Seminar: Einführung in die Theorie elliptischer Kurven

Vortrag 6: Elliptische Kurven über endlichen Kurven

Seminarvortrag von SEBASTIAN DAMRICH
28. Mai 2015

0 Vorbemerkungen

In diesem Vortrag wollen wir dem fünften Kapitel von [Sil86] folgen und elliptische Kurven über endlichen Körpern untersuchen. Der erste Teil wird sich mit der Satz von Hasse, einer Abschätzung für die Anzahl der rationalen Punkten auf einer elliptischen Kurve über einem endlichen Körper, beschäftigen. Im zweiten Teil werden wir die Weil-Vermutungen formulieren und im Spezialfall von elliptischen Kurven mit dem Wissen aus dem ersten Abschnitt beweisen. Im gesamten Vortrag sei p eine Primzahl, $q = p^m$ eine Potenz von p und $\mathbb{F}_q$ der bis auf Isomorphie eindeutige Körper mit q Elementen. Weiter sei $E/\mathbb{F}_q$ eine elliptische Kurve über $\mathbb{F}_q$.

1 Rationale Punkte

Wir wollen in diesem Abschnitt die Anzahl der rationalen Punkte von E über $\mathbb{F}_q$, also die Mächtigkeit von $E(\mathbb{F}_q) = E \cap \mathbb{P}^n(\mathbb{F}_q)$ näherungsweise bestimmen. Vor dem zentralen Resultat des Abschnitts, dem Satz von Hasse, versuchen wir zu motivieren, welche Ergebnisse wir intuitiv erwarten können. Dazu wählen wir für E eine Weierstraß-Gleichung

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

deren Koeffizienten a_i in $\mathbb{F}_q$ gewählt werden können, da E über $\mathbb{F}_q$ definiert ist. Die Anzahl der rationalen Punkte von E über $\mathbb{F}_q$ ist nun gerade die Anzahl der Paare $(x, y) \in \mathbb{F}_q^2$, welche die Gleichung erfüllen, zuzüglich eines Punkts im Unendlichen. Wir erhalten sofort die erste triviale Abschätzung

$$\#E\left(\mathbb{F}_q\right) \leq 2q + 1,$$

denn zu jedem Wert $x \in \mathbb{F}_q$ erhalten wir eine quadratische Gleichung in y, die höchstens zwei Lösungen hat.
Dies können wir noch verfeinern, denn für ungerades p sind ungefähr die Hälfte der Elemente von $\mathbb{F}_q$ Quadrate. Man könnte also erwarten, dass nur für die Hälfte aller Werte für x die quadratische Gleichung mit $y \in \mathbb{F}_q$ eine Lösung hat. Dass die richtige Größenordnung von $\mathbb{F}_q$ tatsächlich $q + 1$ ist, werden wir im Folgenden zeigen.

Dazu rufen wir uns zunächst die Definition einer quadratischen Form und der Cauchy-Schwarz Ungleichung in Gedächtnis:

Definition 1.1
Sei A eine abelsche Gruppe. Eine Funktion $d\colon A \to \mathbb{R}$ heißt quadratische Form*, wenn gilt*

1. *$d(a) = d(-a)$ für alle $a \in A$.*
2. *Die Abbildung $A \times A \to \mathbb{R}, (a, b) \mapsto d(a + b) - d(a) - d(b)$ ist bilinear.*

Eine quadratische Form heißt positiv definit*, wenn zusätzlich gilt*

3. *$d(a) \geq 0$ für alle $a \in A$.*
4. *$d(a) = 0 \Leftrightarrow a = 0$.*

Lemma 1.2 (Cauchy-Schwarz)
Sei A eine ablesche Gruppe und $d\colon A \to \mathbb{Z}$ eine positiv definite, quadratische Form. Dann gilt für alle $\phi, \psi \in A$:

$$|d(\psi - \phi) - d(\psi) - d(\phi)| \leq 2\sqrt{d(\phi)d(\psi)}$$

Beweis. Für $\psi, \phi \in A$ setze $L(\psi, \phi) := d(\psi - \phi) - d(\psi) - d(\phi)$. Da L bilinear ist, erhalten wir mit $d(0) = 0$ für alle $n \in \mathbb{Z}$ und $\phi \in A$:

$$2d(n\phi) = -L(n\phi, n\phi) = -n^2 L(\phi, \phi) = 2n^2 d(\phi)$$

und da weiter d positiv definit ist, gilt für alle $m, n \in \mathbb{Z}$:

$$0 \leq d(m\psi - n\phi) = m^2 d(\psi) + mnL(\psi, \phi) + n^2 d(\phi).$$

Insbesondere erhalten wir für die Wahl $m = -L(\psi, \phi)$ und $n = 2d(\psi)$

$$0 \leq d(\psi)\left(4d(\psi)d(\phi) - L(\psi, \phi)^2\right).$$

Daraus folgt die Behauptung für $d(\psi) \neq 0$. Anderfalls erhalten wir aus der Definitheit von d, dass $\psi = 0$, sodass die Behauptung trivialerweise stimmt. □

Beispiel 1.3. Die Voraussetzungen von Lemma 1.2 sind erfüllt, wenn als abelsche Gruppe A die Gruppe $\mathrm{End}(E)$ der Isogenien von E in sich selbst und als positiv definite, quadratische Form die Gradabbildung $\deg\colon \mathrm{End}(E) \to \mathbb{Z}$ gewählt werden. In dieser Konstellation werden wir Lemma 1.2 im Folgenden Theorem verwenden.

Theorem 1.4 (Hasse, 1930er)
Sei $E/\mathbb{F}_q$ eine elliptische Kurve. Dann gilt

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

Dieses Theorem wurde bereits von Emil Artin in dessen Dissertation vermutet.

Beweis. Sei $\phi : E \to E, (x, y) \mapsto (x^q, y^q)$ der q-te Potenz Frobenius. Für einen Punkt $P \in E = E\left(\overline{\mathbb{F}_q}\right)$ auf der elliptischen Kurve gilt

$$\begin{aligned} P \in E(\mathbb{F}_q) &\Leftrightarrow \sigma(P) = P \text{ für alle } \sigma \in \mathrm{Gal}\left(\overline{\mathbb{F}_q}/\mathbb{F}_q\right) \\ &\Leftrightarrow \phi(P) = P \end{aligned}$$

Für die letzte Äquivalenz beachte man, dass $\overline{\mathbb{F}_q} = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{q^n}$ und dass der q-te Potenz Frobenius die Galoisgruppe $\mathrm{Gal}\left(\mathbb{F}_{q^n}/\mathbb{F}_q\right)$ für alle $n \in \mathbb{N}$ erzeugt.[1]
Also gilt $E\left(\mathbb{F}_q\right) = \ker(1 - \phi)$ und wir erhalten insbesondere $\#E\left(\mathbb{F}_q\right) = \#\ker(1 - \phi)$. Mit einem leichten Korollar aus dem Theorem über das invariante Differential aus Vortrag 4[2] ist $1 - \phi$ separabel und somit erhalten wir erneut nach dem vierten Vortrag[3] $\#\ker(1 - \phi) = \deg(1 - \phi)$. Der q-te Potenz Frobenius hat Grad q, sodass wir mit Lemma 1.2 erhalten

$$|\#E\left(\mathbb{F}_q\right) - q - 1| = |\deg(1 - \phi) - \deg(\phi) - \deg(1)| \leq 2\sqrt{\deg(\phi)\deg(1)} = 2\sqrt{q}. \qquad \square$$

[1] Das Erzeugnis des Frobenius ist dicht in der absoluten Galoisgruppe von $\mathbb{F}_q$.
[2] vgl. Kor. III. 5.5 [Sil86]
[3] vgl. Thm. III. 4.10 [Sil86]

André Weil vermutete ein ähnliches Resultat auch für Kurven höheren Geschlechts, welches als Hasse-Weil Schranke bekannt ist: Unter geeigneten Voraussetzungen gilt für eine glatte, projektive Kurve $C/\mathbb{F}_q$ von Geschlecht g

$$|\#C(\mathbb{F}_q) - q - 1| \leq 2g\sqrt{q}$$

Der Beweis ist ein Korollar der im nächsten Kapitel besprochenen Weil-Vermutungen und wurde durch Pierre Deligne 1974 erbracht [Del74]. Die Bedeutung von $q^{\frac{1}{2}}$ werden wir im zweiten Teil erkennen. Tatsächlich ist die Ungleichung in manchen Fällen strikt, wie zum Beispiel in [Gar01] besprochen wird.

In der heuristischen Herleitung der Größenordnung von $\#E(\mathbb{F}_q)$ zu Beginn des Kapitels wurde implizit davon ausgegangen, dass ein kubisches Polynom in $\mathbb{F}_q[X]$ als Werte ungefähr gleichmäßig Quadrate und Nichtquadrate in $\mathbb{F}_q$ annimmt. Dies werden wir nun mit Hasses Theorem rechtfertigen.

Anwendung 1.5. Sei nun p und damit q ungerade. Sei weiter $f \in \mathbb{F}_q[X]$ ein separables, normiertes Polynom von Grad 3. Wir möchten zeigen, dass f ungefähr gleich oft Quadrate und Nichtquadrate annimmt. Dies zählen wir mit

$$\chi : \mathbb{F}_q \to \{-1, 0, 1\},\ \chi(t) = \begin{cases} 0 & t = 0 \\ -1 & t \text{ ist kein Quadrat} \\ 1 & t \text{ ist ein Quadrat } > 0. \end{cases}$$

Da die Charakteristik von $\mathbb{F}_q$ nicht 2 und f separabel ist, definiert $E : y^2 = f(x)$ eine elliptische Kurve über $\mathbb{F}_q$. Ist nun $f(x)$ für ein $x \in \mathbb{F}_q$ kein Quadrat (bzw. 0 oder ein Quadrat $\neq 0$) gibt es genau 0 (bzw. 1 oder 2) Punkte $(x, y) \in E(\mathbb{F}_q)$. Wir erhalten also den Punkt im Unendlichen nicht vergessend

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

Anwenden von Hasses Theorem liefert nun

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| = |\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Abgesehen vom Wert 0, den f höchstens 3 Mal annehmen kann, nimmt f also modulo q Nichtquadrate und Quadrate $\neq 0$ bis auf einen Fehler von höchstens $2\sqrt{q}$ gleich häufig an.

2 Die Weil-Vermutungen

Die Weil-Vermutungen sind von André Weil 1949 aufgestellte Vermutungen zur Anzahl von rationalen Punkten auf projektiven, glatten Varietäten über endlichen Körpern.[4] Die Anzahl der rationalen Punkte wird dabei in Form einer sogenannten Zeta-Funktion kodiert.

Definition 2.1
Sei $V/\mathbb{F}_q$ eine projektive Varietät. Die Zeta-Funktion *von V über $\mathbb{F}_q$ ist die formale Potenzreihe*

$$Z(V/\mathbb{F}_q, T) = \exp\left(\sum_{n=1}^{\infty} \#V\left(\mathbb{F}_{q^n}\right) \frac{T^n}{n}\right)$$

Es seien die folgenden grundlegenden Resultate für formale Potenzreihen in Erinnerung gerufen:

1. Rechnen mit Potenzreihen erfolgt wie mit absolut konvergenten unendlichen Reihen, also mit termweiser Addition und Cauchyprodukt als Multiplikation. Dabei müssen formale Potenzreihen aber nicht als Reihe konvergieren.

2. Die Exponential- und Logarithmusreihe sind definiert als

$$\exp(T) := \sum_{i=0}^{\infty} \frac{T^i}{i!} \text{ und } \log(1-T) := -\sum_{i=1}^{\infty} \frac{T^i}{i}$$

3. Es gilt unter anderem $\log(\exp(T)) = T$, $\exp(\log(1-T)) = 1-T$

Bemerkung 2.2. Durch das Kodieren der Anzahl rationaler Punkte in die Zeta-Funktion geht keine Information verloren, denn wir gewinnen $\#V(\mathbb{F}_q)$ aus der Zetafunktion zurück durch

$$\#V\left(\mathbb{F}_{q^n}\right) = \frac{1}{(n-1)!} \frac{d^n}{dT^n} \log(Z(V/\mathbb{F}_q, T))\Big|_{T=0}.$$

Im Folgenden wollen wir ein erstes Bespiel für die Zeta-Funktion einer glatten, projektiven Varietät gewinnen und werden sehen, dass die Kodierung der Anzahl rationaler Punkte in der Zeta-Funktion eine einfache Form erziehlt.

Beispiel 2.3. Wir wollen die Zeta-Funktion des projektiven Raums $\mathbb{P}^N$ bestimmen. Die rationalen Punkte über $\mathbb{F}_{q^n}$ sind gerade gegeben durch homogene Koordinaten $[x_0, \ldots, x_N]$ mit $x_i \in \mathbb{F}_{q^n}$. Da hierbei nicht alle Einträge Null sein dürfen und skalare Vielfache aus $\mathbb{F}_{q^n}^{\times}$ identifiziert werden, gilt

$$\#\mathbb{P}^N\left(\mathbb{F}_{q^n}\right) = \frac{(q^n)^{N+1} - 1}{q^n - 1} = \sum_{i=0}^{N} q^{ni}.$$

Für die logarithmierte Zeta-Funktion erhalten wir

$$\log(Z(\mathbb{P}^N/\mathbb{F}_q, T)) = \sum_{n=1}^{\infty} \left(\sum_{i=0}^{N} q^{ni}\right) \frac{T^n}{n} = \sum_{i=0}^{N} \sum_{n=1}^{\infty} \frac{(q^i T)^n}{n} = \sum_{i=0}^{N} -\log(1-q^i T).$$

Einsetzen in die Exponentialpotenzreihe liefert

$$Z(\mathbb{P}^N/\mathbb{F}_q, T) = \frac{1}{(1-T)(1-qT)\cdot\ldots\cdot(1-q^N T)} \in \mathbb{Q}[X]$$

[4] siehe [Wei49]

Überraschenderweise ist die Zeta-Funktion des projektiven Raums also eine rationale Funktion. Die Weil-Vermutungen sagen aus, dass die Zeta-Funktionen glatter, projektiver Varietäten über endlichen Körpern stets solche guten Eigenschaften haben.

Theorem 2.4 (Weil-Vermutungen)
Sei $V/\mathbb{F}_q$ eine glatte, projektive Varietät der Dimension n. Dann gilt

1. *(Rationalität) $Z(V/\mathbb{F}_q, T)$ ist eine rationale Funktion.*
2. *(Funktionalgleichung) Es gibt eine ganze Zahl e, sodass*

$$Z\left(V/\mathbb{F}_q, \frac{1}{q^n T}\right) = \pm q^{\frac{ne}{2}} T^e Z(V/\mathbb{F}_q, T).$$

   Die Zahl e wird auch Euler-Charakteristik von V genannt.

3. *(Riemannsche Vermutung) Es existieren ganzzahlige Polynome $P_0, \ldots, P_{2n}$, sodass*

$$Z(V/\mathbb{F}_q, T) = \frac{P_1 \cdot \ldots \cdot P_{2n-1}}{P_0 \cdot \ldots \cdot P_{2n}}.$$

   Weiter gilt $P_0 = 1 - T$ sowie $P_{2n} = 1 - q^n T$. Außerdem gibt es für alle $1 \leq i \leq 2n-1$ komplexe Zahlen α_{ij} mit $|\alpha_{ij}| = q^{\frac{i}{2}}$, sodass das Polynom P_i faktorisiert als

$$P_i(T) = \prod_j (1 - \alpha_{ij} T).$$

Diese Aussagen sind mittlerweise bewiesen und extrem tiefliegend. Wir werden sie lediglich für den Spezialfall von elliptischen Kurven zeigen.
Bevor wir dies tun und auf die Historie der Vermutungen eingehen, wollen wir zunächst eine Intuition für die Funktionalgleichung und die Riemannsche Vermutung entwickeln. Tatsächlich sind dies Eigenschaften, die im Rahmen der Riemannschen Zeta-Funktion sehr populär sind. Wir werden sie uns im Fall elliptischer Kurven veranschaulichen.

Sei E eine elliptische Kurve. Also gilt $n = 1$ und wie wir später sehen werden $e = 0$.
Nun substituieren wir $T = q^{-s}$ mit $s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$. Da nun eine Zahl in die als formale Potenzreihe definierte Zeta-Funktion eingesetzt wird, müssen wir Konvergenz der entstehenden Reihe prüfen:
Aus dem ersten Abschnitt wissen wir $\#E\left(\mathbb{F}_{q^n}\right) \leq 2q^n + 1$ und erhalten somit, dass

$$\left| \sum_{n=1}^{\infty} \#E\left(\mathbb{F}_{q^n}\right) \frac{q^{-sn}}{n} \right| \leq \sum_{n=1}^{\infty} \left(2\frac{q^{(1-\mathrm{Re}(s))n}}{n} + \frac{q^{-\mathrm{Re}(s)n}}{n} \right)$$

was für $\mathrm{Re}(s) > 1$ offenbar endlich ist, sodass dann auch die Zeta-Funktion

$$Z(E/\mathbb{F}_q, q^{-s}) = \exp\left(\sum_{n=1}^{\infty} \#E\left(\mathbb{F}_{q^n}\right) \frac{q^{-sn}}{n} \right)$$

für $\mathrm{Re}(s) > 1$ wohldefiniert ist. Nach der Rationalitätsaussage der Weil-Vermutungen ist $Z(E/\mathbb{F}_q, T)$ eine rationale Funktion. Setzen wir in diese rationale Funktion $T = q^{-s}$ ein, erhalten wir eine meromorphe Fortsetzung der für $\mathrm{Re}(s) > 1$ als konvergent eingesehenen Zeta-Funktion

$Z(E/\mathbb{F}_q, q^{-s})$ auf ganz $\mathbb{C}$. Diese bezeichnen wir mit $\zeta_{E/\mathbb{F}_q}(s) := Z(E/\mathbb{F}_q, q^{-s})$. Es gilt nun nach der Funktionalgleichung

$$\zeta_{E/\mathbb{F}_q}(s) = Z(E/\mathbb{F}_q, q^{-s}) = \pm Z(E/\mathbb{F}_q, q^{-(1-s)}) = \pm\zeta_{E/\mathbb{F}_q}(1-s).$$

Das ist bis auf das Vorzeichen, welches wie wir gleich sehen sehen stets Plus ist, gerade die Funktionalgleichung der Riemannschen Zeta-Funktion. Die Analogie geht noch weiter:

Sei $\zeta_{E/\mathbb{F}_q}(s) = 0$. Dann folgt mit der Riemannschen Vermutung, dass das Zählerpolynom der Zeta-Funktion eine Nullstelle hat, also $|\alpha_{1j}q^{-s}| = 1$ gilt. Wir wissen ebenfalls durch die Riemannsche Vermutung, dass $|\alpha_{1j}| = q^{\frac{1}{2}}$ ist und erhalten somit

$$q^{\mathrm{Re}(s)} = |q^s| = |\alpha_{1j}| = q^{\frac{1}{2}}.$$

Der Realteil einer komplexen Nullstelle der Zeta-Funktion einer elliptischen Kurve über einem endlichen Körper ist also $\frac{1}{2}$, was gerade der Riemannschen Vermutung für die Riemannsche Zeta-Funktion entspricht.

Historische Einordnung

Bevor wir selbst die Weil-Vermutungen für den Spezialfall von elliptischen Kurven zeigen, wollen kurz auf die Geschichte der Aussagen eingehen.
Die ersten Gedanken, die in Richtung der Weil-Vermutung gehen, finden sich in Teil VII der Disquisitiones Arithmeticae von Carl Friedrich Gauß.[5] In Artikel 358, der sich mit Summen von Einheitswurzeln befasst, wird als Nebenresultat die Anzahl von Lösungen spezieller Weierstraß-Gleichungen modulo einer Primzahl p, also die Anzahl von rationalen Punkten der zugehörigen elliptischen Kurve über $\mathbb{F}_p$ bestimmt und auch ein Analogon zur Riemannschen Vermutung gezeigt.
Im modernen Verständnis machte Emil Artin 1924 den ersten Schritt, indem er die Weil-Vermutungen für den Spezialfall elliptischer Kurven formulierte.[6] Dies konnte 1930 von Helmut Hasse bewiesen werden. Zentraler Beweisschritt dazu war der Satz von Hasse aus dem ersten Abschnitt. In den 1940er Jahren befasste sich André Weil mit der Thematik und stellte die Weil-Vermutungen in ihrer heutigen Form 1949 auf.[7] Zuvor hatte er sie für Kurven und abelsche Varietäten bewiesen.
Weil wies auch darauf hin, dass die Weil-Vermutungen mit Methoden analog zum Lefschetzschen Fixpunktsatz durch Berechnung von Wechselsummen der Koeffizienten bestimmter Kohomologiegruppen gezeigt werden könnten, wenn eine passende Kohomologietheorie entwickelt würde. Dies gab Grothendieck und seiner Schule Anlass zur Erarbeitung von étaler Kohomologie.
Bevor dies Früchte trug, konnte Bernard Dwork 1960 die Rationalitätsaussage mithilfe von Methoden der p-adischen Funktionalanalysis beweisen.[8] Unabhängig davon gelang fünf Jahre später Alexander Grothendieck und Martin Artin der Beweis der Rationalität sowie der Funktionalgleichung mit der von ihnen entwickelten étalen Kohomologie.[9]

[5] siehe [Maz75]
[6] siehe [Art24]
[7] siehe [Wei49]
[8] siehe [Dwo60]
[9] siehe [Gro66]

Der Beweis der Riemannschen Vermutung stellte sich als am schwierigsten heraus. Erst 1974, 25 Jahre nach Aufstellen der Weil-Vermutungen, arbeitete Pierre Deligne dessen Ideen zum Beweis der Riemannschen Vermutung aus und konnte die Weil-Vermutungen damit vollständig zeigen.[10] Er erhielt dafür die Fields Medaille und den später den Abel-Preis. Ebenso konnte Deligne einige verbüffende Folgerungen im Bereich der analystischen Zahlentheorie aus den Weil-Vermutungen ziehen. So bewies er mit deren Hilfe die Ramanuja-Peterson Vermutung und gab Schranken für Exponentialsummen an.[11]
1980 verallgemeinerte Deligne die Weil-Vermutungen und konnte deren neue Form durch eine Modifizierung seines Beweises ebenfalls zeigen. Aus dieser verallgemeinerten Form schloss er schließlich das Harte Lefschetz-Theorem.[12]

Beweis der Weil-Vermutungen für elliptische Kurven

Sei $E/\mathbb{F}_q$ eine elliptische Kurve, sowie $l \neq p$ eine Primzahl. Im fünften Vortrag wurde gezeigt, dass der Tate-Modul $T_l(E)$ als $\mathbb{Z}_l$-Modul gerade $\mathbb{Z}_l \times \mathbb{Z}_l$ ist und eine Isogenie $\psi \in \mathrm{End}(E)$ einen $\mathbb{Z}_l$-Modulhomomorphismus $\psi_l \in \mathrm{End}(T_l(E))$ induziert.[13]
Nach Wahl einer $\mathbb{Z}_l$-Basis von $T_l(E)$ ist ψ_l durch eine 2×2 Matrix mit Einträgen in $\mathbb{Z}_l$ repräsentiert und wir können ψ_l eine Determinate und eine Spur, $\det(\psi_l)$ und $\mathrm{tr}(\psi_l) \in \mathbb{Z}_l$, zuordnen. Diese sind wohldefinierte und nützliche Hilfsmittel:

Lemma 2.5
Es gilt für eine Isogenie $\psi \in \mathrm{End}(E)$ und den induzierten $\mathbb{Z}_l$-Modulhomomorphisumus ψ_l:

$$\begin{aligned} \det(\psi_l) &= \deg(\psi) \\ \mathrm{tr}(\psi_l) &= 1 + \deg(\psi) - \deg(1-\psi). \end{aligned}$$

Insbesondere sind Spur und Determinatne ganzzahlig und basisunabhängig.

Beweis. Seien $v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $v_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ die Standard $\mathbb{Z}_l$-Basis von $T_l(E)$ und sei ψ_l durch $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}_l^{2\times 2}$ repräsentiert. Wir haben nach dem fünften Vortrag eine nicht ausgeartete, bilineare, alternierende 2-Form

$$e : T_l(E) \times T_l(E) \to T_l(\mathbb{F}_q)$$

für welche die zu Isogenien und dualen Isogenien assozierten $\mathbb{Z}_l$-Modulhomomorphismen adjungiert sind.[14] Es gilt:

$$\begin{aligned} e(v_1, v_2)^{\deg(\psi)} &= e([\deg(\psi)]v_1, v_2) = e\left(\left(\hat{\psi}\right)_l \circ \psi_l(v_1), v_2\right) \\ &= e(\psi_l(v_1), \psi_l(v_2)) = e(av_1 + bv_2, cv_1 + dv_2) \\ &= e(v_1, v_2)^{ad-bc} = e(v_1, v_2)^{\det(\psi_l)} \end{aligned}$$

[10] siehe [Del74]
[11] siehe [Del69] und [Del74]
[12] siehe [Del80]
[13] siehe Prop. III 7.1. und Thm. III 7.4. in [Sil86]
[14] vgl. Prop. III 8.3. in [Sil86]

Sei nun $x = \deg(\psi) - \det(\psi_l)$. Dann gilt $e(v_1, xv_2) = 1$ und damit $e(v, xv_2) = 1$ für alle $v \in T_l(E)$, denn e ist bilinear und alternierend. Da e zudem nicht ausgeartet ist, erhalten wir $xv_2 = 0$ und damit $x = 0$ in $\mathbb{Z}_l$. Nun hat $\mathbb{Z}_l$ Charakteristik 0, sodass wir $x = 0$ und folglich $\deg(\psi) = \det(\psi_l)$ schließen. Abschließend bemerken wir, dass für jede 2×2 Matrix A

$$\operatorname{tr}(A) = 1 + \det(A) - \det(1 - A)$$

gilt, sodass auch die Aussage über die Spur folgt. □

Im nächsten Satz verfeinern wir den Satz von Hasse:

Satz 2.6
Es gibt zu einander konjugierte komplexe Zahlen α und β, deren Summe ganzzahlig und deren Norm $\sqrt{q}$ ist, sodass

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

Beweis. Sei $\phi : E \to E$ der q-te Potenz Frobenius. Dann ist ϕ^n der q^n-te Potenz Frobenius, sodass analog zum Beweis des Satz von Hasse gilt

$$\#E\left(\mathbb{F}_{q^n}\right) = \deg(1 - \phi^n).$$

Wir werden $\deg(1-\phi^n)$ bestimmen, indem wir die Determinante des zugehörigen $\mathbb{Z}_l$-Modulhomomorphismus berechnen. Nach Lemma 2.5 ist

$$\det(1 - \phi_l) = T^2 - \operatorname{tr}(\phi_l)T + det(\phi_l)$$

ein ganzzahliges Polynom, zerfällt über $\overline{\mathbb{Q}}$ also zu $(T-\alpha)(T-\beta)$ mit $\alpha, \beta \in \overline{\mathbb{Q}}$, den Eigenwerten von ϕ_l. Zunächst werden wir einsehen, dass α und β die beschriebenen Voraussetzungen erfüllen. Dazu bemerken wir, dass für eine rationale Zahl $\frac{a}{b} \in \mathbb{Q}$, wir nehmen ohne Einschränkung $b > 0$ an, nach Lemma 2.5

$$\det\left(\frac{a}{b} - \phi_l\right) = \frac{\det(a - b\phi_l)}{b} = \frac{\deg(a - b\phi)}{b} \geq 0$$

gilt. Da $\mathbb{Q}$ dicht in $\mathbb{R}$ liegt, gilt für alle $r \in \overline{\mathbb{Q}} \cap \mathbb{R}$, dass $\det(r - \phi_l) \geq 0$ ist. Insbesondere erhalten wir, dass α und β entweder identisch oder komplex konjugiert sind. Weiter gilt nach Koeffizientenvergleich

$$\alpha \cdot \beta = \det(\phi_l) = \deg(\phi) = q \text{ und } \alpha + \beta = \operatorname{tr}(\phi_l) \in \mathbb{Z}.$$

Folglich sind α und β geeignete Kandidaten und wir müssen noch die Gleichung für die Anzahl der rationalen Punkte verifizieren.
Da α und β die Eigenwerte von ϕ_l sind, hat ϕ_l über $\overline{\mathbb{Q}_l} \supseteq \overline{\mathbb{Q}}$ die Jordan-Normal Form

$$\begin{pmatrix} \alpha & * \\ 0 & \beta \end{pmatrix}.$$

Damit hat ϕ_l^n die Jordan-Normal Form

$$\begin{pmatrix} \alpha^n & * \\ 0 & \beta^n \end{pmatrix}$$

und da die Eigenwerte gerade die Nullstellen des charakteristischen Polynoms sind, gilt

$$\det(T - \phi_l) = (T - \alpha^n)(T - \beta^n).$$

Einsetzen von $T = 1$ gibt uns nun genau den Ausdruck den wir zu Beginn bestimmen wollten:

$$\begin{aligned}\#E\left(\mathbb{F}_{q^n}\right) &= \deg(1 - \phi^n) = \det(1 - \phi_l^n) \\ &= (1 - \alpha^n)(1 - \beta^n) = 1 - \alpha^n - \beta^n + q^n.\end{aligned}$$

□

Die Weil-Vermutung für elliptische Kurven ist nun nur noch ein Zusammensetzen der bisherigen Resultate.

Theorem 2.7
Sei $E/\mathbb{F}_q$ eine elliptische Kurve. Dann gilt

$$Z(E/\mathbb{F}_q, T) = \frac{1 - aT + qT^2}{(1 - T)(1 - qT)} \text{ mit } a \in \mathbb{Z}$$

Somit ist insbesondere die Funktionalgleichung erfüllt (mit Pluszeichen und $e = 0$):

$$Z\left(E/\mathbb{F}_q, \frac{1}{qT}\right) = Z\left(E/\mathbb{F}_q, T\right).$$

Außerdem gilt

$$1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T) \text{ mit } |\alpha| = \sqrt{q} = |\beta|.$$

Beweis. Es gilt:

$$\begin{aligned}\log(Z(E/\mathbb{F}_q, T) &= \sum_{n=1}^{\infty} \#E\left(\mathbb{F}_{q^n}\right) \frac{T^n}{n} \\ &\overset{2.6}{=} \sum_{n=1}^{\infty} (1 - \alpha^n)(1 - \beta^n)\frac{T^n}{n} \text{ mit } |\alpha| = \sqrt{q} = |\beta| \text{ und } a := \alpha + \beta \in \mathbb{Z} \\ &= \sum_{n=1}^{\infty} \frac{T^n}{n} - \sum_{n=1}^{\infty} \frac{(\alpha T)^n}{n} - \sum_{n=1}^{\infty} \frac{(\beta T)^n}{n} + \sum_{n=1}^{\infty} \frac{(qT)^n}{n} \\ &= -\log(1 - T) + \log(1 - \alpha T) + \log(1 - \beta T) - \log(1 - qT)\end{aligned}$$

Einsetzen in die Exponentialpotenzreihe ergibt dann

$$Z(E/\mathbb{F}_q, T) = \frac{(1 - \alpha T)(1 - \beta T)}{(1 - T)(1 - qT)} = \frac{1 - aT + qT^2}{(1 - T)(1 - qT).}$$

□

Literatur

[Art24] Artin, Emil: *Quadratische Körper im Gebiete der höheren Kongruenzen. II. Analytischer Teil.* Mathematische Zeitschrift, 19:207–246, 1924.

[Del69] Deligne, Pierre: *Formes modulaires et représentations l-adiques.* Séminaire Bourbaki, 11:139–172, 1968-1969.

[Del74] Deligne, Pierre: *La conjecture de Weil. I.* Publications Mathématiques de l'IHÉS, 43:273–307, 1974.

[Del80] Deligne, Pierre: *La conjecture de Weil. II.* Publications Mathématiques de l'IHÉS, 52:137–252, 1980.

[Dwo60] Dwork, Bernard: *On the rationality of the zeta function of an algebraic variety.* American Journal of Mathematics, 82:631–648, 1960.

[Gar01] Garcia, Arnaldo: *Curves over Finite Fields Attaining the Hasse-Weil Upper Bound.* In: *European Congress of Mathematics*, Band 202, Seiten 199–205. Birkhäuser Basel, 2001.

[Gro66] Grothendieck, Alexander: *Formule de Lefschetz et rationalité des fonctions-L.* Séminaire Bourbaki, 9:41–55, 1964-1966.

[Maz75] Mazur, Barry: *Eigenvalues of Frobenius acting of algebraic varieties over finite fields.* In: *Algebraic Geometry, Acarta 1974*, Band 29, Seiten 231–263. Robin Hartshorne, 1975.

[Sil86] Silverman, Joseph H.: *The Arithmetic of Elliptic Curves.* Springer-Verlag, zweite Auflage, 1986.

[Wei49] Weil, André: *Numbers of solutions of equations in finite fields.* Bull. Amer. Math. Soc., 55:497–508, 1949.