Inhaltsverzeichnis

1 Übung 1

2 Übung 2

3 Übung 3

4 Übung 4

5 Übung 5

5.1 Aufgabe 1

5.2 Aufgabe 2

5.3 Aufgabe 3

5.4 Aufgabe 4

5.5 Aufgabe 5

a)

b)

c) Siehe `Krypto/gap/ElGamal.g`

6 Übung 6

6.1 Aufgabe 1

6.2 Aufgabe 2

- öffentlicher Schlüssel: $(n, e) = (299, 79)$.
- geheimer Schlüsel: $d = 127$.

$$\begin{aligned} ed - 1 &= 79 \times 127 - 1 \\ &= 10033 - 1 \\ &= 10032 \\ &= 2^s \times t \\ &= 2^4 \times 627 \end{aligned}$$

Also $s = 4$ und $t = 627$. Für (2.1.26) müssen wir dann ein $a \in \{1, \ldots, n-1\}$ finden mit

$$\begin{aligned} \operatorname{ggT}(a, n) &= 1 && \text{(1a)} \\ \operatorname{ord}[a^t]_p &\neq \operatorname{ord}[a^t]_q && \text{(1b)} \end{aligned}$$

wobei wir p und q ja gerade noch nicht kennen. Wir ignorieren also die zweite Bedingung (1b) und gehen probabilistisch vor, d.h. wir wählen ein zufälliges $a \in \{1, \ldots, n-1\}$, welches (1a) erfüllt. Mit den so bestimmten Variablen und einem $i \in \{0, \ldots, s-1\} = \{0, 1, 2, 3\}$ haben wir also a, i, t, n sodass

$$\operatorname{ggT}(a^{2^i t} - 1, n) \in \{p, q\}. \tag{2}$$

Zum Beispiel für $a = 224$, welches $\operatorname{ggT}(a, n) = 1$ erfüllt, ergibt sich

$$i = 0 : \operatorname{ggT}(224^{2^0 \times 627} - 1, 299) = 13$$

Also haben wir 13 als Teiler von 299 erkannt, und tatsächlich ist $299/13 = 23$.

Als Beispiel, dass auch $i > 0$ nötig sein kann, z.B. $a = 44$, dann ergibt sich

$$\begin{aligned} i = 0 &: \operatorname{ggT}(44^{2^0 \times 627} - 1, 299) = 1 \\ i = 1 &: \operatorname{ggT}(44^{2^1 \times 627} - 1, 299) = 23 \end{aligned}$$

Als Algorithmus nach (2.1.28) habe ich `Krypto/gap/RSAFactoring.g` geschrieben, dem man n, e, d übergibt (der also bereits annimmt, dass man d aus n und e effizient errechnet hat) und der daraus einen Faktor von n bestimmt.

6.3 Aufgabe 3

ElGamal $\mathbb{Z}_p^*$, $p = 17, a = 3, k = 10$.

a) öffentlicher Schlüssel

$$\begin{aligned} (p, a, k) &= (17, 3, 10) \\ z &= a^k \mod p \\ &= 3^{10} mod 17 \end{aligned}$$

Schnelle Expo mit $a = 3, n = 10, m = 17$:

k	pk	nk	ak	nk mod 2
0	1	10	3	0
1	1	5	9	1
2	9	2	13	0
3	9	1	-1	1
4	-9	0	(Ende)	

$a^3 \mod 17 = -9 \mod 17 = 8 \mod 17$.

Also $z = 8$ und damit ist der öffentliche Schlüssel $(p, a, z) = (17, 3, 8)$.

b) $m = 5, y = 5$.

(langsame Expo im Kopf):

$$\begin{aligned} c &= a^y \mod p \\ &= 3^5 \mod 17 \\ &= 3^4 \cdot 3 \mod 17 \\ &= 81 \cdot 3 \mod 17 \\ &= 13 \cdot 3 \mod 17 \\ &= (-4) \cdot 3 \mod 17 \\ &= -12 \mod 17 \\ &= 5 \mod 17 \end{aligned}$$

$$\begin{aligned} d &= m \cdot z^y \mod p \\ &= 5 \cdot 8^5 \mod 17 \\ &= 5 \cdot 64 \cdot 64 \cdot 8 \mod 17 \\ &= 5(-4)(-4)8 \mod 17 \\ &= 5 \cdot 2 \cdot 64 \mod 17 \\ &= -40 \mod 17 \\ &= -6 \mod 17 \\ &= 11 \mod 17 \end{aligned}$$

$(c, d) = (5, 11)$.

c) $(12, 12) = (c, d)$.

$$\begin{aligned} s &= 12^{-1} \mod 17 \\ 12 \cdot 3 &= 36 \cong 2 \mod 17 \\ 2 \cdot 9 &= 18 \Rightarrow 2^{-1} = 9 \mod 17 \\ (12 \cdot 3)^{-1} &= 9 \mod 17 \\ 12^{-1} \cdot 3^{-1} &= 9 \mod 17 \\ 12^{-1} &= 3 \cdot 9 = 27 = 10 \mod 17 \\ s &= 10 \end{aligned}$$

$$ds^k \mod p = 12 \cdot 10^{10} \mod 17$$

k	pk	nk	ak	nk mod 2
0	1	10	10	0
1	1	5	-2	1
2	-2	2	4	0
3	-2	1	-1	1
4	2	0	(Ende)	

$$12 \cdot 2 \mod 17 = 24 \mod 17 = 7 \mod 17$$

Klartext ist 7.

6.4 Aufgabe 4

Siehe `Krypto/gap/ElGamal.g`.

Zuerst habe ich den Algorithmus zur schnellen Exponentiation names `fex` geschrieben. Dann habe ich den Miller-Rabin-Test implementiert, einmal als Primzahl-Test `MillerRabinTest, MRT` mit Eingaben n, k wobei k die Anzahl der Wiederholungen des Tests ist, und einmal als Primzahl-Generator `MillerRabinGenerator, MRG` mit Eingaben `low, high` das Intervall, in dem nach einer Primzahl gesucht werden soll, und k erneut wie oben.

Mit diesen Hilfsmitteln habe ich dann das Programm `ElGamal` geschrieben, das zu einer Eingabe $n \in \mathbb{N}$ ein Schlüssel-Paar `key.public` und `key.private` (als gap-Records) erzeugt, wobei `key.public` $= (p, a, z)$ und `key.private` $= k$ wobei für die Primzahl p gilt $p \geq n$, und für den geheimen Schlüssel k gilt $k \geq \frac{1}{2}n$.

Der Algorithmus geht nach dem in (2.2.3) Beschriebenen vor mit $f = 2$, d.h. anstatt Primzahl p und Primitivwurzel a getrennt zu wählen, wird ein Paar (m, a) bestimmt, für das m eine Primzahl und a eine Primitivwurzel modulo m ist. Hierbei wird für die erstmalige Primzahl q das Suchintervall $[n, 2n]$ nach Betrand bestimmt, und die Wiederholungen bei 10. Ebenso wird m mit 10 Wiederholungen auf Primzahl getestet.

Sobald man das Paar (p, a) hat, wird ein zufälliger geheimer Schlüssel $k \geq \frac{n}{2}$ gebildet. Anschließend wird noch das für den öffentlichen Schlüssel fehlende $z = a^k \mod p$ berechnet, wobei wiederum die Schnelle Exponentiation zum Einsatz kommt. Damit ist auch der öffentliche Schlüssel `key.public` $= (p, a, z)$ bestimmt, und beide werden zusammen ausgegeben.

6.5 Aufgabe 5

Satz 6.5.1 (Lagrange)**.** Sei G eine endliche Gruppe und $U \leq G$ eine Untergruppe von G. Dann gilt:

(1) $|U|$ teilt $|G|$.

(2) $\left| {}_U\backslash^G \right| = \left| {}^G/_U \right| = \frac{|G|}{|U|}$.

Beweis. Weil G endlich ist, ist U eine endliche Untergruppe von G. Setze $|U| := m \in \mathbb{Z}_{\geq 1}$. Zu jedem $g \in G$ sei $gU := \{gu : u \in U\}$ eine Linksnebenklasse von U. Dann ist die Abbildung

$$g\cdot : U \to gU,\, u \mapsto gu$$

eine Bijektion: Weil $g \in G$ invertierbar ist, definiert g^{-1} die Abbildung

$$g^{-1}\cdot : gU \to U,\, gu \mapsto g^{-1}gu = u$$

und es gilt

$$g \cdot (g^{-1} \cdot (gu)) = g \cdot (u) = gu$$

sowie
$$g^{-1} \cdot (g \cdot (u)) = g^{-1} \cdot (gu) = u$$
also $(g\cdot) \cdot (g^{-1}\cdot) = \mathrm{Id}_{gU}$ und $(g^{-1}\cdot) \cdot (g\cdot) = \mathrm{Id}_U$. Also ist $g\cdot$ bijektiv. Insbesondere gilt $|gU| = |U|$, weil U endlich ist. Damit folgt $|U| = |gU|\ \forall g \in G$.

Es sei ${}^G/_U := \{gU : g \in G\}$ die Menge der Linksnebenklassen von U. Für $g, h \in G$ untersuchen wir den Fall, dass $gU = hU$. Unter der Äquivalenzrelation
$$g \sim h :\Leftrightarrow gU = hU$$
betrachte die Menge ${}^G/_\sim := \{[g]_\sim : g \in G\}$ mit $[g]_\sim := \{h \in G | h \sim g\}$. Offensichtlich gilt ${}^G/_U \simeq {}^G/_\sim$. Im Fall $gU = hU$ gibt es also zu jedem $u_1 \in U$ ein $u_2 \in U$ sodass $gu_1 = hu_2$, also $h^{-1}g = u_1^{-1}u_2 \in U$. Damit stellen wir fest, dass
$$g \sim h \Leftrightarrow gU = hU \Leftrightarrow h^{-1}g \in U \Leftrightarrow g^{-1}h \in U.$$

Die Anzahl der Nebenklassen von U ist also ein Vielfaches von $|U|$, d.h. $\exists n \in \mathbb{Z}_{\geq 1} : \left|{}^G/_U\right| = n \cdot |U| = n \cdot m$.

□

6.6 Aufgabe 6

Siehe `Krypto/gap/EllipticCurve.g`.

Zunächst habe ich eine Funktion `defines_ellipse` geschrieben, die bei Eingabe von a_4, a_6 und dem Körper F überprüft, ob durch $E_0(a_4, a_,6, F)$ eine elliptische Kurve i.S.v. (2.3.10) definiert ist, wobei die Existenz des neutralen Elements ignoriert wird, also nur die Eigenschaften in (2.3.6) überprüft werden, d.h.

$$F \text{ ist ein Körper} \tag{3}$$
$$\mathrm{Char}\, F \neq 2 \tag{4}$$
$$\mathrm{Char}\, F \neq 3 \tag{5}$$
$$4a_4^3 + 27a_6^2 \neq 0 \tag{6}$$

wobei die letzte Gleichung über F gesehen werden sollte.

Für die endlichen Körper benutze ich das gap-Paket `GaussForHomalg` vom homalg_project (`https://github.com/homalg-project/homalg_project`).

a) $a_4 = -7, a_6 = -6, F = \mathbb{Z}_5, P = (3, 0)$

Zunächst betrachte ich die Zahlen als Elemente von $\mathbb{Z}_5$, d.h.

$$\begin{aligned} a_4 \quad \bmod 5 &= -7 & \bmod 5 &= 3 \\ a_6 \quad \bmod 5 &= -6 & \bmod 5 &= 4 \\ P \quad \bmod 5 &= (3,0) & \bmod 5 &= (3,0) \end{aligned}$$

In gap wird das durch Multiplizieren mit 1_F erledigt, d.h. (6) wird so überprüft:
$$1_F * (4 * a_4^3 + 27 * a_6^2) \neq 1_F * 0$$

Auch die Koeffizienten in (6) können wir über $\mathbb{Z}_5$ betrachten:
$$\begin{aligned} 4 \quad \bmod 5 &= 4 \\ 27 \quad \bmod 5 &= 2 \end{aligned}$$

Nun ist aber $4 \cdot 3^3 + 2 \cdot 4^2 \mod 5 = 140 \mod 5 = 0$, also gilt (6) nicht, d.h. mit $a_4 = -7, a_6 = -6, F = \mathbb{Z}_5$ handelt es sich nicht um eine Ellipse (was alle weiteren Rechnungen erübrigt).

Das ergebnis liefert auch unsere Funktion `defines_ellipse`:

```
gap> Z5 := HomalgRingOfIntegers( 5 );
GF(5)
gap> defines_ellipse( -7, -6, Z5 );
false
```

b) $a_4 = -5, a_6 = 5, F = \mathbb{Z}_{11}, P = (4,7)$.

Über $\mathbb{Z}_{11}$ ergibt das

$$\begin{aligned} a_4 \mod 11 &= -5 &\mod 11 &= 6 \\ a_6 \mod 11 &= 5 &\mod 11 &= 5 \\ P \mod 11 &= (4,7) &\mod 11 &= (4,7) \end{aligned}$$

Ebenso die Koeffizienten

$$\begin{aligned} 4 \mod 11 &= 4 \\ 27 \mod 11 &= 5 \end{aligned}$$

Wir stellen fest, $\mathbb{Z}_{11}$ ist ein Körper, nicht von Charakteristik 2 oder 3. Bleibt also (6) zu überprüfen:

$$4 \cdot 6^3 + 5 \cdot 5^2 \mod 11 = 989 \mod 11 = 10 \neq 0 \mod 11.$$

Das ergebnis liefert auch unsere Funktion `defines_ellipse`:

```
gap> Z11 := HomalgRingOfIntegers( 11 );
GF(11)
gap> defines_ellipse( -5, 5, Z11 );
true
```

Nun haben wir also eine elliptische Kurve $E_0(-5, 5, \mathbb{Z}_{11})$ und wollen die Anzahl der Elemente bestimmen. Da sie als x-y-Graph eine Teilmenge der Zahlenebene $\mathbb{Z}_{11}^2$ ist, brauchen wir also nur für endlich viele Punkte zu überprüfen, ob sie auf der elliptischen Kurve liegen. Dazu bestimmen wir zunächst die Gleichung der Kurve:

$$y^2 = x^3 + a_4 x + a_6, \tag{7}$$

also

$$y^2 = x^3 + 6x + 5$$

Dazu habe ich eine Funktion `ellipse_membership` geschrieben, die bei Eingabe eines Punktes $xy \in F^2$ und den Werten a_4, a_6 und F ausgibt, ob xy die Gleichung (7) erfüllt.

Diesen Filter kann ich nun auf die Zahlenebene F^2 anwenden, wenn F endlich ist. Zusammen mit der Funktion `defines_ellipse` habe ich dann die Funktion `ellipticCurve` geschrieben, die zuerst überprüft, ob es sich um eine ellipse handelt, dann ob der Körper endlich ist, und dann die Punkte auf der elliptischen Kurve als Teilmenge von F^2 ausgibt:

```
gap> E0 := ellipticCurve( -5, 5, Z11 );
[ [ 0*Z(11), Z(11)^2 ], [ 0*Z(11), Z(11)^7 ], [ Z(11)^0, Z(11)^0 ],
[ Z(11)^0, Z(11)^5 ], [ Z(11), Z(11)^4 ], [ Z(11), Z(11)^9 ],
```

```
[ Z(11)^2, Z(11)^2 ], [ Z(11)^2, Z(11)^7 ], [ Z(11)^3, Z(11) ],
[ Z(11)^3, Z(11)^6 ], [ Z(11)^5, Z(11)^3 ], [ Z(11)^5, Z(11)^8 ],
[ Z(11)^7, Z(11)^2 ], [ Z(11)^7, Z(11)^7 ], [ Z(11)^9, Z(11) ],
[ Z(11)^9, Z(11)^6 ] ]
gap> Length( E0 );
16
```

Wir dürfen aber auch nicht den Fernpunkt $O \in E_0$ vergessen, der das neutrale Element der Gruppe ist. Die Gruppe hat also insgesamt 17 Elemente.

Damit können wir auf zwei Arten überprüfen, ob der Punkt $P = (4, 7)$ auf E_0 liegt:

Example

```
gap> P := [ 4, 7 ];
[ 4, 7 ]
gap> ellipse_membership( P, -5, 5, Z11 );
true
gap> One( Z11 )*P in E0;
true
```

In Anlehnung an das, was ich in Aufgabe 6.6. c) per Hand ausgerechnet habe, habe ich ein Programm `tangentSlope` geschrieben, das den Punkt P sowie a_4, a_6 und F übergeben bekommt, und dann die Steigung in P an E_0 ausrechnet.

Example

```
gap> tangentSlope( P, -5, 5, Z11 );
Z(11)^7
gap> 7*One( Z11 );
Z(11)^7
```

Mit Punkt P auf der Geraden und der Steigung $a := \texttt{tangentSlope}(P, a_4, a_6, F)$ kann man leicht den y-Achsen-Abschnitt bestimmen:

Example

```
gap> a := tangentSlope( [4, 7], a4, a6, Z11 );
Z(11)^7
gap> lineYintersect( P, a, Z11 );
Z(11)^0
```

Also ist die Tangente $t_P(x) = 7x + 1 \mod 11$.

Nun müssen wir beide Funktionen gleichsetzen und danach die doppelte Nullstelle $x = P_x = 4$ dividieren. Wir bekommen also eine Funktion, der die beiden bekannten x-Werte $x_1 = P_x, x_2 = Q_x$ (im allgemeinen Fall, wenn es kein doppelter Schnittpunkt war) und die Koeffizienten a, b für die Gerade und a_4, a_6 für die elliptische Kurve sowie der Körper F übergeben werden, und die daraus dann den dritten Schnittpunkt R von Gerade und elliptischer Kurve zurückgibt.

Dabei muss eine Polynomdivision durchgeführt werden.

$$
\begin{aligned}
L(P, Q, F) : ax + b = f(x) &= \sqrt{x^3 + a_4 x + a_6} \\
(ax + b)^2 &= x^3 + a_4 x + a_6 \\
a^2 x^2 + 2abx + b^2 &= x^3 + a_4 x + a_6 \\
x^3 - a^2 x^2 + (a_4 - 2ab)x + (a_6 - b^2) &= 0
\end{aligned}
$$

Von diesem Polynom dritten Grades auf der linken Seite kennen wir schon die zwei Lösungen x_1, x_2 von oben. Wir können also beide Nullstellen herausdividieren, also in einem Schritt das Polynom $(x - x_1)(x - x_2) = x^2 - (x_1 + x_2)x + x_1x_2$:

$$\begin{aligned}(x^3 - a^2x^2 + (a_4 - 2ab)x + (a_6 - b^2)) : (x^2 - (x_1 + x_2)x + x_1x_2)\\ = x + (x_1 + x_2 - a^2)\end{aligned}$$

Es ergibt sich nämlich nach dem ersten Divisions-Schritt bei x^2 der Koeffizient $-a^2 - (-(x_1 + x_2)) = (x_1 + x_2 - a^2)$. Dass sich der Rest zu 0 subtrahiert, führt auf die zwei Gleichungen für die x^1- und die x^0-Koeffizienten:

$$\begin{aligned}a_4 - 2ab - x_1x_2 + x_1^2 + 2x_1x_2 + x_2^2 - a^2x_1 - a^2x_2 = 0\\ a_6 - b^2 - x_1^2x_2 - x_1x_2^2 + a^2x_1x_2 = 0\end{aligned}$$

Einsetzen von a und b in Abhängigkeit von x_1 und x_2:

Wir haben dann also den dritten x-Wert $x + (x_1 + x_2 - a^2) = 0$, d.h. $x_3 = a^2 - x_1 - x_2$. Anstatt diesen in die uneindeutige Ellipsen-Gleichung einzusetzen, setzen wir x_3 lieber in die Geradengleichung ein:

$$\begin{aligned}y_3 &= ax_3 + b\\ &= a^3 - ax_1 - ax_2 + b\end{aligned}$$

Damit haben wir also den dritten Punkt $R = (x_3, y_3)$ und das Ergebnis (wenn die Gerade $y = ax + b$ durch die zwei Punkte $P, Q \in E_0$ geht), dass $R = P * Q$.

Für die Berechnung der Gruppenoperation selbst müssen wir noch mit (2.3.11) berechnen:

$$\begin{aligned}P + Q &= 0 * (P * Q)\\ &= 0 * R\\ &= 0 * (x_3, y_3)\\ &= (x_3, -y_3)\end{aligned}$$

c) $a_4 = -43, a_6 = 166, F = \mathbb{R}, P = (3, 8)$.

Da $\mathbb{R}$ ein unendlicher Körper ist, gilt $\operatorname{Char}\mathbb{R} = 0$, und wir brauchen auch nicht in Restklassen zu rechnen. Es gilt also wieder nur die Gleichung (6) zu überprüfen, also

$$4 \cdot (-43)^3 + 27 \cdot 166^2 = 425984 \neq 0$$

Statt über $\mathbb{R}$ rechnen wir in gap über den berechenbaren Körper $\mathbb{Q}$, was am Ergebnis nichts ändert:

Example
```
gap> QQ := HomalgFieldOfRationals();
Q
gap> defines_ellipse( -43, 166, QQ );
true
```

Da es sich bei $E_0(-43, 166, \mathbb{R}) \subset (\mathbb{R}^2 \cup \{O\})$ um einen stetigen Graph handelt, ist die Gruppe unendlich groß.

Um einen Punkt P zu sich selbst zu addieren, also ihn zu verdoppeln in der Gruppen-Operation auf E_0 bildet man die Tangente an der elliptischen Kurve durch P. Wenn die Tangente parallel zur y-Achse verläuft, schneidet sie die elliptische Kurve in keinem weiteren Punkt. In diesem Fall gilt dann $P + P = O$ und die Ordnung von P wäre zwei.

Wie man am Graph der Kurve

$$y^2 = x^3 - 43x + 166,$$

sehen kann, ist der äußerst linke Punkt derjenige, an dem $y = 0$ gilt und der eine Tangente parallel zur y-Achse hat. Da es sich nicht um unseren Punkt $P = (3, 8)$ handelt, können wir also $P + P = O$ ausschließen, d.h. P ist nicht von Ordnung 2.

Wir müssen also die Tangente an E_0 im Punkt $P = (3, 8)$ berechnen. Da sich der Punkt in der oberen Hälfte des Graphes befindet, können wir $y > 0$ annehmen, und damit den Graph nach $y = f(x)$ auflösen:

$$y = f(x) = \sqrt{x^3 - 43x + 166} = (x^3 - 43x + 166)^{1/2}$$

Für die Tangente bilden wir also die Ableitung von f:

$$\begin{aligned} f'(x) &= (3x^2 - 43) \cdot \frac{1}{2} \cdot (x^3 - 43x + 166)^{-1/2} \\ &= \frac{1}{2} \cdot \frac{3x^2 - 43}{\sqrt{x^3 - 43x + 166}} \end{aligned}$$

Die Tangente hat also im Punkt $P = (3, 8)$ die Steigung $f'(3) = -1$. Damit können wir die Tangentenfunktion $t_P(x)$ zur Geraden $L(P, P, \mathbb{R})$ bestimmen:

$$\begin{aligned} t_P(x) &= ax + b \\ t_P(3) &= 8 \\ t'_P(x) &= a = f'(3) = -1 \\ t_P(x) &= -x + b \\ 8 &= -3 + b \\ b &= 11 \\ t_P(x) &= -x + 11 \end{aligned}$$

Nun haben wir mit P einen doppelten Schnittpunkt an E_0 und suchen den dritten Schnittpunkt $R \in L(P, P, \mathbb{R}) \cap E_0$, also setzen wir beide Funktionen gleich und lösen nach x und y auf:

$$\begin{aligned} t_P(x) &= f(x) \\ -x + 11 &= \sqrt{x^3 - 43x + 166} \\ (11 - x)^2 &= x^3 - 43x + 166 \\ 121 - 22x + x^2 &= x^3 - 43x + 166 \\ x^3 - x^2 - 21x + 45 &= 0 \\ (x^3 - x^2 - 21x + 45) : (x - 3) &= x^2 + 2x - 15 \\ (x + 5)(x - 3)(x - 3) &= 0 \end{aligned}$$

also $R = (-5, f(-5)) = (-5, 16)$. Damit haben wir also $P * P$ nach (2.3.10) berechnet. Für die Gruppenoperation auf E_0 müssen wir dann nur noch berechnen

$$\begin{aligned} P + P &= 0 * (P * P) \\ &= 0 * R \\ &= 0 * (-5, 16) \\ &= (-5, -16) \end{aligned}$$

Es muss also nur noch das Vorzeichen vom y-Wert vertauscht werden. Wir halten also fest, $P + P = 2P = (-5, -16)$. Nun sollte die Verbindungsline zwischen P und nP in den meisten Fällen keine Tangente an E_0 mehr sein, sondern eine Sekante. Wir berechnen also der Reihe nach $3P = P + 2P, 4P = P + 3P, \ldots$ bis wir für ein $n \in \mathbb{N}$ haben $nP = 0$.

$$\begin{aligned} L(P, Q, \mathbb{R}) &= \{(1-s)P + sQ \mid s \in \mathbb{R}\} \\ (x, y) &\in L(P, Q, \mathbb{R}) \\ \Leftrightarrow x &= (1-s)P_x + sQ_x \\ y &= (1-s)P_y + sQ_y \end{aligned}$$

Das ergibt für $L(P, 2P, \mathbb{R})$:

$$\begin{aligned} x &= (1-s)3 + s(-5) \\ y &= (1-s)8 + s(-16) \\ x(s) &= 3 - 8s \\ y(s) &= 8 - 24s \\ s(x) &= (x-3)/(-8) \\ y(x) &= 8 - 24(s(x)) \\ &= 8 - 24((x-3)/(-8)) \\ &= 8 + 3(x-3) \\ &= 3x - 1 \end{aligned}$$

Also wieder gleichsetzen

$$\begin{aligned} (3x-1)^2 &= x^3 - 43x + 166 \\ 9x^2 - 6x + 1 &= x^3 - 43x + 166 \\ x^3 - 9x^2 - 37x + 165 &= 0 \end{aligned}$$

Und wir kennen bereits zwei Lösungen $P_x = 3$ und $(2P)_x = -5$, wir können also dividieren:

$$(x^3 - 9x^2 - 37x + 165) : ((x-3)(x+5)) = (x^2 - 6x - 55) : (x+5) = (x - 11)$$

Der dritte Punkt ist also $R = (11, f(11)) = (11, 32)$. Einmal noch das Vorzeichen vom y-Wert tauschen erhalten wir $3P = (11, -32)$.

Wieder die Gerade durch P und $3P$:

$$\begin{aligned}
x &= (1-s)3 + s(11) \\
&= 3 + 8s \\
s(x) &= (x-3)/8 \\
y &= (1-s)8 + s(-32) \\
y(x) &= 8 - 40(s(x)) \\
&= 8 - 40((x-3)/8) \\
&= 8 - 5x + 15 \\
&= -5x + 23
\end{aligned}$$

Wieder gleichsetzen:

$$\begin{aligned}
(-5x+23)^2 &= x^3 - 43x + 166 \\
25x^2 - 230x + 529 &= x^3 - 43x + 166 \\
x^3 - 25x^2 + 187x - 363 &= 0
\end{aligned}$$

Mit den bekannten zwei Lösungen $x = 3$ und $x = 11$:

$$\begin{aligned}
&(x^3 - 25x^2 + 187x - 363) : ((x-3)(x-11)) \\
&= (x^2 - 22x + 121) : (x - 11) \\
&= x - 11
\end{aligned}$$

Wir haben also wieder $x = 11$ herausbekommen. Also $R = (11, f(11)) = (11, 32)$ also $P * 3P = 3P$. Und $P + 3P = 0 * 3P = (11, -(-32)) = (11, 32) = 4P$.

Nun ist die Verbindungslinie zwischen $4P$ und $3P$ parallel zur y-Achse, also $4P * 3P = 0$ und damit

$$4P + 3P = 0 * (4P * 3P) = 0 * 0 = 0 \tag{8}$$

$$\Rightarrow 7P = 4P + 3P = 0 \tag{9}$$

$$\Rightarrow \mathrm{ord}_{E_0} P = 7 \tag{10}$$

Die Ordnung vom Punkt $P = (3, 8)$ beträgt 7.

7 Übung 7

7.1 Aufgabe 1 und 2

Listing 1: PointOnEllipticCurve

```
PointOnEllipticCurve := function( a4, a6, F, p )
  local Px, Pysq, Py, P;
  # statt
  # One(F)*(Py^2) = One(F)*(Px^3 + a4*Px + a6);
  # mit quadratischer reziprozitaet:
  # Random Px in F
  # Berechne Pysq := Px^3 + a4*Px + a6
  # Check ob Pysq quadratischer Rest mod p sein kann
  # Dies liefert die Legendre-Funktion
  # Falls nein, neues Px
  # Falls ja (und p mod 4 = 3), ist
  # Py = Pysq^(1/2)
  # = +/- Pysq^( (p+1)/4 ) mod p;
  #
  repeat
    Px := Int( Random( F ) );
    Pysq := Int( One(F)*(fex( Px, 3, p ) + a4*Px + a6) );
  until Legendre( Pysq, p ) = 1;
  # Pysq is a square mod p
  Py := fex( Pysq, Int((p+1)/4), p );
  # Py := RootMod( Pysq, p );
  P := [ One(F)*Px, One(F)*Py ];
  if not ellipse_membership( P, a4, a6, F, p ) then
    Error("Point does not lie on curve.\n");
  fi;
  return P;
end;
```

Listing 2: ElGamalECWithGivenEllipticCurve

```
ElGamalECWithGivenEllipticCurve := function( a4, a6, p, q )
  local F, k, P, n, Q, key;
  F := HomalgRingOfIntegers( p );
  ## assume that q = group order
  ## find point P with order n | q.
  # Assume q = order of the elliptic curve
  if IsPrime( q ) then
    n := q;
  else
    Error( "Can't calculate order of point P\n" );
  fi;
  P := PointOnEllipticCurve( a4, a6, F, p );
  k := Random( 2, q-2 );
  Q := ftimes( k, P, a4, a6, F, p );
  key := rec();
  key.public := [ Int(a4), Int(a6), p,
    List( P, Int ), n, List( Q, Int ) ];
  key.private := k;
```

```
  return key;
end;
```

Listing 3: `ftimes`

```
ftimes := function( n, P, a4, a6, F, p )
  local po, no, ao;
  po := 0;
  ao := P;
  no := n;
  while no > 0 do
    if (no mod 2 = 1) then
      po := plus(po, ao, a4, a6, F, p );
    fi;
    ao := double( ao, a4, a6, F, p);
    no := Int( Floor( Float( no/2 ) ) );
  od;
  return po;
end;
```

Listing 4: `Blatt7A2`

```
Read( Concatenation(GAPInfo.RootPaths[1],"pkg/Krypto/gap/
   EllipticCurve.g"));

a4 := 2971905224466079395684815679494289029216133291 52;
a6 := 1732456494501728912082472830534951985386718 08088;
p := 1332297598440044874827085558802491743757193798159;
q := 1332297598440044874827085038830181364212942568457;

F := HomalgRingOfIntegers( p );
key := ElGamalECWithGivenEllipticCurve( a4, a6, p, q );
Print( key.public );
```

8 Übung 8

8.1 Aufgabe 1

Diffie-Hellman Key exchange:

Example
```
gap> c := (2^400) mod 467;
137
gap> d := (2^134) mod 467;
84
gap> (c^134) mod 467;
90
gap> (d^400) mod 467;
90
```

Das gemeinsame Geheimnis ist

$$c^s = (a^r \bmod p)^s \bmod p \qquad = (a^s \bmod p)^r \bmod p = a^{rs} \bmod p \qquad = d^r$$

8.2 Aufgabe 3

$$\mathrm{HMAC}_{h,k}(m) = h((k \oplus opad)||h((k \oplus ipad)||m)) \tag{11}$$

$$\begin{aligned}
h &= \mathrm{MD5} \\
k &= 9A45B7FE149BCE60 \\
(k)_2 &= 1001101001000101101101111111111000010100100110111100111001100000 \\
opad &= 010111000101110001011100... \\
k \oplus opad &= 1100011000011001111010111010001001001000110001111001001000111100 \\
ipad &= 001101100011011000110110001101 10... \\
k \oplus ipad &= 1010110001110011100000011100100000100010101011011111100001010110 \\
(k \oplus ipad)_{16} &= AC7381C822ADF856 \\
(m)_{16} &= 000102030405060708090A0B0C0D0E0F \\
(k \oplus ipad)||m &= AC7381C822ADF856000102030405060708090A0B0C0D0E0F \\
(X)_{16} &:= \mathrm{MD5}((k \oplus ipad)||m) \\
&= 0898721134D8E73D7F0209244CFC733F \\
(k \oplus opad)_{16} &= C619EBA248C7923C \\
(Y)_{16} &:= (k \oplus opad)_{16}||X_{16} \\
&= C619EBA248C7923C0898721134D8E73D7F0209244CFC733F \\
\mathrm{HMAC}_{\mathrm{MD5},k}(m) &= \mathrm{MD5}(Y_{16}) \\
&= A4167961D793AE17467720AB1C636951
\end{aligned}$$

8.3 Aufgabe 5

$$\mathbb{Z}_{11}$$
$$(t, n) = (3, 4)$$

$$\begin{aligned}(x_1, y_1) &= (1, 8)\\ (x_2, y_2) &= (4, 8)\\ (x_3, y_3) &= (6, 5)\end{aligned}$$

$$I = \{1, 2, 3\}.$$

$$s = \sum_{i=1}^{3} y_i \prod_{\substack{j \in I \\ j \neq i}} x_j \left(x_j - x_i\right)^{-1} \tag{12}$$

Mit den Werten für x_i und y_i von oben:

$$\begin{aligned}s = {} & 8 \cdot (4 \cdot (4-1)^{-1} \cdot 6 \cdot (6-1)^{-1})\\ & +8 \cdot (1 \cdot (1-4)^{-1} \cdot 6 \cdot (6-4)^{-1})\\ & +5 \cdot (1 \cdot (1-6)^{-1} \cdot 4 \cdot (4-6)^{-1})\\ = {} & 8 \cdot (4 \cdot 3^{-1} \cdot 6 \cdot 5^{-1})\\ & +8 \cdot (1 \cdot (-3)^{-1} \cdot 6 \cdot 2^{-1})\\ & +5 \cdot (1 \cdot (-5)^{-1} \cdot 4 \cdot (-2)^{-1})\\ \equiv {} & (-1) \cdot 6 \cdot 4^{-1} + 4 \cdot (-6)^{-1} + (-2) \cdot (-1)^{-1}\\ \equiv {} & -7 + 3 + 2\\ \equiv {} & 9\end{aligned}$$

9 Übung 9

9.1 Aufgabe 4

(i) Längenpolynom $p(X) = X + 3X^3 + 3X^4$: Summe der Koeffizienten ist 7, d.h. wir wollen 7 Zeichen abbilden, d.h. $\Sigma = \{0, 1, 2, 3, 4, 5, 6\}$.

$$\begin{aligned}
0 &\to 0\\
1 &\to 1\underline{\quad}\\
2 &\to 1\underline{\quad}\\
3 &\to 1\underline{\quad}\\
4 &\to 1\underline{\quad}\text{\textvisiblespace}\\
5 &\to 1\underline{\quad}\text{\textvisiblespace}\\
6 &\to 1\underline{\quad}\text{\textvisiblespace}
\end{aligned}$$

Für 0 wählt man 0 als einzelnes Zeichen aus. Das legt das Anfangszeichen für $1, 2, 3, 4, 5, 6$ schon auf 1 fest. Für $1, 2, 3$ wählt man aus $00, 01, 10, 11$ drei Kombinationen $\underline{\quad}$ aus, dann bleibt die vierte $\underline{\quad}$ übrig für $4, 5, 6$. Weil hiermit aber schon 3 von 4 Zeichen vergeben sind, kann man die drei Zeichen $4, 5, 6$ nur noch an dem letzten Bit $\text{\textvisiblespace}$ unterscheiden 0 oder 1, was aber unmöglich ist.

(ii) Längenpolynom $p(X) = 3X^2 + 3X^4 + X^5$: Summe der Koeffizienten ist 7, d.h. wir wollen 7 Zeichen abbilden, d.h. $\Sigma = \{0, 1, 2, 3, 4, 5, 6\}$.

$$\begin{aligned}
0 &\to 00\\
1 &\to 01\\
2 &\to 10\\
3 &\to 1100\\
4 &\to 1101\\
5 &\to 1110\\
6 &\to 11110
\end{aligned}$$

Hier funktioniert es, für $0, 1, 2$ aus $00, 01, 10, 11$ drei Kombinationen auszuwählen, und die letzte 11 für $3, 4, 5, 6$ zu lassen. Das iteriert man, und an das letzte Zeichen setzt man noch eine 0 an, was aber unnötig ist, da sich 1110 und 1111 sowieso schon an der letzten Stelle unterscheiden. Der Kode mit diesem Längenpolynom ist also nicht optimal, da sich (unabhängig von der Verteilung) ein kürzerer Kode finden lässt, indem man die 0 bei der 6 weglässt.

9.2 Aufgabe 5

b)

$$\begin{aligned}
p &= (p_0, p_1, p_2, p_3)\\
0 &\leq p_3 \leq p_2 \leq p_1 \leq p_0\\
\sum_{i=1}^{4} p_i &= 1
\end{aligned}$$

Einige Beispiele: (i)

$$p = (1, 0, 0, 0)$$

Dazu reicht ein Code $g : \Sigma \to \mathbb{Z}_2^+$, der dem Zeichen 0 ein einzelnes Zeichen zuordnet, und den restlichen drei Zeichen irgendwelche, beliebig lange, unterschiedliche Zeichen, z.B. der aus (a) mit Längenpolynom $X + X^2 + 2X^3$:

$$\begin{aligned}0 &\to 0\\ 1 &\to 11\\ 2 &\to 101\\ 3 &\to 100\end{aligned}$$

Die Länge von $g(1), g(2), g(3)$ spielt für den Erwartungswert keine Rolle, weil die Wahrscheinlichkeiten 0 sind, und es gilt

$$\mathrm{E}(|g(X_{p,1})|) = |g(0)| \cdot 1 + |g(1)| \cdot 0 + |g(2)| \cdot 0 + |g(3)| \cdot 0 = |g(0)| = 1.$$

(ii)

$$p_0 = \frac{1}{2}$$

Wir vergleichen den Erwartungswert $E(|h_{(1,1,2)}|)$ des optimalen Codes h mit Längenvektor $(1, 1, 2)$ mit dem Erwartungswert $E(|h'_{(0,4)}|)$ des optimalen Codes h' mit Längenvektor $(0, 4)$:

$$\begin{aligned}E(|h_{(1,1,2)}|) &= \frac{1}{2}|h(0)| + p_1|h(1)| + p_2|h(2)| + p_3|h(3)|\\ &= \frac{1}{2} \cdot 1 + p_1 \cdot 2 + (p_2 + p_3) \cdot 3\\ &\leq \frac{1}{2} + (p_1 + p_2 + p_3) \cdot 3\\ &= \frac{1}{2} + (1 - \frac{1}{2}) \cdot 3\\ &= \frac{1}{2} + \frac{3}{2} = \frac{4}{2}\\ &= 2 = \frac{1}{2} \cdot 2 + (1 - \frac{1}{2}) \cdot 2 = E(|h'_{(0,4)}|)\end{aligned}$$

Bei $p_0 = \frac{1}{2}$ ist also $E(|h_{(1,1,2)}|) \leq E(|h'_{(0,4)}|)$, d.h. der Kode mit dem Längenpolynom $(0, 1, 1, 2)$ ist sicher optimal.

(iii) Im Fall von $p_0 > \frac{1}{2}$ gilt $1 - p_0 < \frac{1}{2}$. Mit der Abschätzung $p_1 \cdot 2 \leq p_1 \cdot 3$ lösen wir nach p_0 auf:

$$\begin{aligned}p_0 + (1 - p_0) \cdot 3 &< 2\\ p_0 + 3 - 3p_0 &< 2\\ -2p_0 &< -1\\ p_0 &> \frac{1}{2}\end{aligned}$$

Also gilt $E(|h_{(1,1,2)}|) \leq E(|h'_{(0,4)}|)$ für alle $p_0 \geq \frac{1}{2}$.

Wenn nun das erste Zeichen "0" weniger als die Hälfte auftritt (aber trotzdem am häufigsten), brauchen wir vielleicht weitere Kriterien an p_1, p_2, p_3.

(iv)

$$p_1 \leq p_0 < \frac{1}{2} \Rightarrow 1 - 2p_0 > 0$$

Diesmal ohne die zu scharfe Abschätzung für p_1:

$$\begin{aligned} p_0\big|h(0)\big| + p_1\big|h(1)\big| + (1-p_0-p_1)\cdot 3 &< 2 \\ \Leftrightarrow 3 - 2p_0 - p_1 &< 2 \\ \Leftrightarrow -2p_0 - p_1 &< -1 \\ \Leftrightarrow -p_1 &< -1 + 2p_0 \\ \Leftrightarrow p_1 &> 1 - 2p_0 \end{aligned}$$

Also haben wir für p_1 die neue Bedingung:

$$p_0 \geq p_1 > 1 - 2p_0 > 0$$

D.h. der Kode mit Längenpolynom $(1,1,2)$ ist optimal falls $p_0 \in \left[\frac{1}{2}, 1\right]$ oder $p_0 \in \left(0, \frac{1}{2}\right)$ und $p_1 \in \left(1 - 2p_0, p_0\right]$. Der Fall $p_0 = \frac{1}{3} = p_1$ und damit $p_2 + p_3 = 1 - p_0 - p_1 = \frac{1}{3}$ ergibt immer noch

$$p_0\big|h(0)\big| + p_1\big|h(1)\big| + (1-p_0-p_1) = \frac{1}{3}\cdot 1 + \frac{1}{3}\cdot 2 + \frac{1}{3}\cdot 3 = \frac{1}{3} + \frac{2}{3} + 1 = 2$$

Für Werte $p_0 < \frac{1}{3}$ und $p_1 < \frac{1}{3}$ ist der Kode mit Längenpolynom $(1,1,2)$ nicht mehr optimal. Das kann man auch an der Grafik unten ablesen.

(v)

$$p_3 \leq p_2 \leq p_1 < 1 - 2p_0 > 0$$

Da $\big|h(2)\big| = \big|h(3)\big| = 3$, ist die genaue Verteilung zwischen p_2 und p_3 nicht wichtig. Es zählt nur die Summe $p_2 + p_3$, welche wir aber bereits aus $p_2 + p_3 = 1 - p_0 - p_1$ kennen. Der Fall

$$p_1 < 1 - 2p_0$$

muss also nicht weiter behandelt werden: Hier gilt in jedem Fall, dass $E(|h_{(1,1,2)}|) \geq E(|h'_{(0,4)}|)$, also der Kode mit Längenpolynom $4X^2$ optimal ist.

Wir können die Bedingungen an p_0 und p_1 in ein Diagramm zeichnen und die Flächen markieren, in denen jeweils der Kode mit Längenpolynom $X + X^2 + 2X^3$ oder der mit $4X^2$ optimal ist: