Aufgaben

9.1. Zeigen Sie, dass die Bedingung $4a^3 + 27b^2 \neq 0 \bmod p$ für die Kurve

$$y^2 \equiv x^3 + 2x + 2 \bmod 17 \tag{9.3}$$

erfüllt ist.

9.2. Berechnen Sie die Addition der Punkte

1. $(13,7) + (6,3)$
2. $(13,7) + (13,7)$

über der Kurve $y^2 \equiv x^3 + 2x + 2 \bmod 17$. Benutzen Sie nur einen Taschenrechner (und keine Software für ECC-Arithmetik) und zeigen Sie alle Zwischenschritte.

9.3. In diesem Kapitel wurde die Anzahl der Punkte auf der elliptischen Kurve $y^2 \equiv x^3 + 2x + 2 \bmod 17$ mit $\#E = 19$ angegeben. Verifizieren Sie den Satz von Hasse für diese Kurve.

9.4. Wir betrachten die Kurve $y^2 \equiv x^3 + 2x + 2 \bmod 17$. Warum sind *alle* Punkte, bis auf den Punkt im Unendlichen, primitive Elemente?

Bemerkung: Im Allgemeinen sind nicht alle Kurvenpunkte primitive Elemente.

9.5. Sei E eine elliptische Kurve über $\mathbb{Z}_7$:

$$E : y^2 = x^3 + 3x + 2.$$

1. Berechnen Sie alle Punkte von E über $\mathbb{Z}_7$.
2. Was ist die Gruppenordnung? (Hinweis: Das neutrale Element $\mathcal{O}$ muss mitgezählt werden.)
3. Bestimmen Sie die Ordnung des Punktes $\alpha = (0,3)$. Ist α ein primitives Element?

9.6. Wir betrachten Punktmultiplikationen der Form $T = a \cdot P$ mittels des Double-and-Add-Algorithmus, der in Abschnitt 9.2 vorgestellt wurde. In der Praxis liegt der Skalar a zumeist in dem Bereich von $p \approx 2^{160} \cdots 2^{250}$.

1. Zeigen Sie den Ablauf des Algorithmus für $a = 19$ und $a = 160$. Man beachte, dass *keine* Berechnungen auf der elliptischen Kurve notwendig sind. Der Punkt P ist während des Algorithmus lediglich eine Variable.
2. Wie viele (i) Punktadditionen und (ii) Punktverdopplungen sind im Durchschnitt für eine Punktmultiplikation erforderlich, wenn der Skalar $n = \lceil \log_2 p \rceil$ Bit lang ist?
3. Wir nehmen an, dass p eine Primzahl mit 160 Bit ist, d. h. alle Körperelemente und der Skalar haben die gleiche Bitlänge. In einer Software-Implementierungen dauert das Berechnen der Gruppenoperation (Punktaddition oder -verdopplung) 20 μs. Wie lange benötigt die Punktmultiplikation im Durchschnitt?

9.7. Gegeben seien die elliptische Kurve E über $\mathbb{Z}_{29}$ sowie der Basispunkt $P = (8,10)$:

$$E : y^2 \equiv x^3 + 4x + 20 \bmod 29.$$

Berechnen Sie die beiden folgenden Punktmultiplikationen $k \cdot P$ mit dem Double-and-Add-Algorithmus. Zeigen Sie das Zwischenergebnis nach jeder Iteration des Algorithmus.

1. $k = 9$
2. $k = 20$

9.8. Gegeben sei die Kurve aus Aufgabe 9.7. Die Gruppenordnung der Kurve ist $\#E = 37$. Geben sei weiterhin der Punkt $Q = 15 \cdot P = (14,23)$. Berechnen Sie die folgenden Punktmultiplikationen. Versuchen Sie, die geringstmögliche Anzahl an Gruppenoperationen zu verwenden. Versuchen Sie, den bekannten Punkt Q geschickt zu nutzen. Zeigen Sie genau, wie die Berechnungen vereinfacht wurden. Man beachte, dass der Punkt $-P$ auch einfach berechnet werden kann, was ebenfalls zu Rechenerleichterungen führt.

1. $16 \cdot P$
2. $38 \cdot P$
3. $53 \cdot P$
4. $14 \cdot P + 4 \cdot Q$
5. $23 \cdot P + 11 \cdot Q$

Durch geschickten Einsatz von Q und $-P$ sollten die Punktmultiplikationen mit deutlich weniger Operationen möglich sein, als sie der normale Double-and-Add-Algorithmus erfordert.

9.9. Ziel ist es, den Sitzungsschlüssel eines Diffie-Hellman-Protokolls mit elliptischen Kurven (ECDH) zu berechnen. Der private Schlüssel ist $a = 6$ und der öffentliche Schlüssel des Kommunikationspartners Bob hat den Wert $B = (5,9)$. Es wird dabei die elliptische Kurve

$$y^2 \equiv x^3 + x + 6 \bmod 11$$

verwendet.

9.10. In Abschnitt 9.3 ist ein Beispiel für ein ECDH-Protokoll gegeben. Verifizieren Sie beide Skalarmultiplikationen, die Alice durchführt. Zeigen Sie alle Zwischenergebnisse, die innerhalb der Gruppenoperation auftreten.

9.11. Durch die Ausführung eines ECDH haben Alice und Bob den gemeinsamen geheimen Punkt $R = (x,y)$ berechnet. Der Modul der elliptischen Kurve ist eine Primzahl von 64 Bit Länge. Hieraus wird nun ein Sitzungsschlüssel für eine Blockchiffre mit einem 128-Bit-Schlüssel abgeleitet. Die Schlüsselableitung erfolgt dabei als:

$$K_{\mathrm{AB}} = h(x||y)$$

Beschreiben Sie eine *effiziente* Art, einen Brute-Force-Angriff gegen die Blockchiffre durchzuführen. Wie viele Bit Entropie hat der Schlüssel? (Bemerkung: Es ist nicht notwendig, alle Details aufzuführen. Eine Liste, die die notwendigen Schritte beschreibt, ist ausreichend. Es kann angenommen werden, dass Quadratwurzeln modulo p einfach berechnet werden können.)

9.12. Leiten Sie die Formel für Punktaddition auf elliptischen Kurven ab. Gegeben sind die Koordinaten der Punkte P und Q und es werden Ausdrücke für die Koordinaten von $R = (x_3, y_3)$ gesucht.

Hinweis: Zuerst sollte man die Gleichung für eine Gerade durch die beiden Punkte aufstellen. Diese wird in die elliptische Kurvengleichung eingesetzt. Später müssen die Nullstellen des kubischen Polynoms $x^3 + a_2x^2 + a_1x + a_0$ bestimmt werden. Wenn die drei Nullstellen mit x_0, x_1, x_2 bezeichnet werden, kann man ausnutzen, dass gilt: $x_0 + x_1 + x_2 = -a_2$.