<u>Stichworte</u>: $E(\mathbb{Q})$: Beispiele, Satz von Mordell, Rangvermutung, Sätze von Mazur, Nagell-Lutz, Siegel, Faltings, $E(\mathbb{C})$: elliptische Kurve über $\mathbb{C}$ = Torus

§3 Elliptische Kurven über verschiedenen Körpern

<u>Bem.</u>: die Fälle $k = \mathbb{R}, \mathbb{Q}, \mathbb{C}$ sind für die Theorie von Bedeutung, nicht so sehr für die Kryptographie-Anwendungen, wo endl. Körper $\mathbb{F}_{p^r}$ praktisch sind.

§3.1 Elliptische Kurven über $\mathbb{Q}$

1.) <u>Motivation</u>: Betr. die elliptische Kurve $E(k)$ jetzt über $k = \mathbb{Q}$.
Wie findet man möglichst viele rationale Punkte (d.h. $P = (x,y) \in \mathbb{A}^2(\mathbb{Q})$) auf der Kurve $E(\mathbb{Q})$? $\mathcal{O} = [0:1:0]$ ist immer einer, wie findet man affine P?

Die expliziten Formeln zeigen:

- Ist P ein rationaler Punkt auf $E(k)$, so auch $2P, 3P, 4P, \ldots$
- Sind P, Q zwei rationale Punkte, so auch $P+Q$, $P+(P+Q) = 2P+Q$, $P+(2P+Q) = 3P+Q$, $4P+Q, \ldots$ $2P+2Q, \ldots$ usw.

Können so unendlich viele rationale Punkte auf $E(k)$ konstruiert werden? Das hängt von der Ordnung des Punktes P in der Gruppe $(E(k), +)$ ab, d.h. von $\operatorname{ord}(P) = \min\{m \in \mathbb{N};\ mP = \mathcal{O}\}$, falls diese existiert. Das ist ziemlich unklar, wie auch Beispiele zeigen:

2) <u>Bsp.</u>: Sei $E(\mathbb{Q})$: $y^2 = x^3 + 17$. Dann ist $\Delta(E) = -16 \cdot 27 \cdot 17^2 \neq 0$.
Zwei Punkte sind $P = (-2, 3)$ und $Q = (-1, 4)$.

Es ist
$$\begin{aligned}
P + Q &= (4, -9) && \text{Schnitt } G(P,Q) \text{ mit } E(k), \text{ an } x\text{-Achse spiegeln} \\
2P + Q &= (2, 5) && \text{Schnitt } G(P,P+Q) \text{ mit } E(k), \text{ an } x\text{-Achse spiegeln} \\
3P + Q &= \left(\tfrac{1}{4}, -\tfrac{33}{8}\right) && \text{Schnitt } G(P,2P+Q) \text{ mit } E(k), \text{ an } x\text{-Achse spiegeln} \\
4P + Q &= \left(\tfrac{106}{9}, \tfrac{1097}{27}\right) && \vdots \\
5P + Q &= \left(-\tfrac{2228}{961}, -\tfrac{63465}{29791}\right) \\
6P + Q &= \left(\tfrac{76271}{289}, -\tfrac{21063928}{4913}\right) \\
&\vdots
\end{aligned}$$

Offenbar werden die Ergebnisse immer komplizierter; unendlich viele rationale Punkte können auf $E(\mathbb{Q})$ wohl derart konstruiert werden, d.h. vermutlich hat P keine (endliche) Ordnung.

3.) **Bsp.:** Sei $E(\mathbb{Q}): y^2 = x^3 + x$. Der <u>einzige</u> affine rationale Punkt auf $E(\mathbb{Q})$ ist $P=(0,0)$. Dies kann direkt gezeigt werden unter Verwendung, dass die Gleichung $u^4+v^4=w^2$ nur ganzzahlige Lösungen mit $u=0$ oder $v=0$ hat (was auch schon nicht so schnell zu zeigen ist).
Es kann dennoch gesagt werden, dass durch $P, 2P=\mathcal{O}, 3P=P, 4P=\mathcal{O}, \ldots$ alle rationalen Punkte auf $E(\mathbb{Q})$ konstruiert werden können.

4) **Bsp.:** Sei $E(\mathbb{Q}): y^2 = x^3 - 4x^2 + 16$. Dann ist $\Delta(E) = -16\cdot(4(-4)^3 + 27\cdot 16^2) \neq 0$
Eine kurze Suche liefert die 4 rationalen Punkte

$$P_1=(0,4),\ P_2=(4,4),\ P_3=(0,-4)=-P_1,\ P_4=(4,-4)=-P_2.$$

Können hier wie in Bsp. 2.) beliebig viele rationale Punkte konstruiert werden?
Hier ist die Gerade durch P_1 und P_2 die Tangente an $E(k)$ in P_1, weil $4^2 = x^3-4x^2+16 \Leftrightarrow 0 = x^2(x-4)$ ist und $x=0$ doppelte Nst.
Damit ist $-P_1 = P_1 + P_2 = P_3$, also kann so kein weiterer rationaler Punkt konstruiert werden. Auch mit anderen Paaren P_i und P_j der 4 Punkte passiert dies. Vermutlich gibt es außer den 4 angegebenen rationalen Punkten keine weiteren auf $E(\mathbb{Q})$.
Wir haben $P_1=(0,4)$, $2P_1 = -P_2 = P_4$, $3P_1 = P_1 + \overset{-P_2}{\widetilde{P_4}} = P_2$, $4P_1 = P_1 + P_2 = P_3$,
$5P_1 = P_3 + P_1 = (P_1+P_2)+P_1 = 2P_1 + P_2 = -P_2 + P_2 = \mathcal{O}$, d.h. $\mathrm{ord}(P_1) = 5$.

$\rightsquigarrow \langle P_1\rangle = \mathbb{Z}_5$, $\langle P_1\rangle = \{\mathcal{O}, P_1, P_2, P_3, P_4\}$

5.) Die Beispiele legen folgenden Satz nahe:

<u>Satz von **Mordell** (1922):</u>
<u>Sei $E(\mathbb{Q})$ eine elliptische Kurve über $\mathbb{Q}$.</u>
Dann gibt es eine endliche Liste von Punkten $P_1, \ldots, P_s \in E(\mathbb{Q})$, so dass alle (rationalen) Punkte auf $E(\mathbb{Q})$ von diesen erzeugt werden, d.h. $\forall P \in E(\mathbb{Q})\ \exists m_1, \ldots, m_s \in \mathbb{N}_0 : P = m_1P_1 + \ldots + m_sP_s$.
M.a.W.: die Gruppe $(E(\mathbb{Q}), +)$ ist <u>endlich erzeugt.</u>

- Dabei können die Erzeuger endliche Ordnung haben oder nicht.
- Natürlich sind die Erzeuger nicht unbedingt eindeutig bestimmt.

6.) <u>Bem.:</u> In Bsp. 3.) haben wir einen endlichen Erzeuger $P_1 = (0,0)$, $ord(P_1) = 2$,
in Bsp. 4.) haben wir ev. einen endlichen Erzeuger $P_1 = (0,4)$, $ord(P_1) = 5$.
In Bsp. 2.) haben wir ev. einen unendlichen Erzeuger $P_1 = (-2,3)$, welcher ev. nicht der einzige ist. Die von P_1 erzeugte Untergruppe
$\mathbb{Z}\cdot P_1 := \{ m P_1 ;\ m \in \mathbb{Z} \} \leq E(\mathbb{Q})$ ist isomorph zu $\mathbb{Z}$
vermöge $\mathbb{Z}\cdot P_1 \cong \mathbb{Z}$, $m\cdot P_1 \mapsto m$.

7.) Wir können in der Formulierung von 5.) die Unterscheidung zwischen Punkten mit und ohne endlicher Ordnung vornehmen.
Die Teilmenge $T := \{ P \in E(\mathbb{Q});\ ord(P) \in \mathbb{N} \}$ aller Punkte von $E(\mathbb{Q})$ mit endlicher Ordnung ist offenbar eine Untergruppe, die <u>Torsionsgruppe</u> von $E(\mathbb{Q})$ heißt. Somit hat der Satz von Mordell auch die folgende Formulierung:

8.) <u>Satz von Mordell</u>, Formulierung als Aussage über die Gruppenstruktur:
Es gibt ein $r \in \mathbb{N}_0$ mit $\underbrace{E(\mathbb{Q})}_{\text{Gruppe bzgl.} +} \cong \underbrace{\mathbb{Z}^r}_{\text{komponentenweise Addition}} \times T$.

9.) <u>Def.:</u> Die Zahl $r(E)$ heißt <u>Rang von $E(\mathbb{Q})$</u>.

10.) <u>Bem.:</u> Die Torsionsgruppe T ist stets endlich, wie aus dem Struktursatz über endlich erzeugte abelsche Gruppen gefolgert werden kann. Allerdings bleiben Größe von T und Lage der Torsionspunkte $P \in T$ damit unbekannt.
Weiter kann aber $\# E(\mathbb{Q}) = \infty \iff r(E) > 0$ gefolgert werden.

11.) <u>Bsp.:</u>
- $E(\mathbb{Q})$: $y^2 = x^3 - 4 \rightsquigarrow E(\mathbb{Q}) \cong \mathbb{Z}^1$, wobei z.B. $P_1 = (2,2)$ Erzeuger ist.
- Im Bsp. 3.) und 4.): $\mathrm{Rg}\, E(\mathbb{Q}) = 0$. [Ohne Beweis]

12.) Der Rang elliptischer Kurven ist bislang schlecht verstanden.
Offen, d.h. bislang unbewiesen ist z.B. die
<u>Rangvermutung:</u> $\limsup_{E(\mathbb{Q})} r(E) = \infty$.

D.h. man vermutet, dass es zu jedem $C \in \mathbb{R}$ eine elliptische Kurve mit $\operatorname{rg} E(\mathbb{Q}) > C$ gibt. Der aktuelle Weltrekord (2006, von N. Elkies) ist eine elliptische Kurve vom Rang ≥ 28 (da 28 "unabhängige" Punkte unendlicher Ordnung auf ihr gefunden wurde, die Kurve lautet

$$y^2 + xy + y = x^3 - x^2 - ax + b$$

mit $a = 20\,067\,762\,415\,575\,526\,585\,033\,208\,209\,338\,542\,750\,930\,230\,312\,178\,956\,502$

und $b = 34\,481\,611\,795\,030\,556\,467\,032\,985\,690\,390\,720\,374\,855\,944\,359\,319\,180\,361\,266\,008\,296\,291\,939\,448\,732\,243\,429$

Die Torsionsgruppe ist deutlich besser verstanden:

13.) Satz von Nagell-Lutz (Nagell 1935, Lutz 1937):
Sei $E(\mathbb{Q})$ eine elliptische Kurve mit Gleichung $y^2 = x^3 + ax^2 + bx + c$, $a,b,c \in \mathbb{Z}$, und seien $P_1, \ldots, P_s$ alle Torsionspunkte, d.h. $T = \{P_1, \ldots, P_s\}$.
Schreibe die $P_i = (x_i, y_i) \in \mathbb{Q}^2$.
Dann sind alle $x_i, y_i \in \mathbb{Z}$, und für $y_i \neq 0$ gilt $y_i^2 \mid \Delta(E)$.

14.) Satz von Mazur (1977):
Sei $E(\mathbb{Q})$ eine elliptische Kurve mit Gleichung $y^2 = x^3 + ax^2 + bx + c$, $a,b,c \in \mathbb{Z}$, mit Torsionsuntergruppe T. Dann ist $T \cong \mathbb{Z}_n$ mit $n \leq 12$, $n \neq 11$,
oder $T \cong \mathbb{Z}_2 \times \mathbb{Z}_n$ mit $n \in \{2, 4, 6, 8\}$.
Andere Torsionsuntergruppen kann es nicht geben, und alle genannten kommen vor.

Das sind beachtliche, tiefe Sätze. In Bsp. 4.) ist $T \cong \mathbb{Z}_5$, und man kann sehen, dass der Nagell-Lutz-Satz hier korrekt ist: $4^2 \mid \Delta(E)$.

Für $a,b,c \in \mathbb{Z}$ kann es höchstens endlich viele Punkte mit ganzzahligen Koordinaten geben:

15.) Satz von Siegel (1926): Sei $E(\mathbb{Q})$: $y^2 = x^3 + ax^2 + bx + c$ mit $a,b,c \in \mathbb{Z}$ eine elliptische Kurve. Dann gibt es nur endlich viele Kurvenpunkte $(x,y) \in E(\mathbb{Q}) \cap \mathbb{Z}^2$.
[Historische Bem.: Siegel veröffentlichte den ersten Beweis 1926 unter dem Pseudonym "X"]

16.) Im Bsp. 2.) haben genau die Punkte $\mathcal{O}$, $(-2,\pm 3)$, $(-1,\pm 4)$, $(2,\pm 5)$, $(4,\pm 9)$, $(8,\pm 23)$, $(43,\pm 282)$, $(52,\pm 375)$, $(5234,\pm 378661)$ auf der elliptischen Kurve $E(\mathbb{Q})$ ganzzahlige Koordinaten.

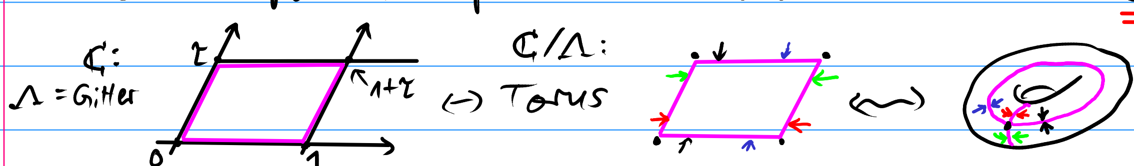
17.) Ellipt. Kurven über $\mathbb{Q}$ sind nicht-sing. alg. Kurven vom Geschlecht 1. Mordell vermutete, dass jede über $\mathbb{Q}$ def. nicht-sing. alg. Kurve vom Geschlecht ≥ 2 höchstens endl. viele Punkte enthält. Diese Vermutung wurde 1983 von G. Faltings für bel. Körper bewiesen, wofür er 1986 auf der ICM in Berkeley mit der Fieldsmedaille ausgezeichnet wurde.

§3.2 Elliptische Kurven über $\mathbb{C}$

18.) Elliptische Kurven über $\mathbb{C}$ können einerseits über die Weierstraßglg. dargestellt werden und zum anderen über ihre Legendre-Normalform mit einer Glg. der Form $y^2 = x(x-1)(x-\lambda)$, vgl. Übungsaufgabe 2a), Blatt 6.
Wir besprechen hier kurz die dritte Darstellung mittels elliptischer Funktionen; ein ganzer Teil der Funktionentheorie behandelt die Theorie elliptischer Funktionen. Wir möchten hier nur erläutern, warum eine elliptische Kurve über $\mathbb{C}$ in diesem Sinne ein Torus ("Doughnut") ist.

Geg. sei $\tau \in \mathbb{C}\setminus\mathbb{R}$, betr. das Gitter $\Lambda := \{a+\tau\cdot b;\ a,b\in\mathbb{Z}\} \subseteq \mathbb{C}$.

19.) Def.: Eine Funktion $f: \mathbb{C}\setminus\mathcal{P} \to \mathbb{C}$ der Form $f(z) := \frac{g(z)}{h(z)}$, g,h holomorph, $h\neq 0$, heißt elliptische Funktion, falls $f(z+\omega) = f(z)$ für alle $z\in\mathbb{C}$ und $\omega\in\Lambda$, (sofern $f(z), f(z+\omega)$ definiert ist, wobei $\mathcal{P} = \{z;\ h(z)=0\}$ die Menge der Polstellen von f ist), d.h. wenn f (doppelt-)periodische Funktion zu Λ ist.
Der Körper der elliptischen Funktionen über Λ sei $\mathbb{C}(\Lambda)$.



Konstruktion eines Torus zum Gitter $\Lambda \subseteq \mathbb{C}$: $\mathbb{C}/\Lambda := \{z+\Lambda;\ z\in\mathbb{C}\}$.
Jedes $z+\Lambda$ kann repräsentiert werden als $z+\Lambda = z'+\Lambda$ mit $z' = \mu+\nu\tau$, $\mu,\nu\in[0,1[$
(hier rosa Bereich ~ "Fundamentalparallelogramm"; die Randverklebung ergibt Torus).

Eine elliptische Funktion ohne Polstellen (oder ohne Nst.) ist konstant (wg. Satz von Liouville aus der Funktionentheorie).

20) <u>Def.:</u> Zu Λ def. $\wp(z) := \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$, $\wp : \mathbb{C}\setminus\Lambda \to \mathbb{C}$,

und $G_{2k}(\Lambda) := \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \frac{1}{\omega^{2k}} \in \mathbb{C}$. Dann heißt $\wp$ die Weierstraß-$\wp$-Funktion und G_{2k} heißt Eisensteinreihe vom Gewicht $2k \in \mathbb{R}_{>2}$.
(Englische Anleitung zur Aussprache: "pay-function")

21) <u>Satz:</u> Sei Λ ein Gitter.
a) Die Eisenstein-Reihe $G_{2k}(\Lambda)$ konvergiert absolut für $k>1$.
b) Die Reihe der Fkt. $\wp$ konvergiert absolut und gleichmäßig auf jeder kompakten Teilmenge von $\mathbb{C}\setminus\Lambda$. Sie definiert eine elliptische Funktion mit zweifachem Pol in jedem Gitterpunkt $\omega\in\Lambda$.

Es gilt somit $\wp'(z) = -2\sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \frac{1}{(z-\omega)^3}$ für $z\in\mathbb{C}\setminus\Lambda$. Die Funktionen $\wp$ und $\wp'$ liefern den "Prototyp" elliptischer Funktionen: Man kann zeigen, dass jede elliptische Fkt. f schreibbar ist als $f(z) = \frac{P_1(\wp(z))}{Q_1(\wp(z))} + \wp'(z)\cdot\frac{P_2(\wp(z))}{Q_2(\wp(z))}$, $P_i, Q_i \in \mathbb{C}[Z]$.

22) <u>Satz:</u> Es gilt $(\wp'(z))^2 = 4(\wp(z))^3 - g_2\cdot\wp(z) - g_3$,
d.h. $(\wp(z), \wp'(z)) \in E(\mathbb{C})$ mit Glg. $y^2 = 4x^3 - g_2 x - g_3$,
wobei $g_2 := 60\,G_4$, $g_3 := 140\,G_6$. Da $g_2^3 - 27g_3^2 \neq 0$, d.h. $\Delta(E)\neq 0$, handelt es sich bei $E(\mathbb{C})$ um eine elliptische Kurve.

Haben so die Abb.: $\varphi: \mathbb{C}/\Lambda \to \mathbb{P}^2(\mathbb{C})$
$$z+\Lambda \mapsto [\wp(z) : \wp'(z) : 1],$$
wobei $\varphi(0+\Lambda) = [0:1:0] = \mathcal{O}$.

Das Bild von φ ist genau die genannte elliptische Kurve $E(\mathbb{C})$. Die Abb. $\varphi: \mathbb{C}/\Lambda \to E(\mathbb{C})$ ist bijektiv und überträgt die Addition "+" auf $\mathbb{C}/\Lambda$, geg. durch $(x+\Lambda)+(y+\Lambda) := (x+y)+\Lambda$, auf $E(\mathbb{C})$, welche sich als unsere bisher studierte Addition + auf $E(\mathbb{C})$ erweist. Der Torus $\mathbb{C}/\Lambda$ wird so mit der elliptischen Kurve $E(\mathbb{C})$ identifiziert. Umgekehrt ist auch jede elliptische Kurve $(E(\mathbb{C}),+)$ beschreibbar als Torus $(\mathbb{C}/\Lambda,+)$.