Zur Berechnung ganzer Punkte auf Mordellkurven über globalen Körpern

Michael E. Pohst

Institut für Mathematik
Technische Universität Berlin

4. Februar, 2015

Mordells Gleichung

ist

$$y^2 = x^3 + \kappa$$

mit einer gegebenen Konstanten κ. Bereits in seinem bekannten Buch aus dem Jahr 1969 untersucht L. J. Mordell diese Gleichung auf die Gesamtheit ihrer Lösungen $x, y \in \mathbb{Z}$ für $\kappa \in \mathbb{Z}$.

Im Vortrag geht es hauptsächlich um Algorithmen zur Berechnung aller Lösungen über den ganzen rationalen Zahlen $R = \mathbb{Z}$ sowie über den **ganzen Zahlen** $R = \mathbb{F}_q[t]$ eines rationalen Funktionenkörpers $\mathbb{F}_q(t)$. Dabei ist der Konstantenkörper $\mathbb{F}_q$ stets endlich, etwa mit $q = p^\ell$ Elementen.

Mordells Beobachtung

Die **Diskriminante** eines normierten Polynoms ist als Produkt der Quadrate der Differenzen seiner Nullstellen definiert.
Mordell bemerkte, dass für jede Lösung (x, y) von $y^2 = x^3 + \kappa$ die Diskriminante des kubischen Polynoms

$$T^3 - 3xT - 2y$$

in der Variablen T die Gestalt

$$\Delta := -108\kappa$$

hat. (Deswegen setzen wir im folgenden voraus, dass die Charakteristik p von $R = \mathbb{F}_q[t]$ stets größer als 3 ist.)

Mordells Beobachtung

Also genügt es, alle normierten kubischen Polynome

$$g(T) = T^3 + aT^2 + bT + c \in R[T]$$

mit der Diskriminante Δ zu bestimmen.

Da die Diskriminanten von $g(T + \alpha)$ $(\alpha \in R)$, von $-g(-T)$ und von $g(T)$ übereinstimmen, suchen wir lediglich nach Vertretern der entsprechenden Äquivalenzklassen.

Reduzible Polynome $g(T)$

Hier besitzt g eine Nullstelle α im Grundring R. Ersetzen wir T durch $T + \alpha$ erhalten wir ein Polynom
$h(T) = T^3 + AT^2 + BT \in R[T]$ mit der gleichen Diskriminante Δ, und es gilt $\Delta = B^2(A^2 - 4B)$.

Die endlich vielen Lösungen der letzten Gleichung lassen sich einfach bestimmen, wenn $R = \mathbb{Z}$ oder $R = \mathbb{F}_q[t]$ ist.

Irreduzible Polynome $g(T)$

Eine Nullstelle ρ (im algebraischen Abschluss des Quotientenkörpers F von R) erzeugt eine kubische Erweiterung $E = F(\rho)$. Die Diskriminante $d(g)$ des Minimalpolynoms $g(T)$ von ρ heißt auch Diskriminante der **Gleichungsordnung** $R[\rho] = R1 + R\rho + R\rho^2$.

Jedes Element β aus E besitzt eine Darstellung $\beta = b_1 + b_2\rho + b_3\rho^2$ mit $b_i \in F$ $(1 \leq i \leq 3)$.

Irreduzible Polynome $g(T)$

Eine Nullstelle ρ (im algebraischen Abschluss des Quotientenkörpers F von R) erzeugt eine kubische Erweiterung $E = F(\rho)$. Die Diskriminante $d(g)$ des Minimalpolynoms $g(T)$ von ρ heißt auch Diskriminante der **Gleichungsordnung** $R[\rho] = R1 + R\rho + R\rho^2$.

Jedes Element β aus E besitzt eine Darstellung $\beta = b_1 + b_2\rho + b_3\rho^2$ mit $b_i \in F$ $(1 \leq i \leq 3)$.

Irreduzible Polynome $g(T)$

Im algebraischen Abschluss $\overline{E}$ zerfällt das Polynom $g(T)$ in Linearfaktoren: $g(T) = (T - \rho^{(1)})(T - \rho^{(2)})(T - \rho^{(3)})$, etwa mit $\rho = \rho^{(1)}$.

Nun ist leicht zu sehen, dass $d(g)$ mit dem Quadrat der Determinante der Matrix mit Einträgen

$$\rho^{(j)^{i-1}} \quad (1 \leq i, j \leq 3) \ .$$

übereinstimmt.

Irreduzible Polynome $g(T)$

Im algebraischen Abschluss $\overline{E}$ zerfällt das Polynom $g(T)$ in Linearfaktoren: $g(T) = (T - \rho^{(1)})(T - \rho^{(2)})(T - \rho^{(3)})$, etwa mit $\rho = \rho^{(1)}$.

Nun ist leicht zu sehen, dass $d(g)$ mit dem Quadrat der Determinante der Matrix mit Einträgen

$$\rho^{(j)^{i-1}} \quad (1 \leq i, j \leq 3) \ .$$

übereinstimmt.

Irreduzible Polynome $g(T)$

Entsprechend schreibt man auch

$$\beta^{(j)} = b_1 + b_2\rho^{(j)} + b_3{\rho^{(j)}}^2 \ .$$

für Elemente $\beta = b_1 + b_2\rho + b_3\rho^2$ aus E.

Die **Maximalordnung** o_E (Ring der ganzen Zahlen) von E besitzt eine R-Basis $\omega_1, \omega_2, \omega_3$. Analog zu oben wird die Diskriminante $d(\omega_1, \omega_2, \omega_3)$ dieser Basis definiert als das Quadrat der Determinante der Matrix mit den Einträgen

$$\omega_i^{(j)} \ (1 \leq i, j \leq 3) \ .$$

Irreduzible Polynome $g(T)$

Entsprechend schreibt man auch

$$\beta^{(j)} = b_1 + b_2\rho^{(j)} + b_3{\rho^{(j)}}^2 \ .$$

für Elemente $\beta = b_1 + b_2\rho + b_3\rho^2$ aus E.

Die **Maximalordnung** o_E (Ring der ganzen Zahlen) von E besitzt eine R-Basis $\omega_1, \omega_2, \omega_3$. Analog zu oben wird die Diskriminante $d(\omega_1, \omega_2, \omega_3)$ dieser Basis definiert als das Quadrat der Determinante der Matrix mit den Einträgen

$$\omega_i^{(j)} \ (1 \leq i, j \leq 3) \ .$$

Irreduzible Polynome $g(T)$

Man sieht wiederum leicht, dass sich die Diskriminanten von Basen von o_E nur durch Quadrate von invertierbaren Elementen von R unterscheiden.

Folglich lässt sich die Diskriminante d_E von E als $d(\omega_1, \omega_2, \omega_3)(R^\times)^2$ definieren.

Wir erhalten also $d(g) = d_E\lambda^2$ für ein $\lambda \in R$, das heißt

$$\Delta = d_E\lambda^2 \ .$$

Dies ergibt eine – im allgemeinen kurze – Liste von Kandidaten für d_E (und damit für E).

Zahlkörper

Im Zahlkörperfall lassen sich kubische Körper E mit beschränkter Diskriminante $|d_E|$ etwa mit Methoden aus der Geometrie der Zahlen berechnen. E wird danach von einem Element ρ erzeugt, bei dem die Koeffizienten seines Minimalpolynoms $m_\rho(T) = T^3 + r_1 T^2 + r_2 T + r_3 \in \mathbb{Z}[T]$ den Bedingungen

$$r_1 \in \{0, 1\},\ r_2 = (r_1^2 - S_2)/2 \text{ mit } |S_2| \leq \sqrt{2|d_E|/3},$$

genügen. Schranken für r_3 lassen sich aus der Ungleichung zwischen arithmetischem und geometrischem Mittel erhalten. Dies ergibt einen $O(|d_E|^{5/4})$ Algorithmus.

Zahlkörper

Mittels Reduktionstheorie kubischer Formen erhielten Belabas und Cohen ein $O(|d_E|)$ Verfahren. In seiner Doktorarbeit 1997 benutzte K. Wildanger Abschätzungen für den Index (statt für r_3) und entwickelte so einen $O(|d_E|^{3/4})$ Algorithmus. Damit konnte er den Bereich für die κ-Werte von weniger als 10^5 auf 10^7 erweitern.

Neue Verbesserungen seiner Ideen erlauben jetzt $|\kappa| < 10^{10}$. Mit den nachfolgend skizzierten klassenkörpertheoretischen Methoden sind wir zuversichtlich, dass wir bis zu 10^{15} kommen können.

Funktionenkörper

Eine Übertragung der geschilderten Ideen auf rationale Funktionenkörper $F := \mathbb{F}_q(t)$ erscheint naheliegend.

Hier sind die Schranken für die Koeffizienten von $m_\rho(T)$ allerdings Schranken für die Grade von Polynomen r_i. Falls also q nicht sehr klein ist, erfordert das Testen aller Kandidaten einen viel zu hohen Aufwand.

Indizes

Wir erinnern uns, dass alle gefundenen Körper E von der Form $F(\rho)$ sind. Wählt man ρ geeignet, besitzen die ganzen Zahlen o_E von E eine R-basis (Ganzheitsbasis) von der Gestalt

$$\omega_1, \omega_2 = \rho, \omega_3 = (\rho^2 + u\rho + v)/d$$

mit $u, v, d \in R$.

Entsprechend müssen wir dann alle Elemente $\alpha \in o_E$ berechnen, die die Bedingung

$$d_E \lambda^2 (R^\times)^2 = d_{R[\alpha]} (R^\times)^2 ,$$

erfüllen, da dann die Diskriminante des Minimalpolynoms von einem Element $\tilde{\alpha} \in \alpha(R^\times)^2$ mit Δ übereinstimmt.

Hierbei heißt λ **Index** von $R[\alpha]$ in o_E.

Indizes

Wir erinnern uns, dass alle gefundenen Körper E von der Form $F(\rho)$ sind. Wählt man ρ geeignet, besitzen die ganzen Zahlen o_E von E eine R-basis (Ganzheitsbasis) von der Gestalt

$$\omega_1, \omega_2 = \rho, \omega_3 = (\rho^2 + u\rho + v)/d$$

mit $u, v, d \in R$.

Entsprechend müssen wir dann alle Elemente $\alpha \in o_E$ berechnen, die die Bedingung

$$d_E \lambda^2 (R^\times)^2 \; = \; d_{R[\alpha]} (R^\times)^2 \;\; ,$$

erfüllen, da dann die Diskriminante des Minimalpolynoms von einem Element $\tilde{\alpha} \in \alpha(R^\times)^2$ mit Δ übereinstimmt.

Hierbei heißt λ **Index** von $R[\alpha]$ in o_E.

Das Verfahren für irreduzible Polynome

1. Berechne alle infrage kommenden Werte D für Diskriminanten kubischer Erweiterungen E von F, das heißt solche $D \in R$, für die Δ/D ein Quadrat I^2 ist. Speichere die Paare (D, I) in einer Liste L_1.
2. Für jedes Paar $(D, I) \in L_1$ berechne die kubischen Erweiterungen E von F mit Diskriminante D. Speichere die erhaltenen Tripel (D, I, E) in einer Liste L_2.
3. Im Ganzheitsring jedes Körpers E von einem Tripel aus L_2 berechne alle Elemente α mit Index I (!). Die Minimalpolynome $T^3 + AT^2 + BT + C$ dieser Elemente werden mit einer Tschirnhaus Transformation $T + A/3 \to T$ auf die Gestalt $T^3 + DT + E$ gebracht (!). Die zugehörigen Punkte (x, y) auf der Mordellkurve erhält man dann mittels $-3x = D$, $2y = \pm E$ (!).

Beispiel

Alle Punkte der Kurve $y^2 = x^3 + 1000000025$ sind

$$
\begin{aligned}
(x, \pm y) \quad \in \{ \quad & (-1000, 5) \\
& (-170, 31545) \\
& (1271, 55256) \\
& (2614, 137337) \\
& (90000002000, 2700000090000005) \ \}
\end{aligned}
$$