Elliptische Kurven über endliche Körper

Brandon Williams - Seminar Elliptische Kurven

Sei im Folgenden K ein endlicher Körper mit $q = p^n$ Elementen, $p = \text{char}(K)$, und E/K eine elliptische Kurve. Sei $\overline{K}$ ein fest gewählter algebraischer Abschluss von K.

Bemerkung: Elliptische Kurven über endliche Körper sind nicht nur von rein mathematischem Interesse! Sie spielen auch eine wichtige Rolle in der Kryptographie - zum Beispiel bei der schnellen Faktorisierung ganzer Zahlen (Algorithmus von Lenstra) oder verschiedene Algorithmen zur Verschlüsselung und digitaler Unterzeichnung von Nachrichten (z.B. Digital Signature Algorithm). Letzteres basiert auf der Tatsache, dass die Multiplikation $Q := [k]P$ von einem Punkt P auf einer elliptischen Kurve schnell zu berechnen ist; aus Q und P die Zahl k zu bestimmen ist dagegen sehr aufwändig.

Die erste Aufgabe dieses Vortrags wird die Schätzung der Anzahl von Punkten in $E(K)$ sein. Zunächst brauchen wir:

Lemma 1: Sei A eine abelsche Gruppe und $d : A \to \mathbb{Z}$ eine positiv definite quadratische Form; d.h.
(i) $d(a+b+c)-d(a+b)-d(b+c)-d(a+c)+d(a)+d(b)+d(c) = 0 \ \ \forall a, b, c \in A$;
(ii) $d(a) \geq 0 \ \ \forall a \in A$ und $d(a) = 0 \Leftrightarrow a = 0$.
Dann gilt für $a, b \in A$:

$$|d(a-b) - d(a) - d(b)| \leq 2\sqrt{d(a)d(b)}.$$

(Diese Ungleichung ist eine Form der Cauchy-Schwarz-Ungleichung).

Beweis: Die Aussage ist trivial für $a = 0$. Sei also $a \neq 0$ und sei $L(a, b) = d(a - b) - d(a) - d(b)$. Dann ist L eine symmetrische Bilinearform, denn

$$L(a + b, c) = d(a + b - c) - d(a + b) - d(c)$$

$$= d(a + c) + d(b + c) - d(a) - d(b) - 2d(c) = L(a, c) + L(b, c).$$

Außerdem gilt für alle $m, n \in \mathbb{Z}$:

$$0 \leq d(ma - nb) = m^2 d(a) + mnL(a, b) + n^2 d(b).$$

Insbesondere mit $m = -L(a, b)$ und $n = 2d(b)$ folgt

$$0 \leq d(a)(4d(a)d(b) - L(a, b)^2),$$

also $L(a,b)^2 \leq 4d(a)d(b)$.

Satz 2 (Hasse): $|\#E(K) - (q+1)| \leq 2\sqrt{q}$.

Beweis: Sei $\varphi : E \to E$, $(x,y) \mapsto (x^q, y^q)$ der Frobeniusmorphismus. Es gilt dann für $P \in E(\overline{K})$: $P \in E(K) \Leftrightarrow \varphi(P) = P$, denn K ist der Fixkörper des q-Frobeniusautomorphismus in $\overline{K}$. Somit ist $E(K) = \mathrm{Kern}[1-\varphi]$ und damit

$$\#E(K) = \#\mathrm{Kern}[1-\varphi] = \deg[1-\varphi].$$

(Für die letzte Gleichung verwenden wir, dass $1-\varphi$ separabel ist.) Dabei ist deg bekanntlich eine positiv definite quadratische Form auf $\mathrm{End}[E]$ mit $\deg[\varphi] = q$ und $\deg[1] = 1$, sodass die Behauptung nun aus Lemma 1 folgt.
Insbesondere: da $q + 1 > 2\sqrt{q}$, folgt dass jede elliptische Kurve über $\mathbb{F}_q$ mindestens einen $\mathbb{F}_q$-rationalen Punkt besitzt.

Wir werden nun die Weil-Vermutungen formulieren: Sei K wie oben und für $n \geq 1$ sei K_n die Erweiterung von K mit $[K_n : K] = n$. Ferner sei V/K eine projektive Varietät.

Definition 3: Die Zetafunktion zu V/K ist die Potenzreihe

$$Z(V/K,T) = \exp(\sum_{n=1}^{\infty} \frac{\#V(K_n)}{n} T^n).$$

(Es gilt also $\#V(K_n) = \frac{1}{(n-1)!} \frac{d^n}{dT^n} \log Z(V/K,T)|_{T=0}$).

Satz 4 (Weil-Vermutungen): Sei $K = \mathbb{F}_q$ und V/K eine glatte projektive Varietät der Dimension n. Dann gilt
(i): $Z(V/K,T) \in \mathbb{Q}(T)$.
(ii): Es gibt ein $\varepsilon \in \mathbb{Z}$ (Euler-Charakteristik von V) mit

$$Z(V/K, \frac{1}{q^n T}) = \pm q^{n\varepsilon/2} T^{\varepsilon} Z(V/K,T).$$

(iii): $Z(V/K,T)$ zerfällt in

$$Z(V/K,T) = \frac{P_1(T) \cdots P_{2n-1}(T)}{P_0(T) \cdots P_{2n}(T)}$$

mit $P_i(T) \in \mathbb{Z}[T]$, $P_0(T) = 1 - T$, $P_{2n}(T) = 1 - q^n T$ und für $1 \leq i \leq 2n-1$ zerfällt $P_i(T)$ über $\mathbb{C}$ in

$$P_i(T) = \prod_j (1 - \alpha_{ij} T) \quad (\text{mit } |\alpha_{ij}| = q^{i/2}).$$

Bemerkung: Sei $\overline{K}/K$ ein algebraischer Abschluss. Ist $\overline{V} = V \times_K \overline{K}$ und φ der Frobenius-Morphismus auf $\overline{V}$, so ist $\#V(K_n)$ gerade die Anzahl von Fixpunkten

von φ^n. Mit einer "geeigneten Kohomologietheorie" würde aus einem Lefschetz-Fixpunktsatz folgen:

$$\#V(K_n) = \sum_i (-1)^i \mathrm{Tr}((\varphi^n)^* | H^i(\overline{V}, ??)).$$

Eine geeignete Kohomologietheorie existiert in der Tat (mehr oder weniger). Wir gehen aber darauf nicht in diesem Vortrag ein.

Wir beweisen nun die Weil-Vermutungen für elliptische Kurven.

Sei $\psi \in \mathrm{End}(E)$ und betrachte den induzierten Endomorphismus $\psi_l \in \mathrm{End}(T_l(E))$ auf dem Tate-Modul, wobei $l \neq \mathrm{char}(K)$ eine fest gewählte Primzahl ist.

Proposition 5: Sei $\psi \in \mathrm{End}(E)$. Dann gilt

$$\det(\psi_l) = \deg(\psi) \quad \text{und} \quad \mathrm{tr}(\psi_l) = 1 + \deg(\psi) - \deg(1 - \psi).$$

Insbesondere hängen diese nicht von l ab.

Beweis: Sei $\{v_1, v_2\}$ eine $\mathbb{Z}_l$ - Basis für $T_l(E)$ und sei die Darstellungsmatrix von ψ_l bzgl. dieser Basis gegeben durch

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Außerdem sei $e : T_l(E) \times T_l(E) \to T_l(\mu)$ die Weil-Paarung. Dann gilt

$$\begin{aligned} e(v_1, v_2)^{\deg\psi} &= e([\deg\psi]v_1, v_2) = e(\hat{\psi}_l \circ \psi_l(v_1), v_2) \\ &= e(\psi_l(v_1), \psi_l(v_2)) = e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(v_1, v_2)^{ad-bc} = e(v_1, v_2)^{\det\psi_l}. \end{aligned}$$

Da e nicht ausgeartet ist, ist $e(v_1, v_2)$ keine Einheitswurzel, so dass folgt: $\deg\psi = \det\psi_l$. (nämlich: wäre $e(v_1, v_2)^n = e(n * v_1, v_2) = e(v_1, n * v_2) = 1$, so folgt, dass v_1, v_2 n-torsion wären und damit keine Basis bildeten).
Wegen $\mathrm{tr}(M) = 1 + \det(M) - \det(1 - M)$ folgt die Behauptung.

Sei nun φ wieder der Frobenius-Morphismus. Nach den obigen Überlegungen gibt es $\alpha, \beta \in \mathbb{C}$ sodass

$$P(T) := \det(T - \varphi_l) = T^2 - \mathrm{tr}(\varphi_l)T + \det(\varphi_l)T = (T - \alpha)(T - \beta).$$

Außerdem gilt nach Lemma 1:

$$\Delta(P) = \mathrm{tr}(\varphi_l)^2 - 4\det(\varphi_l) \leq 4\deg(\varphi_l)\deg(1) - 4\deg(\varphi_l) = 0,$$

d.h. P hat entweder eine doppelte Nullstelle oder zwei komplex konjugierten. Also ist $|\alpha| = |\beta|$. Wegen $\alpha\beta = \det\varphi_l = \deg\varphi_l = q$ folgt $|\alpha| = |\beta| = \sqrt{q}$.
Da φ_l^n nun das characteristische Polynom $(T - \alpha^n)(T - \beta^n)$ hat, folgt

$$\#E(K_n) = \deg(1 - \varphi^n) = \det(1 - \varphi_l^n) = 1 - \alpha^n - \beta^n + q^n.$$

Satz 6 (Weil-Vermutungen, elliptische Kurven): Sei $E/\mathbb{F}_q$ eine elliptische Kurve. Dann existiert ein $a \in \mathbb{Z}$ mit

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

Ferner gilt $Z(E/\mathbb{F}_q, \frac{1}{q}T) = Z(E/\mathbb{F}_q, T)$.

Beweis: Es gilt

$$\log Z(E/\mathbb{F}_q, T) = \sum_{n=1}^{\infty} \frac{\#E(K_n)}{n} T^n = \sum_{n=1}^{\infty} \frac{1 - \alpha^n - \beta^n + q^n}{n} T^n$$

$$= -\log(1-T) + \log(1-\alpha T) + \log(1-\beta T) - \log(1-qT).$$

Also ist

$$Z(E/\mathbb{F}_q, T) = \frac{(1-\alpha T)(1-\overline{\alpha} T)}{(1-T)(1-qT)}.$$

Wähle $a = \alpha + \beta = 1 + q - \deg(1-\varphi) \in \mathbb{Z}$. Die Funktionalgleichung ist offensichtlich.

Bemerkung: Ersetzt man $T = q^{-s}$ und definiert man $\zeta_{E/K}(s) = Z(E/K, q^{-s})$, so übersetzt sich die Funktionalgleichung zu $\zeta_{E/K}(1-s) = \zeta_{E/K}(s)$ und es gilt

$$\zeta_{E/K}(s) = 0 \;\Rightarrow\; |q^s| = \sqrt{q} \;\Rightarrow\; \mathrm{Re}[s] = \frac{1}{2}.$$

Aus diesem Grund nennt sich Satz 4 (iii) auch Riemannsche Vermutung.

Literatur:

J. Silverman. *Arithmetic of Elliptic Curves* (1986).