Übungen zur Vorlesung Kryptographie

Blatt 9

Aufgabe 33: (Quadriken)

Bestimmen Sie die Typen der folgenden Quadriken. Sie dürfen sie einfach von einem Rechner bzw einer Webseite bzw einer App zeichnen lassen und so auf den Typ schließen.

$$Q_1 = \{(x, y) \in \mathbb{R}^2 \mid y^2 - x^2 + xy - 1 = 0\}, \quad Q_2 = \{(x, y) \in \mathbb{R}^2 \mid y^2 + x^2 + xy - 1 = 0\}$$

$$Q_3 = \{(x, y) \in \mathbb{R}^2 \mid y^2 - x^2 + xy = 0\}, \quad Q_4 = \{(x, y) \in \mathbb{R}^2 \mid y^2 - x - y - 1 = 0\}$$

Eine der Quadriken ist eine Parabel. Begründen Sie für diese mathematisch genau, warum es nichts anderes sein kann.

Aufgabe 34: (Aufwärmübung zu elliptischen Kurven)

Lösen Sie diese Aufgabe nur per Hand, also ohne jede Computerhilfe.

(a) Zeigen Sie, dass die Gleichung $y^2 = x^3 + 3x + 1$ eine elliptische Kurve E über $\mathbb{F}_7$ definiert, und dass die Gleichung $y^2 = x^3 + x + 2$ keine elliptische Kurve E über $\mathbb{F}_7$ definiert.

(b) Welche der Punkte $p = (5, 1)$, $q = (3, 1)$ und $r = (2, -1)$ liegen auf E ?

(c) Was sind jeweils die inversen Elemente von $p = (2, 6)$, $q = (3, 3)$ und $r = (6, 2)$ in E ?

(d) Berechnen Sie $(2, 1) \odot (3, 3)$ und $(4, 0) \odot (5, 1)$ in E .

(Graphisch oder mit Formel, aber beschreiben Sie, wie Sie vorgehen.)

(e) Was ist $(4, 0) \odot (4, 0)$? Warum?

Aufgabe 35: (Elliptische Kurven mit Primzahlordnung)

Es ist sehr praktisch, wenn die Ordnung einer elliptischen Kurve eine Primzahl p ist (warum nochmal?). Für große p ist es aber nicht einfach, so eine zu finden. Diese Aufgabe soll das ein wenig illustrieren.

(a) Finden Sie alle a und b , so dass die Anzahl der Elemente der elliptischen Kurve über $\mathbb{F}_{13}$ mit der Gleichung $y^2 = x^3 + ax + b$ eine Primzahl ist. Berechnen Sie den Anteil dieser an allen Möglichkeiten, die a, b zu wählen. Berechnen Sie auch den Anteil der a, b , die keine Gruppe liefern. (Als Abgabe reichen die Anteile, als Prozentzahl, oder als $0 < x < 1$.)

(b) Machen Sie dasselbe für $\mathbb{F}_{701}$.

sagemath kennt elliptische Kurven über $\mathbb{F}_p$, siehe

<https://wiki.sagemath.org/quickref?action=AttachFile&do=view&target=quickref-nt.pdf>

Aufgabe 36: (Elemente der Ordnung 2)

Erinnerung: ein Element g in einer Gruppe G hat **Ordnung** k , falls $g^k = e$ ist (e das neutrale Element), und für alle $i \in \{1, \dots, k-1\}$ gilt: $g^i \neq e$.

(a) Bestimmen Sie jeweils alle Elemente der Ordnung zwei in den beiden Gruppen E und E^* in Beispiel 6.2 des Skripts.

(b) Zeigen Sie, dass eine elliptische Kurve als Gruppe maximal drei Elemente der Ordnung zwei hat.

(Ein plausibles Bild über $\mathbb{R}$ gibt bereits Teilpunkte, ein formales Argument gibt volle Punktzahl.)

Abgabe bis Mittwoch 11.6.2025 bis 14 Uhr per Email an die Tutorin.

Lisa Harms lharms+krypto@techfak.de
 Lisa Henetmayr lhenetmayr+krypto@techfak.de