Seminar Kryptographie

Satz von Hasse-Weil

Autor:
Philipp Hessler

Dozent:
Dr. Mohamed Barakat

23. Mai 2011

Inhaltsverzeichnis

1 Motivation

Im Folgenden beschäftigen wir uns mit der Anzahl der Elemente der Gruppe über einer elliptischen Kurve. Zunächst einige Beispiele dazu:

Beispiel 1. Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2+xy = x^3+1$. Wie viele Elemente hat die Gruppe $E(\mathbb{F}_2)$?

Um diese Anzahl zu berechnen, berechnen wir alle Punkte auf der Kurve. Dazu gehen wir alle Möglichkeiten für x durch und lösen die Gleichung nach y auf. Natürlich ist in jedem Fall der Punkt im Unendlichen **O** auf der Kurve.

Damit ergibt sich folgende Tabelle:

x	x^3+1	y^2+xy	y	Punkte
0	1	y^2	1	$(0,1)$
1	0	y^2+y	0	$(1,0)$
			1	$(1,1)$
O			**O**	**O**

$E(\mathbb{F}_2)$ hat also 4 Elemente.

Was passiert, wenn man dieselbe Kurve nicht über $\mathbb{F}_2 = \{0,1\}$, sondern über $\mathbb{F}_4 = \{0,1,\omega,\omega^2\}$ mit $\omega^2+\omega+1=0$ betrachtet?

Beispiel 2. Wie viele Elemente hat die Gruppe $E(\mathbb{F}_4)$?

Mit demselben Verfahren wie im vorherigen Beispiel ergibt sich.

x	x^3+1	y^2+xy	y	Punkte
0	1	y^2	1	$(0,1)$
1	0	y^2+y	0	$(1,0)$
			1	$(1,1)$
ω	0	$y^2+\omega y$	0	$(\omega,0)$
			ω	(ω,ω)
ω^2	0	$y^2+\omega^2 y$	0	$(\omega^2,0)$
			ω^2	(ω^2,ω^2)
O			**O**	**O**

$E(\mathbb{F}_2)$ hat also 8 Elemente.

Dieses Verfahren ist offensichtlich nur für kleine Gruppen praktikabel. Das folgende Beispiel klären wir am Ende mit Hilfe des Satzes von Hasse-Weil.

Beispiel 3. Wie viele Elemente hat die Gruppe $E(\mathbb{F}_{2^{101}})$?

Wir suchen also eine Möglichkeit die Anzahl der Elemente einer Gruppe über einer elliptischen Kurve abzuschätzen und wenn möglich genau zu berechnen. Genau das ermöglicht uns der Satz von Hasse-Weil:

Theorem 4 (Satz von Hasse-Weil)**.** *Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $a := q + 1 - \#E(\mathbb{F}_q)$. Dann gilt:*

$$|a| \leq 2\sqrt{q} \tag{1}$$

Sei $x^2 - ax + q = (x - \alpha)(x - \beta)$. Dann gilt für alle $n \geq 1$:

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n) \tag{2}$$

2 Frobenius Endomorphismus

Um diesen Satz zu beweisen, müssen wir uns zunächst mit dem Frobenius Endomorphismus beschäftigen. Nicht alle Eigenschaften dieser Abbildung werden hier gezeigt. Die fehlenden Beweise findet man in [Was08].

Definition 5. Sei $\mathbb{F}_q$ ein endlicher Körper mit algebraischem Abschluss $\overline{\mathbb{F}_q}$. Die Frobenius-Abbildung $\phi_q : \overline{\mathbb{F}_q} \longrightarrow \overline{\mathbb{F}_q}$ ist definiert durch $\phi_q(x) := x^q$.

Auf elliptischen Kurven gilt $\phi_q(x, y) = (x^q, y^q)$ und $\phi_q(\mathbf{O}) = \mathbf{O}$.

Lemma 6. *ϕ_q ist ein Endomorphismus von E vom Grad q und nicht separabel.*

Beweis. [Was08, S. 53] □

Wir benötigen aus diesem Lemma nur die Aussage $\deg(\phi_q) = q$ direkt. Die Tatsache, dass ϕ_q ein Endomorphismus ist, fließt aber in einige der Lemmas ein.

Betrachten wir nun, was passiert, wenn man ϕ_q auf die Elemente einer elliptischen Kurve anwendet.

Beispiel 7. Sei E eine elliptische Kurve über $\mathbb{F}_4$ gegeben durch $y^2+xy = x^3+1$.

(x, y)	$\phi_q(x, y)$
$(0, 1)$	$(0, 1)$
$(1, 0)$	$(1, 0)$
$(1, 1)$	$(1, 1)$
$(\omega, 0)$	$(\omega, 0)$
(ω, ω)	(ω, ω)
$(\omega^2, 0)$	$(\omega^2, 0)$
(ω^2, ω^2)	(ω^2, ω^2)
$\mathbf{O}$	$\mathbf{O}$

Offenbar ist ϕ_q auf einer elliptischen Kurve gerade die Identität. Diese Beobachtung verfeinern wir nun.

Lemma 8. *Sei $(x, y) \in E(\overline{\mathbb{F}_q})$. Dann gilt:*

1. $\phi_q(x,y) \in E(\overline{\mathbb{F}_q})$
2. $(x,y) \in E(\mathbb{F}_q) \iff \phi_q(x,y) = (x,y)$

Beweis. Sei $(x,y) \in E(\overline{\mathbb{F}_q})$. Dann erfüllen x und y die Weierstrassgleichung

$$\begin{aligned} y^2 + a_1xy + a_3y &= x^3 + a_2x^2 + a_4x + a_6 \\ \implies (y^2 + a_1xy + a_3y)^q &= (x^3 + a_2x^2 + a_4x + a_6)^q \end{aligned}$$

Da q eine Potenz der Charakteristik von $\mathbb{F}_q$ ist, gilt $(\alpha+\beta)^q = \alpha^q + \beta^q$ für $\alpha, \beta \in \overline{\mathbb{F}_q}$ (siehe [Bar11, S. 32]).

$$\implies (y^2)^q + (a_1xy)^q + (a_3y)^q = (x^3)^q + (a_2x^2)^q + (a_4x)^q + (a_6)^q$$

Außerdem gilt für $\alpha \in \overline{\mathbb{F}_q}$, dass $\alpha \in \mathbb{F}_q$ genau dann, wenn $\alpha^q = \alpha$. Durch Umformen der Gleichung erhält man

$$\implies (y^q)^2 + a_1x^qy^q + a_3y^q = (x^q)^3 + a_2(x^q)^2 + a_4x^q + a_6$$

Also ist $\phi_q(x,y) \in E(\mathbb{F}_q)$. Das zeigt den ersten Teil.

Sei nun $(x,y) \in E(\mathbb{F}_q)$. Dies gilt genau dann, wenn $x, y \in \mathbb{F}_q$, da wir $(x,y) \in E(\overline{\mathbb{F}_q})$ vorausgesetzt haben. Es ist aber weiter

$$x, y \in \mathbb{F}_q \iff \phi_q(x) = x, \phi_q(y) = y$$

Das ist nach Definition äquivalent zu $\phi_q(x,y) = (x,y)$. Hiermit ist der zweite Teil bewiesen. □

Mit Hilfe dieses Lemmas können wir nun einen ersten Zusammenhang zwischen dem Frobenius-Endomorphismus und den Elementen von $E(\mathbb{F}_q)$ herstellen.

Proposition 9. *Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $n \geq 1$. Dann gilt:*

1. $\ker(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$
2. $\phi_q^n - 1$ *ist ein separabler Endomorphismus, also gilt:*

$$\deg(\phi_q^n - 1) = \#\ker(\phi_q^n - 1) \overset{(1.)}{=} \#E(\mathbb{F}_{q^n}) \tag{3}$$

Beweis. Beachte zunächst, dass $\phi_q^n = \phi_{q^n}$ gilt. Dann ist die erste Aussage eine Umformulierung der zweiten Aussage des letzten Lemmas.

Die Separabilität folgt aus Proposition 13. Die behauptete Gleichung ist dann eine direkte Folgerung von Proposition 14. □

Diese Proposition wird nun ein wichtiger Baustein im Beweis des Satzes von Hasse-Weil sein. Allerdings wird er oft nur als Voraussetzung zur Anwendung anderer Sätze verwendet werden.

3 Beweis Satz von Hasse-Weil

Um den ersten Teil des Satzes zu beweisen, benötigen wir zunächst noch ein Lemma.

Lemma 10. *Seien $r, s \in \mathbb{Z}$ mit $\gcd(s, q) = 1$. Dann gilt:*

$$\deg(r\phi_q - s) = r^2 q + s^2 - rsa \tag{4}$$

Beweis. Zur Erinnerung: $a = q + 1 - \#E(\mathbb{F}_q)$. Mit (3) aus Proposition 9 ergibt sich dann $a = q + 1 - \det(\phi_q - 1)$.

Mittels Proposition 15 und $\deg(\phi_q) = q$ und $\deg(-1) = 1$ folgt

$$\begin{aligned}\deg(r\phi_q - s) &\overset{(4)}{=} r^2 \deg(\phi_q) + s^2 \deg(-1) + rs\left(\deg(\phi_q - 1) - \deg(\phi_q) - \deg(-1)\right)\\ &= r^2 q + s^2 + rs\left(\deg(\phi_q - 1) - q - 1\right)\\ &= r^2 q + s^2 - rsa\end{aligned}$$

□

Nun sind wir bereit für den ersten Teil des Satzes.

Theorem 4 (Satz von Hasse-Weil (1. Teil))**.** *Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $a := q + 1 - \#E(\mathbb{F}_q)$. Dann gilt:*

$$|a| \leq 2\sqrt{q} \tag{1}$$

Beweis. Da der Grad nach Definition nicht negativ sein kann, gilt nach dem Lemma für alle $r, s \in \mathbb{Z}$ mit $\gcd(s, q) = 1$

$$\begin{aligned}0 \leq \deg(\phi_q) &= r^2 q + s^2 - rsa\\ \Longrightarrow 0 &\leq q\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1\end{aligned}$$

Die Menge $\left\{\frac{r}{s} \text{ mit } \gcd(s, q) = 1\right\}$ ist dicht in $\mathbb{R}$. Um dies zu sehen, kann man s als Potenzen von 2 oder 3 wählen (eines von beidem ist zulässig) und r beliebig.

Daher gilt sogar für alle $x \in \mathbb{R}$

$$0 \leq qx^2 - ax + 1$$

Also hat die quadratische Funktion $f(x) = qx^2 - ax + 1$ höchstens eine Nullstelle. Die Diskriminante darf daher nicht positiv sind.

$$\begin{aligned}&\Longrightarrow a^2 - 4q \leq 0\\ &\Longrightarrow |a| \leq 2\sqrt{q}\end{aligned}$$

□

Bevor wir den zweiten Teil des Satzes beweisen, müssen wir uns erneut den Frobenius Endomorphismus ansehen.

Theorem 11. *Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $a = q + 1 - \#E(\mathbb{F}_q)$. Dann ist $\phi_q^2 - a\phi_q + q = 0$ als Endomorphismus auf E und a ist die eindeutige ganze Zahl mit dieser Eigenschaft. Es handelt sich also um das Minimalpolynom von ϕ_q.*

Außerdem gilt für $m \in \mathbb{N}$ mit $\gcd(m, q) = 1$

$$a \equiv \mathit{Trace}((\phi_q)_m) \ (\mathit{mod}\ m) \tag{5}$$

Beweis. Falls $\phi_q^2 - a\phi_q + q$ nicht der Null-Endomorphismus ist, dann gilt für den Kern nach Proposition 14:

$$\#\ker(\phi_q^2 - a\phi_q + q) \leq \deg(\phi_q^2 - a\phi_q + q)$$

Der Kern muss in diesem Fall also endlich sein. Wir werden zeigen, dass der Kern unendlich ist, also muss dann $\phi_q^2 - a\phi_q + q$ der Null-Endomorphismus sein.

Sei $m \in \mathbb{N}$ mit $\gcd(m, q) = 1$.

Bezeichne mit $(\phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$ den Frobenius Endomorphismus auf den m-Torsionspunkten $E[m] := \left\{P \in E(\overline{\mathbb{F}_q}) \text{ mit } mP = \mathbf{O}\right\}$.

Wir wissen, dass $\phi_q - 1$ separabel ist nach Proposition 13. Also gilt

$$\#\ker(\phi_q - 1) = \deg(\phi_q - 1)$$

Mit Proposition 16 gilt dann weiter

$$\equiv \det\left((\phi_q)_m - I\right)$$

Diese Determinante kann man nun berechnen und erhält

$$= sv - tu - (s + v) + q \ (\mathrm{mod}\ m) \tag{6}$$

Wenn man nun ϕ_q statt $\phi_q - 1$ betrachtet, ergibt sich mit denselben Argumenten die folgende Gleichungskette:

$$sv - tu = \det\left((\phi_q)_m\right) \equiv \deg(\phi_q) = q \ (\mathrm{mod}\ m) \tag{7}$$

Durch Einsetzen von (7) in (6) erhält man nun

$$\mathrm{Trace}\left((\phi_q)_m\right) = s + v \equiv a \ (\mathrm{mod}\ m) \tag{5}$$

Mit dem Satz von Cayley-Hamilton oder durch einfaches Nachrechnen ergibt sich

$$(\phi_q)_m^2 - a\,(\phi_q)_m + qI \equiv 0 \ (\mathrm{mod}\ m)$$

Da diese Aussage für unendlich viele solche m gilt, haben wir

$$\phi_q^2 - a\phi_q + q = 0$$

Was nun noch zu zeigen ist, ist die Eindeutigkeit der Zahl a.

Angenommen, es gibt ein $a' \neq a$ mit $\phi_q^2 - a'\phi_q + q = 0$. Dann ist

$$(a - a')\phi_q = (\phi_q^2 - a'\phi_q + q) - (\phi_q^2 - a\phi_q + q) = 0$$

Da ϕ_q nach Theorem 17 surjektiv ist muss für jeden Punkt $P \in E(\overline{\mathbb{F}_q})$ gelten, dass $(a - a')P = \mathbf{O}$. Betrachte alle $P \in E[m]$ mit $\gcd(m, q) = 1$. Dann folgt, dass $a - a' \equiv 0 \pmod{m}$ gilt. Da dies wieder für unendlich viele m gilt, muss sogar $a - a' = 0$ sein, also ist a eindeutig. □

Im zweiten Teil des Satzes von Hasse-Weil taucht der Term $\alpha^n + \beta^n$ auf, wobei α und β Nullstellen des Polynoms $x^2 - ax + q$ sein sollen. Wir hätten gerne, dass dieser Term immer eine ganze Zahl ist. Das folgende Lemma garantiert uns die Ganzzahligkeit und liefert uns zudem eine Möglichkeit, den Term rekursiv zu berechnen.

Lemma 12. *Sei $s_n = \alpha^n + \beta^n$. Dann ist $s_0 = 2$, $s_1 = a$ und $s_{n+1} = as_n - qs_{n-1}$.*

Beweis. Da α eine Nullstelle von $x^2 - ax + q$ ist, gilt $\alpha^2 - a\alpha + q = 0$. Durch Multiplizieren mit α^{n-1} erhält man $\alpha^{n+1} = a\alpha^n - q\alpha^{n-1}$.

Genauso erhält man $\beta^{n+1} = a\beta^n - q\beta^{n-1}$.

Durch Addieren dieser beiden Gleichungen erhält man schließlich

$$\begin{aligned} s_{n+1} &= \alpha^{n+1} + \beta^{n+1} = a\alpha^n - q\alpha^{n-1} + a\beta^n - q\beta^{n-1} \\ &= a\left(\alpha^n + \beta^n\right) - q\left(\alpha^{n-1} + \beta^{n-1}\right) \\ &= as_n - qs_{n-1} \end{aligned}$$

□

Theorem 4 (Satz von Hasse-Weil (2. Teil))**.** *Sei E eine elliptische Kurve über $\mathbb{F}_q$ und $a_1 := q + 1 - \#E(\mathbb{F}_q)$. Sei weiter $x^2 - a_1x + q = (x - \alpha)(x - \beta)$. Dann gilt für alle $n \geq 1$:*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n) \tag{2}$$

Beweis. Da wir in diesem Beweis a einmal für die Kurve über $\mathbb{F}_q$ und einmal für die Kurve über $\mathbb{F}_{q^n}$ benötigen, schreiben wir $a_1 = q + 1 - \#E(\mathbb{F}_q)$ und $a_n = q^n + 1 - \#E(\mathbb{F}_{q^n})$.

Sei $f(x) = (x^n - \alpha^n)(x^n - \beta^n) = x^{2n} - (\alpha^n + \beta^n)x^n + q^n$.

Da $x^n - \alpha^n = (x - \alpha)(x^{n-1} + \alpha x^{n-2} + \alpha^2 x^{n-3} + \ldots \alpha^{n-2}x + \alpha^{n-1})$ wird $f(x)$ von $x - \alpha$ geteilt.

Analog sieht man, dass $f(x)$ von $x - \beta$ geteilt wird, also sogar von $(x - \alpha)(x - \beta) = x^2 - a_1x + q$.

Sei $Q(x) = \frac{f(x)}{x^2 - a_1x + q}$. Dann ist $Q(x)$ ein ganzzahliges Polynom, da f nach dem vorherigen Lemma nur ganzzahlige Koeffizienten und $x^2 - a_1x + q$ Leitkoeffizient 1 hat.

Damit ergibt sich durch Einsetzen von ϕ_q

$$\left(\phi_q^n\right)^2 - (\alpha^n + \beta^n)\,\phi_q^n + q^n = Q(\phi_q)\left(\phi_q^2 - a_1\phi_q + q\right) = 0$$

da $x^2 - a_1x + q$ das Minimalpolynom von ϕ_q ist.

Wir haben also $x^2 - (\alpha^n + \beta^n)\, x + q^n = 0$ für $x = \phi_q^n = \phi_{q^n}$. Mit der Eindeutigkeitsaussage aus dem letzten Theorem folgt dann, dass $q^n + 1 - \#E(\mathbb{F}_{q^n}) = a_n = \alpha^n + \beta^n$. □

4 Anwendung

Wir wollen nun den Satz anwenden um die Beispiele zu Beginn zu berechnen.

Beispiel 2. Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2+xy = x^3+1$. Wir wissen bereits $q = 2$, $\#E(\mathbb{F}_2) = 4$, also $a = q+1-\#E(\mathbb{F}_q) = -1$. Betrachte nun $x^2 - ax + q$:

$$x^2 + x + 2 = \left(x - \frac{-1+\sqrt{-7}}{2}\right)\left(x - \frac{-1-\sqrt{-7}}{2}\right)$$

Wieviele Elemente hat $E(\mathbb{F}_4)$?

$$\begin{aligned}\#E(\mathbb{F}_4) &= q^2 + 1 - (\alpha^2 + \beta^2)\\ &= 4 + 1 - \left(\frac{-1+\sqrt{-7}}{2}\right)^2 - \left(\frac{-1-\sqrt{-7}}{2}\right)^2\\ &= 8\end{aligned}$$

Beispiel 3. Sei E eine elliptische Kurve über $\mathbb{F}_2$ gegeben durch $y^2+xy = x^3+1$. Wir wissen $q = 2$, $\#E(\mathbb{F}_2) = 4$, $a = -1$, $\alpha = \frac{-1+\sqrt{-7}}{2}$, $\beta = \frac{-1-\sqrt{-7}}{2}$

Wieviele Elemente hat $E(\mathbb{F}_{2^{101}})$?

$$\begin{aligned}\#E(\mathbb{F}_{2^{101}}) &= 2^{101} + 1 - \left(\frac{-1+\sqrt{-7}}{2}\right)^{101} - \left(\frac{-1-\sqrt{-7}}{2}\right)^{101}\\ &= 2535301200456455833701195805484\end{aligned}$$

Diese Zahl lässt sich mit der Rekursionsformel aus Lemma 12 berechnen. Das Verfahren vom Anfang, das Aufzählen aller Elemente, wäre bei dieser Menge an Punkten ein aussichtsloses Unterfangen.

5 Fazit

Mit dem Satz von Hasse-Weil lässt sich die Anzahl der Elemente einer Gruppe einer elliptischen Kurve über $\mathbb{F}_q$ abschätzen durch $\#E(\mathbb{F}_q) \geq q + 1 - 2\sqrt{q}$ und $\#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$.

Falls die Anzahl über $\mathbb{F}_q$ bekannt ist, so kann die Anzahl über $\mathbb{F}_{q^n}$ einfach berechnet werden. Voraussetzung dazu ist allerdings, dass die Kurve nur mit Koeffizienten aus $\mathbb{F}_q$ definiert ist!

A Verwendete Sätze

Proposition 13. *Sei E eine elliptische Kurve über $\mathbb{F}_q$, wobei q eine Potenz der Primzahl p ist. Seien r und s ganze Zahlen nicht beide 0. Dann gilt: Der Endomorphismus $r\phi_q + s$ ist separabel genau dann, wenn p nicht s teilt.*

Beweis. [Was08, S. 58-59] □

Proposition 14. *Sei $\alpha \neq 0$ ein separabler Endomorphismus auf der elliptischen Kurve E. Dann gilt* $\deg \alpha = \#\ker(\alpha)$.

Falls $\alpha \neq 0$ nicht separabel ist, dann gilt $\deg \alpha > \#\ker(\alpha)$.

Beweis. [Was08, S. 53-54] □

Proposition 15.

$$\begin{aligned}\deg(a\alpha + b\beta) = a^2 \deg(\alpha) + b^2 \deg(\beta) \\ + ab(\deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta))\end{aligned}$$

Beweis. [Was08, S. 89-90] □

Proposition 16. *Sei α ein Endomorphismus auf einer elliptischen Kurve E über dem Körper K. Sei n eine positive ganze Zahl, die nicht durch die Charakteristik von K geteilt werden kann. Dann gilt* $\det(\alpha_n) \equiv \deg(\alpha) \pmod{n}$.

Beweis. [Was08, S. 89] □

Theorem 17. *Sei E eine elliptische Kurve über einem Körper K. Sei $\alpha \neq 0$ ein Endomorphismus auf E. Dann ist $\alpha : E(\overline{K}) \longrightarrow E(\overline{K})$ surjektiv.*

Beweis. [Was08, S. 55] □

Literatur

[Bar11] Mohamed Barakat, *Lecture Notes Cryptography*, Website, Winter Term 2010/11, Available online at http://www.mathematik.uni-kl.de/~barakat/Lehre/WS10/Cryptography/; visited on June 2nd 2011.

[Was08] Lawrence C. Washington, *Elliptic Curves - Number Theory and Cryptography*, 2^{nd} ed., Discrete Mathematics and its Application, Chapman & Hall / CRC, 2008.