

Komplexe Multiplikation: von numerisch bis symbolisch

Andreas Enge
(INRIA Bordeaux–Sud-Ouest)

andreas.enge@math.u-bordeaux.fr

Die Theorie der komplexen Multiplikation vereint in bemerkenswerter Weise Analysis (Funktionentheorie, Riemannsche Flächen) und Algebra (Zahlentheorie, Klassenkörpertheorie). In der Praxis führt das dazu, daß sich algebraische, diskrete Objekte mit analytischen, numerischen Methoden berechnen lassen.

Anwendungen

Die Hauptanwendung der komplexen Multiplikation besteht darin, elliptische Kurven über einem endlichen Körper mit vorab bekannter Punktezahl zu konstruieren. Sei $D < 0$ eine quadratische Diskriminante und q eine Primzahlpotenz, so daß die Gleichung

$$4q = t^2 - v^2D \quad (1)$$

eine Lösung in ganzen Zahlen t, v mit $\text{ggT}(t, v) = 1$ besitzt. Dann gibt es eine elliptische Kurve über \mathbb{F}_q mit $N = q + 1 - t$ Punkten; wir werden im folgenden sehen, wie sich eine solche Kurve in Zeit $O(\tilde{|D|}) := O(|D| \log^{O(1)} |D|)$ bestimmen läßt.

Dies kann ausgenutzt werden, um für die Kryptographie geeignete Kurven zu berechnen. Mit den Fortschritten beim Zählen der Punkte auf zufälligen Kurven¹ wurde diese Anwendung zunächst obsolet, um dann im Zuge paarungsbasierter Kryptographie² eine Renaissance zu feiern — die dort auftretenden Restriktionen lassen sich nicht “zufällig” erfüllen.

Eine weitere wichtige Anwendung sind Primzahlbeweise und -zertifikate (ECPP) nach [1], wie sie z.B. im Computeralgebrasystem MAGMA implementiert sind.

Elliptische Kurven mit komplexer Multiplikation

Eine *elliptische Kurve* E ist eine affine Kurve der Gleichung $Y^2 = X^3 + aX + b$, wobei a, b Elemente eines Körpers sind. (Im folgenden ist dies \mathbb{C} oder ein endlicher Körper \mathbb{F}_q ; für Körper der Charakteristik 2 oder 3 muß die Gleichung leicht angepaßt werden.) Die Punkte auf der Kurve zusammen mit einem “unendlich fernen” Punkt bilden eine algebraische abelsche Gruppe, in der die Summe zweier Punkte durch rationale Formeln in ihren Koordinaten und in a und b gegeben ist. Über \mathbb{C} läßt sich dieses Gruppengesetz auch analytisch darstellen: Für ein Gitter \mathfrak{a} liefert die Differentialgleichung

der Weierstraßschen Funktion $\wp_{\mathfrak{a}}$ eine Parametrisierung $(\wp_{\mathfrak{a}}, \wp'_{\mathfrak{a}}/2) : \mathbb{C}/\mathfrak{a} \rightarrow E$ als Riemannsche Fläche; das Gruppengesetz entspricht der Addition in \mathbb{C}/\mathfrak{a} .

Ein *Multiplikator* oder *Endomorphismus* von E ist dann ein $\alpha \in \mathbb{C}$ mit $\alpha\mathfrak{a} \subseteq \mathfrak{a}$. Neben dem trivialen Fall, in dem nur die ganzen Zahlen als Multiplikatoren auftreten, kann es vorkommen, daß der Endomorphismenring die Ordnung \mathcal{O}_D der Diskriminante D in einem imaginär-quadratischen Zahlkörper $K = \mathbb{Q}(\sqrt{D})$ ist; man spricht dann von *komplexer Multiplikation*. Dies ist genau dann der Fall, wenn \mathfrak{a} ein eigentliches Ideal von \mathcal{O}_D ist.

Eine elliptische Kurve ist bis auf Isomorphie durch ihre j -Invariante $j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}$ charakterisiert. Im Fall komplexer Multiplikation läßt sich diese auch wie folgt darstellen: Sei $\mathbb{H} = \{z \in \mathbb{C} : \Im z > 0\}$, und für ein Ideal $\mathfrak{a} = \left(A, \frac{-B + \sqrt{D}}{2}\right)$ von \mathcal{O}_D sei $\tau = \frac{-B + \sqrt{D}}{2A}$ der Basisquotient in \mathbb{H} . Dann gibt es eine meromorphe Funktion $j : \mathbb{H} \rightarrow \mathbb{C}$ mit $j(\mathfrak{a}) := j(\tau) = j(E)$. Die Funktion j ist *modular* für $\Gamma = \text{Sl}_2(\mathbb{Z})/\{\pm 1\}$: Für $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ gilt

$$j(Mz) := j\left(\frac{az + b}{cz + d}\right) = j(z). \quad (2)$$

Dies zeigt, daß $j(\mathfrak{a})$ nur von \mathfrak{a} , nicht jedoch von der Wahl einer speziellen Basis und somit von τ abhängt. Wegen der Basisquotientenbildung hängt $j(\mathfrak{a})$ genauer nur von der *Idealklasse* von \mathfrak{a} modulo Hauptidealen ab. Bezeichnet Cl_D die *Klassengruppe* der Ordnung \mathcal{O}_D und $h_D := |\text{Cl}_D|$ ihre *Klassenzahl*, so gibt es also bis auf Isomorphie genau h_D verschiedene elliptische Kurven mit komplexer Multiplikation durch \mathcal{O}_D — ein erster Brückenschlag zur Zahlentheorie.

Wegen (2) ist j invariant unter der Translation $z \mapsto z + 1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} z$ und läßt sich daher als Funktion der Fourier-transformierten Variablen $q = e^{2\pi iz}$ betrachten. Dann gilt

$$j = q^{-1} + \sum_{k=0}^{\infty} c_k q^k \quad (3)$$

mit $c_k \in \mathbb{Z}$; mit anderen Worten, j ist eine meromorphe Funktion auf der Kompaktifizierung der Riemannschen Fläche $\Gamma \backslash \mathbb{H}$. Praktisch bedeutet (3), daß sich j in jedem

¹F. Vercauteren: *Counting points on curves over finite fields*, Computeralgebra-Rundbrief 43, 2008, S. 16–19

²F. Heß: *Kryptographie mit elliptischen Kurven*, Computeralgebra-Rundbrief 39, 2006, S. 14–18

Argument $\tau \in \mathbb{H}$ numerisch mit beliebiger Genauigkeit berechnen läßt.

Elliptische Kurven über endlichen Körpern

Endomorphismen haben auch eine rein algebraische Interpretation. So entspricht die Multiplikation mit der vierten Einheitswurzel i auf der Kurve $Y^2 = X^3 + X$ der Abbildung $(x, y) \mapsto (-x, iy)$, die in der Tat nach viermaliger Anwendung zur Identität wird. Allgemeiner werden Endomorphismen algebraisch als rationale Abbildungen der elliptischen Kurve (gesehen über dem algebraischen Abschluß des Grundkörpers) auf sich selbst definiert, die gleichzeitig Gruppenhomomorphismen sind.

Über dem algebraischen Abschluß $\overline{\mathbb{F}}_q$ eines endlichen Grundkörpers \mathbb{F}_q spielt der *Frobenius-Endomorphismus* eine besondere Rolle. Er ist durch die rationale Abbildung $\pi : (x, y) \mapsto (x^q, y^q)$ gegeben, wobei der kleine Fermatsche Satz und $a, b \in \mathbb{F}_q$ implizieren, daß das Bild eines Punktes auf E (mit Koordinaten in $\overline{\mathbb{F}}_q$) wieder auf E liegt. Ebenso zeigt die \mathbb{F}_q -Rationalität der Additionsformeln, daß π ein Gruppenhomomorphismus ist. Dabei läßt π die \mathbb{F}_q -rationalen Punkte auf E invariant, so daß es sich nicht um die Multiplikation mit einer ganzen Zahl handeln kann; in diesem Sinne haben also alle elliptischen Kurven über \mathbb{F}_q *komplexe Multiplikation*. Falls $\mathbb{F}_q = \mathbb{F}_{p^m}$ mit p prim ist, besagt der Satz von Deuring genauer, daß "fast alle" elliptischen Kurven über \mathbb{F}_q sich durch Reduktion nach p einer Kurve über \mathbb{C} mit komplexer Multiplikation ergeben, wobei der Endomorphismenring erhalten bleibt [5]. (Davon ausgenommen sind die *supersingulären* Kurven, deren Anteil etwa $1/p$ beträgt.) Insbesondere kann π als ein Element der Norm q einer Ordnung \mathcal{O}_D betrachtet werden, woraus sich (1) ergibt.

Klassenkörpertheorie

Es muß noch geklärt werden, was genau mit der an sich unsinnigen Formulierung, "eine Kurve über \mathbb{C} modulo einer Primzahl p zu reduzieren", gemeint ist. Seien $K = \mathbb{Q}(\sqrt{D})$, $\alpha_i = \left(A_i, \frac{-B_i + \sqrt{D}}{2}\right)$, $i = 1, \dots, h_D$, ein Vertretersystem von Cl_D und $K_D = K(j(\alpha_1))$. Der erste Hauptsatz der komplexen Multiplikation [6, §9] besagt, daß K_D/K eine Galois-Erweiterung mit Gruppe Cl_D ist. Die Reduktion findet daher nicht nach p , sondern nach einem Primideal \mathfrak{P} in K_D statt, das über p liegt und Trägheitsgrad m hat; das Ergebnis sind dann h_D Werte von j -Invarianten in $\mathbb{F}_q = \mathbb{F}_{p^m}$. Genauer sind die $j(\alpha_i)$ ganz-algebraisch, und $j(\mathcal{O}_D) \in K_D \cap \mathbb{R}$, wodurch das *Klassenpolynom*

$$H_D(X) = \prod_{i=1}^{h_D} \left(X - j \left(\frac{-B_i + \sqrt{D}}{2A_i} \right) \right) \quad (4)$$

in $\mathbb{Z}[X]$ liegt. Die $j(\alpha_i) \bmod \mathfrak{P}$ sind also schlicht die Nullstellen in \mathbb{F}_q von $H_D(X) \bmod p$, womit die Berechnungen wieder auf symbolischer Ebene angelangt sind.

Algorithmus

Die obigen Ausführungen lassen sich direkt in einen Algorithmus übersetzen:

- 1) Wähle D und $q = p^m$ mit (1), so daß die Punktezahl $N = q + 1 - t$ die gewünschten Eigenschaften hat.
- 2) Bestimme ein Vertretersystem von Cl_D der Form $\alpha_i = \left(A_i, \frac{-B_i + \sqrt{D}}{2}\right)$, $i = 1, \dots, h_D$.
- 3) Berechne numerisch die Werte von j in den α_i , z.B. mittels (3), und das Klassenpolynom H_D wie in (4).
- 4) Runde die Koeffizienten von H_D auf ganze Zahlen, reduziere modulo p und bestimme eine Nullstelle $\bar{j} \in \mathbb{F}_q$.
- 5) Sei γ ein quadratischer Nichtrest in \mathbb{F}_q . Die beiden elliptischen Kurven $E : Y^2 = X^3 + aX + b$ und $E' : Y^2 = X^3 + a\gamma^2 X + b\gamma^3$ mit $k = \frac{\bar{j}}{1728 - \bar{j}}$, $a = 3k$, $b = 2k$ haben j -Invariante \bar{j} , und eine hat $q + 1 - t$, die andere $q + 1 + t$ Punkte.

In 1) wäre es wünschenswert, sowohl q als auch N festzulegen; dann gilt i.a. $|D| \approx q$, was diesen Ansatz für größere Werte von q nicht praktikabel macht. Stattdessen hält man i.a. D fest und löst entweder die diophantische Gleichung (1) für verschiedene Werte von q oder wählt zufällige Werte t, v , bis q in (1) zu einer Primzahlpotenz wird. Alternativ kann man q fixieren und versuchen, (1) für kleine Werte von D zu lösen; oder man kann N festhalten, verliert dafür aber die Kontrolle über q .

Die Existenz *zweier* Kurven in 5) mit derselben j -Invariante, aber verschiedener Punktezahl scheint zunächst der Tatsache zu widersprechen, daß die j -Invariante elliptische Kurven bis auf Isomorphie charakterisiert. In der Tat gilt diese Charakterisierung nur über $\overline{\mathbb{F}}_q$, und die beiden Kurven sind genauer über \mathbb{F}_{p^2} isomorph. (Für $D = -4$ und $D = -3$ gibt es nicht nur zwei, sondern vier bzw. sechs Möglichkeiten; dies entspricht der Anzahl der Einheitswurzeln in \mathcal{O}_D .)

Beispiel

Für $D = -23$ und $p = 6427752177035949684186306721878284835035747081564392976559049$ ist (1) mit $t = -5070602400912913102387185451082$ und $v = 1992$ erfüllt; dann hat $N = 4 \cdot 1606938044258987421046576680470838859359164998666695040502533$ einen Primfaktor von 200 Bit, und die im folgenden berechnete Kurve kann in einem Kryptosystem mit einem Sicherheitsniveau von 100 Bit verwendet werden.

Die Klassengruppe wird durch die drei Ideale $\left(1, \frac{-1+i\sqrt{23}}{2}\right)$ und $\left(2, \frac{\mp 1+i\sqrt{23}}{2}\right)$ repräsentiert; die zugehörigen Werte von j sind $j_1 = -3493225, 6999699 \dots$ und $j_{2/3} = 737, 84998496668 \dots \pm 1764, 0189386127 \dots i$. Man berechnet $H_{-23}(X) = X^3 + 3491749, 99 \dots X^2 - (5151296875, 00 \dots + 0, 87 \dots \cdot 10^{-10}i) X + 12771880859374, 90 \dots = X^3 + 3491750X^2 - 5151296875X + 12771880859375$.

Modulo p erhält man die Nullstelle $\bar{j} = 270 22464776947513721864100007729950899118299475 70287185881304$ und die Kurve $Y^2 = X^3 + 579798479 89453991104160798789265455110899542658590728 79574388X + 348883774594671367325858145477016 7989955380608272899190630631$ mit j -Invariante \bar{j} und mit N Punkten.

Komplexität

Die Klassenpolynome H_D zeichnen sich durch sehr große Koeffizienten aus, wie das obige Beispiel anschaulich illustriert: Schon das kleinste Polynom vom Grad 3 für $D = -23$ läßt sich nicht mehr mit dem Taschenrechner oder doppelter Genauigkeit bestimmen; denn es ist klar, daß die Anzahl der Gleitkommastellen mindestens der Anzahl n der Stellen des größten Koeffizienten entsprechen muß, um korrekt runden zu können.

Man kann zeigen, daß $n \in O(\sqrt{|D|})$ und weiterhin $h_D \in O(\sqrt{|D|})$, so daß die Gesamtgröße von H_D in $O(|D|)$ liegt. Dabei sind die Konstanten und logarithmischen Faktoren in O explizit, siehe [9, 2].

Sei $M(n) \in O(n)$ die Komplexität der Multiplikation zweier Zahlen mit n Stellen. In [9, 7] werden zwei Algorithmen beschrieben, mit denen sich die benötigten h_D Werte von j mit einer amortisierten Komplexität von $O(M(n))$ pro Wert berechnen lassen, was zu einer Gesamtkomplexität des Algorithmus von $O(|D|)$ führt — dies ist quasilinear in der Ausgabegröße!

Der erste Ansatz berechnet $O(n)$ Terme von (3) und nutzt aus, daß sich mittels Algorithmen der modernen Computeralgebra ein Polynom vom Grad $O(n)$ in $O(n)$ Argumenten in derselben Zeit $O(nM(n))$ auswerten läßt wie in einem einzigen Argument [10, §10.1]. Das zweite Verfahren benutzt Newton-Iterationen auf einer Funktion, die als wesentlichen Baustein das arithmetisch-geometrische Mittel (AGM) enthält — dieses läßt sich dank quadratischer Konvergenz in $O(M(n))$ berechnen.

Numerische Betrachtungen

Der Algorithmus mit Gleitkommaberechnungen ist numerisch sehr stabil; für große Klassenzahlen reicht es in der Praxis, die Genauigkeit um 1% höher zu wählen als die erwartete Stellenzahl der Koeffizienten. Für die Auswertung von j läßt sich dies leicht plausibel machen. Anstelle von (3) geht man für kleinere Klassenzahlen

von der Dedekindschen η -Funktion aus und verwendet die folgenden Formeln; der resultierende Algorithmus hat eine Komplexität von $O(|D|^{5/4})$ anstatt $O(|D|)$:

$$\eta(q) = q^{1/24} \sum_{k=-\infty}^{\infty} (-1)^k q^{k(3k-1)/2} \quad (5)$$

$$f_1(q) = \frac{\eta(q^{1/2})}{\eta(q)}, \quad j = (f_1^{24} + 16)^3 / f_1^{24}.$$

Das quadratische Wachstum der Exponenten in (5) führt dazu, daß der absolute Fehler in den Potenzen von q sehr schnell abnimmt; die Kumulation von Fehlern durch die Additionen und Subtraktionen in (5) ist also praktisch vernachlässigbar, und der gesamte Rundungsfehler ist im wesentlichen durch die ersten beiden Terme $1 - q$ bestimmt.

Ab einem Polynomgrad von etwa 100 000 ist der Algorithmus von [7] mit Komplexität in $O(|D|)$ auch praktisch schneller. Das AGM zweier Zahlen a_0, b_0 , gemeinsamer Grenzwert der beiden Folgen $a_{i+1} = \frac{a_i+b_i}{2}$, $b_{i+1} = \sqrt{a_i b_i}$, ist numerisch unkritisch, sobald die beiden Ausgangszahlen z.B. im selben Quadranten liegen; das weiterhin benutzte Newton-Verfahren stabilisiert die Auswertung zusätzlich.

Software

Die Arithmetik von komplexen Zahlen beliebiger Genauigkeit ist in der C-Bibliothek MPC implementiert und steht auf <http://www.multiprecision.org/> unter der LGPL frei zur Verfügung. Dort findet sich auch ein unter der GPL stehendes Programm, das den oben beschriebenen Algorithmus zur komplexen Multiplikation implementiert.

Ausblick

Anstelle der Klassenpolynome (4) verwendet man in der Praxis Polynome zu alternativen Modulfunktionen, die asymptotisch um einen konstanten Faktor kleiner sind. Typischerweise liegt dieser Faktor zwischen 12 und 72. Für ausführlichere Abhandlungen sei auf das in Kürze erscheinende Buch [11] und das erste Kapitel von [8] hingewiesen.

Es soll nicht unerwähnt bleiben, daß neben dem hier dargestellten komplexen Lift auch ein p -adischer Lift des Klassenpolynomes möglich ist [4, 3]. Auch dieser ist quasilinear in der Ausgabegröße, so daß beide Algorithmen schließlich nicht durch ihre Laufzeit, sondern durch den verfügbaren Speicherplatz begrenzt sind: Das größte mit dem Gleitkommaalgorithmus berechnete Klassenpolynom hat einen Grad von $h_D = 100 000$ und belegt etwa 5 GB im Hauptspeicher, wobei die Rechenzeit nur etwa 3 Tage beträgt und mögliche Parallelisierungen nicht implementiert wurden [9].

Vor Kurzem wurde ein ebenfalls quasilinear, rein symbolischer Algorithmus entwickelt, der Koeffizient

nach Koeffizient mittels des chinesischen Restsatzes berechnet und ausgibt [2, 12]. Dadurch kommt er mit weniger Hauptspeicher aus, und Rekordberechnungen erreichen eine Klassenzahl von 5 000 000. Für kleinere Klassenzahlen bis etwa 1000 bleibt der numerische Algorithmus die beste Wahl.

Literatur

- [1] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Mathematics of Computation*, 61(203):29–68, 1993.
- [2] Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter. Computing Hilbert class polynomials. In Alf van der Poorten and Andreas Stein, editors, *Algorithmic Number Theory — ANTS-VIII*, volume 5011 of *Lecture Notes in Computer Science*, pages 282–295, Berlin, 2008. Springer-Verlag.
- [3] Reinier Bröker and Peter Stevenhagen. Elliptic curves with a given number of points. In Duncan Buell, editor, *Algorithmic Number Theory — ANTS-VI*, volume 3076 of *Lecture Notes in Computer Science*, pages 117–131, Berlin, 2004. Springer-Verlag.
- [4] Jean-Marc Couveignes and Thierry Henocq. Action of modular correspondences around CM points. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory — ANTS-V*, volume 2369 of *Lecture Notes in Computer Science*, pages 234–243, Berlin, 2002. Springer-Verlag.
- [5] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abhandlungen aus dem mathematischen Seminar der hamburgischen Universität*, 14:197–272, 1941.
- [6] Max Deuring. Die Klassenkörper der komplexen Multiplikation. In *Enzyklop. d. math. Wissenschaften*, volume I 2 Heft 10. Teubner, Stuttgart, 2e edition, 1958.
- [7] Régis Dupont. Fast evaluation of modular functions using Newton iterations and the AGM. To appear in *Mathematics of Computation*, http://www.lix.polytechnique.fr/Labo/Regis.Dupont/preprints/Dupont_FastEvalMod.ps.gz, 2007.
- [8] Andreas Enge. *Courbes algébriques et cryptologie*. Habilitation à diriger des recherches, Université Denis Diderot, Paris 7, 2007.
- [9] Andreas Enge. The complexity of class polynomial computation via floating point approximations. *Mathematics of Computation*, 78(266):1089–1107, 2009.
- [10] Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, 1999.
- [11] Reinhard Schertz. *Complex Multiplikation*. Cambridge University Press, Cambridge, 2010.
- [12] Andrew V. Sutherland. Computing Hilbert class polynomials with the Chinese remainder theorem. Preprint ArXiv 0903.2785v1, 2009.