Prof. Dr. Stefan Wewers
Institut für Reine Mathematik

Seminar im SS 15

Ausgewählte Themen aus Algebra und Zahlentheorie

Stand: 12.2.2015

Wir werden eine Reihe von Themen aus dem Bereich Algebra und Zahlentheorie behandeln. Jedes Thema wird von einer Gruppe von 2-3 Studierenden bearbeitet. Es wird eine gemeinsame Ausarbeitung angefertigt, und jedes Mitglied der Gruppe hält einen eigenen Vortrag.

Mögliche Themen sind:

- Punktezählen und Zeta-Funktionen
- Faktorisieren mit elliptischen Kurven
- Quadratische Formen und Idealklassen
- Gitter und der LLL-Algorithmus
- Gröbner-Basen und Eliminationstheorie

Im Folgenden beschreibe ich zu jedem Thema den mathematischen Kontext und die möglichen Ziele der Vorträge. Die genaue Ausgestaltung der Vorträge wird dem Vorwissen und der Anzahl der Vortragenden angepasst.

1 Punktezählen und Zeta-Funktionen

Wir fixieren einen endlichen Körper $\mathbb{F}_q$ mit q Elementen (wobei q Potenz einer Primzahl p ist). Für jedes $n \in \mathbb{N}$ erhalten wir eine eindeutige Erweiterung $\mathbb{F}_{q^n}/\mathbb{F}_q$ vom Grad n. Dann ist $\mathbb{F}_{q^n}$ der Körper mit q^n Elementen.

Seien $F_1, \ldots, F_m \in \mathbb{F}_q[x_1, \ldots, x_r]$ Polynome in den Unbekannten $x_1, \ldots, x_r$ und mit Koeffizienten in $\mathbb{F}_q$. Wir bezeichnen mit $X(\mathbb{F}_{q^n}) \subset \mathbb{F}_{q^n}^r$ die Lösungsmenge des Gleichungssystems

$$F_1(x) = \ldots = F_m(x) = 0,$$

wobei $x = (x_1, \ldots, x_r) \in \mathbb{F}_{q^n}^r$. In der Sprache der algebraischen Geometrie heißt X eine *affine Varietät* über dem Körper $\mathbb{F}_q$, und $X(\mathbb{F}_{q^n})$ ist die Menge der *$\mathbb{F}_{q^n}$-rationalen Punkte*.

Wir interessieren uns für die Zahlenfolge

$$n \mapsto N_n := |X(\mathbb{F}_{q^n})|.$$

Ein in der Mathematik häufig angewendeter Trick zum Analysieren von Zahlenfolgen besteht darin, eine *erzeugende Funktion* zu definieren, d.h. die Folge als eine formale Potenzreihe zu schreiben. In unserer speziellen Situation hat es sich gezeigt, dass die folgende Variante dieses Tricks am Besten funktioniert.

Definition 1.1 Die *Zeta-Funktion* von X ist die formale Potenzreihe

$$Z(X,T) := \exp\Big(\sum_{n\geq 1} N_n \cdot \frac{T^n}{n}\Big) \in \mathbb{Q}[[T]].$$

Die ersten vier Terme von $Z(X,T)$ sehen so aus:

$$Z(X,T) = 1 + N_1 T + \frac{N_1^2 + N_2}{2} T^2 + \frac{N_1^3 + 3N_1N_2 + 2N_3}{6} T^3 + \dots$$

Aus der Definition folgt, dass die *logarithmische Ableitung* von $Z(X,T)$ gerade die erzeugende Funktion der Folge (N_n) ist:

$$d\log Z(X,T) = \frac{Z(X,T)'}{Z(X,T)} = \sum_{n\geq 1} N_n \cdot T^n.$$

Die Zeta-Funktion $Z(X,T)$ erfüllt eine Reihe von bemerkenswerten Eigenschaften, die sogenannten *Weil-Vermutungen*. In dem Spezialfall einer *algebraischen Kurve* X wurden diese Vermutungen 1924 von Emil Artin aufgestellt und für elliptische Kurven 1934 von Hasse und für allgemeine Kurven 1948 von André Weil bewiesen. Die allgemeine Form der Weil-Vermutungen wurden 1949 von Weil formuliert und avancierte schnell zum heiligen Gral der algebraischen Geometrie. In den 60er und 70er Jahren wurden die Weil-Vermutungen schließlich bewiesen, hauptsächlich von Dwork, Grothendieck und Deligne. Die für diesen Zweck entwickelten Theorien (wie zum Beispiel die *étale Kohomologie*) füllen Tausende von Seiten.

Wir verfolgen im Seminar das vergleichsweise bescheidene Ziel, die Weil-Vermutung für mindestens ein (nichttriviales) Beispiel zu beweisen. Dazu beschränken wir uns zuallererst auf den Fall einer *elliptischen Kurve*

$$E : y^2 = x^3 + ax + b$$

über $\mathbb{F}_q$ (d.h. $a, b \in \mathbb{F}_q$ mit $\Delta = -27a^3 - 4b^2 \neq 0$).[1] Dabei betrachten wir E als eine ebene, *projektive* Kurve, d.h. E besitzt neben den Punkten (x,y) mit $y^2 = x^3 + ax + b$ auch einen unendlich fernen Punkt $\mathcal{O}$. Sei $Z(E,T)$ die Zeta-Funktion von E.

[1] Wir nehmen hier zusätzlich an, dass $p \neq 2, 3$ gilt.

Satz 1.2 (Hasse, 1934) (i) *Die Zeta-Funktion von E ist eine rationale Funktion der Form*

$$Z(E,T) = \frac{1 - a_q T + qT^2}{(1-T)(1-qT)},$$

wobei

$$a_q := q + 1 - |E(\mathbb{F}_q)|.$$

(ii) *Es gilt die Abschätzung*

$$|a_q| \leq 2\sqrt{q}.$$

Auch der Beweis dieses Satzes würde uns etwas zu weit führen. Ziel der Vortragenden sollte sein, ein sanfte Einführung in das Themengebiet zu geben und dann die Zeta-Funktion von *einer* speziellen elliptischen Kurve auszurechnen. Es bietet sich das Beispiel der Kubik

$$X : x^3 + y^3 = 1$$

über $\mathbb{F}_p$ an. Hier gilt (siehe [6], Chapter IV, §2):

Satz 1.3 (Gauss) *Sei $M_p := |X(\mathbb{F}_p)|$ die Anzahl der $\mathbb{F}_p$-rationalen Punkte der (projektiven!) Kurve X.*

(a) Falls $p \not\equiv 1 \pmod 3$ so gilt $M_p = p + 1$.

(b) Falls $p \equiv 1 \pmod 3$, so gibt es ganze Zahlen $A, B \in \mathbb{Z}$ so dass

$$4p = A^2 + 27B^2.$$

Die Zahlen A, B sind eindeutig bis auf ihr Vorzeichen, und wenn wir das Vorzeichen von A so wählen, dass $A \equiv 1 \pmod 3$, dann gilt

$$M_p = p + 1 + A.$$

Einen Beweis findet man in [6], Chapter IV, §2. Man beachte, dass dieser Satz die Abschätzung

$$|p + 1 - M_p| \leq 2\sqrt{p}$$

aus dem Satz von Hasse bestätigt. Einen Beweis des Satzes von Hasse für den Fall der hier betrachteten Kurve X siehe [4], Chapter 11, §3. Allerdings wird dort ein viel allgemeinerer Satz bewiesen, mit entsprechend großem Aufwand. Alternativ könnten die Vortragenden die elliptische Kurve

$$E_n : y^2 = x^3 - n^2 x$$

über $\mathbb{F}_p$ betrachten (mit $n \in \mathbb{N}$ und $p \nmid 2n$). Der Satz von Hasse wird in diesem Fall recht übersichtlich in [5], Chaper 2, §1-2, bewiesen.

Literatur: [6], Chapter IV, §1-2, [4], Chapters 8,10,11, [5], Chapter II, §1-2.

2 Faktorisieren mit elliptischen Kurven

Der Fundamentalsatz der Arithmetik besagt, dass sich jede natürliche Zahl $m > 1$ auf eindeutige Weise als ein Produkt von Primzahlen schreiben lässt:

$$m = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r},$$

mit Primzahlen $p_1 < p_2 < \ldots < p_r$. Es schließt sich sofort die folgende Frage an: wie kann man die Primfaktorzerlegung von m effizient berechnen, wenn m sehr groß ist? Dieses Problem heisst das *Faktorisierungsproblem*. Es hat eine ernorme praktische Relevanz, da viele kryptographische Verfahren auf der Annahme beruhen, dass das Faktorisierungsproblem in einem gewissen Sinne 'schwer' ist (siehe [3], Chapter 3).

Ein besonders interessantes Faktorisierungsverfahren wurde 1987 von Lenstra veröffentlicht. Bis dato ist es das beste Faktorisierungsverfahren für Zahlen m mit höchstens mittelgroßen Primfaktoren (etwa $p < 10^{30}$). Die Grundidee baut auf einem Algorithmus von Pollard auf; Lenstras Innovation bestand darin, die multiplikative Gruppe $\mathbb{F}_p^\times$ (wobei p ein unbekannter Primfaktor von m ist) durch die Punktgruppe vieler zufällig gewählter elliptischer Kurven E über $\mathbb{F}_p$ zu ersetzen.

Die Funktionsweise des Algorithmus ist sehr ausführlich in [6], Chapter IV, §4, beschrieben. Eine Alternative ist [3], §5.6.

3 Quadratische Formen und Idealklassen

Unter einer *(binären) quadratischen Form* verstehen wir ein Polynom

$$f(x, y) = ax^2 + bxy + cy^2$$

mit ganzzahligen Koeffizienten $a, b, c \in \mathbb{Z}$. Eine Grundfrage der Zahlentheorie ist dann, für eine gegebene quadratischen Form f und eine ganze Zahl n die Lösungen der Gleichung

$$f(x, y) = n, \qquad x, y \in \mathbb{Z},$$

zubestimmen. Häufig ist es auch von Interesse, die Lösungsmenge in Abhängigkeit von n und den Koeffizienten a, b, c zu untersuchen.

Zwei quadratische Formen f, g heißen *äquivalent*, wenn g aus f durch eine Substitution der Form

$$\begin{aligned} x' &= \alpha x + \beta y, \\ y' &= \gamma x + \delta y, \end{aligned}$$

mit $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ und $\alpha\delta - \gamma\beta = 1$, hervorgeht. Es ist klar, dass dies eine Äquivalenzrealation auf der Menge aller quadratischen Formen ist, und dass die Lösbarkeit der Gleichung $f(x, y) = n$ nur von der Äquivalenzklasse von f abhängt. Es stellt sich daher das Problem, die Menge aller Äquivalenzklassen zu bestimmen.

Die ganze Zahl

$$D := b^2 - 4ac$$

heißt die *Diskriminante* der quadratischen Form f. Man prüft leicht nach, dass D nur von der Äquivalenzklasse von f abhängt und die Kongruenz $D \equiv 0, 1 \pmod 4$ erfüllt. Umgekehrt gibt es zu jedem $D \neq 0$ mit $D \equiv 0, 1 \pmod 4$ mindestens eine quadratische Form mit Diskriminante D. Das erste Hauptergebnis der Theorie ist nun:

Satz 3.1 *Sei $D \in \mathbb{Z}$, D kein Quadrat. Dann gibt es nur endlich viele Äquivalenzklassen binärer quadratischer Formen mit Diskriminante D.*

Der Beweis dieses Satzes ist vollkommen konstruktiv und beruht darauf, dass jede quadratische Form äquivalent ist zu einer im Wesentlichen eindeutigen *reduzierten* Form. Die Menge aller reduzierten Formen zu fester Diskriminante lässt sich (zumindest für kleine Werte von $|D|$) leicht aufzählen.

Hauptziel der Vorträge sollte sein, den Zusammenhang zwischen Äquivalenzklassen binärer quadratischer Formen und Idealklassen quadratischer Zahlkörper zu erläutern.

Literatur: [9], II, §8+§10, [8], §19.

4 Gitter und der LLL-Algorithmus

Unter einem *Gitter* verstehen wir eine diskrete Untergruppe $L \subset V$, wobei V ein euklidischer Vektorraum ist. Man kann zeigen, dass ein Gitter $L \subset V$ ein freier $\mathbb{Z}$-Modul vom Rang $n \leq \dim V$ ist, erzeugt von $\mathbb{R}$-linear unabhängigen Vektoren $v_1, \ldots, v_n$,

$$L = \langle v_1, \ldots, v_n \rangle_{\mathbb{Z}} = \{ \sum_i a_i v_i \mid a_i \in \mathbb{Z} \}.$$

Wir nennen $(v_1, \ldots, v_n)$ eine *Basis* von L und n die *Dimension*. Ohne Einschränkung dürfen wir annehmen, dass $V = \mathbb{R}^m$ der euklidische Standardraum ist.

Gitter spielen in vielen Gebieten der Mathematik eine Rolle. Ein extrem wichtiges Problem ist das *Problem des kürzesten Vektors* (SVP): gegeben ein Gitter L mit Basis $(v_1, \ldots, v_n)$, finde einen kürzesten Vektor (ungleich Null),

$$v_0 \in L, \quad \|v_0\| = \min\{\|v\| \mid v \in L, v \neq 0\}.$$

Varianten sind das *Problem des nächsten Vektors* (SVP) und das *Problem der kürzesten Basis* (SBP). Alle diese Probleme sind (unter gewissen Zusatzannahmen) NP-vollständig, d.h. ein Algorithmus, der das Problem löst, hat immer eine Laufzeit, die im schlechtesten Fall exponentiell von der Eingabegröße (und insbesondere von der Dimension von L) abhängt. Siehe z.B. [3], §6.5.

Der LLL-Algorithmus[2] löst eine schwächere Version des Problems der kürzesten Basis in polynomialer Zeit. In Dimension $n = 2$ reduziert sich LLL zu der klassischen Gitterreduktion nach Gauss (die implizit auch im Thema 3 ein Rolle spielt), siehe [3], §612.1. Der allgemeine Fall wird in [3], §6.12.2 beschrieben.

Eine interessante Anwendung des LLL-Algorithmus ist das Finden von *Ganzheitsrelationen*. Angenommen, wir möchten eine bestimmte algebraische Zahl $\theta \in \mathbb{C}$ exakt bestimmen, kennen aber nur eine numerische Approximation θ_0 von θ (d.h. $|\theta - \theta_0|$ ist sehr klein). Konkret muss man für die *exakte* Bestimmung von θ ein ganzzahliges Polynom

$$f = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$$

mit $f(\theta) = 0$ finden. Wenn $|\theta - \theta_0|$ hinreichend klein ist, so ist auch

$$|f(\theta_0)| = |a_0 + a_1\theta_0 + \ldots + a_n\theta_0^n|$$

klein. Der gesuchte Vektor $(a_0, \ldots, a_n) \in \mathbb{Z}^n$ ist eine sogenannte *approximative Ganzheitsrelation* zwischen den komplexen Zahlen $1, \theta_0, \ldots, \theta_0^n$. Mithilfe des LLL-Algorithmus ist es möglich, solche Ganzheitsrelationen unter gewissen Annahmen effektiv zu finden.

Für diese und weitere Anwendungen des LLL-Algorithmus in der Zahlentheorie siehe [7].

5 Gröbner-Basen und Eliminationstheorie

Ein Grundproblem der Algebra ist das Lösen algebraischer Gleichungen. Unter einer algebraischen Gleichung verstehen wir hier ein System von Polynomgleichungen

$$f_1(x) = \ldots = f_m(x) = 0, \tag{1}$$

wobei $f_i \in k[x_1, \ldots, x_n]$ Polynome über einem Körper k in n Unbekannten $x_1, \ldots, x_n$ sind. Ist K/k eine Körpererweiterung, so ist jedes Tupel $(a_1, \ldots, a_n) \in K^n$ mit $f_i(a) = 0$ für alle i eine *Lösung* von (1) in K.

In der Linearen Algebra lernt man, *lineare Gleichungssysteme* zu lösen, also den Spezialfall eines algebraischen Gleichungsystems, in dem die Polynome f_i alle den Grad 1 haben. Der fundamentale Lösungsalgorithmus ist das *Gausssche Eliminationsverfahren*: jedes lineare Gleichungsystem

$$\begin{aligned} a_{1,1}x_1 + \ldots + a_{1,n}x_n &= b_1, \\ \vdots \qquad\qquad & \quad \vdots \\ a_{m,1}x_1 + \ldots + a_{m,n}x_n &= b_m, \end{aligned}$$

kann man durch eine endliche Folge elementarer Zeilenumformungen in eine gewisse *Stufenform* bringen, an der dann die Lösungsmenge durch sukzessive

[2] benannt nach seinen Erfindern, A. Lenstra, H. Lenstra und L. Lovász

Elimination der Variablen abgelesen werden kann. Die *Eliminationstheorie* ist in gewissem Sinne eine Verallgemeinerung dieses Verfahrens auf nichtlineare Polynomgleichungen. Genauer liefert diese Theorie ein konstruktives Verfahren, mit dem man das Lösen von allgemeinen Gleichungssystemen auf das Lösen von einzelnen Polynomgleichungen in *einer* Variablen reduzieren kann.[3]

Die Grundidee ist die folgende. Die Lösungsmenge des Gleichungssystems (1) hängt offenbar nur von dem von den Polynomen $f_1, \ldots, f_m$ erzeugten Ideal ab,

$$I := (f_1, \ldots, f_m) \lhd k[x_1, \ldots, x_n].$$

Für $k = 0, \ldots, n-1$ definieren wir das *kte Eliminationsideal* $I_k \lhd k[x_{1+k}, \ldots, x_n]$ als

$$I_k := I \cap k[x_{1+k}, \ldots, x_n].$$

Ist $g_1, \ldots, g_N \in k[x_{1+k}, \ldots, x_n]$ ein Erzeugendensystem von I_k, so liefert das Gleichungssystem

$$g_1 = \ldots = g_N = 0 \tag{2}$$

notwendige Bedingungen für die Lösungen von (1), die nur von den Werten der Variablen $x_{k+1}, \ldots, x_n$ abhängen. Eine Lösung $(a_{k+1}, \ldots, a_n) \in k^{n-k}$ von (2) heißt eine *k-partielle Lösung* von (1). Wir bezeichnen mit $V_k \subset k^{n-k}$ die Lösungsmenge von I_k. Das allgemeine Eliminationsverfahren besteht nun darin, sukzessive für $k = 0, \ldots, n$

- Erzeuger des Eliminationsideals I_k und
- die Lösungsmenge V_k zu bestimmen.

Um dieses Programm in die Tat umzusetzen, benötigt man die Theorie der *Gröbner-Basen* und insbesondere den *Buchberger-Algorithmus*. Mithilfe dieser Theorie ist es u.A. möglich, explizit ein Erzeugendensystem $g_1, \ldots, g_N$ von I und Indizes $n = N_0 \geq \ldots \geq N_n$ zu bestimmen, so dass

$$I_k = (g_1, \ldots, g_{N_k}),$$

für $k = 0, \ldots, n$. Ist nun $k > 0$ und $(a_{k+1}, \ldots, a_n)$ eine vorgegebene k-partielle Lösung, so erhält man alle $(k-1)$-partiellen Lösungen der Form $(a_k, \ldots, a_n)$ durch das Lösen des Gleichungssystems

$$g_i(x_k, a_{k+1}, \ldots, a_n) = 0, \qquad i = N_k + 1, \ldots, N_{k-1}. \tag{3}$$

Der Punkt ist, dass (3) ein System von Polynomgleichungen in nur einer Variablen ist.

Die Vortragenden sollten eine kurze Einführung in die Problematik geben (mit expliziten Beispielen) und anschließend die Theorie der Gröbner-Basen soweit entwickeln, dass man den hier erklärten Eliminationsalgorithmus erklären kann. Dieses Material wird in [2], Chapter 1, §1-3, und Chapter 2, §1, sehr schön zusammengefasst und in [1], Chapter 2,3, ausführlicher erklärt.

Literatur: [1], Chapter 2,3, [2], Chapter 1, §1-3, Chapter 2, §1.

[3] Man erhält im gewissen Sinne eine konstruktive Version des Nullstellensatzes.

References

[1] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Springer-Verlag, 2nd edition, 1997.

[2] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*. Springer-Verlag, 1998.

[3] J. Hoffstein, J. Pipher, and J.H. Silverman. *An Introduction to Mathematical Cryptography*. Springer-Verlag, 2008.

[4] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, 2nd edition, 1990.

[5] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Springer-Verlag, 2nd edition, 1993.

[6] J.H. Silverman and J. Tate. *Rational Points on Elliptic Curves*. Springer-Verlag, 1992.

[7] D. Simon. Selected applications of LLL in number theory. In Nguyen and Vallée, editors, *The LLL algorithm*, pages 265–282. Springer-Verlag, 2010.

[8] S. Müller-Stach und J. Piontkowski. *Elementare und algebraische Zahlentheorie*. Vieweg, 2006.

[9] D.B. Zagier. *Zetafunktionen und quadratische Körper*. Springer-Verlag, 1981.