y\rangle$ überein, woraus wir $\langle x, y\rangle^{-1} \bmod \langle a, b\rangle = \frac{\langle u,v\rangle}{g}$ schließen.

Um $\langle 2, 5\rangle$ modulo $\langle 5, 5\rangle$ zu invertieren, verwenden wir erneut Algorithmus 3.3:

$$\begin{array}{rcrcrcr} \langle 5,5\rangle &=& \color{red}{\langle 1,-1\rangle} &\cdot& \langle 2,5\rangle &+& \langle -2,2\rangle \\ \langle 2,5\rangle &=& \color{red}{\langle 1,-2\rangle} &\cdot& \langle -2,2\rangle &+& \color{blue}{\langle 0,-1\rangle} \\ \hline \langle -2,2\rangle &=& \color{red}{\langle 2,2\rangle} &\cdot& \langle 0,-1\rangle &+& \langle 0,0\rangle \end{array} \qquad \begin{array}{rcrcrcr} \color{green}{\langle 0,0\rangle} &=& \color{red}{\langle 1,-1\rangle} &\cdot& \color{green}{\langle 0,-1\rangle} &+& \langle 1,1\rangle \\ \langle 0,-1\rangle &=& \color{red}{\langle 1,-2\rangle} &\cdot& \langle 1,1\rangle &+& \color{blue}{\langle -3,0\rangle} \end{array}$$

Der resultierende Wert $\langle -3, 0\rangle$ ist nur bis auf eine Einheit (± 1 oder $\pm i$) als Faktor das gesuchte Inverse. Der nötige Faktor ergibt sich wegen

$$\langle 2, 5\rangle\langle -3, 0\rangle \bmod \langle 5, 5\rangle = \langle -6, -15\rangle \bmod \langle 5, 5\rangle = \langle 9, 0\rangle = \langle -1, 0\rangle \bmod \langle 5, 5\rangle$$

zu -1, denn das liefert

$$\langle 2, 5\rangle\langle 3, 0\rangle \bmod \langle 5, 5\rangle = \langle 6, 15\rangle \bmod \langle 5, 5\rangle = \langle 1, 0\rangle$$

Achtung: Die Gleichung $\langle -6, -15\rangle \bmod \langle 5, 5\rangle = \langle -1, 0\rangle \bmod \langle 5, 5\rangle$ darf *nicht* so interpretiert werden, dass komponentenweise modulo 5 zu rechnen ist, wie man an der Tatsache $\langle -6, -15\rangle \bmod \langle 5, 5\rangle = \langle 9, 0\rangle$ sieht. Bei Moduli, deren Absolutbeträge von Real- und Imaginärteil nicht übereinstimmen, könnte ein derartiger Verdacht gar nicht aufkommen.