# 3. Elliptische Kurven über endlichen Körpern

Im ersten Abschnitt dieses Kapitels stellen wir die Frobeniusabbildung für elliptische Kurven über endlichen Körpern vor. Im zweiten und dritten Abschnitt gehen wir kurz auf verschiedene Verfahren ein, um die Gruppenordnung von $E(\mathbb{F}_q)$ zu bestimmen. Der vierte Abschnitt behandelt die sogenannten supersingulären elliptischen Kurven. Dies ist für kryptographische Zwecke relevant, da Kurven mit bestimmter Gruppenordnung und supersinguläre Kurven keine kryptographische Sicherheit bieten, wie wir in Kapitel 4 sehen werden.

In diesem Kapitel bezeichnen wir mit $F$ immer einen endlichen Körper, d.h. es ist $F = \mathbb{F}_q$ für eine Primzahlpotenz $q = p^r$. Die Charakteristik von $F$ ist also gleich $p$. Mit $\overline{F}$ bezeichnen wir den algebraischen Abschluß von $F$ (siehe 6.7).

Wie schon in Abschnitt 2.1 können wir zu einer Weierstraßgleichung mit Koeffizienten in $F$ nicht nur die elliptische Kurve $E(F)$ betrachten, sondern für jeden Erweiterungskörper $L$ von $F$ auch die elliptische Kurve $E(L)$ über $L$. Hier fassen wir die Weierstraßgleichung einfach als eine Gleichung über $L$ auf und betrachten Lösungen in $L$. Natürlich gilt

$$E(F) \subset E(L).$$

Insbesondere erhalten wir eine elliptische Kurve $E(\overline{F})$ über dem algebraischen Abschluß $\overline{F}$ von $F$.

## 3.1 Der Frobenius

**Lemma 3.1.1** *Es sei $E(F)$ eine elliptische Kurve über dem endlichen Körper $F = \mathbb{F}_q$. Dann vermittelt die Abbildung*

A. Werner, *Elliptische Kurven in der Kryptographie*

$$\begin{aligned} \phi: \quad \mathbb{P}^2(\overline{F}) &\longrightarrow \mathbb{P}^2(\overline{F}) \\ [x:y:z] &\longmapsto [x^q:y^q:z^q] \end{aligned}$$

*einen Homomorphismus von Gruppen*

$$\phi: E(\overline{F}) \to E(\overline{F}).$$

*Dieser wird Frobeniusendomorphismus (oder kurz Frobenius) genannt.*

**Beweis:** Zunächst ist klar, daß $\phi$ wirklich eine Abbildung von $\mathbb{P}^2(\overline{F})$ nach $\mathbb{P}^2(\overline{F})$ ist, denn zum einen können $x^q, y^q$ und $z^q$ nur dann gleichzeitig verschwinden, wenn dies schon für $x, y$ und $z$ gilt, und zum anderen erhält die Abbildung $\phi$ die Äquivalenzrelation, mit der $\mathbb{P}^2(\overline{F})$ definiert ist. Die elliptische Kurve $E(F)$ sei durch das Weierstraßpolynom

$$g(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

mit Koeffizienten $a_1, a_2, a_3, a_4$ und $a_6$ in $F$ gegeben. Es sei $P = [x : y : z]$ ein Punkt in $E(\overline{F})$, d.h. $x, y$ und $z$ sind Elemente aus $\overline{F}$, so daß $g(x,y,z) = 0$ ist. Also ist auch

$$g(x,y,z)^q = 0.$$

Wenn wir nun mehrmals hintereinander ausnutzen, daß für alle $c$ und $d$ in $\overline{F}$ die Gleichung

$$(c+d)^q = c^q + d^q$$

gilt (siehe 6.6.2), so folgt:

$$\begin{aligned} (y^q)^2z^q + a_1^q x^q y^q z^q + a_3^q y^q (z^q)^2 - (x^q)^3 - a_2^q (x^q)^2 z^q \\ - a_4^q x^q (z^q)^2 - a_6^q (z^q)^3 = 0. \end{aligned}$$

Da die $a_i$ in $F$ enthalten sind, gilt $a_i^q = a_i$, so daß

$$g(x^q, y^q, z^q) = 0$$

folgt. Also ist $\phi(P)$ wirklich wieder ein Punkt in $E(\overline{F})$.

Es bleibt zu zeigen, daß die so definierte Abbildung $\phi: E(\overline{F}) \to E(\overline{F})$ mit der Gruppenoperation verträglich ist. Nun ist $\phi([0:1:0]) = [0:1:0]$, also $\phi(O) = O$. Für alle $P \in E(\overline{F})$ gilt also

$$\phi(P+O) = \phi(P) = \phi(P) + O = \phi(P) + \phi(O).$$

Wenn $P_1$ und $P_2$ zwei Punkte ungleich $O$ in $E(\overline{F})$ sind, so können wir Satz 2.3.13 anwenden. Ist $P_1 = (x_1, y_1)$ und $P_2 = (x_2, y_2)$ in affinen Koordinaten, so daß $P_1 + P_2 \neq O$ ist, so gilt $P_1 + P_2 = (x_3, y_3)$ mit

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \text{ und } y_3 = -(\lambda + a_1)x_3 - \nu - a_3$$

und gewissen $\lambda, \nu$ in $\overline{F}$.

Daher ist

$$\phi(P_1 + P_2) = (x_3^q, y_3^q)$$

in affinen Koordinaten, wobei

$$x_3^q = (\lambda^q)^2 + a_1\lambda^q - a_2 - x_1^q - x_2^q \text{ und } y_3^q = -(\lambda^q + a_1)x_3^q - \nu^q - a_3$$

ist. Hier haben wir denselben Trick wie oben angewandt: Wir ziehen den Exponenten $q$ in die einzelnen Summanden hinein und lassen ihn dann bei den $a_i \in F$ einfach weg. Auf dieselbe Weise sieht man auch, daß $\lambda^q$ und $\nu^q$ gerade die mit $\phi(P_1) = (x_1^q, y_1^q)$ und $\phi(P_2) = (x_2^q, y_2^q)$ definierten Konstanten $\lambda$ und $\nu$ sind. Also folgt nach 2.3.13:

$$(x_3^q, y_3^q) = \phi(P_1) + \phi(P_2), \text{ und damit}$$

$$\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2).$$

Der Fall $P_1 + P_2 = O$ läßt sich genauso behandeln. □

## 3.2 Punkte zählen

Gegeben sei nun eine elliptische Kurve $E(F)$ mit der Weierstraßgleichung

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Wie können wir die Anzahl der Lösungen dieser Gleichung, also die Anzahl der Punkte in $E(F)$ bestimmen?

Wir wissen, daß genau ein Punkt aus $E(F)$, nämlich $O = [0:1:0]$, nicht im affinen Raum $\mathbb{A}^2(F)$ liegt. Also besteht $E(F)$ aus $O$ und den Lösungen der affinen Weierstraßgleichung

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

in $\mathbb{A}^2(F)$. Es genügt also, diese zu zählen. Setzen wir ein beliebiges $x$ aus $F$ in diese Gleichung ein (dafür gibt es $q$ Möglichkeiten), so erhalten wir eine quadratische Gleichung für $y$. Zu festem $x$ gibt es also höchstens zwei Werte $y \in F$, so daß $(x, y)$ eine Lösung ist. Daher erhalten wir die folgende obere Schranke für die Anzahl der Punkte in $E(F)$:

$$\#E(F) \leq 2q + 1.$$

Wir nehmen für den Moment einmal an, daß die Charakteristik von $F = \mathbb{F}_q$ nicht 2 ist. Dann können wir nach 2.3.2 ebenfalls annehmen, daß $a_1 = a_3 = 0$ ist. Unsere affine Weierstraßgleichung sieht also so aus:

$$y^2 = x^3 + a_2x^2 + a_4x + a_6 =: h(x).$$

Falls $h(x) = 0$ ist, so ist $y = 0$ die einzige Lösung. Falls $h(x) \neq 0$ und ein Quadrat in $\mathbb{F}_q$ ist, so finden wir zwei Lösungen $(x, y)$ und $(x, -y)$ dieser Gleichung, und falls $h(x)$ kein Quadrat in $\mathbb{F}_q$ ist, so hat $y^2 = h(x)$ gar keine Lösung. Es liegt daher nahe, folgende Funktion zu betrachten:

$$\chi : \mathbb{F}_q^\times \to \{-1, 1\},$$

wobei $\chi(x) = 1$, falls $x$ ein Quadrat in $\mathbb{F}_q$ ist (d.h. $x = z^2$ für ein $z \in \mathbb{F}_q$) und $\chi(x) = -1$, falls $x$ kein Quadrat in $\mathbb{F}_q$ ist.

Man kann leicht nachrechnen, daß sich $\chi$ auch folgendermaßen beschreiben läßt: Für einen beliebigen Erzeuger $\zeta$ der zyklischen Gruppe $\mathbb{F}_q^\times$ ist

$$\chi(\zeta^k) = 1 \text{ , falls } k \text{ gerade, und}$$
$$\chi(\zeta^k) = -1 \text{ , falls } k \text{ ungerade ist.}$$

Mit dieser Beschreibung sieht man auch, daß $\chi$ ein Gruppenhomomorphismus ist, d.h.

$$\chi(x_1x_2) = \chi(x_1)\chi(x_2)$$

gilt. Diese Abbildung $\chi$ heißt quadratischer Charakter und wird offenbar durch das Legendresymbol (siehe 6.3) gegeben, falls $q = p$ ist. Nach unserer Beschreibung des quadratischen Charakters sind die Hälfte der Elemente in $\mathbb{F}_q^\times$ Quadrate. Wir können $\chi$ zu einer Abbildung

$$\chi : \mathbb{F}_q \to \{-1, 0, 1\}$$

ergänzen, indem wir $\chi(0) = 0$ setzen. Dann hat für jedes $x \in \mathbb{F}_q$ die Gleichung $y^2 = h(x)$ genau $(\chi(h(x)) + 1)$-viele Lösungen $y$ in $\mathbb{F}_q$. Wir können also alle Lösungen der affinen Weierstraßgleichung durch

$$\sum_{x \in \mathbb{F}_q} (\chi(h(x)) + 1)$$

zählen. Daher folgt, wenn wir noch den Punkt $O$ berücksichtigen,

$$\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} (\chi(h(x)) + 1) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(h(x)).$$

In manchen Fällen kann man damit $\#E(\mathbb{F}_q)$ berechnen:

**Beispiel:**

1) Es sei $E(\mathbb{F}_{31})$ gegeben durch die affine Weierstraßgleichung

$$y^2 = x^3 - x \text{ über } \mathbb{F}_{31}.$$

In $\mathbb{F}_{31}$ ist $-1$ kein Quadrat. (Das folgt z.B. aus dem quadratischen Reziprozitätsgesetz (siehe 6.3.5), da $31 \equiv 3 \bmod 4$ ist). Also ist $\chi(-1) = -1$, woraus für alle $x$ in $\mathbb{F}_{31}$ mit $x^3 - x \neq 0$

$$\chi((-x)^3 - (-x)) = \chi(-(x^3 - x)) = \chi(-1)\chi(x^3 - x) = -\chi(x^3 - x)$$

folgt.

Die Gleichung $x^3 - x = 0$ ist nur für $x = 0, x = 1$ und $x = -1$ erfüllt, und in diesen Fällen ist natürlich $\chi(x^3 - x) = 0$. Für jedes $x \neq 0, 1, -1$ aus $\mathbb{F}_{31}$ gilt also: entweder $x^3 - x$ ist ein Quadrat in $\mathbb{F}_{31}$ oder $(-x)^3 - (-x)$ ist ein Quadrat in $\mathbb{F}_{31}$. Auf jeden Fall ist

$$\chi(x^3 - x) + \chi((-x)^3 - (-x)) = 0.$$

Also folgt:

$$\#E(\mathbb{F}_{31}) = 1 + 31 + \sum_{\substack{x \in \mathbb{F}_{31}^\times \\ x \neq \pm 1}} \chi(x^3 - x) = 32,$$

da sich die Beiträge für $x \in \mathbb{F}_{31}^\times$ paarweise wegheben.

2) Dieses Beispiel kann man noch etwas verallgemeinern: Mit demselben Argument kann man zeigen, daß für alle Primzahlen $p \equiv 3 \bmod 4$ die elliptische Kurve $E(\mathbb{F}_p)$, gegeben durch

$$y^2 = x^3 + ax$$

für ein beliebiges $a \neq 0$ in $\mathbb{F}_p$, gerade $(p+1)$-viele Punkte hat. Auch hier ist nämlich $-1$ kein Quadrat in $\mathbb{F}_p$.

Für eine beliebige elliptische Kurve $E(\mathbb{F}_q)$ wird die Summe

$$\sum_{x \in \mathbb{F}_q} \chi(h(x))$$

im allgemeinen ungleich Null sein. Allerdings scheint es plausibel, daß die von Null verschiedenen Werte $h(x)$ einigermaßen gleichmäßig in $\mathbb{F}_q^\times$ verteilt sind, so daß in etwa die Hälfte von ihnen ein Quadrat, die andere Hälfte hingegen kein Quadrat ist. Dann wäre der Term $\sum_{x \in \mathbb{F}q} \chi(h(x))$ zumindest nicht allzu groß, da die Summanden ungleich 0 in etwa zur Hälfte gleich 1 und zur Hälfte gleich $-1$ sind. In der Tat gibt es eine Abschätzung für den Term

$$\sum_{x \in \mathbb{F}_q} \chi(h(x)) = \#E(\mathbb{F}_q) - q - 1$$

durch den sogenannten Satz von Hasse, die besser ist als unsere Schranke

$$\#E(\mathbb{F}_q) - q - 1 \leq q.$$

Sie gilt ganz allgemein, d.h. wir lassen ab sofort unsere Voraussetzung $a_1 = a_3 = 0$ wieder fallen.

**Satz 3.2.1** *(Hasse) Es sei $E(F)$ eine beliebige elliptische Kurve über dem endlichen Körper $F = \mathbb{F}_q$. Dann gilt*

$$|\#E(F) - q - 1| \leq 2\sqrt{q}.$$

**Beweis:** Hier wird mehr Theorie über elliptische Kurven benötigt, als wir bisher entwickelt haben. Daher verweisen wir auf [Si], Theorem 1.1, S. 131. □

Man kann die Anzahl der Punkte auf einer elliptischen Kurve $E(F)$ über dem endlichen Körper $F$ mit $q$ Elementen also folgendermaßen abschätzen:

$$-2\sqrt{q}+q+1 \leq \#E(F) \leq 2\sqrt{q}+q+1.$$

Wir wollen nun kurz erklären, wieso die Zahl $q+1-\#E(F)$ auch oft "Spur des Frobenius" genannt wird.

Für jede Primzahl $l \neq p = \mathrm{char}(F)$ und alle $n \geq 1$ sei

$$E[l^n] = \{P \in E(\overline{F}) : l^n P = 0\}.$$

Man überlegt sich leicht, daß $E[l^n]$ eine Untergruppe von $E(\overline{F})$ ist. Außerdem kennt man ihre Gruppenstruktur, es gilt nämlich

$$E[l^n] \simeq \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$$

als endliche abelsche Gruppe (siehe [Si], Korollar 6.4, S. 89).

Betrachtet man für festes $l$ alle $E[l^n]$ gleichzeitig, so erhält man den Tatemodul $T_l(E)$ der elliptischen Kurve $E(\overline{F})$. Dieser ist definiert als Menge aller Ketten von Punkten $P_n \in E[l^n]$, die sukzessive mit der $l$-Multiplikation auf $E(\overline{F})$ ineinander überführt werden:

$$T_l(E) = \{(P_n)_{n\geq 1} : P_n \in E[l^n] \text{ und } lP_{n+1} = P_n \text{ für alle } n \geq 1\}.$$

Genauer gesagt ist $T_l(E)$ der inverse Limes der Gruppen $E[l^n]$. Das schreibt man auch als

$$T_l(E) = \lim_{\leftarrow} E[l^n].$$

Wir können die Elemente von $T_l(E)$ komponentenweise addieren. Auf ähnliche Weise betrachtet man alle Gruppen $\mathbb{Z}/l^n\mathbb{Z}$ gleichzeitig und definiert den Ring

$$\mathbb{Z}_l = \{(x_n)_{n\geq 1} : x_n \in \mathbb{Z}/l^n\mathbb{Z} \text{ und } x_{n+1} \equiv x_n \bmod l^n \text{ für alle } n \geq 1\}$$

(siehe 6.9).

Der Tatemodul $T_l(E)$ ist nun ein freier $\mathbb{Z}_l$-Modul vom Rang 2, d.h. es gibt eine Basis $x, y \in T_l(E)$, so daß

$$T_l(E) = \mathbb{Z}_l x \oplus \mathbb{Z}_l y.$$

Der Frobeniusendomorphismus $\phi : E(\overline{F}) \to E(\overline{F})$ induziert eine $\mathbb{Z}_l$-lineare Abbildung

$$\phi_l : T_l(E) \to T_l(E),$$

gegeben durch

$$\phi_l(P_n)_{n\geq 1} = (\phi(P_n))_{n\geq 1}.$$

Das ist wohldefiniert, da $\phi$ als Gruppenhomomorphismus $E[l^n]$ wieder nach $E[l^n]$ abbildet, denn aus $l^n P = O$ folgt $O = \phi(l^n P) = l^n \phi(P)$. Aus $\phi(lP) = l\phi(P)$ folgt außerdem, daß $(\phi(P_n))_{n\geq 1}$ wieder in $T_l(E)$ liegt.

Wenn wir nun wie oben eine Basis $x, y$ des $\mathbb{Z}_l$-Moduls $T_l(E)$ wählen, so läßt sich die lineare Abbildung $\phi_l$ darstellen durch eine $2 \times 2$-Matrix

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

mit Einträgen in $\mathbb{Z}_l$, d.h. es ist

$$\phi_l(x) = a_{11}x + a_{21}y \text{ und } \phi_l(y) = a_{12}x + a_{22}y.$$

Wir definieren nun tr $\phi_l$ (die Spur ("trace") des Frobenius) als die Spur der Matrix $A$, also

$$\text{tr } \phi_l = \text{ tr } A = a_{11} + a_{22}$$

und det $\phi_l$ (die Determinante des Frobenius) als die Determinante der Matrix $A$, also

$$\det \phi_l = \det A = a_{11}a_{22} - a_{12}a_{21}.$$

Nun gilt für jede $(2 \times 2)$-Matrix $A$:

$$A^2 - (\text{tr } A) \cdot A + \det A \cdot E = 0,$$

wobei $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ die Einheitsmatrix ist. (Das folgt aus der Tatsache, daß $A$ Nullstelle ihres charakteristischen Polynoms ist, läßt sich aber auch leicht direkt nachrechnen.)

Also folgt für die Abbildung $\phi_l$ auf $T_l(E)$:

$$\phi_l^2 - (\text{tr } \phi_l) \cdot \phi_l + (\det \phi_l) \cdot id = 0.$$

Man kann nun die Spur und die Determinante des Frobenius folgendermaßen berechnen:

**Proposition 3.2.2** *Es ist* $\det \phi_l = q$ *und* $\operatorname{tr} \phi_l = q + 1 - \#E(F)$.

**Beweis:** Dies geht über unsere Mittel hinaus. Wir verweisen daher auf [Si], Kapitel V, §2. □

Es gilt also

$$\phi_l^2 - (1 + q - \#E(F)) \cdot \phi_l + q \cdot id = 0.$$

Man kann nun zeigen, daß der Übergang von einem Homomorphismus der elliptischen Kurve zu einer linearen Abbildung des Tatemoduls injektiv ist. Daraus folgt, daß dieselbe Gleichung auch schon für den Frobeniusendomorphismus $\phi$ von $E(\overline{F})$ gilt:

$$\phi^2 - (1 + q - \#E(F)) \cdot \phi + q \cdot id = 0;$$

d.h. für jedes $P \in E(\overline{F})$ ist

$$\phi^2(P) - (1 + q - \#E(F))\phi(P) + qP = O.$$

Ein effektiver Algorithmus zur Bestimmung von $\#E(F)$ ist der sogenannte Schoof-Algorithmus, dessen Grundidee wir im folgenden Abschnitt kurz vorstellen wollen.

## 3.3 Der Schoof-Algorithmus

Wir nehmen an, daß $\operatorname{char}(F) > 2$ ist und daß $E(F)$ durch die affine Weierstraßgleichung

$$y^2 = x^3 + a_4 x + a_6$$

gegeben ist. (Falls außerdem $\operatorname{char}(F) \neq 3$ ist, findet man nach 2.3.2 immer eine Weierstraßgleichung dieser Gestalt.)

Die Spur des Frobenius $t = q + 1 - \#E(F)$ wird hier nicht als Ganzes, sondern modulo der ersten Primzahlen $l = 2, 3, 5, 7, \ldots$ bestimmt. Wieviele dieser Informationen $t$ mod $l$ braucht man, um $t$ und damit $\#E(F)$ zu berechnen?

Es seien $l_1 = 2, l_2 = 3, l_3 = 5, \ldots, l_r$ die ersten $r$ Primzahlen. Nach dem Chinesischen Restsatz (siehe 6.2.1) vermittelt die Restklassenabbildung

$$\mathbb{Z} \to \mathbb{Z}/l_1\mathbb{Z} \times \ldots \times \mathbb{Z}/l_r\mathbb{Z}$$

eine Bijektion $\mathbb{Z}/(l_1 \cdot \ldots \cdot l_r)\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/l_1\mathbb{Z} \times \ldots \times \mathbb{Z}/l_r\mathbb{Z}$. Falls

$$-\frac{l_1 \cdot \ldots \cdot l_r}{2} < t < \frac{l_1 \cdot \ldots \cdot l_r}{2},$$

so ist $t$ durch seine Restklasse in $\mathbb{Z}/(l_1 \cdot \ldots \cdot l_r)\mathbb{Z}$, und damit auch durch die $r$ Restklassen

$$(t \bmod l_1, t \bmod l_2, \ldots, t \bmod l_r)$$

eindeutig bestimmt.

Nach dem Satz von Hasse ist $-2\sqrt{q} \leq t \leq 2\sqrt{q}$, es genügt also, $r$ so zu wählen, daß

$$l_1 \cdot \ldots \cdot l_r > 4\sqrt{q}$$

ist.

Wir bestimmen zunächst $t$ mod 2. Offenbar ist $t \equiv \#E(F) \bmod 2$, so daß wir nur testen müssen, ob $\#E(F)$ gerade oder ungerade ist. Für festes $x \in F$ mit $x^3 + a_4x + a_6 \neq 0$ hat die Gleichung $y^2 = x^3 + a_4x + a_6$ keine oder zwei Lösungen $y$. Also ist die Anzahl aller Lösungen $(x, y)$ mit $y \neq 0$ gerade. Diese Punkte im affinen Raum können wir somit vernachlässigen. Es bleiben $O$ und die affinen Punkte $(x, 0)$ übrig. Falls die Gleichung $x^3 + a_4x + a_6 = 0$ eine Lösung $x_0 \in F$ hat, so können wir die linke Seite über dem algebraischen Abschluß $\overline{F}$ faktorisieren als

$$x^3 + a_4x + a_6 = (x - x_0)(x - x_1)(x - x_2)$$

mit $x_1$ und $x_2$ aus $\overline{F}$. Wie im Beweis von 2.3.3 kann man aus der Nicht-singularität von $E(F)$ schließen, daß die Nullstellen $x_0$, $x_1$ und $x_2$ paarweise verschieden sind.

Da $x_0 + x_1 + x_2 = 0$ ist (als Koeffizient vor $x^2$), sind $x_1$ und $x_2$ entweder beide in $F$ oder beide nicht in $F$. Im ersten Fall gibt es drei Punkte der Form $(x, 0)$ in $E(F)$, im zweiten Fall nur einen. Jedenfalls ist die Anzahl dieser Punkte ungerade. Wenn wir den Nullpunkt $O$ noch berücksichtigen, so gilt demnach $\#E(F) \equiv 1 \bmod 2$ (und damit $t \equiv 1 \bmod 2$) genau dann, wenn $x^3 + a_4x + a_6$ keine Lösung in $F$ hat, das Polynom $X^3 + a_4X + a_6$ also nicht von einem Faktor der Form $(X - b)$ für $b \in F$ geteilt wird. Da $X^q - X = \prod_{b \in F}(X - b)$ ist, ist dies genau dann der Fall, wenn im Polynomring $F[X]$

$$ggT(X^3 + a_4X + a_6, X^q - X) = 1$$

gilt, und das läßt sich effektiv testen.

Für $l \geq 3$ ist die Bestimmung von $t \bmod l$ schwieriger. Wir können hier nur sehr kurz die grundlegende Idee skizzieren, genauere Informationen findet man in [Sch1] und [Sch3].

In 3.2 haben wir gesehen, daß der Frobenius $\phi : E(\overline{F}) \to E(\overline{F})$ der Gleichung

$$\phi^2(P) - t\phi(P) + qP = O \text{ für alle } P \in E(\overline{F})$$

genügt.

Gesucht ist nun eine Zahl $\tau \in \{0, \ldots, l-1\}$ so daß die Gleichung

$$\phi^2(P) - \tau\phi(P) + qP = O$$

für jeden Punkt $P$ aus der endlichen Untergruppe

$$E[l] = \{P \in E(\overline{F}) : lP = O\}$$

gilt. Falls wir ein solches $\tau$ finden, so muß nämlich für jedes $P \neq O$ in $E[l]$

$$(t - \tau)\phi(P) = O$$

sein. Nun ist $\phi(P)$ ebenfalls ein Punkt $\neq O$ in $E[l]$, d.h. $\phi(P)$ hat die Ordnung $l$ in der Gruppe $E(\overline{F})$. Daher muß $l$ ein Teiler von $t - \tau$ sein, so daß

$$t \equiv \tau \bmod l$$

ist. Wir haben also unsere Restklasse $t \bmod l$ gefunden!

Wie findet man aber solch eine Zahl $\tau$? Kurz gesagt, kann man die Aussage

$$\text{“}\phi^2(P) - \tau\phi(P) + qP = O \text{ für alle } P \in E[l]\text{”}$$

in eine Polynomgleichung übersetzen, indem man die Polynome benutzt, die in den expliziten Formeln 2.3.13 vorkommen, und die sogenannten Divisionspolynome, mit denen man testen kann, ob ein Punkt in $E[l]$ liegt.

Für $\tau = 0, 1, 2, \ldots, l-1$ probiert man nun der Reihe nach, ob diese Polynomgleichung erfüllt ist. Sobald dies der Fall ist, hat man das richtige $\tau$ gefunden.

## 3.4 Supersinguläre elliptische Kurven

**Definiton 3.4.1** *Die elliptische Kurve $E(F)$ heißt supersingulär, falls $p = char(F)$ die Spur des Frobenius* tr $\phi_l = q + 1 - \#E(F)$ *teilt.*

Hier muß man aufpassen, daß man supersingulär nicht mit singulär verwechselt! Elliptische Kurven sind definitionsgemäß immer nichtsingulär (und zwar für beliebige Grundkörper). Eine elliptische Kurve über einem endlichen Körper kann zusätzlich supersingulär sein oder nicht.

Ein einfaches Beispiel für eine supersinguläre Kurve ist die elliptische Kurve $E(\mathbb{F}_2)$ über $\mathbb{F}_2$, die durch die affine Weierstraßgleichung

$$y^2 + y = x^3 + x + 1$$

gegeben wird.

Man kann leicht nachrechnen, daß diese affine Gleichung keine Lösungen über $\mathbb{F}_2$ besitzt. Also ist $E(\mathbb{F}_2) = \{O\}$, so daß die Zahl $q + 1 - \#E(\mathbb{F}_2) = 2$ in der Tat durch 2 teilbar ist.

Das folgende Lemma besagt, daß Supersingularität bei Übergang zu einem Erweiterungskörper erhalten bleibt.

**Lemma 3.4.2** *Es sei $E(\mathbb{F}_q)$ eine elliptische Kurve über $\mathbb{F}_q$. Falls $E(\mathbb{F}_q)$ supersingulär ist, so auch $E(\mathbb{F}_{q^k})$ für alle $k \geq 1$.*

**Beweis:** Wir zeigen die Behauptung mit Induktion nach $k$. Wir nehmen also an, die Kurven

$$E(\mathbb{F}_q), E(\mathbb{F}_{q^2}), \ldots, E(\mathbb{F}_{q^k})$$

sind supersingulär.

Wie am Ende von Abschnitt 3.2 betrachten wir für eine fest gewählte Primzahl $l \neq p = \text{char}(\mathbb{F}_q)$ die lineare Abbildung $\phi_l : T_l(E) \to T_l(E)$, die durch den Frobenius auf dem Tatemodul induziert wird. Diese wiederum induziert eine lineare Abbildung $\phi_l : V_l \to V_l$, wobei $V_l$ der zweidimensionale $\mathbb{Q}_l$-Vektorraum ist, der durch Basiswechsel aus $T_l(E)$ entsteht, d.h. $V_l = \mathbb{Q}_l x \oplus \mathbb{Q}_l y$, falls $T_l(E) = \mathbb{Z}_l x \oplus \mathbb{Z}_l y$ ist. Das charakteristische Polynom von $\phi_l$ auf $V_l$ ist

$$X^2 - (\operatorname{tr} \phi_l)X + \det \phi_l,$$

also nach 3.2.2

$$X^2 - (q + 1 - \#E(\mathbb{F}_q))X + q.$$

Über einem geeigneten Erweiterungskörper zerfällt es in Linearfaktoren, d.h. es gilt

$$X^2 - (q + 1 - \#E(\mathbb{F}_q))X + q = (X - a)(X - b),$$

wobei $a$ und $b$ die Eigenwerte von $\phi_l$ sind. Wenn wir einen Eigenvektor zu $a$ zu einer Basis ergänzen, so hat $\phi_l$ bezüglich dieser Basis die Koordinatenmatrix

$$A = \begin{pmatrix} a & c \\ 0 & b \end{pmatrix}$$

mit einem Koeffizienten $c$, der uns nicht weiter interessiert. Offenbar ist die Spur des Frobenius $\operatorname{Tr}(\phi_l) = a + b$.

Wir bezeichnen nun für $m \geq 1$ mit

$$\phi(\mathbb{F}_{q^m}) : E(\overline{\mathbb{F}}_{q^m}) \to E(\overline{\mathbb{F}}_{q^m})$$

den Frobenius, der zum Grundkörper $\mathbb{F}_{q^m}$ gehört. (Dieser wird also von der Abbildung $x \mapsto x^{q^m}$ induziert.) Mit dieser Terminologie ist $\phi = \phi(\mathbb{F}_q)$. Es gilt definitionsgemäß

$$\phi(\mathbb{F}_{q^m}) = \phi(\mathbb{F}_q)^m = \phi^m,$$

wobei $\phi^m$ die $m$-fache Hintereinanderausführung von $\phi$ bezeichnet. Also folgt auch

$$\phi_l(\mathbb{F}_{q^m}) = \phi_l^m.$$

Daher ist $A^m$ die Koordinatenmatrix zu $\phi_l(\mathbb{F}_{q^m})$, woraus sofort

$$\operatorname{Tr} \phi_l(\mathbb{F}_{q^m}) = a^m + b^m$$

folgt. Unsere Induktionsvoraussetzung besagt also, daß $p$ die Spuren des Frobenius $a + b, a^2 + b^2, \ldots, a^k + b^k$ teilt. Wir müssen zeigen, daß auch $a^{k+1} + b^{k+1}$ ein Vielfaches von $p$ ist, denn dann ist $E(\mathbb{F}_{q^{k+1}})$ supersingulär.

Dazu berechnen wir

$$(a + b)^{k+1} = \sum_{l=0}^{k+1} \binom{k+1}{l} a^l b^{k+1-l}$$

$$= a^{k+1} + b^{k+1} + \sum_{l=1}^{k} \binom{k+1}{l} a^l b^{k+1-l}$$

Nun fassen wir jeweils die äußeren Terme in der Summe zusammen und erhalten

$$\begin{aligned}
&\sum_{l=1}^{k} \binom{k+1}{l} a^l b^{k+1-l} \\
&= \binom{k+1}{1} \text{ ab } (b^{k-1} + a^{k-1}) + \binom{k+1}{2} a^2 b^2 (b^{k-3} + a^{k-3}) \\
&\quad + \ldots + \begin{cases} \binom{k+1}{\frac{k+1}{2}} a^{\frac{k+1}{2}} b^{\frac{k+1}{2}} & \text{, falls } k+1 \text{ gerade} \\ \binom{k+1}{\frac{k}{2}} a^{\frac{k}{2}} b^{\frac{k}{2}} (b+a) & \text{, falls } k+1 \text{ ungerade.} \end{cases}
\end{aligned}$$

Wenn wir noch beachten, daß nach 3.2.2

$$ab = \det A = q$$

ist, so ist jeder Term in dieser Summe ein ganzzahliges Vielfaches von $p$. Dasselbe gilt für $(a+b)^{k+1}$, so daß auch $a^{k+1} + b^{k+1}$ ein Vielfaches von $p$ sein muß. □

Für $p \geq 3$ können wir folgendes Kriterium für Supersingularität zeigen:

**Proposition 3.4.3** *Es sei $p \geq 3$ und $E(\mathbb{F}_p)$ eine elliptische Kurve über $\mathbb{F}_p$, die durch eine Weierstraßgleichung der Form*

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6 = h(x)$$

*gegeben ist. Dann ist $E(\mathbb{F}_p)$ supersingulär genau dann, wenn der Koeffizient von $x^{p-1}$ in dem Polynom $h(x)^{\frac{p-1}{2}}$ (über $\mathbb{F}_p$) gleich Null ist.*

**Beweis:** Wir haben in 3.2 schon gesehen, daß

$$\#E(\mathbb{F}_p) - 1 - p = \sum_{x \in \mathbb{F}_p} \chi(h(x))$$

ist, wobei

$$\chi : \mathbb{F}_p \to \{-1, 0, 1\}$$

die Fortsetzung des quadratischen Charakters $\chi : \mathbb{F}_p^\times \to \{-1, 1\}$ ist.

Es sei $\zeta$ ein Erzeuger der zyklischen Gruppe $\mathbb{F}_p^\times$. Dann ist $\chi(\zeta^k) = 1$, falls $k$ gerade, und $\chi(\zeta^k) = -1$, falls $k$ ungerade ist. Nun ist $\zeta^{\frac{p-1}{2}} = -1$ in $\mathbb{F}_p$, wie z. B. aus der Gleichung $\zeta^{\frac{p-1}{2}} + 1 = \zeta^{\frac{p-1}{2}} + \zeta^{p-1} = \zeta^{\frac{p-1}{2}}(1 + \zeta^{\frac{p-1}{2}})$ folgt. Also ist

$$\chi(\zeta^k) \equiv \zeta^{\frac{p-1}{2}k} \bmod p.$$

Daher gilt für alle $x \in \mathbb{F}_p^\times$ (und trivialerweise auch für $x = 0$):

$$\chi(x) \equiv x^{\frac{p-1}{2}} \bmod p.$$

Wir wollen nun zunächst zeigen, daß für alle natürlichen Zahlen $j \geq 1$ folgende Gleichung in $\mathbb{F}_p$ gilt:

$$\sum_{x \in \mathbb{F}_p} x^j = \begin{cases} -1, & \text{falls } (p-1) \text{ ein Teiler von } j \text{ ist} \\ 0, & \text{falls } (p-1) \text{ kein Teiler von } j \text{ ist.} \end{cases}$$

Wir können nämlich die Summe auf der linken Seite auch schreiben als

$$\sum_{x \in \mathbb{F}_p} x^j = 0 + \sum_{k=0}^{p-2} (\zeta^k)^j = \sum_{k=0}^{p-2} \zeta^{kj}.$$

Falls nun $(p-1)$ ein Teiler von $j$ ist, so ist $\zeta^j = 1$, also folgt

$$\sum_{k=0}^{p-2} \zeta^{kj} = p - 1 = -1$$

in $\mathbb{F}_p$.

Falls $(p-1)$ kein Teiler von $j$ ist, so ist $\zeta^j \neq 1$. Wir wählen ein $x \in \mathbb{Z}$ mit $x \equiv \zeta^j \bmod p$. Dann ist

$$\sum_{k=0}^{p-2} x^k = \frac{1 - x^{p-1}}{1 - x}$$

nach der geometrischen Summenformel, da $x \neq 1$ ist. Wir betrachten beide Seiten modulo $p$ und erhalten

$$\sum_{k=0}^{p-2} \zeta^{kj} = \frac{1 - \zeta^{j(p-1)}}{1 - \zeta^j} = 0,$$

da $(\zeta^{p-1})^j = 1$ ist.

Definitionsgemäß ist $E(\mathbb{F}_p)$ supersingulär genau dann, wenn

$$\#E(\mathbb{F}_p) - 1 - p = \sum_{x \in \mathbb{F}_p} \chi(h(x)) \equiv 0 \bmod p$$

ist, also genau dann, wenn $\sum_{x \in \mathbb{F}_p} h(x)^{\frac{p-1}{2}} = 0$ in $\mathbb{F}_p$ ist. Nun ist

$$h(x)^{\frac{p-1}{2}} = (x^3 + a_2 x^2 + a_4 x + a_6)^{\frac{p-1}{2}}.$$

Wenn wir das ausmultiplizieren, erhalten wir ein Polynom in $x$ vom Grad $3\frac{p-1}{2}$:

$$h(x)^{\frac{p-1}{2}} = x^{3\frac{p-1}{2}} + b_{3\frac{p-1}{2}-1} x^{3\frac{p-1}{2}-1} + \ldots + b_2 x^2 + b_1 x + b_0$$

mit gewissen Koeffizienten $b_i \in \mathbb{F}_p$.

Wir benutzen nun unsere Formel für $\sum_{x \in \mathbb{F}_p} x^j$, um auszurechnen

$$\begin{aligned} \sum_{x \in \mathbb{F}_p} h(x)^{\frac{p-1}{2}} &= \sum_{x \in \mathbb{F}_p} x^{3\frac{p-1}{2}} + \ldots + b_2 \sum_{x \in \mathbb{F}_p} x^2 + b_1 \sum_{x \in \mathbb{F}_p} x + b_0 \sum_{x \in \mathbb{F}_p} 1 \\ &= -b_{p-1} \text{ in } \mathbb{F}_p, \end{aligned}$$

denn die einzige Zahl $j \in \{1, 2, \ldots, 3\frac{p-1}{2}\}$, die ein Vielfaches von $(p-1)$ ist, ist $(p-1)$ selbst. Alle anderen Beiträge müssen verschwinden. Daher ist $\sum_{x \in \mathbb{F}_p} h(x)^{\frac{p-1}{2}} = 0$ in $\mathbb{F}_p$ genau dann, wenn der Koeffizient $b_{p-1}$ vor $x^{p-1}$ in $h(x)^{\frac{p-1}{2}}$ verschwindet. □

Wir betrachten noch einmal unser altes Beispiel

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

aus Kapitel 2. Wir haben in Abschnitt 2.1 gesehen, daß die so definierte Kurve singulär über $\mathbb{F}_2$ und nicht-singulär über $\mathbb{F}_p$ für $p \geq 3$ ist. Im letzteren Fall gibt uns diese affine Weierstraßgleichung also eine elliptische Kurve $E(\mathbb{F}_p)$. Wann ist $E(\mathbb{F}_p)$ supersingulär?

Wir wenden das Kriterium aus Proposition 3.4.3 an und berechnen

$$(x^3 + x)^{\frac{p-1}{2}} = \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} x^{3j} x^{\frac{p-1}{2}-j} \text{ in } \mathbb{F}_p.$$

Es kommen also nur Potenzen der Form $x^{\frac{p-1}{2}+2j}$ vor. Nun ist

$$\frac{p-1}{2} + 2j = p-1 \text{ genau dann, wenn } 2j = \frac{p-1}{2}$$

ist. Das kann nur eintreten, wenn $\frac{p-1}{2}$ gerade, also $p \equiv 1 \bmod 4$ ist. In diesem Fall ist der Koeffizient vor $x^{p-1}$ gleich $\binom{\frac{p-1}{2}}{\frac{p-1}{4}}$, und diese Zahl verschwindet nicht in $\mathbb{F}_p$. $E(\mathbb{F}_p)$ ist hier also nicht supersingulär. Falls hingegen $p \equiv 3 \bmod 4$ ist, so kommt gar kein $x^{p-1}$-Summand vor, in diesem Fall ist $E(\mathbb{F}_p)$ also supersingulär.

Das paßt mit unseren alten Berechnungen in Abschnitt 2.1 zusammen. Dort haben wir nämlich gesehen, daß die affine Gleichung $y^2 = x^3 + x$ über $\mathbb{F}_3$ und über $\mathbb{F}_5$ je drei Lösungen hat. Also folgt ($O$ nicht vergessen!)

$$\#E(\mathbb{F}_3) = 4, \text{ daher gilt } 3 | (\#E(\mathbb{F}_3) - 3 - 1) \text{ und}$$

$$\#E(\mathbb{F}_5) = 4, \text{ daher gilt } 5 \not| (\#E(\mathbb{F}_5) - 5 - 1).$$

Falls $\mathrm{char}(F) = 2$ ist, läßt sich Proposition 3.4.3 nicht anwenden. In diesem Fall gibt es aber ein ganz einfaches Kriterium für Supersingularität:

**Proposition 3.4.4** *Es sei $\mathrm{char}(F) = 2$ und $E(F)$ eine elliptische Kurve, gegeben durch die affine Weierstraßgleichung*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

*Dann ist $E(F)$ supersingulär genau dann, wenn $a_1 = 0$ ist.*

**Beweis:** Definitionsgemäß ist $E(F)$ supersingulär, falls die Spur des Frobenius $q + 1 - \#E(F)$ gerade ist. Da hier $q = 2^r$ ist, ist das genau dann der Fall, wenn $\#E(F)$ ungerade ist.

Nun ist die Anzahl der Elemente in der endlichen abelschen Gruppe $E(F)$ gerade genau dann, wenn es ein Element $P \in E(F)$ der Ordnung 2 gibt. (Wie jede endliche abelsche Gruppe ist $E(F)$ isomorph zu einem Produkt $\mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_s\mathbb{Z}$. Wenn $\#E(F)$ gerade ist, so muß eines der $d_i$ gerade sein, so daß $\mathbb{Z}/d_i\mathbb{Z}$ und damit $E(F)$ ein Element der Ordnung 2 enthält.)

Es genügt also zu zeigen: Es gibt ein $P \neq O$ in $E(F)$ mit $2P = O$ genau dann, wenn $a_1 \neq 0$ ist. Nach unseren expliziten Additionsformeln 2.3.13 gilt: $P = (x, y)$ erfüllt $2P = O$ genau dann, wenn

$$2y + a_1 x + a_3 = 0, \text{ also } a_1 x + a_3 = 0$$

ist.

Falls nun $a_1 \neq 0$ ist, so setzen wir

$$x = -\frac{a_3}{a_1}.$$

Außerdem wählen wir ein $y \in F$ mit

$$y^2 = x^3 + a_2 x^2 + a_4 x + a_6.$$

Dies ist möglich, da im Fall $\mathrm{char}(F) = 2$ *jedes* Element in $F$ ein Quadrat ist. (Für 0 ist das ohnehin klar. Die Einheitengruppe $F^\times$ ist zyklisch, erzeugt von einem $\zeta$ der Ordnung $q - 1 = 2^r - 1$. Also gilt $\zeta^{2^r} = \zeta^{2^r - 1} \cdot \zeta = \zeta$, so daß $\zeta$ und damit auch jedes andere Element von $F^\times$ in der Tat ein Quadrat ist).

Dann gilt $a_1 x + a_3 = 0$ und $y^2 + y(a_1 x + a_3) = x^3 + a_2 x^2 + a_4 x + a_6$, also ist $P = (x, y)$ ein Punkt in $E(F)$ der Ordnung 2.

Wir nehmen nun umgekehrt an, daß $E(F)$ einen Punkt $P = (x, y)$ der Ordnung 2 enthält, d.h. es gilt

$$a_1 x + a_3 = 0.$$

Falls hier $a_1 = 0$ ist, so muß auch $a_3 = 0$ sein. $E(F)$ wird also durch die Gleichung

$$f(x, y) = y^2 - x^3 - a_2 x^2 - a_4 x - a_6 = 0.$$

gegeben.

Es ist

$$\frac{\partial f}{\partial y}(x, y) = 0 \text{ und } \frac{\partial f}{\partial x}(x, y) = x^2 + a_4,$$

wenn man die Rechenregeln in Charakteristik 2 berücksichtigt. Da jedes Element von $F$ ein Quadrat in $F$ ist, gibt es ein $x \in F$ mit

$$x^2 + a_4 = 0$$

und ein $y \in F$ mit

$$y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

Dann ist $P = (x, y)$ ein Punkt in $E(F)$, für den beide Ableitungen verschwinden. Das kann aber nicht sein, da $E(F)$ nicht-singulär ist.

Der Fall $a_1 = 0$ kann also hier nicht auftreten, so daß in der Tat $a_1 \neq 0$ folgt. □

Wir werden im folgenden Kapitel sehen, daß supersinguläre Kurve für kryptographische Zwecke schlecht geeignet sind.