Früchte einer langjährigen Zusammenarbeit

Festkoloquium Prof. Dr. Horst Günter Zimmer

Saarbrücken, 25. Oktober, 2002.

Attila Pethő

Universität Debrecen

1. Anfang

- EUROCAL '85, Linz
- XVI. Steiermärkisch-Mathematischen Symposium, Stift Rein, 1986
- Conference on Number Theory, Budapest, 1987 $\rightarrow$ gemeinsame Projektidee: Saarbrücken, Düsseldorf und Debrecen
- Colloquium on Computational Number Theory, Debrecen, 1989. Prof. Zimmer war Mitglied der Organisationskomitee

Besuch in Debrecen 1987

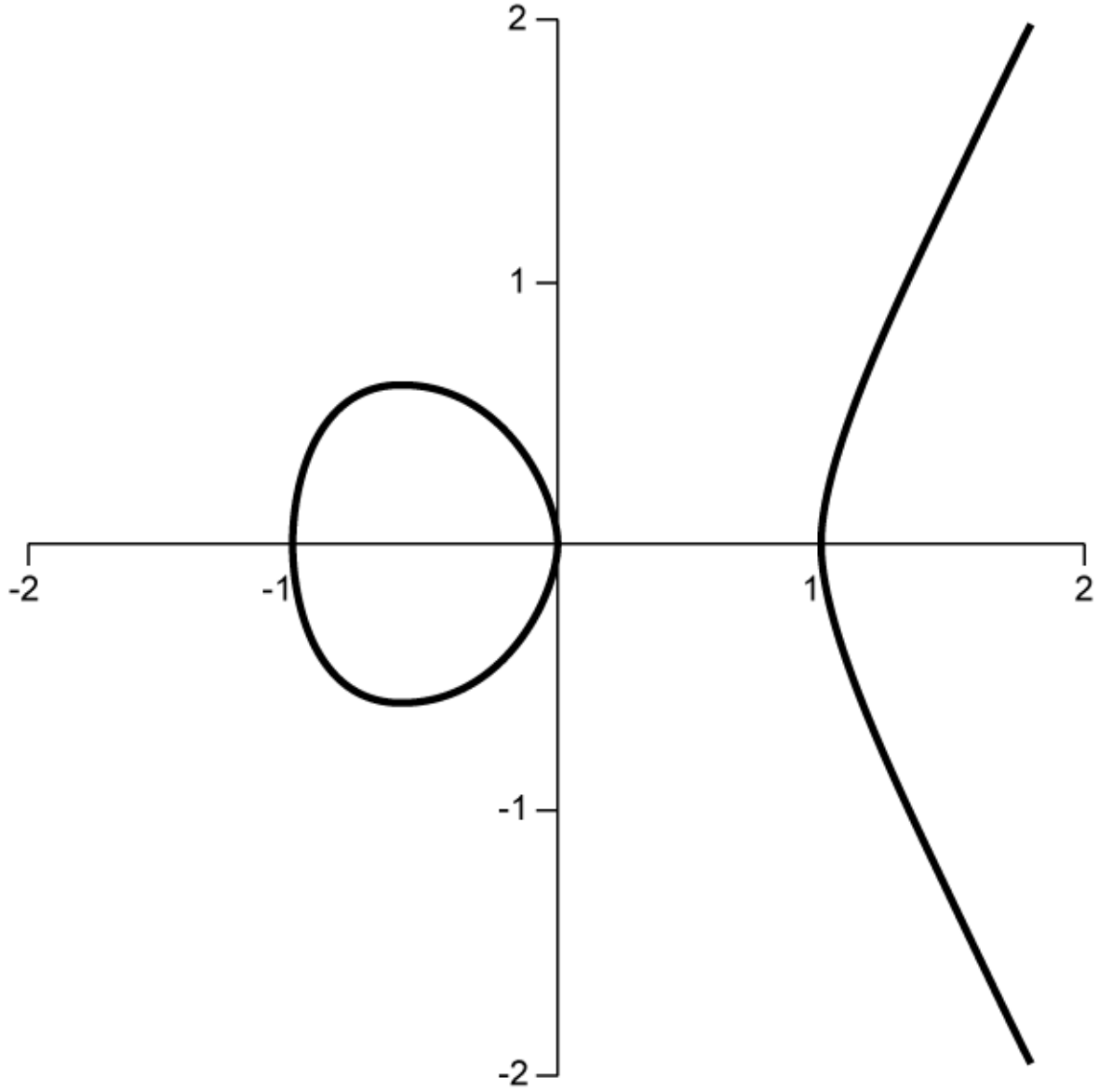
2. Elliptische Kurven

Es sei $\mathbf{K}$ ein Körper und $a_1, a_2, a_3, a_4, a_6 \in \mathbf{K}$, dann heißt die Menge

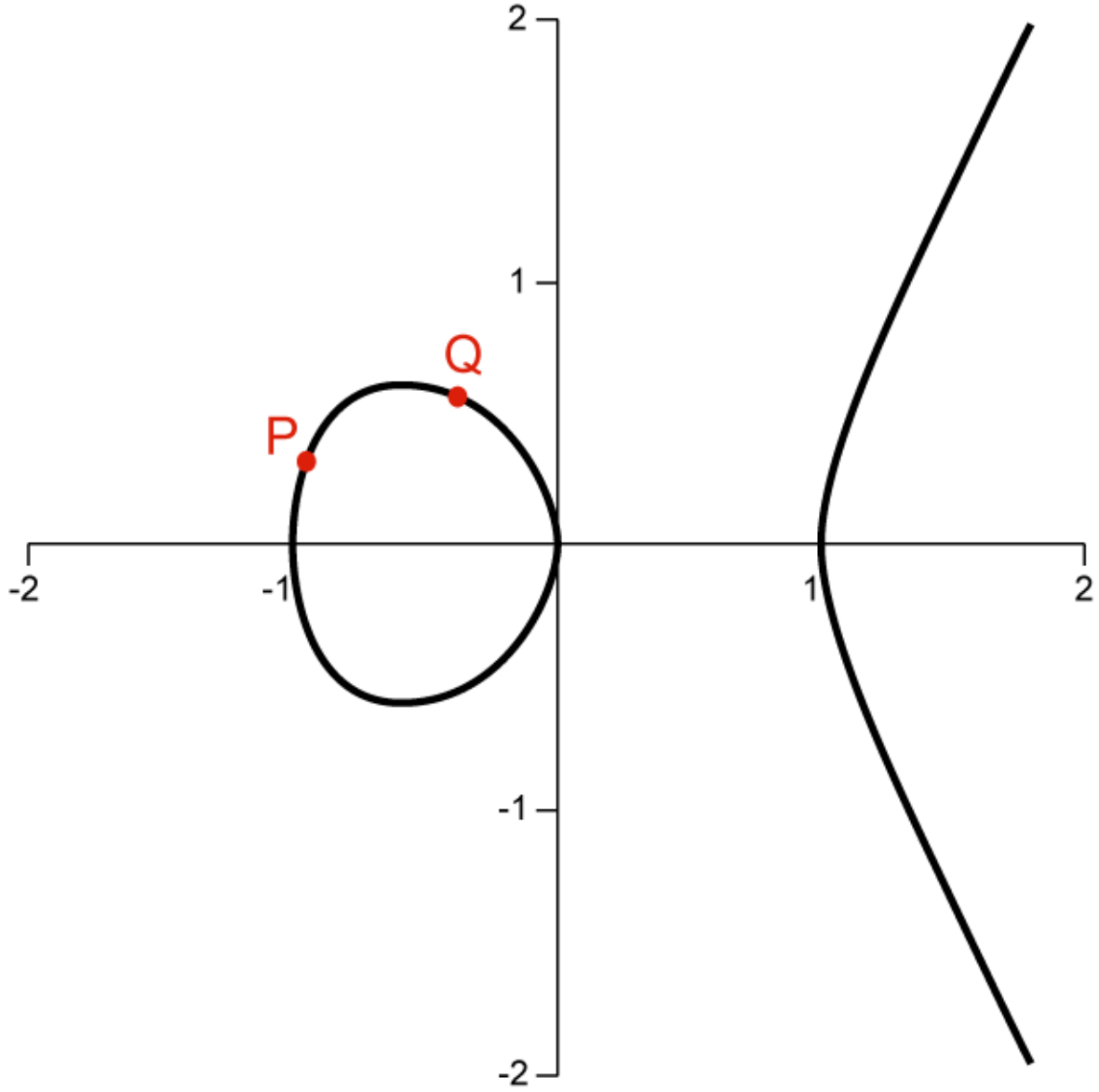
$$E(\mathbf{K}) = \{(x, y) \in \mathbf{K}^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$$

eine elliptische Kurve über $\mathbf{K}$, falls ihre Diskriminante Δ nicht verschwindet .

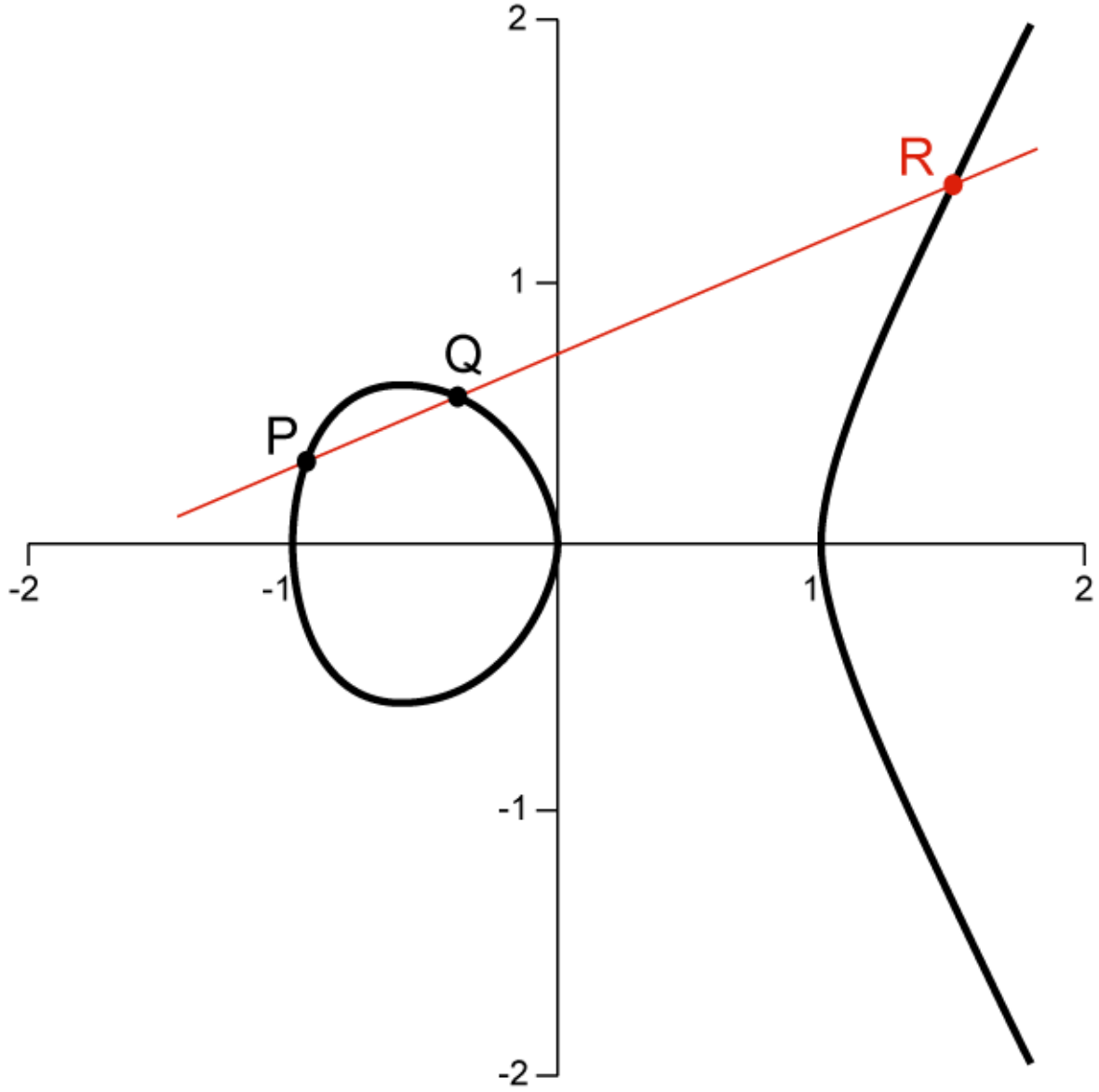
Die Menge $E(\mathbf{K})$ ausgestattet mit dem Sekanten-Tangenten Verfahren bildet eine Abelsche Gruppe.



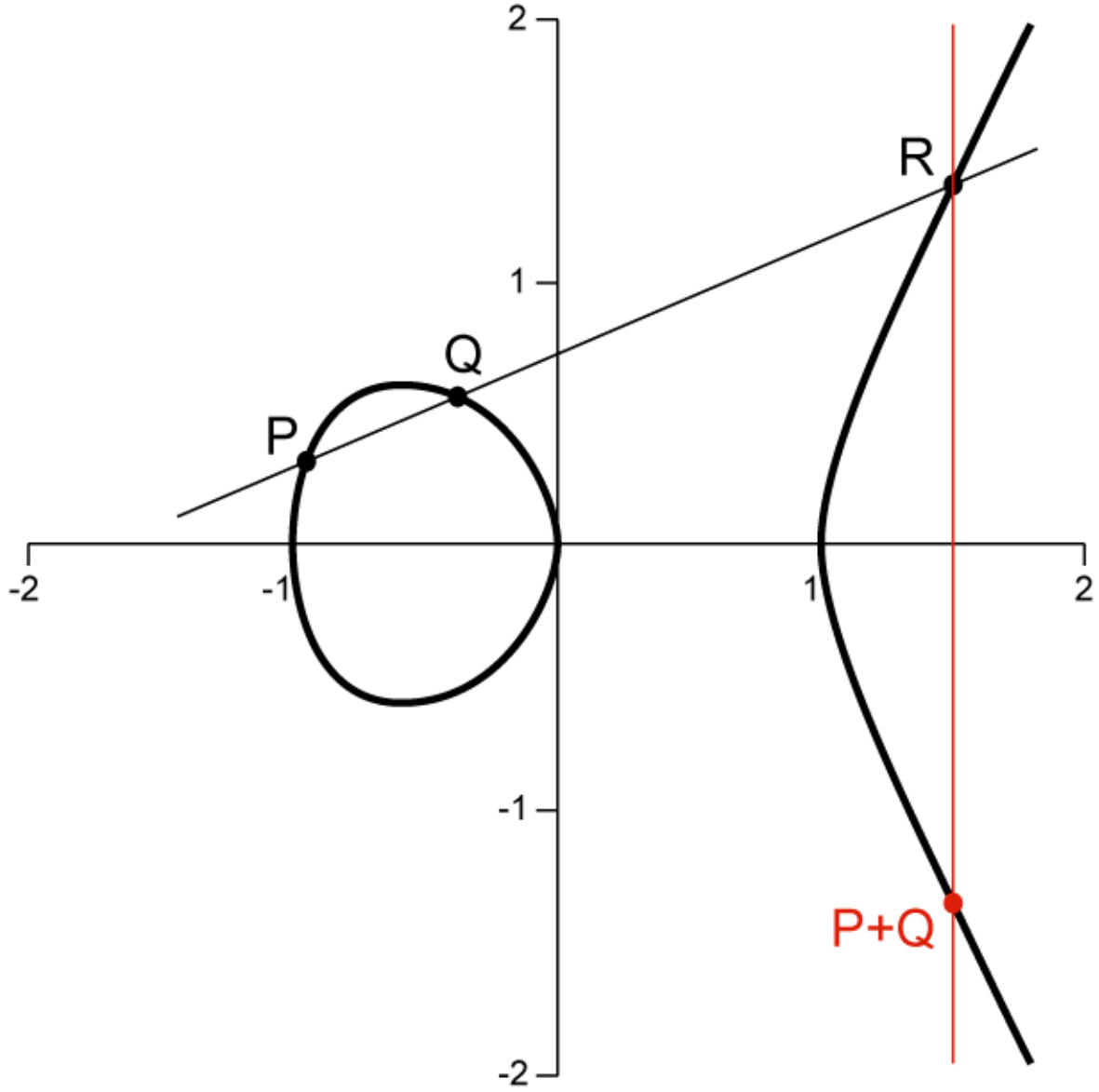
Addition auf der Kurve $y^2 = x^3 - x$ für $\mathbf{K} = \mathbf{R}$, Schritt 1.



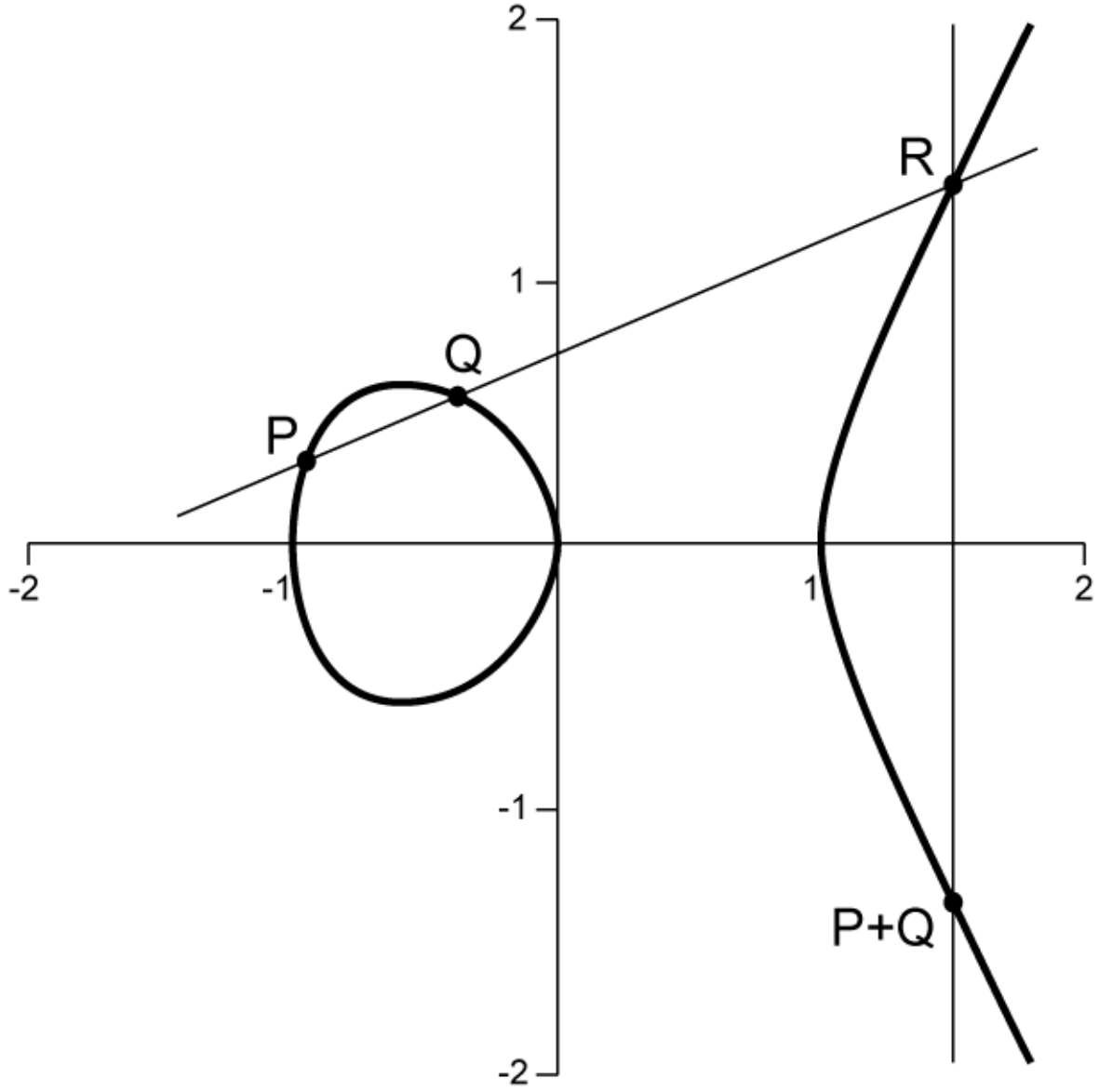
Addition auf der Kurve $y^2 = x^3 - x$ für $\mathbf{K} = \mathbf{R}$, Schritt 2.



Addition auf der Kurve $y^2 = x^3 - x$ für $\mathbf{K} = \mathbf{R}$, Schritt 3.



Addition auf der Kurve $y^2 = x^3 - x$ für $\mathbf{K} = \mathbf{R}$, Schritt 4.



Addition auf der Kurve $y^2 = x^3 - x$ für $\mathbf{K} = \mathbf{R}$, Schritt 5.

Satz 1 (Mordell-Weil). *Ist* $\mathbf{K}$ *ein algebraischer Zahlkörper, dann ist* $E(\mathbf{K})$ *eine endlich erzeugte Abelsche Gruppe, d.h*

$$E(\mathbf{K}) \simeq E(\mathbf{K})_{\mathsf{tors}} \oplus \mathbf{Z}^r.$$

Dieser grundliegende Satz impliziert viele Probleme, z.B.

1. Gebe eine obere Schranke für $|E(\mathbf{K})_{\text{tors}}|$ an.

2. Charakterisiere die Struktur von $E(\mathbf{K})_{\text{tors}}$.

3. Kann r beliebig groß sein?

4. Kann eine Basis der Torsionsfreie Anteil von $E(\mathbf{K})$ algorithmisch bestimmt werden?

Herr Zimmer und seine Studenten haben mit allen dieser Probleme beschäftigt und haben wichtige Beiträge geleistet.

Zum 3. erwähne ich die Arbeiten von Th. Kretschmer (1986) und U. Schneiders (1991).

3. Torsionsstrukturen

Satz 2 (Mazur, 1977).

$$E(\mathbf{Q})_{\text{tors}} \simeq \begin{cases} \mathbf{Z}/m\mathbf{Z} & : \quad 1 \leq m \leq 10, m = 12 \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2m\mathbf{Z} & : \quad m = 1, 2, 3, 4 \end{cases}$$

Satz 3 (Merel, 1996). *Sei* $[\mathbf{K} : \mathbf{Q}] = n$*, dann gibt es eine nur von* n *abhängige Konstante* c*, so daß*

$$|E(\mathbf{K})_{\text{tors}}| \leq c.$$

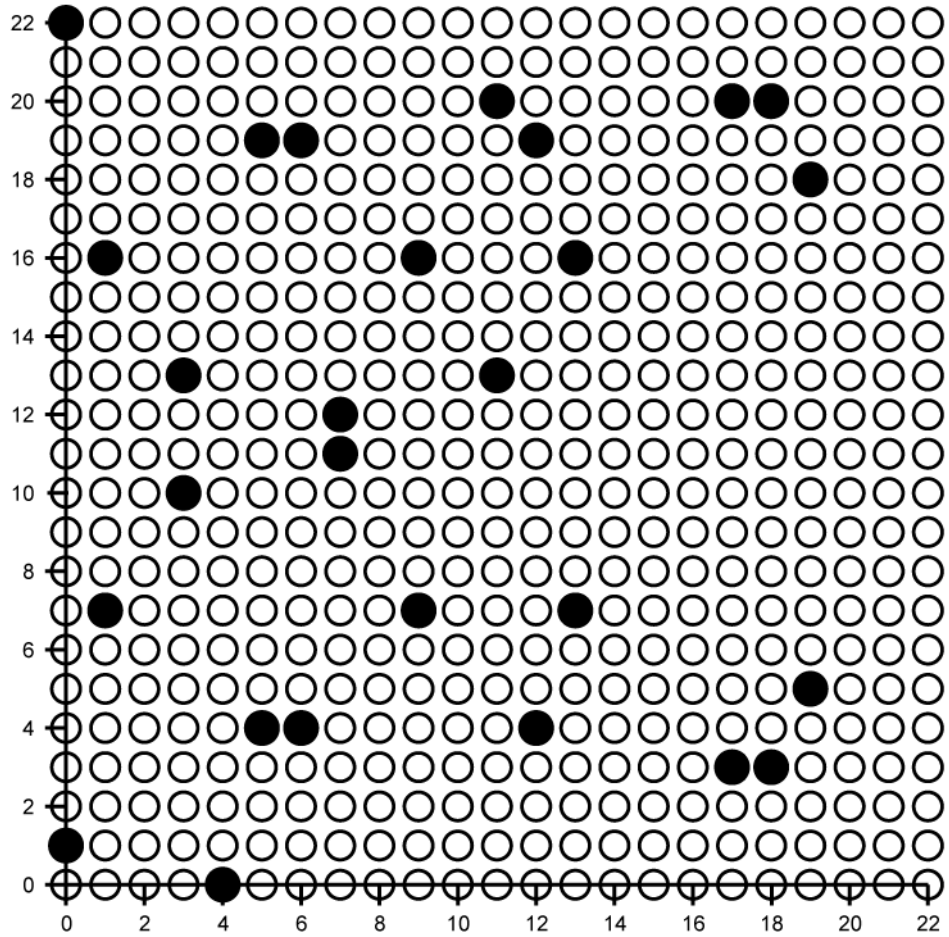
Beobachtung von Prof. Zimmer $\approx$ 1980: *Ist die j-Invariante von $E(\mathbf{K})$ ganz, dann gilt der Beschränktheitssatz.$\rightarrow$ Ist n klein, dann können die mögliche Torsionsstrukturen bestimmt werden.*

Auf diesem Problemkreis haben: Ch. Abel-Hollinger, H.G. Folz, H.H. Müller, J. Stein, H. Ströher, Th. Weis, Chr. Wentz, sowie G.W. Fung, A. Pethő und H.C. Williams gearbeitet.

Die Verwirklichung erfolgt in mehreren, umfangreichen Schritten (Beispiel $n = 3$ A.P., Th. Weis und H.G. Zimmer, 1997):

1. **Reduktionstheorie** liefert eine endliche Liste.

Elliptische Kurven über endlichen Körper spielen hier eine wichtige Rolle.



Das Bild von $E(\mathbf{K})$ für einen endlichen Körper $\mathbf{K}$,
$E(\mathbf{F}_{23}) : y^2 = x^3 + x + 1$.

Satz 4 (Hasse). *Es sei $q = p^t$ mit einer Primzahl p. Dann gilt*

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

Z.B. $|E(\mathbf{F}_{23})| = 27$ und $27 - 24 = 3 < 2\sqrt{23} \approx 9.59$.

Im Falle $n = 3$ liefert Reduktionstheorie:

$$E(\mathbf{K})_{\text{tors}} \simeq \begin{cases} \mathbf{Z}/m\mathbf{Z} & : \ 1 \leq m \leq 14, 16, 18, 20, 22, 24, \\ & \quad 26, 28, 32, 36, 48, 72, 96, 144 \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mu\mathbf{Z} & : \ 1 \leq \mu \leq 9, 12, 18, 24, 36 \\ \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\nu\mathbf{Z} & : \ \nu = 1, 2, 4, 8, 16 \\ \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/2\mu\mathbf{Z} & : \ \mu = 2, 3, 4, 6, 9, 12, 18 \\ \mathbf{Z}/6\mathbf{Z} \oplus \mathbf{Z}/2\mu\mathbf{Z} & : \ \mu = 3, 4, 6, 8, 12 \\ \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/\nu\mathbf{Z} & : \ \nu = 4, 6 \\ \mathbf{Z}/12\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}. \end{cases}$$

2. Parametrisierung mit der Ganzheit der j-Invariante liefert Bedingungen für die Koeffizienten der Kurve.

Es reicht nur für
$\mathbf{Z}/m\mathbf{Z}, 2 \leq m \leq 13$,
$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mu\mathbf{Z}, \mu = 2, 4, 6, 8$,
$\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$ und
$\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$
eine Parametrisierung zu finden.

Beispiel: $\mathbf{Z}/5\mathbf{Z}$. Sei $\mathbf{p}$ eine endliche Stelle von $\mathbf{K}$ und $\alpha \in \mathbf{K}^*$.

$$E : y^2 + (1-\alpha)xy - \alpha y = x^3 - \alpha x^2$$

$$j = \frac{((\alpha^2 - 11\alpha - 1)^2 + 5\alpha(2(\alpha^2 - 11\alpha - 1) + \alpha))^3}{\alpha^5(\alpha^2 - 11\alpha - 1)}$$

Bedingungen:

$\alpha \in \mathbf{U_K}$
$0 \leq v_{\mathbf{p}}(\alpha^2 - 11\alpha - 1) \leq 3v_{\mathbf{p}}(5)$
$v_{\mathbf{p}}(\alpha - 1) = 0$, falls $\mathbf{p}|11$.

3. Übergang zur Systeme von Normgleichungen. Die Bedingungen für die Bewertungen können als Systeme von Normgleichungen ausgedrückt werden.

Beispiel 1: $\mathbf{Z}/5\mathbf{Z}$.

$$\begin{aligned} N(\alpha) &= \pm 1 \\ N(\alpha^2 - 11\alpha - 1) &= \pm 5^m, 0 \leq m \leq 9. \end{aligned}$$

Beispiel 2: $\mathbf{Z}/7\mathbf{Z}$.

$$\begin{aligned} N(\alpha) &= \pm 1 \\ N(\alpha - 1) &= \pm 1 \\ N(\alpha^3 - 8\alpha^2 + 5\alpha + 1) &= \pm 7^m,\ 0 \leq m \leq 6. \end{aligned}$$

4. Lösung der Normgleichungssysteme. Der Körper K ist nicht spezifiziert, nur sein Grad!

Schlüsselidee: betrachte die Konjugierten von α als Unbekannten, $X = \alpha^{(1)}, Y = \alpha^{(2)}, Z = \alpha^{(3)}$ und löse das Gleichungssystem in ganzen kubischen Zahlen.

Beispiel 1: $\mathbf{Z}/5\mathbf{Z}$.

$$\begin{aligned} XYZ &= \pm 1 \\ (X^2 - 11X - 1)(Y^2 - 11Y - 1)(Z^2 - 11Z - 1) &= \pm 5^m, \quad 0 \le m \le 9. \end{aligned}$$

Beispiel 2: $\mathbf{Z}/7\mathbf{Z}$.

$$\begin{aligned} XYZ &= \pm 1 \\ (X-1)(Y-1)(Z-1) &= \pm 1 \\ (X^3 - 8X^2 + 5X + 1)(Y^3 - 8Y^2 + 5Y + 1)(Z^3 - 8Z^2 + 5Z + 1) &= \pm 7^m, \\ & \quad 0 \le m \le 6. \end{aligned}$$

Diese Gleichungssysteme werden mit der Hilfe von umfassende Gröbner-Basen und Eliminationstheorie gelöst. Man bekommt

- parametrisierte Familien, oder
- endlich viele, oder
- keine

kubische Polynome, welche Nullstellen $\mathbf{K}$ und $E(\mathbf{K})$ erzeugen. Als Parameter treten auch die Fibonacci und Lucas Zahlen auf.

5. Abschluß. Kann eine Gruppe von Liste 2. nicht auftreten, dann können seine Obergruppen auch nicht auftreten.

Im endlichen Fall können die tatsächliche Torsionsstrukturen bestimmt werden.

Satz 5. *Die Torsionsgruppen elliptischer Kurven mit ganzer j-Invariante über einem kubischen Zahlkörper sind isomorph mit*

$$\begin{array}{ll} \mathbf{Z}/m\mathbf{Z} & : \ 1 \leq m \leq 10, m = 14 \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2m\mathbf{Z} & : \ m = 1, 2, 3. \end{array}$$

Es existieren unendlich viele Kurven nur mit $|E(\mathbf{K})_{\text{tors}}| \leq 5$.

Ist $\mathbf{K}$ *zyklisch, dann existieren unendlich viele Kurven nur mit* $|E(\mathbf{K})_{\text{tors}}| \leq 4$.

4. Basis für die MW-Gruppe

In seiner Diplomarbeit studierte J. Gebel den Manin-Algorithmus und implementierte den in SIMATH.

Er hat eine Basis für alle Mordellsche Kurven $y^2 = x^3 + k$ mit $|k| \leq 10000$ bis auf der Ausnahme $k = 7823$ bestimmt. Er erweiterte seine Rechnungen bis zum $|k| \leq 100.000$ unter der Annahme der Birch-Swinnerton Dyer Vermutung - d.h. der analytischer Rang einer elliptirscher Kurve ist gleich seines geometrischen Rang.

Herr Gebel bewies, daß der Rang der Kurve $y^2 = x^3 + 7823$ ist Eins und die Torsion ist trivial, er konnte aber einen Erzeugender der MW-Gruppe nicht finden.

Den Erzeugender hat M. Stoll (2002) mittels 4-Abstieg bestimmt.

"I proudly present the generator of the Mordell-Weil group of $y^2 = x^3 + 7823$:

$$\begin{aligned} x &= 22635821433214215021002092335177 77 \\ &\quad / \quad 11981673410095561^2 \\ y &= -1863981525846233056248375514855967700281447766557 56 \\ &\quad / \quad 11981673410095561^3 \end{aligned}$$

This point has canonical height 77.617773768638... as expected."

5. Berechnung S-ganzen Punkte

S eine enliche Menge rationalen Primzahlen,

$\mathbf{Z}_S = \{r \in \mathbf{Q} : |r|_p \leq 1, p \notin S\}$,

$\mathbf{Z}_S = \mathbf{Z}$ wenn $S = \emptyset$,

$E(\mathbf{Z}_S) = E(\mathbf{Q}) \cap \mathbf{Z}_S^2$.

Satz 6 (L.J. Mordell, K. Mahler). $E(\mathbf{Z}_S)$ *ist endlich.*

Satz 7 (A. Baker, 1968). $E(\mathbf{Z})$ *ist effektiv berechenbar.*

Die Methoden von Mordell, Siegel und Baker liefern Algorithmen für die Bestimmung sämtlicher (S-)ganzen Punkte. Sie sind von *algebraischer Zahlentheoretischen* Natur.

Auf die Ochoa Kurve:

$$y^2 = x^3 - 440067x + 106074110$$

scheitern die algebraische Zahlentheoretische Methoden.

S. Lang (1964) schlägte eine andere Vorgehensweise vor, welche die Gruppenstruktur von $E(\mathbf{Q})$ ausnutzt.

D. Zagier (1987) dachte die Idee von Lang weiter.

R. Stroeker und N. Tzanakis, J. Gebel, A. P. und H.G. Zimmer, N. Smart (1994) haben für $E(\mathbf{Z})$ den Algorithmus vollständig beschrieben.

R. Stroeker und B.M.M. de Weger (1994) haben sämtliche ganze Punkte auf der Ochoa Kurve bestimmt.

A. P., H.G. Zimmer, J. Gebel und E. Herrmann, (1999): Verallgemeinerung für $E(\mathbf{Z}_S)$.

Ausflug während der Tagung in Durham, August, 2000.

Weitere Verallgemeinerungen:

- $E(\mathbf{Z_K})$ N. Smart and N. Stephens (1997)

- $E : y^2 = ax^4 + bx^3 + cx^2 + dx + e,\ a, \ldots, e \in \mathbf{Z},\ (x, y) \in \mathbf{Z}^2$ N. Tzanakis (1996)

- $E : y^2 = ax^4 + bx^3 + cx^2 + dx + e,\ a, \ldots, e \in \mathbf{Z},\ (x, y) \in \mathbf{Z}_S^2$ E. Herrmann (1999)

- $E : f(x, y) = 0,\ f(x, y) \in \mathbf{Z}[x, y]$ deg $f = 3$ R. Stroeker and B.M.M. de Weger (2001)

- $E(\mathbf{Z}_{\mathbf{K},S})$ und für Kurven vom Geschlecht Eins: E. Herrmann, A. P, und H.G. Zimmer.

5.1. Höhen

Seien $a_1, a_2, a_3, a_4, a_6 \in \mathbf{Z}$ und

$$E(\mathbf{Q}) = \{(x, y) \in \mathbf{Q}^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$$

Für $P \in E(\mathbf{Q})$ gibt es zwei Darstellungen:

- $P = (x, y) = \left(\frac{\xi}{\zeta^2}, \frac{\eta}{\zeta^3}\right)$ mit $\gcd(\xi, \zeta) = \gcd(\eta, \zeta) = 1$ und
- $P = n_1P_1 + \ldots n_rP_r + T$, wobei $P_1, \ldots, P_r$ eine Basis der MW-Gruppe von $E(\mathbf{Q})$; $n_1, \ldots, n_r \in \mathbf{Z}$ und T einen Torsionspunkt ist.

- Naive Höhe: $h(P) = \frac{1}{2} \log \max\{|\xi|, \eta^2\}$
- Néron-Tate Höhe: $\widehat{h}(P) = \lim_{n\to\infty} \frac{h(nP)}{n^2}$
- MW Höhe: $N(P) = \max\{|n_1|, \ldots, |n_r|\}$.

Intermezo

Die erste gemeinsame Resultat

Seien: $\mathbf{K}$ ein algebraischer Zahlkörper

$r_1, \ldots, r_k \in \mathbf{Z}, r_k \neq 0$

$G_0, \ldots, G_{k-1} \in E(\mathbf{K})$ unabhängig und

$$G_{n+k} = r_1 G_{n+k-1} + \ldots + r_k G_n, n \geq 0$$

$\{G_n\}_{n=0}^{\infty}$ lineare rekurzive Folge auf $E(\mathbf{K})$.

$\alpha_1, \ldots, \alpha_t$ die Wurzeln von $x^k - r_1 x^{k-1} - \ldots - r_k$.

Satz 8 (Pethő und Zimmer, 1990). *Wenn* $|\alpha_1| > |\alpha_2| \geq |\alpha_t|$, *dann gilt*

$$\hat{h}(G_n) = d|\alpha_1|^{2n}(1 + o(1)),$$

für alle $n > n_0$ *mit* $d > 0$.

Beispiel: Seien $E(\mathbf{Q}) : y^2 = x^3 - 388800, G_0 = (76, 224), G_1(124, 1232)$, $k = 2, r_1 = r_2 = 1$, dann sind G_0, G_1 über $\mathbf{Q}$ linear unabhängig, man bekommt eine "Fibonacci Folge" auf $E(\mathbf{K})$ und

$$\hat{h}(G_n) \approx 2.063 \left(\frac{3 + \sqrt{5}}{2}\right)^n - 1.096(-1)^n + e^{-n}.$$

Fortsetzung, 5.1 Höhen

$\widehat{h}(P)$ ist eine positive semidefinite Form auf $E(\mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{R}$.

Sei λ die kleinste Eigenwert der Matrix $(\widehat{h}(P_i, P_j))_{1 \leq i,j \leq r}$.

Satz 9 (Zimmer, 1978). *Es gibt positive Konstanten* c_1, c_2 *mit*

$$c_1 \leq \widehat{h}(P) - h(P) \leq c_2.$$

Einfache lineare Algebra impliziert

$$N(P) \leq \sqrt{\frac{\widehat{h}(P)}{\lambda}} \leq \sqrt{\frac{h(P) + c_2}{\lambda}}.$$

5.2 Obere Abschätzung für $N(P)$

Es gibt zwei Möglichkeiten:

a.) Durch untere Abschätzungen für Linearformen in elliptischen Logarithmen, S. David (1995) oder G. Rémond und F. Urfels (1996)

b.) Anwendung der Methode von A. Baker

Satz 10 (L. Hajdu und T. Herendi, 1998). *Seien* $a, b \in \mathbf{Z}$ *mit* $\Delta_0 = 4a^3 + 27b^2 \neq 0$, $|S| = s$, $Q = \max\{p \in S : p \neq \infty\}$. *Sei* $P \in E(\mathbf{Z}_S)$, *where* $E : y^2 = x^3 + ax + b$. *Dann gilt*

$$h(P) \leq b_2(s) Q^{24} (\log^* Q)^{4s-2} |\Delta_0|^2 (\log |\Delta_0|)^{12},$$

wobei $b_2(s)$ *hängt nur von* s *ab.*

Verallgemeinerung für beliebige $\mathbf{K}$: Hajdu, Herendi, Herrmann und Pethő (200?) durch Anwendung Ideen von Y. Bugeaud (1997).

5.3 Obere Abschätzung für Linearformen in elliptischen Logarithmen

Komplexe und p-adische Funktionentheorie.

Für jede $P = (x, y) \in E(\mathbf{C})$ gibt es ein $u \in \mathbf{C}$ mit

$$(x, y) = (\wp(u), \wp'(u)),$$

wobei $\wp$ die zu $E(\mathbf{C})$ gehörige Weierstraße $\wp$-Funktion bezeichnet.

Sei Λ der Periodengitter von $\wp$. Dann ist die Umkehrfunktion $\tilde{\psi}(P)$ von $\wp$ auf $\mathbf{C}/\Lambda$ eindeutig und es gilt

$$\tilde{\psi}(P + Q) = \tilde{\psi}(P) + \tilde{\psi}(Q), P, Q \in E(\mathbf{C}).$$

Sei $\Lambda = \omega_1\mathbf{Z} + \omega_2\mathbf{Z}, \omega_1 \in \mathbf{R}, \omega_2 \in i\mathbf{R}$ und setze $\psi(P) = \tilde{\psi}(P)/\omega_1$.

Die p-adische elliptische Logarithmen $\psi_p(P), p \in S$ werden durch Verwendung formalen Gruppen definiert.

Schließlich erreicht man den Satz

Satz 11. *Es sei $P \in \mathbf{Z}_S$ mit $h(P)$ groß genug. Dann existiert ein $\mathbf{p} \in \mathbf{S}$ so daß*

$$\left| \sum_{i=1}^{r} n_i \psi_p(P_i) + n_{r+1} \right|_{\mathbf{p}} \leq c_3 \exp\{-(\lambda/s)N^2(P) + c_2/s\},$$

wobei $n_{r+1} \in \mathbf{Z}$, falls $\mathbf{p} = \infty$ und $n_{r+1} = 0$ sonst.

5.4 Reduktion der oberen Schranke

Dazu benutzt man eine Methode vom B.M.M. de Weger

Die Mordellsche Gleichung $y^2 = x^3 + k$

Table 3: Summary $|k| \leq 10\,000$

number of integer points	number of curves of rank					total number of curves
	0	1	2	3	4	
0	6459	6884	997	22		14362
1	24	3				27
2	45	2503	1462	108	1	4119
3		4				4
4		99	535	126		760
5	4	3				7
6		24	277	103	6	410
7		2				2
8		12	94	41	1	148
9		2				2
10		8	28	29	1	66
12		1	17	16	2	36
14		1	6	10	1	18
16			5	9		14
18			3	5	1	9
20				4	1	5
22			1	3	2	6
24				1	1	2
26			1			1
28					1	1
32				1		1
$\sum$	6532	9546	3426	478	18	20000

Irvin Kaplanski (Salute to Euler and Dixson on the occasion of Hy's 65th birthday) nannte diese Arbeit "remarkable".

Zusammenfassung

In unserer Zusammenarbeit sind

1 Tagung und Proceedins

15 wissenschaftliche Publikationen

3 Diplomarbeiten

4 Dissertationen

entstanden.

Danke Günter !