Dr. Dirk Frettlöh 31.5.2023

Übungen zur Vorlesung Kryptographie

Blatt 9

Aufgabe 33: (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 vorgingen.)
(e) Was ist $(4, 0) \odot (4, 0)$? Warum?

Aufgabe 34: (Wann ist's keine Gruppe?)
Für welche Werte von b liefert $y^2 = x^3 - 3x + b$ keine elliptische Kurve über $\mathbb{R}$? Für welche Werte von b liefert $y^2 = x^3 + b$ keine elliptische Kurve über $\mathbb{R}$? Zeichnen Sie all diese Kurven (gerne mit einer geeigneten Software). Erläutern Sie, warum die jeweils keine Gruppe liefern.

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: (Ordnung von E ist ungefähr p)
Sei E eine elliptische Kurve über $\mathbb{F}_p$ (wie in Def. 6.1).

(a) Zeigen Sie, dass E spiegelsymmetrisch bezüglich der x-Achse ist. (Also: ist $(x, y) \in E$, dann auch $(x, -y) \in E$. Das $\mathcal{O}$ kann hier ignoriert werden.)

(b) Zeigen Sie, dass E spiegelsymmetrisch bezüglich der Achse $\{(x, \frac{p}{2}) \mid x \in \mathbb{R}\}$ ist.
(Zwar ist $\frac{p}{2}$ nicht in E oder $\mathbb{F}_p$, aber das Spiegeln haut dennoch hin.)

(c) Zeigen Sie: für die Ordnung $|E|$ von E gilt: $|E| \leq 2p + 1$.

Abgabe bis Dienstag 6.6.2023 bis 23:59 Uhr per Email an den Tutor.
Bitte auf jeder Abgabe das Tutorium angeben!

Jakob Niermann janiermann+krypto@techfak.de
Tim Lakämper tlakaemper+krypto@techfak.de