

# Zahlentheoretische Methoden in der Kryptographie II

Vorlesungsskript von Arne Winterhof

28. Oktober 2003

Dieses Skript ist die schriftliche Ausarbeitung einer Vorlesung, die ich im Sommersemester 2002 an der Universität Wien gehalten haben.

Arne Winterhof

# Inhaltsverzeichnis

<b>1</b>	<b>Motivation</b>	<b>1</b>
1.1	Grundbegriffe . . . . .	1
1.2	Der Diffie-Hellman Schlüsselaustausch . . . . .	2
1.3	Das RSA-Verfahren . . . . .	2
1.4	Algorithmen zur Berechnung des diskreten Logarithmus . . . . .	3
<b>2</b>	<b>Endliche Körper</b>	<b>6</b>
2.1	Charakterisierung . . . . .	6
2.2	Konstruktion endlicher Körper . . . . .	8
2.3	Spur und Norm . . . . .	10
2.4	Konstruktion irreduzibler Polynome . . . . .	12
2.5	Ein schneller Algorithmus zur Berechnung des diskreten Logarithmus in endlichen Körpern . . . . .	14
<b>3</b>	<b>Das XTR Public-Key Kryptosystem</b>	<b>17</b>
3.1	Grundlagen . . . . .	17
3.2	Polynome der Form $X^3 - cX^2 + c^pX - 1$ . . . . .	18
3.3	Der XTR-Diffie-Hellman Schlüsselaustausch . . . . .	21
<b>4</b>	<b>Elliptische Kurven</b>	<b>23</b>
4.1	Definition und Gruppenstruktur . . . . .	23
4.2	Die Anzahl der Punkte einer elliptischen Kurve . . . . .	27
<b>5</b>	<b>Polynomdarstellungen des diskreten Logarithmus</b>	<b>31</b>
5.1	Der XTR diskrete Logarithmus . . . . .	31
5.2	Der elliptische Kurven diskrete Logarithmus . . . . .	32
<b>6</b>	<b>Primzahltest und Faktorisierung mit elliptischen Kurven</b>	<b>34</b>
6.1	Primzahltest . . . . .	34
6.2	Faktorisierung . . . . .	36

# Kapitel 1

## Motivation

### 1.1 Grundbegriffe

**Klartext:** Nachricht, die übermittelt werden soll.

**Chiffretext:** verschlüsselte Nachricht.

**Schlüssel:** Informationsträger für die Verschlüsselung des Klartextes bzw. die Entschlüsselung des Chiffretextes.

**Alphabet:** Menge von "Zeichen", aus denen die Nachricht besteht.

**Nachrichtenblock:** ein einzelnes Zeichen, ein Zeichenpaar, Zeichentripel oder allgemein ein  $n$ -Tupel von Zeichen.

**Verschlüsselungsabbildung:** Abbildung  $f$  von der Menge aller Klartext-Nachrichtenblöcke  $\mathcal{P}$  in die Menge aller Chiffretextblöcke  $\mathcal{C}$ .

**Entschlüsselungsabbildung:** Abbildung  $f^{-1}$ , die aus dem Chiffretext den Klartext wieder herstellt.

**Kryptosystem:**  $\mathcal{P} \xrightarrow{f} \mathcal{C} \xrightarrow{f^{-1}} \mathcal{P}$ .

**Beispiel:** (Lineare Substitutionschiffre)

$$\mathcal{P} = \mathcal{C} = \mathbb{Z}/m\mathbb{Z}$$

$$f(x) \equiv ax + b \pmod{m}, \quad a, b \in \mathbb{Z}, \quad \text{ggT}(a, m) = 1$$

$$f^{-1}(y) \equiv a^{-1}(y - b) \pmod{m}$$

Chiffrierungsschlüssel:  $(a, b)$

Dechiffrierungsschlüssel:  $(a^{-1}, -a^{-1}b)$

**Das Prinzip von Kerckhoffs:** Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung der Art des Kryptosystems abhängen. Die Sicherheit gründet sich nur auf die Geheimhaltung des Schlüssels.

Ab jetzt befassen wir uns mit dem Fall, dass sich zwei Parteien  $A$  und  $B$ , die geheime Nachrichten austauschen möchten, nur über einen offenen Kanal auf einen Schlüssel einigen können (Public-Key Kryptographie).

## 1.2 Der Diffie-Hellman Schlüsselaustausch

1.  $A$  und  $B$  einigen sich auf eine Gruppe  $G$  und ein Element  $a \in G$  (mit großer Ordnung), d. h.  $(a, G)$  ist öffentlich.
2.  $A$  wählt einen persönlichen Schlüssel  $x$  und veröffentlicht  $a^x \in G$ .  
 $B$  wählt einen persönlichen Schlüssel  $y$  und veröffentlicht  $a^y \in G$ .
3.  $A$  berechnet den Schlüssel  $K = (a^y)^x \in G$ .  
 $B$  berechnet den Schlüssel  $K = (a^x)^y \in G$ .

Die Sicherheit des Diffie-Hellman Schlüsselaustausches beruht auf der Unangreifbarkeit des diskreten Logarithmus Problems:

Bestimme zu gegeben  $n \in \langle a \rangle \leq G$  den Exponenten  $0 \leq x \leq \text{ord}(a) - 1$  mit  $n = a^x$ . Die Zahl  $x$  heißt *diskreter Logarithmus* (oder *Index*) von  $n$  zur Basis  $a$  und wird mit  $\text{ind}_a(n)$  bezeichnet.

In der Praxis werden für  $G$  folgende Gruppen verwendet:

- Die Gruppe  $\mathbb{F}_p^*$  der primen Restklassen modulo einer Primzahl  $p$ .
- Die multiplikative Gruppe  $\mathbb{F}_{2^r}^*$  eines endlichen Erweiterungskörpers von  $\mathbb{F}_2$  vom Grad  $r$ .
- Die Gruppe der Punkte einer elliptischen Kurve über einem endlichen Körper.
- A. Lenstra und E. Verheul schlugen 1999 eine Modifikation des Diffie-Hellman Schlüsselaustausches für endliche Erweiterungskörper von  $\mathbb{F}_p$  vom Grad 6 vor, die XTR genannt wird.

## 1.3 Das RSA-Verfahren

**RSA Schlüsselerzeugung:**

$A$  macht folgendes:

1. Erzeuge zwei große Primzahlen  $p$  und  $q$  von etwa derselben Größe.
2. Berechne  $n = pq$  und  $\varphi(n) = (p - 1)(q - 1)$ .
3. Wähle  $1 < e < \varphi(n)$  mit  $\text{ggT}(e, \varphi(n)) = 1$ .

4. Berechne mit dem Euklidischen Algorithmus  $1 < d < \varphi(n)$ , so dass

$$ed \equiv 1 \pmod{\varphi(n)}.$$

5. Der öffentliche Schlüssel von  $A$  ist  $(n, e)$ , der private ist  $d$ .

**RSA-Verschlüsselung:**

$B$  macht folgendes:

1. Hole den öffentlichen Schlüssel  $(n, e)$  von  $A$ .
2. Stelle die Nachricht  $m$  als Element aus  $\{0, 1, \dots, n - 1\}$  dar.
3. Berechne  $c \equiv m^e \pmod{n}$ .
4. Übermittle  $c$  an  $A$ .

$A$  macht folgendes:

- Berechne mit dem privaten Schlüssel  $d$  die Nachricht  $c^d \equiv m \pmod{n}$  (nach Euler-Fermat).

**RSA-Annahme:** Sei  $n = pq$ ,  $1 < e < \varphi(n)$  mit  $\text{ggT}(e, \varphi(n)) = 1$  und  $c \in \mathbb{Z}$ , dann kann  $m \in \mathbb{Z}$  mit  $m^e \equiv c \pmod{n}$  (ohne Kenntnis von  $p$  oder  $q$ ) nicht effizient berechnet werden.

*Bemerkung:* Die Sicherheit des RSA-Verfahrens beruht auf der Annahme, dass eine Zahl  $n = pq$  nicht effizient in seine Faktoren  $p$  und  $q$  zerlegt werden kann (*Faktorisierungsproblem*).

## 1.4 Algorithmen zur Berechnung des diskreten Logarithmus

Ein Algorithmus für eine Gruppe  $G$  heißt *generisch*, wenn er nur die Gruppenoperation benutzt. (Z. B. bei  $\mathbb{F}_p^*$  darf der Algorithmus nur Multiplikationen und keine Additionen benutzen.) Wir beschränken uns auf den Fall, dass  $G$  zyklisch ist und von  $g$  erzeugt wird.

*Baby-Step Giant-Step Algorithmus:*

1. Setze  $m = \lceil \sqrt{|G|} \rceil$ .
2. Erstelle eine Tabelle (Baby-Step)

$j$	$0$	$1$	$2$	$\dots$	$m - 1$
$g^j$	$g^0$	$g^1$	$g^2$	$\dots$	$g^{m-1}$

3. Berechne  $g^{-m}$  und setze  $a_0 = a$ .
4. Für  $i = 0, \dots, m - 1$ 
  - (a) Teste, ob  $a_i$  in der zweiten Zeile der obigen Tabelle steht und lese das zugehörige  $j$  ab.
  - (b) Falls ja, setze  $\text{ind}_g(a) = im + j$ . Stopp.
  - (c) Setze  $a_{i+1} = a_i g^{-m}$  (Giant-Step).

**Satz 1** *Der Baby-Step Giant-Step Algorithmus berechnet den diskreten Logarithmus in  $O(|G|^{1/2})$  Gruppenoperationen.*

*Pohlig-Hellman Algorithmus:*

1. Berechne die Primfaktorzerlegung der Gruppenordnung:  $|G| = p_1^{e_1} \cdots p_r^{e_r}$ .
2. Für  $i = 1, \dots, r$  berechne  $x_i \equiv \text{ind}_g(a) \pmod{p_i^{e_i}}$  (z.B. mit Baby-Step-Giant-Step).
3. Bestimme eine gemeinsame Lösung  $0 \leq x \leq |G| - 1$  von  $x \equiv x_i \pmod{p_i^{e_i}}$ ,  $i = 1, \dots, r$  und setze  $\text{ind}_g(a) = x$ .

*Beispiel:*  $\mathbb{F}_{251}^*$ ,  $g = 71$ ,  $a = 210$

1.  $|G| = 250 = 2 \cdot 5^3$
2.  $g^{|G|/2} \equiv 71^{125} \equiv 250 \pmod{251}$ ,  
 $a^{|G|/2} \equiv 210^{125} \equiv 250 \pmod{251}$ ,  
 $x_1 = \text{ind}_{250}(250) = 1$  (Index modulo 2).
3.  $g^{|G|/5} \equiv 71^{50} \equiv 20 \pmod{251}$ ,  
 $a^{|G|/5} \equiv 210^{50} \equiv 149 \pmod{251}$ ,  
 $l_0 = \text{ind}_{20}(149) = 2$  (Index modulo 5),  
 $g^2 \equiv 21 \pmod{251}$ ,  
 $(ag^{-2})^{|G|/25} \equiv 113 \pmod{251}$ ,  
 $l_1 = \text{ind}_{20}(113) = 4$  ( $l_0 + 5l_1$  ist Index modulo 25),  
 $g^{4 \cdot 5} \equiv 115 \pmod{251}$ ,  $g^{22} \equiv 156 \pmod{251}$ ,  
 $(ag^{-22})^{|G|/125} \equiv 149 \pmod{251}$ ,  
 $l_2 = \text{ind}_{20}(149) = 2$  ( $l_0 + 5l_1 + 25l_2$  ist Index modulo 125).
4.  $\text{ind}_{71}(210) \equiv 1 \pmod{2}$ ,  $\text{ind}_{71}(210) \equiv 72 \pmod{125}$ ,  
 $\text{ind}_{71}(210) = 197$ .

**Satz 2** *Ist die Faktorisierung der Gruppenordnung bekannt, so berechnet der Pohlig-Hellman Algorithmus den diskreten Logarithmus in*

$$O\left(\sum_{i=1}^r e_i(\log |G| + \sqrt{p_i})\right)$$

*Gruppenoperationen*

*Forderung:*  $|G|$  sollte einen großen Primteiler haben.

# Kapitel 2

## Endliche Körper

Grundlagen über Gruppen, Ringe, Körper, Polynome und Körpererweiterungen werden als bekannt vorausgesetzt (siehe z. B. Lidl/Niederreiter [5, Kapitel 1]).

### 2.1 Charakterisierung

**Beispiel:**  $\mathbb{F}_p := \{0, 1, \dots, p-1\}$ ,  $p$  Primzahl

$$\begin{aligned} a + b = c & \iff p \text{ teilt } a + b - c, \\ ab = c & \iff p \text{ teilt } ab - c, \end{aligned} \quad a, b, c \in F_p$$

$(\mathbb{F}_p, +, \cdot)$  ist ein endlicher Körper

**Beispiel:**  $\mathbb{F}_5$

$+$	$0$	$1$	$2$	$3$	$4$	$\cdot$	$0$	$1$	$2$	$3$	$4$
$0$	$0$	$1$	$2$	$3$	$4$	$0$	$0$	$0$	$0$	$0$	$0$
$1$	$1$	$2$	$3$	$4$	$0$	$1$	$0$	$1$	$2$	$3$	$4$
$2$	$2$	$3$	$4$	$0$	$1$	$2$	$0$	$2$	$4$	$1$	$3$
$3$	$3$	$4$	$0$	$1$	$2$	$3$	$0$	$3$	$1$	$4$	$2$
$4$	$4$	$0$	$1$	$2$	$3$	$4$	$0$	$4$	$3$	$2$	$1$

**Definition 1** Ist  $\mathbb{K}$  ein Körper und existiert eine natürliche Zahl  $n$  mit  $na = 0$  für alle  $a \in \mathbb{K}$ , dann heißt das kleinste natürliche  $n$  mit dieser Eigenschaft die Charakteristik von  $\mathbb{K}$ . Falls solch ein  $n$  nicht existiert, so habe  $\mathbb{K}$  die Charakteristik 0.

**Lemma 1** Ein endlicher Körper  $\mathbb{K}$  hat Primzahlcharakteristik.

*Beweis:* Sei  $0 \neq a \in \mathbb{K}$ . Da  $\mathbb{K}$  endlich ist, gilt  $n_1 a = n_2 a$  für zwei ganze Zahlen  $0 < n_1 < n_2$  und somit  $(n_2 - n_1)a = 0$ , weswegen  $\mathbb{K}$  Charakteristik  $n > 1$  hat. Wäre  $n = kl$  zusammengesetzt mit  $1 < k, l < n$ , so würde wegen der Existenz von  $k^{-1}$  aus  $na = kla = 0$  im Widerspruch zur Definition der Charakteristik  $la = k^{-1}0 = 0$  folgen.  $\square$

**Lemma 2** Ist  $\mathbb{K}$  ein Körper der Charakteristik  $p$ , so gilt

$$(a + b)^{p^n} = a^{p^n} + b^{p^n} \quad \text{für } a, b \in \mathbb{K}, n \in \mathbb{N}.$$

*Beweis:* Die Binomialkoeffizienten

$$\binom{p}{i} = \frac{p(p-1) \cdots (p-i+1)}{1 \cdot 2 \cdots i}, \quad 0 < i < p,$$

sind ganze Zahlen und da  $p$  prim ist, kann  $p$  nicht weggekürzt werden, so dass  $\binom{p}{i}$  durch  $p$  teilbar ist. Nach dem Binomischen Lehrsatz gilt dann

$$(a + b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} b^i + b^p = a^p + b^p.$$

Induktiv erhalten wir dann für  $n \geq 2$ :

$$(a + b)^{p^n} = (a^p + b^p)^{p^{n-1}} = a^{p^n} + b^{p^n}.$$

□

**Lemma 3** Die Anzahl der Elemente eines endliche Körpers  $\mathbb{K}$  ist eine Primzahlpotenz.

*Beweis:* Jeder endliche Körper besitzt einen kleinsten Unterkörper (*Primkörper*), der isomorph zu  $\mathbb{F}_p$  mit einer Primzahl  $p$  ist.  $\mathbb{K}$  ist also ein endlich dimensionaler Vektorraum über  $\mathbb{F}_p$  der Dimension  $r \geq 1$ , hat also  $p^r$  Elemente. □

**Lemma 4** Ist  $\mathbb{K}$  ein endlicher Körper mit  $q$  Elementen, so gilt  $a^q = a$ ,  $a \in \mathbb{K}$ .

*Beweis:* Für  $a = 0$  ist die Aussage trivial und für  $a \neq 0$  gilt  $a^{q-1} = 1$  nach dem kleinen Fermat. □

**Lemma 5** Ist  $\mathbb{K}$  ein endlicher Körper mit  $q$  Elemente, so hat das Polynom  $X^q - X \in \mathbb{K}[X]$  die Faktorisierung

$$X^q - X = \prod_{a \in \mathbb{K}} (X - a).$$

*Beweis:* Das Polynom  $X^q - X$  hat höchstens  $q$  Nullstellen. Lemma 4 liefert die Nullstellen. Mit Polynomdivision lassen sich die Nullstellen sukzessive abspalten. □

**Satz 3** Zu jeder Primzahlpotenz  $q$  gibt es bis auf Isomorphie genau einen endlichen Körper  $\mathbb{F}_q$ .

*Beweis:* Existenz: Für  $q = p^r$  sei  $\mathbb{K}$  der Zerfällungskörper von  $X^q - X$  über  $\mathbb{F}_p$  (d. h.  $X^q - X = (X - a_1) \cdots (X - a_q)$  mit  $a_1, \dots, a_q \in \mathbb{K}$ ). Dann ist  $S = \{a \in \mathbb{K} \mid a^q = a\}$  ein Unterkörper von  $\mathbb{K}$  wegen

$$(a - b)^q = a^q - b^q = a - b, \quad a, b \in S$$

und

$$(ab^{-1})^q = a^q(b^q)^{-1} = ab^{-1}, \quad a, b \in S \setminus \{0\}.$$

Wegen  $(X^q - X)' = qX^{q-1} - 1 = -1 \neq 0$  hat  $X^q - X$  keine doppelten Nullstellen und es gilt  $|S| = q$ . Außerdem zerfällt  $X^q - X$  über  $S$ , woraus  $S = \mathbb{K}$  folgt.

Eindeutigkeit: Dieses folgt aus der Eindeutigkeit von Zerfällungskörpern.  $\square$

**Satz 4** Die multiplikative Gruppe  $\mathbb{F}_q^*$  eines endlichen Körpers ist zyklisch.

*Beweis:* Sei  $q - 1 = p_1^{r_1} \cdots p_m^{r_m}$  die Primfaktorzerlegung von  $q - 1$ . Die Polynome  $X^{(q-1)/p_i} - 1$  haben höchstens  $(q-1)/p_i < q-1$  Nullstellen in  $\mathbb{F}_q$ ,  $i = 1, \dots, m$ . Sei  $a_i \in \mathbb{F}_q^*$  keine Nullstelle von  $X^{(q-1)/p_i} - 1$  und  $b_i := a_i^{(q-1)/p_i^{r_i}}$ ,  $i = 1, \dots, m$ . Wegen  $b_i^{p_i^{r_i}} = 1$  und  $b_i^{p_i^{r_i-1}} = a_i^{(q-1)/p_i} \neq 1$  ist die Ordnung von  $b_i$  gleich  $p_i^{r_i}$ . Das Element  $b = b_1 \cdots b_m$  hat die Ordnung  $q - 1$ , da sonst  $1 = b^{(q-1)/p_i} = b_1^{(q-1)/p_i} \cdots b_m^{(q-1)/p_i} = b_i^{(q-1)/p_i}$  für ein  $i$  gelten würde. Da die Ordnung  $p_i^{r_i}$  von  $b_i$  aber dann  $(q-1)/p_i$  teilen müsste, erhält man einen Widerspruch.  $\square$

**Definition 2** Ein Element  $a \in \mathbb{F}_q^*$  der Ordnung  $q - 1$  heißt primitives Element.

**Satz 5**  $\mathbb{F}_{q^d}$  ist genau dann ein Unterkörper von  $\mathbb{F}_{q^r}$ , wenn  $d$  ein Teiler von  $r$  ist.

*Beweis:*  $\mathbb{F}_{q^r}$  ist ein Vektorraum über  $\mathbb{F}_{q^d}$  der Dimension  $t$ , weswegen  $q^r = q^{dt}$ . Ist umgekehrt  $d$  ein Teiler von  $r$ , dann ist  $q^d - 1$  ein Teiler von  $q^r - 1$  ( $q^r - 1 = (q^d - 1)(1 + q^d + q^{2d} + \dots + q^{(r/d-1)d})$ ) und daher  $X^{q^d} - X$  ein Teiler von  $X^{q^r} - X$ . (Mit  $n = q^r - 1$  und  $m = q^d - 1$  gilt  $X(X^n - 1) = X(X^m - 1)(1 + X^m + X^{2m} + \dots + X^{(n/m-1)m})$ .) Der Zerfällungskörper von  $X^{q^d} - X$  über  $\mathbb{F}_q$ , d. h.  $\mathbb{F}_{q^d}$ , ist daher ein Teilkörper von  $\mathbb{F}_{q^r}$ .  $\square$

*Beispiel:*  $\mathbb{F}_{q^{12}}$  hat die Unterkörper  $\mathbb{F}_q, \mathbb{F}_{q^2}, \mathbb{F}_{q^3}, \mathbb{F}_{q^4}, \mathbb{F}_{q^6}, \mathbb{F}_{q^{12}}$ .

## 2.2 Konstruktion endlicher Körper

Für ein Polynom  $f(X) \in \mathbb{F}_q[X]$  sei  $\mathbb{F}_q[X]/(f(X))$  die Menge der Polynome vom Grad kleiner als  $\text{grad}(f)$  mit den Operationen

$$\begin{aligned} g_1(X) + g_2(X) = g_3(X) & \iff f(X) \text{ teilt } g_1(X) + g_2(X) - g_3(X), \\ g_1(X)g_2(X) = g_3(X) & \iff f(X) \text{ teilt } g_1(X)g_2(X) - g_3(X), \end{aligned}$$

$g_1(X), g_2(X), g_3(X) \in \mathbb{F}_q[X]/(f(X))$ .

**Lemma 6**  $\mathbb{F}_q[X]$  ist ein Hauptidealring und für  $f(X) \in \mathbb{F}_q[X]$  ist  $\mathbb{F}_q[X]/(f(X))$  genau dann ein Körper, wenn  $f(X)$  irreduzibel ist.

*Beweis:*  $\mathbb{F}_q[X]$  ist ein Euklidischer Ring (Polynomdivision) und jeder Euklidische Ring ist ein Hauptidealring ( $(f(X), g(X)) = (\text{ggT}(f(X), g(X)))$ ).

$\mathbb{F}_q[X]/(f(X))$  ist offensichtlich ein kommutativer Ring mit 1.

Ist  $f(X) = g(X)h(X)$  reduzibel, so ist  $\mathbb{F}_q[X]/(f(X))$  nicht nullteilerfrei und daher kein Körper. Ist  $f(X)$  irreduzibel, so ist das Ideal  $(f(X))$  maximal.  $(f(X)) \subset (g(X)) \iff g(X)$  teilt  $f(X)$ , also  $g(X) = \text{const}$ , d.h.  $(g(X)) = \mathbb{F}_q[X]$ , oder  $g(X) = \text{const}f(X)$ , d.h.  $(g(X)) = (f(X))$ . Sei  $a(X) \notin (f(X))$ , so ist  $J = \{a(X)r(X) + m(X) \mid r(X) \in \mathbb{F}_q[X], m(X) \in (f(X))\}$  ein Ideal, also  $J = \mathbb{F}_q[X]$ . Somit existieren  $r(X)$  und  $m(X)$  mit  $a(X)r(X) + m(X) = 1$ , also  $a(X)^{-1} \in \mathbb{F}_q[X]/(f(X))$ .  $\square$

*Beispiel:*  $X^3 + X + 1$  ist irreduzibel über  $\mathbb{F}_2$  und  $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3 + X + 1) = \{a + bX + cX^2 \mid a, b, c \in \mathbb{F}_2\}$  ist ein Körper. Die Multiplikationsregel lautet:

$$(a + bX + cX^2)(d + eX + fX^2) = (ad + bf + ce) + (ae + bd + bf + ce + cf)X + (af + be + cd + cf)X^2.$$

**Lemma 7** Ist  $f(X) \in \mathbb{F}_q[X]$  irreduzibel vom Grad  $r$  und  $\alpha$  eine Nullstelle von  $f(X)$ , so ist  $\mathbb{F}_{q^r}$  isomorph zu  $\mathbb{F}_q(\alpha)$ . (Das Element  $\alpha$  heißt dann erzeugendes Element von  $\mathbb{F}_{q^r}$  über  $\mathbb{F}_q$ .)

*Beweis:*  $\varphi : \mathbb{F}_q[X]/(f(X)) \rightarrow \mathbb{F}_q(\alpha)$ ,  $\varphi(g(X)) = g(\alpha)$ , ist ein Isomorphismus.  $\square$

*Beispiel:* Sei  $\alpha$  eine Nullstelle von  $X^3 + X + 1$  über  $\mathbb{F}_2$ , so gilt  $\mathbb{F}_8 = \mathbb{F}_2(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{F}_2\}$  mit der Multiplikation

$$(a + b\alpha + c\alpha^2)(d + e\alpha + f\alpha^2) = (ad + bf + ce) + (ae + bd + bf + ce + cf)\alpha + (af + be + cd + cf)\alpha^2.$$

**Korollar 1** Ist  $p \equiv 3 \pmod{4}$  und  $i$  eine Nullstelle von  $X^2 + 1$ , so gilt

$$\mathbb{F}_{p^2} = \mathbb{F}_p(i).$$

*Beweis:*  $-1$  ist genau dann quadratischer Rest modulo  $p$ , wenn  $p \equiv 1 \pmod{4}$  ist. Falls  $p \equiv 3 \pmod{4}$ , so hat das Polynom  $X^2 + 1$  keine Nullstelle in  $\mathbb{F}_p$  und ist daher irreduzibel, woraus die Behauptung folgt. (Ein Polynom vom Grad 2 oder 3 ist genau dann irreduzibel, wenn es keine Nullstellen hat. Für Polynome höheren Grades gilt das aber nicht mehr.)  $\square$

**Korollar 2** Ist  $p \equiv 2 \pmod{3}$  und  $\rho$  eine Nullstelle von  $X^2 + X + 1$ , so gilt

$$\mathbb{F}_{p^2} = \mathbb{F}_p(\rho).$$

*Beweis:* Wegen  $\rho^3 = \rho^2\rho = 1$  ist  $\rho$  ein Element der Ordnung 3. Aus  $p \equiv 2 \pmod{3}$  folgt  $\rho^p = \rho^2 \neq \rho$  und daher  $\rho \notin \mathbb{F}_p$ .  $X^2 + X + 1$  besitzt also keine Nullstelle in  $\mathbb{F}_p$  und ist daher irreduzibel, woraus die Behauptung folgt.  $\square$

**Korollar 3** Ist  $p \equiv \pm 3 \pmod{8}$  und  $\alpha$  eine Nullstelle von  $X^2 - 2$ , so gilt

$$\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha).$$

*Beweis:* Nach dem quadratischen Ergänzungssatz ist 2 genau dann quadratischer Nichtrest modulo  $p$ , wenn  $p \equiv \pm 3 \pmod{8}$ .  $\square$

**Korollar 4** Ist  $a$  ein quadratischer Nichtrest modulo  $p$  und  $\alpha$  eine Nullstelle von  $X^2 - a$ , so gilt

$$\mathbb{F}_{p^2} = \mathbb{F}_p(\alpha).$$

*Beispiel:*  $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{3}) \iff p \equiv \pm 5 \pmod{12}$ .

**Satz 6** Addition und Subtraktion in  $\mathbb{F}_{p^r}$  benötigen  $O(r)$   $\mathbb{F}_p$ -Additionen bzw. Subtraktionen, d.h.  $O(r \log p)$  Bitoperationen.

Multiplikation und Division in  $\mathbb{F}_{p^r}$  benötigen  $O(r^2)$   $\mathbb{F}_p$ -Operationen, d.h.  $O(r^2 \log^2 p)$  Bitoperationen.

*Beweis:* Zwei Elemente aus  $\mathbb{F}_{p^r} = \mathbb{F}_p[X]/(f(X))$  können als Polynome über  $\mathbb{F}_p$  vom Grad kleiner  $r$  aufgefasst werden. Addition und Subtraktion werden Koeffizientenweise durchgeführt. Bei der Multiplikation werden zunächst die Polynome miteinander multipliziert und anschließend modulo  $f(X)$  reduziert. Dividiert wird mit Hilfe des Euklidischen Algorithmus für Polynome.  $\square$

*Beispiel:*  $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$ , gesucht:  $X^{-1}$   
 $X^2 + X + 1 = X(X + 1) + 1 \iff 1 = X^2 + X + 1 - X(X + 1)$   
 $\implies X^{-1} = (X + 1) \in \mathbb{F}_4$

## 2.3 Spur und Norm

**Definition 3**

$$\text{Sp}_{q^r|q} : \mathbb{F}_{q^r} \rightarrow \mathbb{F}_q, \quad \text{Sp}_{q^r|q}(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \dots + \alpha^{q^{r-1}}.$$

$$\text{Nm}_{q^r|q} : \mathbb{F}_{q^r} \rightarrow \mathbb{F}_q, \quad \text{Nm}_{q^r|q}(\alpha) = \alpha \cdot \alpha^q \cdot \alpha^{q^2} \cdot \dots \cdot \alpha^{q^{r-1}} = \alpha^{(q^r-1)/(q-1)}.$$

**Satz 7** Ist  $f(X) = X^r + a_{r-1}X^{r-1} + \dots + a_1X + a_0$  irreduzibel über  $\mathbb{F}_q$  und sei  $\alpha$  eine Nullstelle von  $f(X)$ , dann gilt

$$f(X) = (X - \alpha)(X - \alpha^q) \cdots (X - \alpha^{q^{r-1}})$$

und daher

$$a_{r-1} = -\text{Sp}_{q^r|q}(\alpha) \quad \text{und} \quad a_0 = (-1)^r \text{Nm}_{q^r|q}(\alpha).$$

*Beweis:* Aus  $f(\alpha) = 0$  folgt  $f(\alpha^{q^i}) = \alpha^{q^i r} + a_{r-1}\alpha^{q^i(r-1)} + \dots + a_1\alpha^{q^i} + a_0 = (\alpha^r + a_{r-1}\alpha^{r-1} + \dots + a_1\alpha + a_0)^{q^i} = f(\alpha)^{q^i} = 0$ ,  $i = 1, \dots, r-1$ . Die Elemente  $\alpha^{q^i}$  sind paarweise verschieden, da sonst  $\alpha = \alpha^{q^j}$  für ein  $0 < j < r$  und somit  $\alpha \in \mathbb{F}_{q^j}$ .  $\square$

**Lemma 8**

$$\text{Sp}_{q^r|q}(\alpha^q) = \text{Sp}_{q^r|q}(\alpha), \quad \alpha \in \mathbb{F}_{q^r};$$

$$\text{Sp}_{q^r|q}(a) = ra, \quad a \in \mathbb{F}_q;$$

*Die Spur ist surjektiv;*

$$\text{Sp}_{q^r|q}(\gamma) = 0 \text{ genau dann, wenn } \gamma = \alpha^q - \alpha \text{ für ein } \alpha \in \mathbb{F}_{q^r}.$$

*Beweis:* Die ersten beiden Aussagen sind trivial.

Es gilt  $\text{Sp}_{q^r|q}(\alpha) = c$  genau dann, wenn  $\alpha$  Nullstelle des Polynoms  $f_c(X) = X + X^q + \dots + X^{q^{r-1}} - c$  ist. Jedes dieser  $q$  Polynome hat höchstens  $q^{r-1}$  Nullstellen. Da jedes der  $q^r$  Elemente  $\alpha \in \mathbb{F}_{q^r}$  Nullstelle genau eines dieser Polynome ist, hat jedes  $f_c(X)$  genau  $q^{r-1}$  Nullstellen.

Nach der ersten Aussage des Lemmas gilt  $\text{Sp}_{q^r|q}(\alpha^q - \alpha) = 0$ . Sei umgekehrt  $\text{Sp}_{q^r|q}(\gamma) = 0$  und  $\alpha$  eine Nullstelle von  $X^q - X - \gamma$ . Wir müssen  $\alpha \in \mathbb{F}_{q^r}$ , d.h.  $\alpha^{q^r} = \alpha$ , zeigen:

$$\begin{aligned} 0 &= \text{Sp}_{q^r|q}(\gamma) = \gamma + \gamma^q + \dots + \gamma^{q^{r-1}} \\ &= (\alpha^q - \alpha) + (\alpha^{q^2} - \alpha^q) + \dots + (\alpha^{q^r} - \alpha^{q^{r-1}}) = \alpha^{q^r} - \alpha. \end{aligned}$$

$\square$

**Lemma 9**

$$\text{Nm}_{q^r|q}(\alpha) = 0 \text{ genau dann, wenn } \alpha = 0;$$

$$\text{Nm}_{q^r|q}(\alpha^q) = \text{Nm}_{q^r|q}(\alpha), \quad \alpha \in \mathbb{F}_{q^r};$$

$$\text{Nm}_{q^r|q}(a) = a^r, \quad a \in \mathbb{F}_q;$$

*Die Norm ist surjektiv;*

$$\text{Nm}_{q^r|q}(\gamma) = 1 \text{ genau dann, wenn } \gamma = \alpha^{q-1}, \alpha \in \mathbb{F}_{q^r}.$$

*Beweis:* Die ersten drei Aussagen sind trivial. Für  $c \in \mathbb{F}_q^*$  gilt  $\text{Nm}_{q^r|q}(\alpha) = c$  genau dann, wenn  $\alpha$  Nullstelle von  $f_c(X) = X^{(q^r-1)/(q-1)} - c$  ist.  $f_c(X)$  hat höchstens  $(q^r - 1)/(q - 1)$  Nullstellen. Jedes der  $q^r - 1$  Elemente  $\alpha \in \mathbb{F}_{q^r}^*$  ist Nullstelle genau eines  $f_c(X)$ , weswegen  $f_c(X)$  genau  $(q^r - 1)/(q - 1)$  Nullstellen besitzt.

Es gilt  $\text{Nm}_{q^r|q}(\gamma) = \gamma^{(q^r-1)/(q-1)} = 1$  genau dann, wenn  $\gamma = \omega^{a(q-1)}$ , wobei  $\omega$  ein primitives Element von  $\mathbb{F}_{q^r}$  ist.  $\square$

## 2.4 Konstruktion irreduzibler Polynome

Nach Abschnitt 2.2 ist die Suche nach irreduziblen Polynomen über  $\mathbb{F}_p$  wesentlich für die Konstruktion endlicher Körper.

### Polynome vom Grad $p^k$

**Lemma 10** Sei  $\gamma \in \mathbb{F}_{p^r}$ . Dann ist das Polynom  $X^p - X - \gamma$  genau dann irreduzibel über  $\mathbb{F}_{p^r}$ , wenn es keine Nullstelle in  $\mathbb{F}_{p^r}$  besitzt.

*Beweis:* Sei  $\alpha$  eine Nullstelle von  $X^p - X - \gamma$ . Die Nullstellen von  $X^p - X$  sind genau die Elemente von  $\mathbb{F}_p$ . Daher sind die Nullstellen von  $X^p - X - \gamma$  genau die Elemente  $\alpha + c$  mit  $c \in \mathbb{F}_p$  und somit

$$X^p - X - \gamma = \prod_{c \in \mathbb{F}_p} (X - \alpha - c).$$

Ist  $\alpha \in \mathbb{F}_{p^r}$ , so auch  $\alpha + c$  und  $X^p - X - \gamma$  ist reduzibel.

Ist umgekehrt  $g(X) = \prod_{i=1, \dots, s} (X - \alpha - c_i) \in \mathbb{F}_{p^r}[X]$  ein nichttrivialer Faktor von  $X^p - X - \gamma$ , so muss der Koeffizient  $-(s\alpha + c_1 + \dots + c_s)$  von  $g(X)$  an der Stelle  $X^{s-1}$  in  $\mathbb{F}_{p^r}$  liegen. Wegen  $0 < s < p$  ist  $s$  invertierbar und somit  $\alpha \in \mathbb{F}_{p^r}$ .  $\square$

**Satz 8** Sei  $\gamma \in \mathbb{F}_{p^r}$ . Dann ist das Polynom  $X^p - X - \gamma$  genau dann irreduzibel über  $\mathbb{F}_{p^r}$ , wenn  $\text{Sp}_{p^r|p}(\gamma) \neq 0$ .

*Beweis:* Nach Lemma 8 haben wir  $\text{Sp}_{p^r|p}(\gamma) = 0$  genau dann, wenn  $\gamma = \alpha^p - \alpha$  mit einem  $\alpha \in \mathbb{F}_{p^r}$ , d. h.  $\alpha$  ist eine Nullstelle von  $X^p - X - \gamma$ . Die Behauptung folgt aus Lemma 10.  $\square$

*Bemerkung:* Die Anzahl der Elemente  $\gamma \in \mathbb{F}_{p^r}$  mit  $\text{Sp}_{p^r|p}(\gamma) \neq 0$  ist  $p^r(1 - 1/p) \geq p^r/2$ .

**Korollar 5** Für  $a \in \mathbb{F}_p^*$  ist das Polynom  $X^p - X - a$  irreduzibel über  $\mathbb{F}_p$ .

*Beispiel:*  $X^2 + X + 1$  ist irreduzibel über  $\mathbb{F}_2$  und somit  $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$  mit einer Nullstelle  $\alpha$  von  $X^2 + X + 1$ .

$X^2 + X + \alpha$  ist irreduzibel über  $\mathbb{F}_4$  und somit  $\mathbb{F}_{16} = \mathbb{F}_4(\beta)$  mit einer Nullstelle  $\beta$  von  $X^2 + X + \alpha$ .

$X^2 + X + \alpha\beta$  ist irreduzibel über  $\mathbb{F}_{16}$  und somit  $\mathbb{F}_{256} = \mathbb{F}_{16}(\gamma)$  mit einer Nullstelle  $\gamma$  von  $X^2 + X + \alpha\beta$ .

$(X - \gamma)(X - \gamma^2)(X - \gamma^4)(X - \gamma^8)(X - \gamma^{16})(X - \gamma^{32})(X - \gamma^{64})(X - \gamma^{128}) = X^8 + X^6 + X^5 + X^4 + X^3 + X + 1$  ist irreduzibel über  $\mathbb{F}_2$

## Polynome mit einem Grad, der $q - 1$ teilt

**Satz 9** Ist  $\omega$  ein primitives Element von  $\mathbb{F}_q$  und  $t$  ein Teiler von  $q - 1$ , so ist das Polynom  $X^t - \omega$  irreduzibel über  $\mathbb{F}_q$ .

*Beweis:* Sei  $\alpha$  eine Nullstelle von  $X^t - \omega$ . Wegen  $t|(q-1)$  gilt  $t|(1+q+q^2+\dots+q^{t-1})$ ,  $\alpha^{q^t-1} = (\alpha^{t(q-1)})^{(1+q+q^2+\dots+q^{t-1})/t} = (\omega^{q-1})^{(1+q+q^2+\dots+q^{t-1})/t} = 1$  und somit  $\alpha \in \mathbb{F}_{q^t}$ . Ist  $\alpha \in \mathbb{F}_{q^d}$  mit  $d|t$ , so gilt  $1 = \alpha^{q^d-1} = \omega^{(q^d-1)/t}$  und somit  $(q-1)|(q^d-1)/t$  bzw.  $t|(q^d-1)/(q-1) = 1+q+\dots+q^{d-1}$ . Wegen  $t|(q-1)$  folgt  $t|d$  und  $d=t$ . Daher gilt  $\mathbb{F}_{q^t} = \mathbb{F}_q(\alpha) = \mathbb{F}_q[X]/(X^t - \omega)$  und  $X^t - \omega$  ist irreduzibel.  $\square$

*Beispiel:* Sei  $\alpha$  eine Nullstelle des über  $\mathbb{F}_2$  irreduziblen Polynoms  $X^2 + X + 1$ , also  $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ . Dann ist  $\alpha$  auch ein primitives Element von  $\mathbb{F}_4$  und das Polynom  $X^3 - \alpha$  ist irreduzibel über  $\mathbb{F}_4$ . Deshalb ist  $\mathbb{F}_{64} = \mathbb{F}_4(\beta)$  mit einer Nullstelle  $\beta$  von  $X^3 - \alpha$ .

$(X - \beta)(X - \beta^2)(X - \beta^4)(X - \beta^8)(X - \beta^{16})(X - \beta^{32}) = X^6 + X^3 + 1$  ist irreduzibel über  $\mathbb{F}_2$ .

## Polynome von beliebigem Grad

*Induktive Konstruktionsskizze für  $\mathbb{F}_{q^r}$ :*

Wir nehmen an, dass wir  $\mathbb{F}_{q^d}$  für alle  $d < r$  konstruieren können.

Ist  $r$  eine Potenz der Charakteristik von  $\mathbb{F}_q$  oder ein Teiler von  $q - 1$ , so können wir  $\mathbb{F}_{q^r}$  nach den beiden vorherigen Abschnitten konstruieren. Anderenfalls bestimmen wir die Ordnung  $d$  von  $q$  modulo  $r$ , d.h.  $r$  ist ein Teiler von  $q^d - 1$ . Nach Voraussetzung können wir  $\mathbb{F}_{q^d}$  konstruieren und nach dem vorherigen Abschnitt  $\mathbb{F}_{q^{dr}}$ . Ist  $\omega$  ein primitives Element von  $\mathbb{F}_{q^{dr}}$ , so ist  $\xi = \omega^{(q^{dr}-1)/(q^r-1)} = \text{Nm}_{q^{dr}|q^r}(\omega)$  ein primitives Element von  $\mathbb{F}_{q^r}$  und somit  $\mathbb{F}_{q^r} = \mathbb{F}_q(\xi)$ . Das Polynom  $f(X) = \prod_{i=0}^{r-1} (X - \xi^{q^i}) \in \mathbb{F}_q[X]$  ist dann irreduzibel.

*Beispiel:* Konstruktion von  $\mathbb{F}_{2^5}$ :

Die Ordnung von 2 modulo 5 ist 4. Wir können  $\mathbb{F}_{2^4} = \mathbb{F}_2(\alpha, \beta)$  wie im obigen Beispiel konstruieren, wobei  $\alpha$  eine Nullstelle von  $X^2 + X + 1$  und  $\beta$  eine Nullstelle von  $X^2 + X + \alpha$  ist.  $\beta$  ist ein primitives Element von  $\mathbb{F}_{2^4}$  und daher  $X^5 - \beta$  irreduzibel über  $\mathbb{F}_{2^4}$ , d.h.  $\mathbb{F}_{2^{20}} = \mathbb{F}_{2^4}(\gamma) = \mathbb{F}_2(\alpha, \beta, \gamma)$ , wobei  $\gamma$  eine Nullstelle von  $X^5 - \beta$  ist. Für  $\delta := \text{Sp}_{2^{20}|2^5}(\gamma) = \gamma + \alpha\beta\gamma^2 + (\alpha + \alpha\beta)\gamma^4 + (1 + \alpha\beta)\gamma^3$  gilt  $\delta^2 \neq \delta$  und somit  $\mathbb{F}_{2^5} = \mathbb{F}_2(\delta)$ . Somit ist  $(X - \delta)(X - \delta^2)(X - \delta^4)(X - \delta^8)(X - \delta^{16})$  irreduzibel über  $\mathbb{F}_2$ .

*Bemerkung:* Irreduzible Polynome von kleinem Grad können auch durch Probieren gefunden werden.

*Beispiel:* Wir bestimmen alle irreduziblen Polynome vom Grad  $\leq 5$  über  $\mathbb{F}_2$ :

grad= 1:  $X, X + 1$ .

grad= 2:  $X^2 + X + 1$  (alle anderen Polynome vom Grad 2 haben eine Nullstelle 0 oder 1, d.h. sie sind durch  $X$  oder  $X + 1$  teilbar).

grad= 3:  $X^3 + X^2 + 1, X^3 + X + 1$  (alle anderen haben eine Nullstelle).

grad= 4:  $X^4 + X^3 + X^2 + X + 1, X^4 + X^3 + 1, X^4 + X + 1$  ( $X^4 + X^2 + 1 = (X^2 + X + 1)^2$  und alle anderen Polynome haben eine Nullstelle).

grad= 5:  $X^5 + X^2 + 1, X^5 + X^3 + 1, X^5 + X^4 + X^2 + X + 1, X^5 + X^4 + X^3 + X + 1, X^5 + X^3 + X^2 + X + 1, X^5 + X^4 + X^3 + X^2 + 1$  (alle anderen sind entweder durch  $X^2 + X + 1$  teilbar oder haben eine Nullstelle).

## Bestimmung primitiver Elemente

Eingabe: Primzahlpotenz  $q$  und Faktorisierung von  $q - 1 = p_1^{e_1} \cdots p_m^{e_m}$

Ausgabe: ein primitives Element  $\gamma$  von  $\mathbb{F}_q$

1. Wähle (zufällig) ein Element  $\gamma \in \mathbb{F}_q^*$
2. Für  $i = 1, \dots, m$ : Falls  $\gamma^{(q-1)/p_i} = 1$ , dann gehe zu 1.
3.  $\gamma$  ist ein primitives Element von  $\mathbb{F}_q$ .

Bemerkungen: 1. Die Wahrscheinlichkeit, dass ein zufällig gewähltes Element ein primitives Element ist, ist  $\varphi(q-1)/(q-1)$ .

2. Die Korrektheit des Algorithmus folgt aus der Tatsache, dass die Ordnung eines Elementes ein Teiler von  $q-1$  sein muss.

## 2.5 Ein schneller Algorithmus zur Berechnung des diskreten Logarithmus in endlichen Körpern

*Index-Calculus:*

Sei  $\gamma$  ein primitives Element von  $\mathbb{F}_q$  und  $\alpha \in \mathbb{F}_q^*$ . Bestimme  $\text{ind}_\gamma(\alpha)$ .

1. Wähle eine Teilmenge  $S = \{\beta_1, \dots, \beta_t\} \subseteq \mathbb{F}_q^*$ , so dass ein wesentlicher Anteil der Elemente von  $\mathbb{F}_q^*$  als Produkt von Elementen aus  $S$  ausgedrückt werden kann.
2. (a) Wähle (zufällig)  $k$  mit  $0 \leq k \leq q-2$  und berechne  $\gamma^k$ .  
(b) Versuche  $\gamma^k$  als Produkt von Elementen aus  $S$  zu schreiben:

$$\gamma^k = \prod_{i=1}^t \beta_i^{c_i}, \quad c_i \geq 0.$$

Falls dies gelingt, logarithmiere beide Seiten:

$$k \equiv \sum_{i=1}^t c_i \text{ind}_\gamma(\beta_i) \pmod{q-1}. \quad (2.1)$$

- (c) Wiederhole (a) und (b) bis  $t+c$  verschiedene Gleichungen der Form (2.1) erzeugt wurden ( $c$  ist eine kleine natürliche Zahl, so dass das entstandene Gleichungssystem mit hoher Wahrscheinlichkeit eine eindeutige Lösung besitzt).
3. Löse das in 2. erzeugte lineare Gleichungssystem, um  $\text{ind}_\gamma(\beta_i)$ ,  $1 \leq i \leq t$ , zu bestimmen.
4. (a) Wähle (zufällig)  $k$  mit  $0 \leq k \leq q-2$  und berechne  $\alpha\gamma^k$ .  
 (b) Versuche  $\alpha\gamma^k$  als Produkt von Elementen aus  $S$  zu schreiben:

$$\alpha\gamma^k = \prod_{i=1}^t \beta_i^{d_i}, \quad d_i \geq 0.$$

Falls der Versuch nicht gelingt, wähle in (a) ein anderes  $k$ . Anderenfalls ergibt Logarithmieren:

$$\text{ind}_\gamma(\alpha) \equiv \sum_{i=1}^t d_i \text{ind}_\gamma \beta_i - k \pmod{q-1}.$$

*Bemerkungen:*

1. Für  $\mathbb{F}_p$  wählt man als *Faktorbasis*  $S$  die ersten Primzahlen, für  $\mathbb{F}_{2^r} = \mathbb{F}_2[X]/(f(X))$  die Menge aller irreduziblen Polynome von kleinem Grad.
2. Der Index-Calculus Algorithmus berechnet den diskreten Logarithmus in Laufzeit ungefähr  $O(e^{\sqrt{\ln q \ln \ln q}})$  Bitoperationen.

*Beispiel:*

$f(X) = X^7 + X + 1$  ist irreduzibel über  $\mathbb{F}_2$  und daher  $\mathbb{F}_{2^7} = \mathbb{F}_2[X]/(f(X))$ . Das Polynom  $X$  ist ein primitives Element. Wir bestimmen  $\text{ind}_X(X^4 + X^3 + X^2 + X + 1)$ .

1.  $S = \{X, X+1, X^2+X+1, X^3+X+1, X^3+X^2+1\}$  (Menge der über  $\mathbb{F}_2$  irreduziblen Polynome vom Grad  $\leq 3$ .)

2.

$$\begin{aligned} X^{18} &= X^6 + X^4 &= X^4(X+1)^2 \\ X^{105} &= X^6 + X^5 + X^4 + X &= X(X+1)^2(X^3+X^2+1) \\ X^{72} &= X^6 + X^5 + X^3 + X^2 &= X^2(X+1)^2(X^2+X+1) \\ X^{45} &= X^5 + X^2 + X + 1 &= (X+1)^2(X^3+X+1) \\ X^{121} &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 &= (X^3+X+1)(X^3+X^2+1) \end{aligned}$$

$$\begin{aligned}
18 &= 4 + 2\text{ind}_X(X + 1) \\
105 &= 1 + 2\text{ind}_X(X + 1) + \text{ind}_X(X^3 + X^2 + 1) \\
72 &= 2 + 2\text{ind}_X(X + 1) + \text{ind}_X(X^2 + X + 1) \\
45 &= 2\text{ind}_X(X + 1) + \text{ind}_X(X^3 + X + 1) \\
121 &= \text{ind}_X(X^3 + X + 1) + \text{ind}_X(X^3 + X^2 + 1)
\end{aligned}$$

3.  $\text{ind}_X(X + 1) = 7$ ,  $\text{ind}_X(X^2 + X + 1) = 56$ ,  $\text{ind}_X(X^3 + X + 1) = 314$ ,  
 $\text{ind}_X(X^3 + X^2 + 1) = 90$ .

4.  $k = 66$ :

$$\alpha\gamma^k = (X^4 + X^3 + X^2 + X + 1)X^{66} = X^5 + X^3 + X = X(X^2 + X + 1)^2.$$

$$\text{ind}_X(X^4 + X^3 + X^2 + X + 1) = 1 + 2\text{ind}_X(X^2 + X + 1) - 66 = 47.$$

*Bemerkung:*

Betrachtet man eine Untergruppe  $U = \langle \alpha \rangle \leq \mathbb{F}_q^*$  der Ordnung  $l$ , so kann man den Index-Calculus Algorithmus nicht direkt auf die Untergruppe anwenden, sondern man muss Index-Calculus für  $\mathbb{F}_q^*$  benutzen. Für  $U$  hat man nur Quadratwurzelalgorithmen (z.B. Baby-Step Giant-Step). Je nachdem, ob  $\sqrt{l}$  oder  $e^{\sqrt{\ln q \ln \ln q}}$  kleiner ist, ist Baby-Step Giant-Step oder Index-Calculus schneller.

*Beispiel:*

$$e^{\sqrt{\ln q \ln \ln q}} \geq 2^{50} \text{ (gegenüber Index-Calculus sicher)} \Rightarrow q > 2^{320}.$$

$$l^{1/2} \geq 2^{50} \text{ (gegenüber Baby-Step Giant-Step sicher)} \Rightarrow l \geq 2^{100}.$$

Demnach ist  $l$  von der Größe  $q^{1/3}$  geeignet. Z.B. können wir eine Untergruppe der Ordnung ungefähr  $p^2$  in  $\mathbb{F}_{p^6}$  nehmen. Ein Nachteil ist jedoch, dass man mit Elementen von  $\mathbb{F}_{p^6}$  rechnet. Eine Multiplikation benötigt also 36 Multiplikationen in  $\mathbb{F}_p$ . Im folgenden Kapitel wird eine Alternative beschrieben, die diese Anzahl verringert.

# Kapitel 3

## Das XTR Public-Key Kryptosystem

### 3.1 Grundlagen

Sei  $p \equiv 2 \pmod{3}$  eine Primzahl, so dass  $p^2 - p + 1$  einen Primfaktor  $l > 3$  besitzt. Sei  $\gamma$  ein Element von  $\mathbb{F}_{p^6}^*$  der Ordnung  $l$ .

**Lemma 11** *Das Element  $\gamma$  liegt in keinem echten Unterkörper von  $\mathbb{F}_{p^6}$ .*

*Beweis:* Es gilt  $\text{ggT}(p^2 - 1, p^2 - p + 1) = 3$  und  $\text{ggT}(p^3 - 1, p^2 - p + 1) = 1$  und somit  $\text{ggT}(p^2 - 1, l) = \text{ggT}(p^3 - 1, l) = 1$ , da  $l > 3$ . Somit kann nicht  $\gamma^{p^2-1} = 1$  oder  $\gamma^{p^3-1} = 1$  gelten und  $\gamma$  kein Element von  $\mathbb{F}_{p^2}$  oder  $\mathbb{F}_{p^3}$  sein.  $\square$

**Lemma 12** *Für  $p \equiv 2 \pmod{3}$  und  $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_{p^2}$  gilt:*

1. Die Berechnung von  $\alpha_1^p$  ist frei;
2. Die Berechnung von  $\alpha_1^2$  benötigt drei Multiplikationen in  $\mathbb{F}_p$ ;
3. Die Berechnung von  $\alpha_1\alpha_2$  benötigt vier Multiplikationen in  $\mathbb{F}_p$ ;
4. Die Berechnung von  $\alpha_1\alpha_3 - \alpha_2\alpha_3^p$  benötigt vier Multiplikationen in  $\mathbb{F}_p$ .

*Beweis:*  $\mathbb{F}_{p^2} = \{a\alpha + b\alpha^2 \mid a, b \in \mathbb{F}_p\}$  mit  $\alpha^2 + \alpha + 1 = 0$ .

1. Wegen  $\alpha^3 = 1$  gilt  $\alpha^p = \alpha^2$  und deshalb  
 $(a\alpha + b\alpha^2)^p = a\alpha^p + b\alpha^{2p} = a\alpha^2 + b\alpha^4 = b\alpha + a\alpha^2$ .
2.  $(a\alpha + b\alpha^2)^2 = a^2\alpha^2 + 2ab + b^2\alpha = (a^2 - 2ab)\alpha^2 + (b^2 - 2ab)\alpha$ .
3.  $(a\alpha + b\alpha^2)(c\alpha + d\alpha^2) = ac\alpha^2 + ad + bc + bd\alpha = (bd - ad - bc)\alpha + (ac - ad - bc)\alpha^2$ .
4.  $(a\alpha + b\alpha^2)(e\alpha + f\alpha^2) - (c\alpha + d\alpha^2)(f\alpha + e\alpha^2)$   
 $= (e(c - b - d) + f(b - a + d))\alpha + (e(a - b + c) + f(d - a - c))\alpha^2$ .  $\square$

Im folgenden sei

$$\mathrm{Sp}(\alpha) = \mathrm{Sp}_{p^6|p^2}(\alpha) = \alpha + \alpha^{p^2} + \alpha^{p^4}, \alpha \in \mathbb{F}_{p^6}.$$

**Lemma 13** Für  $\alpha = \gamma^i$  mit  $0 \leq i \leq l-1$  gilt

$$\mathrm{Sp}(\alpha) = \alpha + \alpha^{p^{-1}} + \alpha^{-p}.$$

*Beweis:* Wegen  $\alpha^l = (\gamma^l)^i = 1$  und  $l|p^2 - p + 1$  gilt  $\alpha^{p^2} = \alpha^{p^{-1}}$  und  $\alpha^{p^4} = \alpha^{(p^{-1})^2} = \alpha^{p^2 - 2p + 1} = \alpha^{-p}$ .  $\square$

**Lemma 14** Die Nullstellen des Polynoms

$$X^3 - \mathrm{Sp}(\gamma)X^2 + \mathrm{Sp}(\gamma)^p X - 1 \in \mathbb{F}_{p^2}[X] \text{ sind } \gamma, \gamma^{p^2} = \gamma^{p^{-1}} \text{ und } \gamma^{p^4} = \gamma^{-p}.$$

*Beweis:*

$$\begin{aligned} & (X - \gamma)(X - \gamma^{p^{-1}})(X - \gamma^{-p}) \\ &= X^3 - (\gamma + \gamma^{p^{-1}} + \gamma^{-p})X^2 + (\gamma^p + \gamma^{1-p} + \gamma^{-1})X - 1 \\ &= X^3 - \mathrm{Sp}(\gamma)X^2 + \mathrm{Sp}(\gamma)^p X - 1. \end{aligned}$$

$\square$

Ziel: Finde  $c \in \mathbb{F}_{p^2}$ , so dass  $c = \mathrm{Sp}(\gamma)$  mit einem  $\gamma \in \mathbb{F}_{p^6}$  der Ordnung  $l > 3$  mit  $l|p^2 - p + 1$ , ohne  $\gamma$  oder  $\mathbb{F}_{p^6}$  explizit zu konstruieren.

### 3.2 Polynome der Form $X^3 - cX^2 + c^p X - 1$

Für  $c \in \mathbb{F}_{p^2}$  sei  $F(c, X) = X^3 - cX^2 + c^p X - 1 \in \mathbb{F}_{p^2}[X]$  mit Nullstellen  $\alpha_0, \alpha_1, \alpha_2 \in \mathbb{F}_{p^6}$  und  $c_n = \alpha_0^n + \alpha_1^n + \alpha_2^n$  für  $n \in \mathbb{Z}$ .

**Lemma 15** 1.  $c = c_1$ ;

2.  $\alpha_0 \alpha_1 \alpha_2 = 1$ ;

3.  $\alpha_0^n \alpha_1^n + \alpha_0^n \alpha_2^n + \alpha_1^n \alpha_2^n = c_{-n}, n \in \mathbb{Z}$ ;

4.  $F(c, \alpha_j^{-p}) = 0, j = 0, 1, 2$ ;

5.  $c_{-n} = c_n^p, n \in \mathbb{Z}$ ;

6. Entweder haben alle  $\alpha_j$  eine Ordnung  $l$  mit  $l|p^2 - p + 1, l > 3$ , oder alle  $\alpha_j \in \mathbb{F}_{p^2}$ ;

7.  $c_n \in \mathbb{F}_{p^2}, n \in \mathbb{Z}$ .

*Beweis:*

1.-2. trivial

3. folgt aus 2.

4. Aus  $F(c, \alpha_j) = \alpha_j^3 - c\alpha_j^2 + c^p\alpha_j - 1 = 0$  folgt  $\alpha_j \neq 0$  und  $F(c, \alpha_j)^p = \alpha_j^{3p} - c^p\alpha_j^{2p} + c\alpha_j^p - 1 = 0 = -\alpha_j^{3p}(\alpha_j^{-3p} - c\alpha_j^{-2p} + c^p\alpha_j^{-p} - 1) = -\alpha_j^{3p}F(c, \alpha_j^{-p}) = 0$ .

5. Aus 4. folgt bis auf Umbenennung der Elemente entweder  $\alpha_j = \alpha_j^{-p}, j = 0, 1, 2$  oder  $\alpha_0 = \alpha_0^{-p}$  und  $\alpha_1 = \alpha_2^{-p}$  oder  $\alpha_0 = \alpha_1^{-p}$  und  $\alpha_1 = \alpha_2^{-p}$ . In allen Fällen folgt 5.

6. Falls  $\alpha_j = \alpha_j^{-p}, j = 0, 1, 2$ , so teilt die Ordnung aller  $\alpha_j, j = 0, 1, 2$ , den Wert  $p+1 \mid p^2-1$ , woraus  $\alpha_j \in \mathbb{F}_{p^2}$  folgt.

Falls  $\alpha_0 = \alpha_0^{-p}$  und  $\alpha_1 = \alpha_2^{-p} = \alpha_1^{p^2}$ , so ist die Ordnung von  $\alpha_0$  ein Teiler von  $p+1$  und die Ordnungen von  $\alpha_1$  und  $\alpha_2$  teilen  $p^2-1$ .

Im Fall  $\alpha_0 = \alpha_1^{-p}, \alpha_1 = \alpha_2^{-p}$  folgt aus 2.

$$1 = \alpha_j \alpha_j^{p^2} \alpha_j^{-p} = \alpha_j^{p^2-p+1}, \quad j = 0, 1, 2.$$

Somit sind die Ordnungen von  $\alpha_0, \alpha_1, \alpha_2$  Teiler von  $p^2-p+1$ . Das Element  $\alpha_j$  liegt genau dann in  $\mathbb{F}_{p^2}$ , wenn seine Ordnung ein Teiler von  $p^2-1$  ist. Wegen  $\text{ggT}(p^2-1, p^2-p+1) = 3$  hat  $\alpha_j$  dann die Ordnung 1 oder 3. Gilt z.B.  $\alpha_0^3 = 1$ , so teilt die Ordnung von  $\alpha_0$  die Zahl  $p^2-1$  und  $\alpha_0$  ist ein Element von  $\mathbb{F}_{p^2}$ . Die anderen beiden Elemente  $\alpha_2 = \alpha_0^{-p}$  und  $\alpha_1 = \alpha_2^{-p}$  erfüllen dann ebenfalls die Bedingung  $\alpha_j^3 = 1$  und sind ebenfalls Elemente von  $\mathbb{F}_{p^2}$ .

7. Sind alle  $\alpha_j \in \mathbb{F}_{p^2}$ , so auch  $c_n = \alpha_0^n + \alpha_1^n + \alpha_2^n$ . Anderenfalls sind alle  $\alpha_j$  keine Elemente von  $\mathbb{F}_{p^2}$ , also  $F(c, X)$  irreduzibel und es gilt z.B.  $\alpha_1 = \alpha_0^{p^2}$  und  $\alpha_2 = \alpha_0^{p^4}$ . Daraus folgt  $c_n = \text{Sp}(\alpha_0^n) \in \mathbb{F}_{p^2}$ .  $\square$

**Korollar 6** *Das Polynom  $F(c, X)$  ist genau dann irreduzibel, wenn die Ordnung aller seiner Nullstellen Teiler von  $p^2-p+1$  und  $> 3$  sind.*

### Lemma 16

1.  $c_{u+v} = c_u c_v - c_v^p c_{u-v} + c_{u-2v}, u, v \in \mathbb{Z}$ ;

2.  $F(c_n, \alpha_j^n) = 0, j = 0, 1, 2, n \in \mathbb{Z}$ ;

3.  $F(c, X)$  ist genau dann reduzibel über  $\mathbb{F}_{p^2}$ , wenn  $c_{p+1} \in \mathbb{F}_p$ .

*Beweis:*

1. Nach dem vorherigen Lemma 2. und 5. folgt 1.
2. Wegen  $(X - \alpha_0^n)(X - \alpha_1^n)(X - \alpha_2^n)$   
 $= X^3 - (\alpha_0^n + \alpha_1^n + \alpha_2^n)X^2 + (\alpha_0^n\alpha_1^n + \alpha_0^n\alpha_2^n + \alpha_1^n\alpha_2^n)X - \alpha_0^n\alpha_1^n\alpha_2^n$   
 $= X^3 - c_n X^2 + c_n^p - 1 = F(c_n, X)$  gilt  $F(c_n, \alpha_j^n) = 0$ .
3. Ist  $F(c, X)$  reduzibel, so gilt  $\alpha_j \in \mathbb{F}_{p^2}$ ,  $j = 0, 1, 2$ . Es folgt  $\alpha_j^{(p+1)p} = \alpha_j^{p+1}$   
 also  $\alpha_j^{p+1} \in \mathbb{F}_p$  und  $c_{p+1} = \alpha_0^{p+1} + \alpha_1^{p+1} + \alpha_2^{p+1} \in \mathbb{F}_p$ .  
 Sei umgekehrt  $c_{p+1} \in \mathbb{F}_p$ , dann gilt  $c_{p+1}^p = c_{p+1}$ ,  $F(c_{p+1}, X) = X^3 - c_{p+1}X^2 +$   
 $c_{p+1}X - 1$  und  $F(c_{p+1}, 1) = 0$ , also  $\alpha_j^{p+1} = 1$  und somit  $\alpha_j \in \mathbb{F}_{p^2}$  für ein  $j$ ,  
 weswegen  $F(c, X)$  reduzibel über  $\mathbb{F}_{p^2}$  ist.  $\square$

**Korollar 7** Seien  $c, c_{n-1}, c_n$  und  $c_{n+1}$  gegeben.

1. Die Berechnung von  $c_{2n} = c_n^2 - 2c_n^p$  benötigt drei Multiplikationen in  $\mathbb{F}_p$ .
2. Die Berechnung von  $c_{2n-1} = c_{n-1}c_n - c^p c_n^p + c_{n+1}^p$  benötigt vier Multiplikationen in  $\mathbb{F}_p$ .
3. Die Berechnung von  $c_{2n+1} = c_{n+1}c_n - c c_n^p + c_{n-1}^p$  benötigt vier Multiplikationen in  $\mathbb{F}_p$ .

*Beweis:* Lemma 12 und Lemma 16.  $\square$

Definiere  $S_n(c) := (c_{n-1}, c_n, c_{n+1})$

**Satz 10**  $S_n(c)$ ,  $n \geq 2$ , kann in  $11 \log(n) - 4$  Multiplikationen in  $\mathbb{F}_p$  berechnet werden.

*Beweis:*  $n = 2$ : Wir haben  $c_0 = 3$  und  $c_1 = c$ . Die Elemente  $c_2$  und  $c_3$  lassen sich mit 7 Multiplikation aus  $c_0$  und  $c_1$  berechnen.

Ist  $n = 2m > 2$  gerade, so läßt sich  $S_{2m}(c)$  aus  $S_m(c)$  mit 11 Multiplikationen berechnen. Nach Induktionsvoraussetzung benötigt man also  $11 + 11 \log(m) - 4 = 11 \log n - 4$  Multiplikationen.

Ist  $n = 2m+1 > 3$  ungerade, so lässt sich  $S_n(c)$  aus  $S_m(c)$  mit 10 Multiplikationen berechnen. Nach Induktionsvoraussetzung benötigt man also  $10 + 11 \log(m) - 4 < 10 + 11(\log(n) - 1) - 4 < 11 \log(n) - 4$  Multiplikationen.

$S_3(c)$  lässt sich aus  $S_2(c)$  mit drei Multiplikationen berechnen.  $\square$

*Bemerkungen:*

1. Zum Vergleich:  $\gamma^n$  kann in  $72 \log(n)$  Multiplikationen in  $\mathbb{F}_p$  berechnet werden.

2. Für zufällig gewähltes  $c \in \mathbb{F}_{p^2}$  ist die Wahrscheinlichkeit, dass  $F(c, X) \in \mathbb{F}_{p^2}[X]$  irreduzibel ist gleich

$$\frac{p^2 - p - 2}{3p^2} \xrightarrow{p \rightarrow \infty} \frac{1}{3}.$$

## Bestimmung von $c$

1. Wähle (zufällig)  $c \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$  und berechne  $c_{p+1}$ .
2. Falls  $c_{p+1} \in \mathbb{F}_p$  gehe zu 1.

**Satz 11** *Der obige Algorithmus berechnet ein Element  $c \in \mathbb{F}_{p^2}$  mit der Eigenschaft, dass  $c = \text{Sp}(\gamma)$  für ein  $\gamma \in \mathbb{F}_{p^6}$  der Ordnung  $l > 3$  mit  $l|p^2 - p + 1$ .*

*Beweis:* Nach Lemma 16.3. ist  $F(c, X)$  genau dann irreduzibel, wenn  $c_{p+1} \notin \mathbb{F}_p$ , d.h. die Nullstellen von  $F(c, X)$  liegen nicht in  $\mathbb{F}_{p^2}$  und haben Ordnungen  $l > 3$  mit  $l|p^2 - p + 1$  nach Lemma 15.6.  $\square$

## 3.3 Der XTR-Diffie-Hellman Schlüsselaustausch

$A$  und  $B$  einigen sich auf eine Primzahl  $p$  und ein Element  $c = \text{Sp}(\gamma) \in \mathbb{F}_{p^2}$ .

1.  $A$  wählt (zufällig)  $1 < a < l - 2$  und berechnet

$$S_a(\text{Sp}(\gamma)) = (\text{Sp}(\gamma^{a-1}), \text{Sp}(\gamma^a), \text{Sp}(\gamma^{a+1})) \in \mathbb{F}_{p^2}^3$$

und sendet  $\text{Sp}(\gamma^a)$  an  $B$ .

2.  $B$  wählt (zufällig)  $1 < b < l - 2$  und berechnet

$$S_b(\text{Sp}(\gamma)) = (\text{Sp}(\gamma^{b-1}), \text{Sp}(\gamma^b), \text{Sp}(\gamma^{b+1})) \in \mathbb{F}_{p^2}^3$$

und sendet  $\text{Sp}(\gamma^b)$  an  $A$ .

3.  $A$  erhält  $\text{Sp}(\gamma^b)$  von  $B$  und berechnet

$$S_a(\text{Sp}(\gamma^b)) = (\text{Sp}(\gamma^{(a-1)b}), \text{Sp}(\gamma^{ab}), \text{Sp}(\gamma^{(a+1)b})) \in \mathbb{F}_{p^2}^3$$

und wählt  $K = \text{Sp}(\gamma^{ab}) \in \mathbb{F}_{p^2}$ .

4.  $B$  erhält  $\text{Sp}(\gamma^a)$  von  $A$  und berechnet

$$S_b(\text{Sp}(\gamma^a)) = (\text{Sp}(\gamma^{a(b-1)}), \text{Sp}(\gamma^{ab}), \text{Sp}(\gamma^{(a+1)b})) \in \mathbb{F}_{p^2}^3$$

und wählt  $K = \text{Sp}(\gamma^{ab}) \in \mathbb{F}_{p^2}$ .

*Bemerkungen:*

1. Der Name XTR ist die Kurzform von ECSTR = Efficient Compact Subgroup Trace Representation.
2. Die Sicherheit des XTR-Diffie-Hellman Schlüsselaustausches beruht auf der Unangreifbarkeit des XTR diskreten Logarithmus Problems:  
Zu gegebenen  $a = \text{Sp}(\gamma^x) \in \mathbb{F}_{p^2}$  bestimme ein  $x$  mit  $0 \leq x \leq l - 1$ . (Der Exponent  $x$  ist nicht eindeutig. Wegen  $\text{Sp}(\gamma^x) = \text{Sp}(\gamma^{p^2x}) = \text{Sp}(\gamma^{p^4x})$  reicht es einen der drei Werte  $x, p^2x$  oder  $p^4x$  modulo  $l$  zu finden.)
3. Grob gesagt liefert XTR die Sicherheit von  $\mathbb{F}_{p^6}$  (gegenüber Index-Calculus), benötigt aber nur Rechnungen in  $\mathbb{F}_{p^2}$ .

Literatur über XTR zum Runterladen: <http://www.ecstr.com/>

# Kapitel 4

## Elliptische Kurven

### 4.1 Definition und Gruppenstruktur

**Definition 4** Eine elliptische Kurve  $E$  über einem Körper  $\mathbb{K}$  ist die Menge der Lösungen  $(x, y) \in \mathbb{K}^2$  einer kubischen Polynomialgleichung der Form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, a_2, a_3, a_4, a_6 \in \mathbb{K}, \quad (4.1)$$

zusammen mit einem Punkt  $O$ , genannt Punkt im Unendlichen.

**Definition 5** Sei  $\mathbb{E}$  ein Erweiterungskörper von  $\mathbb{K}$  und  $E$  eine elliptische Kurve über  $\mathbb{K}$  definiert durch (4.1). Ein Punkt  $(x, y) \in \mathbb{E}^2$  heißt *singulär*, falls die Gleichung (4.1) und die partiellen Ableitungen

$$2y + a_1x + a_3 = 0 \quad (4.2)$$

und

$$a_1y = 3x^2 + 2a_2x + a_4 \quad (4.3)$$

gleichzeitig erfüllt sind.

Die elliptische Kurve  $E$  heißt *singulär*, wenn (4.1)–(4.3) eine gemeinsame Lösung (in einem Erweiterungskörper) haben.

Bemerkungen:

1. Man kann zeigen, dass singuläre elliptische Kurven für kryptographische Zwecke ungeeignet sind.
2. Ist die Charakteristik von  $\mathbb{K}$  ungleich 2, so läßt sich (4.1) mit der Substitution  $y \rightarrow y - (a_1x + a_3)/2$  in die Form

$$y^2 = x^3 + Ax^2 + Bx + C, \quad A, B, C \in \mathbb{K}, \quad (4.4)$$

bringen.

3. Ist die Charakteristik von  $\mathbb{K}$  ungleich 2, 3, so lässt sich (4.4) mit der Substitution  $x \rightarrow x - A/3$  in die Form

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{K}, \quad (4.5)$$

bringen.

4. Ist die Charakteristik von  $\mathbb{K}$  gleich 2, so lässt sich (4.1) in eine der beiden folgenden Formen bringen:

$$y^2 + ay = x^3 + by + c, \quad a, b, c \in \mathbb{K}, \quad (4.6)$$

oder

$$y^2 + xy = x^3 + ax^2 + b, \quad a, b \in \mathbb{K}. \quad (4.7)$$

(Falls  $a_1 = 0$  substituiere  $x \rightarrow x + a_2/3$ . Falls  $a_1 \neq 0$  substituiere  $x \rightarrow a_1^2 x + a_1^{-1} a_3$ ,  $y \rightarrow a_1^3 y$ , um die Form  $y^2 + xy = x^3 + Ax^2 + Bx + C$  zu bekommen; danach substituiere  $y \rightarrow y + B$ .)

**Lemma 17** Sei  $\mathbb{K}$  ein Körper mit Charakteristik  $\neq 2, 3$  und  $E$  eine elliptische Kurve über  $\mathbb{K}$  definiert durch (4.5). Die Kurve ist genau dann singulär, wenn  $4a^3 + 27b^2 = 0$ .

*Beweis:* Die Kurve  $E$  ist genau dann singulär, wenn das folgende Gleichungssystem eine Lösung besitzt:

$$\begin{aligned} F(x, y) &= y^2 - x^3 - ax - b = 0, \\ F_x(x, y) &= -3x^2 - a = 0, \\ F_y(x, y) &= 2y = 0. \end{aligned}$$

Der Punkt  $(x_1, y_1)$  ist genau dann eine Lösung dieses Gleichungssystems, wenn  $y_1 = 0$ ,  $a = -3x_1^2$  und  $b = y_1^2 - x_1^3 - ax_1 = 2x_1^3$ , woraus  $4a^3 + 27b^2 = 0$  folgt. Gilt umgekehrt  $4a^3 + 27b^2 = 0$  also  $b = \pm \frac{2a}{3} \sqrt{-\frac{a}{3}}$ , so ist der Punkt  $(\mp \sqrt{-\frac{a}{3}}, 0)$  singulär.  $\square$

*Beispiele:* 1. Die durch  $y^2 = x^3$  definierte elliptische Kurve ist singulär über jedem Körper der Charakteristik  $\neq 2$ .

2. Die durch  $y^2 = x^3 + ax + b$  definierten elliptischen Kurven sind genau für  $(a, b) \in \{(0, 0), (2, 3), (2, 2), (3, 1), (3, 4)\}$  über  $\mathbb{F}_5$  singulär.

**Lemma 18** Sei  $\mathbb{K}$  ein Körper mit Charakteristik 2 und  $E$  eine elliptische Kurve über  $\mathbb{K}$  definiert durch (4.6) oder (4.7). Die Kurve ist genau dann singulär, wenn  $a = 0$  in (4.6) oder  $b = 0$  in (4.7).

*Beweis:* Eine durch (4.6) definierte Kurve  $E$  ist offensichtlich nur dann singulär, wenn  $a = 0$ . Für  $a = 0$  ist ein Punkt  $(x, y)$  mit  $x^2 = b$  und  $y^2 = x^3 + bx + c$  ein singulärer Punkt.

Eine durch (4.7) definierte Kurve  $E$  ist genau dann singulär, wenn die gemeinsame Lösung  $(x, y) = (0, 0)$  von  $x = 0$  und  $y = x^2$  auch (4.7) erfüllt. Dieses ist genau dann der Fall, wenn  $b = 0$ .  $\square$

**Lemma 19** *Sei  $\mathbb{K}$  ein Körper der Charakteristik 3 und  $E$  eine elliptische Kurve über  $\mathbb{K}$  definiert durch (4.4), so ist  $E$  genau dann singulär, wenn  $A^3C + B^3 - A^2B^2 = 0$ .*

*Beweis:* Ein Punkt  $(x, y)$  ist genau dann singulär, wenn

$$y^2 = x^3 + Ax^2 + Bx + C, \quad 2y = 0 \quad \text{und} \quad -Ax + B = 0.$$

Ist  $A = 0$ , so ist  $E$  nur dann singulär, wenn  $B = 0$ . Falls  $A = B = 0$ , so ist jeder Punkt  $(x, 0)$  mit  $x^3 + C = 0$  singulär.

Ist  $A \neq 0$ , so ist  $E$  genau dann singulär, wenn  $(A^{-1}B, 0)$  auf  $E$  liegt, d.h.  $(A^{-1}B)^3 + A(A^{-1}B)^2 + A^{-1}B^2 + C = 0$ , woraus die Behauptung folgt.  $\square$

Wir betrachten ab jetzt nur noch nicht singuläre elliptische Kurven.

**Definition 6** ( $\mathbb{K} = \mathbb{R}$ )

*Sei  $E$  eine elliptische Kurve über den reellen Zahlen und  $P, Q$  auf  $E$ . Wir definieren  $-P$  und  $P + Q$  in folgender Weise:*

1.  $P = O$ :  $-O = O, O + Q = Q$ .
2.  $P = (x, y) \neq O$ :  $-P = (x, -y)$ .
3.  $P = (x_1, y_1), Q = (x_2, y_2) \neq O$  mit  $x_1 \neq x_2$ : Die Gerade durch  $P$  und  $Q$  schneidet die Kurve in genau einem dritten Punkt  $R$  und wir setzen  $P + Q = -R$ .
4.  $Q = -P \neq O$ :  $P + Q = O$ .
5.  $P = Q \neq O$ : Die Tangente an  $E$  in  $P$  schneidet  $E$  in genau einem weiteren Punkt  $R$  und wir setzen  $P + P = -R$ .

**Satz 12** *Sei  $E$  eine elliptische Kurve über den reellen Zahlen definiert durch (4.5) und  $P = (x_1, y_1), Q = (x_2, y_2) \neq O$  auf  $E$  mit  $x_1 \neq x_2$ . Dann gilt für  $P + Q = (x_3, y_3)$ :*

$$x_3 = \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2, \quad (4.8)$$

$$y_3 = -y_1 + \left( \frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3), \quad (4.9)$$

und für  $P + P = (x_4, y_4)$  mit  $y_1 \neq 0$ :

$$x_4 = \left( \frac{3x_1^2 + a}{2y_1} \right) - 2x_1, \quad (4.10)$$

$$y_4 = -y_1 + \left( \frac{3x_1^2 + a}{2y_1} \right) (x_1 - x_4). \quad (4.11)$$

*Beweis:*  $\underline{P \neq Q}$ , (d.h.  $\underline{x_1 \neq x_2}$ ):

Sei  $y = \alpha x + \beta$  die Gerade durch  $P$  und  $Q$ , d.h.

$$\begin{aligned} y_1 &= \alpha x_1 + \beta \\ y_2 &= \alpha x_2 + \beta \end{aligned} \Rightarrow \alpha = \frac{y_2 - y_1}{x_2 - x_1}, \beta = y_1 - \alpha x_1.$$

$-(P + Q) = (x_3, -y_3)$  ist der dritte Schnittpunkt der Geraden  $y = \alpha x + \beta$  mit  $E$ . Einsetzen der Geradengleichung in die Gleichung der elliptischen Kurve liefert:

$$x^3 - \alpha^2 x^2 + (a - 2\alpha\beta)x + b - \beta^2 = 0 = (x - x_1)(x - x_2)(x - x_3).$$

Der Koeffizient von  $x^2$  ist  $-(x_1 + x_2 + x_3) = -\alpha^2$  und somit

$$x_3 = \alpha^2 - x_1 - x_2 = \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2.$$

Die zweite Koordinate von  $P + Q$  ist

$$y_3 = -(\alpha x_3 + \beta) = -y_1 + \alpha(x_1 - x_3) = -y_1 + \left( \frac{y_2 - y_1}{x_2 - x_1} \right) (x_1 - x_3).$$

$\underline{P = Q \neq -P}$ , (d.h.  $y_1 \neq 0$ )

Sei  $y = \alpha x + \beta$  die Tangente an  $E$  im Punkt  $P$ , d.h.  $\alpha = \frac{dy}{dx}$  in  $x_1$ . Implizites Ableiten von  $y^2 = x^3 + ax + b$  ergibt  $2y y' = 3x^2 + a$ , somit  $y' = \frac{3x^2 + a}{2y}$  und daher  $\alpha = \frac{3x_1^2 + a}{2y_1}$  und  $\beta = y_1 - \alpha x_1$ .

Sei  $-2P = (x_4, -y_4)$  der zweite Schnittpunkt der Tangente  $y = \alpha x + \beta$  mit  $E$ . Einsetzen der Geradengleichung liefert

$$x^3 - \alpha^2 x^2 + (a - 2\alpha\beta)x + b - \beta^2 = 0 = (x - x_1)^2(x - x_4)$$

also

$$x_4 = \alpha^2 - 2x_1 = \left( \frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1$$

und

$$y_4 = -(\alpha x_4 + \beta) = -y_1 + \left( \frac{3x_1^2 + a}{2y_1} \right) (x_1 - x_4).$$

□

*Bemerkung:* Analog kann man Rechenregeln für Punkte auf einer elliptischen Kurve definiert durch (4.1) herleiten.

**Definition 7** ( $\mathbb{K} = \mathbb{F}_q$ )

Sei  $E$  eine elliptische Kurve über  $\mathbb{F}_q$ ,  $q = p^r$ ,  $p > 3$ , definiert durch (4.5), so definieren wir  $O + Q = Q$  und  $P + Q$  durch (4.8) – (4.11) für  $P, Q \in E \setminus \{O\}$ .

*Bemerkung:* Mit ähnlichen Formeln kann man auch eine Addition für elliptische Kurven über  $\mathbb{F}_{p^r}$  im Fall  $p = 2$  oder  $3$  definieren.

**Satz 13** Sei  $E$  eine elliptische Kurve über  $\mathbb{F}_q$  und  $+$  die oben definierte Punktaddition auf  $E$ . Dann ist  $(E, +)$  eine abelsche Gruppe.

ohne Beweis

□

## 4.2 Die Anzahl der Punkte einer elliptischen Kurve

**Satz 14 (Hasse-Weil)** Für die Anzahl  $N$  der Punkte auf einer elliptischen Kurve über  $\mathbb{F}_q$  gilt:  $|N - q - 1| \leq 2q^{1/2}$ .

ohne Beweis

□

*Beispiel:*  $y^2 = x^3 + ax + b$  über  $\mathbb{F}_5$ :

a	b	N
0	0	singulär
0	1	6
0	2	6
0	3	6
0	4	6
1	0	4
1	1	9
1	2	4
1	3	4
1	4	9
2	0	2
2	1	7
2	2	singulär

a	b	N
2	3	singulär
2	4	7
3	0	10
3	1	singulär
3	2	5
3	3	5
3	4	singulär
4	0	8
4	1	8
4	2	3
4	3	3
4	4	8

*Bemerkungen:*

1. Ist  $q = p$  eine Primzahl, so existiert zu jedem  $N$  mit

$$p + 1 - \lfloor 2p^{1/2} \rfloor \leq N \leq p + 1 + \lfloor 2p^{1/2} \rfloor$$

eine elliptische Kurve mit  $N$  Punkten. Für  $q = p^r$ ,  $r > 1$ , gilt die analoge Aussage mit Ausnahme von  $N$  mit  $N \equiv 1 \pmod{p}$ .

2. Eine elliptische Kurve über  $\mathbb{F}_{p^r}$  mit  $N$  Punkten heißt *supersingulär*, wenn  $N \equiv 1 \pmod{p}$ . Man kann zeigen, dass supersinguläre elliptische Kurven für kryptographische Zwecke schlechte Eigenschaften haben.
3. Eine über  $\mathbb{F}_q$  definierte elliptische Kurve  $E$  lässt sich auch als Kurve über jedem Erweiterungskörper  $\mathbb{F}_{q^r}$  auffassen. Die zugehörigen Punkte nennt man  $\mathbb{F}_{q^r}$ -rationale Punkte.

**Satz 15** Sei  $E$  eine über  $\mathbb{F}_q$  definierte elliptische Kurve und  $N_r$  die Anzahl der  $\mathbb{F}_{q^r}$ -rationalen Punkte. Seien  $\alpha$  und  $\bar{\alpha}$  die (komplexen) Nullstellen des Polynoms  $X^2 + (N_1 - q - 1)X + q$ , so gilt

$$N_r = |\alpha^r - 1|^2 = q^r + 1 - \alpha^r - \bar{\alpha}^r.$$

ohne Beweis □

*Beispiel:* Kurven über  $\mathbb{F}_2$

1.  $y^2 + y = x^3 + bx + c$ ,  $b, c \in \{0, 1\}$  :

$$N_1 = \begin{cases} 1, & b = c = 1, \\ 3, & b = 0, \\ 5, & b = 1, c = 0, \end{cases} \Rightarrow \text{supersingulär.}$$

$$N_r = \begin{cases} 2^r + 1 - (1+i)^r - (1-i)^r, & b = c = 1, \\ 2^r + 1 - (\sqrt{2}i)^r - (-\sqrt{2}i)^r, & b = 0, \\ 2^r + 1 - (-1+i)^r - (-1-i)^r, & b = 1, c = 0. \end{cases}$$

$$\text{Z.B. : } N_2 = \begin{cases} 5, & b = 1, \\ 9, & b = 0. \end{cases}$$

2.  $y^2 + xy = x^3 + ax^2 + 1$ ,  $a \in \{0, 1\}$  :

$$N_1 = \begin{cases} 2, & a = 1, \\ 4, & a = 0. \end{cases}$$

$$N_r = \begin{cases} 2^r + 1 - \left(\frac{1}{2} + \frac{\sqrt{7}i}{2}\right)^r - \left(\frac{1}{2} - \frac{\sqrt{7}i}{2}\right)^r, & a = 1, \\ 2^r + 1 - \left(-\frac{1}{2} + \frac{\sqrt{7}i}{2}\right)^r - \left(-\frac{1}{2} - \frac{\sqrt{7}i}{2}\right)^r, & a = 0. \end{cases}$$

$$\text{Z.B. : } N_2 = 8.$$

*Bemerkung:* Satz 15 liefert eine erste Methode zur Konstruktion geeigneter Gruppen. Man zählt die Anzahl  $N_1$  der Punkte über einem sehr kleinen endlichen Körper  $\mathbb{F}_q$  und berechnet daraus die Anzahl  $N_r$  der Punkte über einem (sehr großen) endlichen Erweiterungskörper  $\mathbb{F}_{q^r}$ . Ist  $N_r$  durch eine große Primzahl  $l$  teilbar, so sucht man einen Punkt  $P$  der Ordnung  $l$  und benutzt die von  $P$  erzeugte zyklische Gruppe.

## Die Kurve $y^2 = x^3 - x$ über $\mathbb{F}_p$

**Lemma 20** Für  $p \equiv 3 \pmod{4}$  ist die durch  $y^2 = x^3 - x$  definierte elliptische Kurve über  $\mathbb{F}_p$  supersingulär und hat  $N = p + 1$  Punkte.

*Beweis:* Sei  $(\cdot)$  das Legendre-Symbol. Dann gilt

$$\begin{aligned} N &= 1 + \sum_{x \in \mathbb{F}_p} \left( 1 + \left( \frac{x^3 - x}{p} \right) \right) \\ &= p + 1 + \sum_{x=1}^{(p-1)/2} \left( \left( \frac{x^3 - x}{p} \right) + \left( \frac{(-x)^3 - (-x)}{p} \right) \right) = p + 1, \end{aligned}$$

da  $\left( \frac{-1}{p} \right) = -1$ . □

**Lemma 21 (Zwei-Quadrate-Satz)** Jede Primzahl  $p \equiv 1 \pmod{4}$  lässt sich eindeutig als  $p = a^2 + b^2$  mit natürlichen Zahlen  $a, b$ , wobei  $a$  gerade und  $b$  ungerade ist, schreiben.

ohne Beweis □

*Beispiel:*  $5 = 2^2 + 1^2$ ,  $13 = 2^2 + 3^2$ ,  $17 = 4^2 + 1^2$ ,  $29 = 2^2 + 5^2$ ,  $37 = 6^2 + 1^2$ ,  $41 = 4^2 + 5^2$

**Satz 16** Sei  $p \equiv 1 \pmod{4}$  eine Primzahl mit  $p = a^2 + b^2$ . Dann gilt für die Anzahl  $N$  der Punkte der durch  $y^2 = x^3 - x$  über  $\mathbb{F}_p$  definierten Kurve

$$N = \begin{cases} p + 1 + 2b, & \text{falls } 4|a \text{ und } b \equiv 3 \pmod{4} \text{ oder } 4 \nmid a \text{ und } b \equiv 1 \pmod{4}, \\ p + 1 - 2b, & \text{sonst.} \end{cases}$$

ohne Beweis □

*Beispiel:*

$$p = 5, N = 8,$$

$$p = 13, N = 8,$$

$$p = 17, N = 16,$$

$$p = 29, N = 28,$$

$$p = 37, N = 40,$$

$$p = 41, N = 32.$$

## Ein Algorithmus zum Punkte zählen über $\mathbb{F}_p$

Sei  $E$  eine elliptische Kurve über  $\mathbb{F}_p$ ,  $p > 3$ , definiert durch (4.5). Dann liefert die Formel

$$N = p + 1 + \sum_{x \in \mathbb{F}_p} \left( \frac{x^3 + ax + b}{p} \right)$$

einen Algorithmus mit  $O(p \log p)$  Operationen in  $\mathbb{F}_p$  ( $p$  Berechnungen des Legendesymbols).

Der folgende **Baby-Step Giant-Step Algorithmus** benötigt  $O(p^{1/4+\varepsilon})$  Operationen in  $\mathbb{F}_p$  und berechnet die Ordnung  $l$  eines zufällig gewählten Punktes  $P$  auf  $E$ . Wir beschränken uns auf den Fall, dass  $(E, +)$  zyklisch ist und  $P$  ein erzeugendes Element ist.

1. (Baby-Step)  
Setze  $s = \lfloor p^{1/4} \rfloor$  und berechne  $P, 2P, 3P, \dots, sP$   
(und damit auch  $-P, -2P, -3P, \dots, -sP$ ).
2. (Giant-Step)  
Berechne  $Q = (2s + 1)P$  und  $R = (p + 1)P$ . Setze  $t = \lfloor 2\sqrt{p}/(2s + 1) \rfloor$  und berechne  $R + iQ$ ,  $i = 0, \pm 1, \pm 2, \dots, \pm t$ .  
Es existiert ein Paar  $(i, j)$  mit  $i \in \{0, \pm 1, \pm 2, \dots, \pm t\}$  und  $j \in \{0, \pm 1, \dots, \pm s\}$ ,  
so dass  $R + iQ = jP$ .  
Für  $N = p + 1 + (2s + 1)i - j$  gilt  $NP = O$ .

*Bemerkung:*

Es existiert ein polynomialer Punkte zählalgorithmus (Schoof:  $O(\log^8 p)$ ).

# Kapitel 5

## Polynomdarstellungen des diskreten Logarithmus

### 5.1 Der XTR diskrete Logarithmus

Sei  $p \equiv 2 \pmod{3}$  eine Primzahl,  $l > 3$  ein Primteiler von  $p^2 - p + 1$  und  $\gamma \in \mathbb{F}_{p^6}$  ein Element der Ordnung  $l$ . Für  $\alpha \in \mathbb{F}_{p^6}$  betrachten wir die Spur  $\text{Sp}(\alpha)$  von  $\alpha$  in  $\mathbb{F}_{p^2}$ . Für  $\xi \in \text{Sp}(\langle \gamma \rangle)$ , ist das XTR diskrete Logarithmen Problem die Suche nach  $0 \leq x \leq l-1$ , so dass  $\xi = \text{Sp}(\gamma^x)$ . ( $x$  ist zwar nicht eindeutig, aber  $p^2x$  und  $p^4x$  modulo  $l$  sind die einzigen anderen Lösungen von  $\xi = \text{Sp}(\gamma^x)$ .) Sei  $\xi_x \in \mathbb{F}_{p^2}$ ,  $0 \leq x \leq l-1$ , definiert durch

$$\xi_x = x_0\beta_0 + x_1\beta_1 \quad \text{falls} \quad x = x_0 + x_1p, \quad 0 \leq x_0, x_1 \leq p-1,$$

wobei  $\{\beta_0, \beta_1\}$  eine fixierte Basis von  $\mathbb{F}_{p^2}$  über  $\mathbb{F}_p$  ist.

**Satz 17** Sei  $f(X) \in \mathbb{F}_{p^2}[X]$  ein Polynom vom Grad  $d$ , so dass

$$f(\text{Sp}(\gamma^x)) = \xi_x \quad \text{für } x \in S$$

für eine Teilmenge  $S \subset \{0, 1, \dots, l-1\}$ . Dann gilt

$$d \geq \frac{|S|(|S|-1)}{5(l-1)(2p-1)}.$$

*Beweis:* Wir dürfen  $|S| > 2$  annehmen. Betrachte

$$D = \{1 \leq a \leq l-1 \mid a \equiv y-x \pmod{l}, x, y \in S\}.$$

Offensichtlich existiert ein  $a \in D$  mit wenigstens

$$\frac{|S|(|S|-1)}{|D|} \geq \frac{|S|(|S|-1)}{l-1}$$

Darstellungen  $a \equiv y - x \pmod{l}$ ,  $x, y \in S$ . Wähle dieses  $a$  und setze

$$R = \{x \in S \mid a + x \equiv y \pmod{l} \text{ mit } y \in S\}.$$

Wir haben  $|R| \geq |S|(|S| - 1)/(l - 1)$ . Für  $x \in R$  existieren höchstens fünf verschieden  $\omega \in \mathbb{F}_{p^2}$ , nämlich  $\omega = \xi_a, \xi_a + \beta_1, \xi_a - \xi_l, \xi_a - \xi_l + \beta_1$ , oder  $\xi_a - \xi_l - \beta_1$ , so dass

$$f(\text{Sp}(\gamma^{a+x})) = \xi_x + \omega = f(\text{Sp}(\gamma^x)) + \omega.$$

Daher hat wenigstens eines der fünf Polynome  $h_\omega(X) \in \mathbb{F}_{p^6}[X]$ ,

$$h_\omega(X) = X^{dp} (f(\gamma^a X + (\gamma^a X)^{p-1} + (\gamma^a X)^{-p}) - f(X + X^{p-1} + X^{-p}) - \omega)$$

mindestens  $|R|/5$  Nullstellen, wobei wir

$$\text{Sp}(\gamma^x) = \gamma^x + \gamma^{p^2x} + \gamma^{p^4x} = \gamma^x + \gamma^{(p-1)x} + \gamma^{-px}$$

benutzt haben. Der Hauptkoeffizient von  $h_\omega(X)$  ist  $\gamma^{ad(p-1)} - 1$  mal dem Hauptkoeffizienten von  $f(X)$  und daher  $d \geq l$  oder

$$d(2p - 1) = \text{grad}(h_\omega) \geq \frac{|R|}{5} \geq \frac{|S|(|S| - 1)}{5(l - 1)}.$$

□

**Bemerkung:** Wegen  $\text{Sp}(\gamma^x) = \text{Sp}(\gamma^{p^2x}) = \text{Sp}(\gamma^{p^4x})$  hat die größte mögliche Teilmenge  $S$  die Kardinalität  $|S| = (l + 2)/3 \leq (p^2 - p + 7)/9$ .

## 5.2 Der elliptische Kurven diskrete Logarithmus

**Satz 18** Sei  $E$  eine elliptische Kurve über  $\mathbb{F}_p$  mit  $p > 3$ , definiert durch eine Gleichung der Form (4.5),  $P$  ein Punkt auf  $E$  der Ordnung  $l$  und genüge  $f(X) \in \mathbb{F}_p[X]$  der Bedingung

$$f(x) = n, \quad 1 \leq n \leq \lfloor l/2 \rfloor \iff \exists y \in \mathbb{F}_p : (x, y) = nP.$$

Dann gilt

$$\text{grad}(f) \geq \frac{l}{6} - 1.$$

*Beweis.* Sei  $R = \{n \mid 2 \leq n \leq \lfloor l/2 \rfloor - 1\}$ . Setze  $d = \text{grad}(f)$ ,  $f(X) = \sum_{i=0}^d a_i X^i$  und  $nP = (x_n, y_n)$  für  $1 \leq n \leq \lfloor l/2 \rfloor$ . Wir betrachten das folgende Gleichungssystem:

$$\begin{aligned} f(x_{n+1}) - f(x_n) - 1 &= n + 1 - n - 1 = 0, \\ f(x_{n-1}) - f(x_n) + 1 &= n - 1 - n + 1 = 0, \end{aligned} \tag{5.1}$$

für  $n \in R$ .

Nach Satz 12 haben wir

$$(n \pm 1)P = (x_n, y_n) + (x_1, \pm y_1) = \left( \frac{A(x_n) \mp 2y_n y_1}{(x_n - x_1)^2}, \frac{\pm B(x_n) - y_n C(x_n)}{(x_n - x_1)^3} \right),$$

mit

$$A(X) = x_1 X^2 + (x_1^2 + a)X + (x_1 + 2)a$$

und Polynomen  $B(X)$  und  $C(X)$ . Setzt man dieses in (5.1) ein, so ergibt sich

$$\begin{aligned} 0 = f(x_{n\pm 1}) - f(x_n) \mp 1 &= \sum_{i=0}^d a_i \left( \frac{A(x_n) \mp 2y_n y_1}{(x_n - x_1)^2} \right)^i - \sum_{i=0}^d a_i x_n^i \mp 1 \\ &= \frac{U(x_n) \mp y_n V(x_n)}{(x_n - x_1)^{2d}} - \sum_{i=0}^d a_i x_n^i \mp 1 \end{aligned}$$

mit Polynomen  $U(X)$  und  $V(X)$  und  $\text{grad}(U) \leq 2d$ . Addiert man die Gleichungen, so erhält man

$$0 = \frac{U(x_n)}{(x_n - x_1)^{2d}} - \sum_{i=0}^d a_i x_n^i.$$

Somit hat das Polynom

$$h(X) = (X - x_1)^{2d} \sum_{i=0}^d a_i X^i - U(X)$$

vom Grad  $3d$  wenigstens  $|R|$  Nullstellen und es gilt  $3d \geq |R| \geq \lfloor l/2 \rfloor - 2$ , woraus das Ergebnis folgt.  $\square$

*Bemerkung:* Entsprechende Ergebnisse können auch für  $p = 2$  und  $p = 3$  hergeleitet werden.

# Kapitel 6

## Primzahltest und Faktorisierung mit elliptischen Kurven

Analog zu elliptischen Kurven über Körpern kann man auch elliptische Kurven über  $\mathbb{Z}/n\mathbb{Z}$  definieren:

$$E = \{(x, y) \in (\mathbb{Z}/n\mathbb{Z})^2 \mid y^2 = x^3 + ax + b\} \cup O$$

mit  $a, b \in \mathbb{Z}/n\mathbb{Z}$ . Weiterhin lassen sich die Formeln (4.8) – (4.11) anwenden, sofern die dort auftretenden Nenner teilerfremd zu  $n$  sind. Ist das nicht der Fall, so ist  $n$  zusammengesetzt und der größte gemeinsame Teiler von diesem Nenner und  $n$  ist ein nichttrivialer Teiler von  $n$ . Wir betrachten daher nur den Fall, dass alle im Folgenden auftretenden Nenner zu  $n$  teilerfremd sind.

**Lemma 22** Sei  $p$  ein Teiler von  $n$ ,  $E'$  die Kurve über  $\mathbb{Z}/p\mathbb{Z}$  definiert durch dieselbe Gleichung wie  $E$  über  $\mathbb{Z}/n\mathbb{Z}$ ,  $O \neq P = (x_1, y_1) \in E$  und  $O \neq P' = (x'_1, y'_1) \in E'$  mit  $x_1 \equiv x'_1 \pmod{p}$  und  $y_1 \equiv y'_1 \pmod{p}$ . Dann gilt:

$$lP = O \iff lP' = O.$$

*Beweis:* Da nach Voraussetzung bei der Berechnung von  $jP$ ,  $2 \leq j \leq l-1$ , die Nenner teilerfremd zu  $n$  sind, erhält man  $jP' \equiv jP \pmod{p}$ . Sei  $(l-1)P = (x_2, y_2)$  und  $(l-1)P' = (x'_2, y'_2) \equiv (l-1)P \pmod{p}$ .

Die Gleichung  $lP = O$  ist äquivalent mit  $x_1 \equiv x_2 \pmod{n}$  und  $y_1 \equiv y_2 \pmod{n}$ . Hieraus folgt  $x'_1 \equiv x_1 \equiv x_2 \equiv x'_2 \pmod{p}$  und  $y'_1 \equiv y_1 \equiv -y_2 \equiv -y'_2 \pmod{p}$ , was gleichwertig mit  $lP' = O$  ist.

Sei umgekehrt  $lP' = O$ , also  $x_1 \equiv x_2 \pmod{p}$  und  $y_1 \equiv -y_2 \pmod{p}$ . Wegen  $\text{ggT}(x_2 - x_1, n) = 1$  folgt daraus  $x_1 \equiv x_2 \pmod{n}$  und somit  $lP = O$ .  $\square$

### 6.1 Primzahltest

**Lemma 23** Sei  $n$  eine natürliche Zahl und  $E$  eine elliptische Kurve über  $\mathbb{Z}/n\mathbb{Z}$  definiert durch die Gleichung  $y^2 = x^3 + ax + b$ . Sei  $l$  eine ganze Zahl und  $q$  ein

Primteiler von  $l$  mit  $q > (n^{1/4} + 1)^2$ . Falls es einen Punkt auf  $E$  mit

$$(1) lP = O \quad \text{und} \quad (2) l/qP \neq O$$

gibt, so ist  $n$  prim.

*Beweis:* Falls  $n$  nicht prim wäre, so würde eine Primzahl  $p \leq \sqrt{n}$  existieren, die  $n$  teilt. Sei  $E'$  die elliptische Kurve definiert durch dieselbe Gleichung wie  $E$  aber über  $\mathbb{F}_p$  und  $l'$  die Ordnung der Gruppe  $E'$ . Nach Hasse-Weil gilt

$$l' \leq p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2 \leq (n^{1/4} + 1)^2 < q$$

und daher  $\text{ggT}(q, l') = 1$ , weshalb eine ganze Zahl  $u$  mit  $uq \equiv 1 \pmod{l'}$  existiert. Sei  $P'$  auf  $E'$  der Punkt  $P$  modulo  $p$  betrachtet. Dann gilt auf  $E'$

$$l/qP' = uql/qP' = ulP' = O$$

nach (1) im Widerspruch zu (2) und Lemma 22. □

*Algorithmus:*

1. Wähle zufällig  $a, x, y \in \mathbb{Z}/n\mathbb{Z}$  und setze  $b = y^2 - x^3 - ax \in \mathbb{Z}/n\mathbb{Z}$ . (Dann liegt  $P = (x, y)$  auf der durch  $y^2 = x^3 + ax + b$  definierten Kurve  $E$ .)
2. Bestimme die Anzahl  $l$  der Punkte auf  $E$  (z.B. mit Schoofs Algorithmus).
3. Ist  $l$  nicht von der Form  $l = kq$  mit kleinem  $k$  und einem  $q$ , das 'wahrscheinlich' prim ist, gehe zu 1.
4. Berechne  $lP$  und  $kP = l/qP$ .
5. Ist  $lP \neq O$ , so ist  $n$  zusammengesetzt.
6. Ist  $lP = O$  und  $kP = O$ , so gehe zu 1.
7. Ist  $lP = O$  und  $kP \neq O$ , so ist  $n$  'wahrscheinlich' prim.
8. Wende den Algorithmus auf  $q$  statt  $n$  an.

*Bemerkung:* Der Algorithmus führt den Primzahltest für  $n$  sukzessive auf Primzahltests für Zahlen  $n_1 = q \leq n/2$ ,  $n_2 \leq n/4$ , usw. zurück. Stellt man nach  $t \leq \log(n)$  Durchläufen fest, dass  $n_t$  eine Primzahl ist, so auch  $n_{t-1}, \dots, n_1$  und  $n$ .

## 6.2 Faktorisierung

Der folgende Algorithmus von Lenstra berechnet einen nichttrivialen Teiler  $d$  einer zusammengesetzten Zahl  $n$ .

1. Wähle eine elliptische Kurve über  $\mathbb{Z}$ :

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

und einen Punkt  $P = (x, y)$  auf  $E$ .

2. Berechne  $t = \text{ggT}(4a^3 + 27b^2, n)$ .  
Falls  $1 < t < n$  setze  $d = t$ . Stopp  
Falls  $t = n$  gehe zu 1.

3. Wähle Konstanten  $B$  und  $C$  und setze

$$k = \prod_{\substack{l \leq B \\ l \text{ prim}}} l^{\alpha_l} \quad \text{mit } \alpha_l = \left\lfloor \frac{\log(C)}{\log(l)} \right\rfloor.$$

(Die Zahl  $k$  ist das Produkt aller Primzahlpotenzen  $l^{\alpha_l}$  mit Primzahlen  $l \leq B$  und  $l^{\alpha_l} \leq C$ .)

4. Versuche  $kP$  über  $\mathbb{Z}/n\mathbb{Z}$  zu berechnen. Taucht bei den Additionsformeln ein Nenner  $u$  mit  $d = \text{ggT}(u, n) > 1$  auf, dann stopp.

*Bemerkungen:*

1. Man kann zeigen, dass für  $t = 1$  und zusammengesetztes  $n$  mit hoher Wahrscheinlichkeit im letzten Schritt des Algorithmus ein  $d > 1$  auftaucht.
2. Die Laufzeit des Algorithmus hängt von der Wahl der Konstanten  $B$  und  $C$  ab.

# Literaturverzeichnis

- [1] I. Blake, G. Seroussi, N. Smart: Elliptic Curves in Cryptography, Cambridge University Press, 1999.
- [2] A. Enge: Elliptic Curves and Their Applications to Cryptography - An Introduction. Kluwer Academic Publishers, 1999.
- [3] D. Jungnickel: Finite Fields: Structure and Arithmetics. BI-Wissenschaftsverlag, 1993.
- [4] N. Koblitz: A course in number theory and cryptography. Springer 1987.
- [5] R. Lidl, H. Niederreiter: Finite Fields. Cambridge University Press, 1983.
- [6] A. J. Menezes: Elliptic Curve Public Key Cryptosystems. Kluwer Academic Publishers, 1993.
- [7] A. Menezes, P. Oorschot, S. Vanstone: Handbook of applied cryptography. CRC Press, 1997.