Courbes elliptiques, courbes modulaires, correspondances, relèvements canoniques

Résumé de trois exposés donnés à Besançon
par Jean-Marc Couveignes
à l'occasion des journées jeunes chercheurs

9 octobre 2002

1 Introduction

Dans ces trois exposés on a rappelé les bases de la théorie des fonctions elliptiques et modulaires dans le but de définir le relèvement canonique d'une courbe elliptique et de présenter des algorithmes efficaces pour le calculer.

2 Premier exposé

On rappelle la théorie des fonctions elliptiques complexes, fonction de Weierstrass associée à un réseau, formes modulaires G_4 et G_6, invariant modulaire j, action de $PSL_2(\mathbb{Z})$ sur les demi plan de Poincaré, courbes $Y_0(N)$ et $X_0(N)$, revêtements associés, fonctions $j(\tau)$ et $j'(\tau) = j(N\tau)$ sur $X_0(N)$, involution d'Atkin-Lehner, calcul et propriétés arithmétiques de l'équation modulaire

$$E_N(j(\tau), j(N\tau)) = 0,$$

différentielles $\frac{dj}{j}$ et $\frac{G_6}{G_4}d\tau$ et on montre que

$$\frac{dj'}{dj} = N\frac{j'}{j}\frac{G_4}{G'_4}\frac{G'_6}{G_6}.$$

On étudie l'anneau des endomorphismes en s'attardant sur le cas de la multiplication complexe, l'action du groupe des classes $\mathcal{C}\ell(\Delta)$ sur l'ensemble $\mathcal{ELL}_\Delta(\bar{\mathbb{Q}})$ des classes d'isomorphisme des courbes elliptiques à multiplication complexe par l'ordre quadratique de discriminant $-\Delta$, et le lien avec la théorie du corps de classes.

3 Deuxième exposé

On s'intéresse ici à la correspondance modulaire de niveau N, image de $X_0(N)$ dans $X(1) \times X(1)$ par l'application qui associe à l'isogénie cyclique $E \to E'$ de degré N, le couple $(j(E), j(E'))$. Cette correspondance, vue comme courbe plane $\mathcal{X}_N$, a des points singuliers. On calcule la valeur de la pente $\frac{dj'}{dj}$ en une place P diagonale de $\mathcal{X}_N$. Une telle place représente un endomorphisme $\mathcal{L}$

cyclique de degré N d'une courbe elliptique E à multiplication complexe. Par différentiation à l'origine, $\mathcal{L}$ peut être vu comme un nombre complexe, entier quadratique imaginaire de norme N et on montre que si $j(E) \neq 0, 1728$ alors la pente $\frac{dj'}{dj}$ vaut $\mathcal{L}\mathcal{L}^* = \mathcal{L}/\bar{\mathcal{L}}$ en P.

Soit maintenant p un entier premier ne divisant pas N. La courbe $X_0(N)$ a bonne réduction modulo p et pour peu que l'invariant $j(E)$ de E ne soit pas p-adiquement proche de 0 ou de 1728 (ce qui s'exprime aisément en termes de l'anneau d'endomorphismes de E) les fonctions $j - j(E)$ et $j' - j(E)$ sont des uniformisantes en P et le restent modulo p. La série qui donne $j' - j(E)$ en fonction de $j - j(E)$ a donc des coefficients p-adiquement entiers, le premier étant bien sûr $\mathcal{L}\mathcal{L}^*$.

Ainsi la correspondance de niveau N induit un automorphisme du disque p-adique de rayon 1 autour des points de $X(1)$ à multiplication complexe. En outre, si p ne divise pas $\mathcal{L}\mathcal{L}^* - 1$ alors cet automorphisme a P comme unique point fixe.

Quant à la correspondance de niveau p, elle induit une application p-adiquement contractante de ce disque qui a elle aussi un unique point fixe.

Le groupe des idéaux principaux inversibles premiers à p de $End(E)$ agit donc sur un voisinage p-adique de P. L'action sur les points périodiques de ce système dynamique p-adique s'exprime grâce à l'application d'Artin.

4 Troisième exposé

Soit $\underline{E}$ une courbe elliptique sur un corps fini de caractéristique p et soit D l'ensemble des classes d'isomorphismes de courbes elliptiques sur $\mathbb{C}_p$ qui se reduisent modulo p sur $\underline{E}$. L'invariant modulaire j fait de D un disque p-adique de rayon 1. À tout endomorphisme $\mathcal{L}$ premier à p de $\underline{E}$ on peut associer un automorphisme analytique $[\mathcal{L}]$ de D.

Si $\underline{E}$ est régulière, l'endomorphisme de Frobenius Φ donne lieu quant à lui à une application contractante $[\Phi]$ de D. Le relèvement canonique E^0 de $\underline{E}$ est alors défini dans [14] comme unique point fixe de $[\Phi]$. Cette définition est algorithmique. Si $\mathcal{L}$ est un endomorphisme premier à p de $\underline{E}$ tel que $\mathbb{Z}[\mathcal{L}]$ ait un conducteur premier à p alors E^0 est l'unique point fixe de $[\mathcal{L}]$.

Satoh utilise E^0 pour calculer le nombre de points rationnels de $\underline{E}$. Ce nombre se déduit efficacement de l'étude de l'endomorphisme de Frobenius du groupe formel de E^0. Si p est petit, cette méthode est plus rapide que celle proposée par René Schoof (étude de l'action de Frobenius sur les points de ℓ-torsion pour des ℓ petits et différents de p.) Si p est grand on peut calculer efficacement le relèvement canonique de $\underline{E}$ comme point fixe de la correspondance associée à un endomorphisme $\mathcal{L}$ friable de E. Dire que $\mathcal{L}$ est friable signifie qu'il est produit de petits idéaux premiers de $End(\underline{E})$.

Si $\underline{E}$ est supersingulière et si $\mathcal{L}$ est un endomorphisme de $\underline{E}$ premier à p tel que le discriminant de $\mathbb{Z}[\mathcal{L}]$ soit premier à p alors $[\mathcal{L}]$ a un unique point fixe qui ne dépend que de $\underline{E}$ et de $\mathbb{Z}[\mathcal{L}]$.

Références

[1] A.O. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61 :29–68, 1993.

[2] J. Brezinski and M. Eichler. On the embeddings of imaginary quadratic orders in definite quaternion algebras. *J. Reine Angew. Math.*, 426 :91–105, 1992.

[3] Jean-François Mestre. Lettre à P. Gaudry et R. Harley, décembre 2000. *Private communication.*

[4] J.-M. Couveignes and T. Henocq. Action of modular correspondences around CM points. In C. Fieker and D. Kohel, editors, *Algorithmic Number Theory V*. Springer, 2002.

[5] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkoerper. *Abhandlungen aus dem Mathematischen Seminar der Univ. Hamburg*, 14 :197–272, 1941.

[6] M. Eichler. The basis problem for modular forms and the traces of the hecke operators. *Lecture Notes in Math.*, 320, 1973.

[7] D. Garbanati. An algorithm for the representation of zero by a quadratic form. *J. Pure Appl. Algebra*, 13 :57–63, 1978.

[8] Alice Gee and Peter Stevenhagen. Generating class fields using Shimura reciprocity. *Lecture Notes in Computer Science*, 1423 :441–453, 1998.

[9] David Kohel. *Endomorphism rings of elliptic curves over finite fields.* Thesis. University of California at Berkeley, 1996.

[10] J. Lagarias and A. Odlyzko. Effective versions of the Chebotarev density theorem. In A. Fröhlich, editor, *Algebraic Number Fields.* Academic Press, 1977.

[11] Serge Lang. *Elliptic functions, second edition.* GTM. Springer, 1987.

[12] H. W. Lenstra and A. Lenstra. Algorithms in number theory. *Handbook of Theoretical Computer Science, Algorithms and Complexity*, A :673–718, 1990.

[13] H. W. Lenstra and C. Pomerance. A rigorous time bound for factoring integers. *Journal of the American Mathematical Society*, 5(3) :483–516, 1992.

[14] J. Lubin, J.-P. Serre, and J. Tate. Elliptic curves and formal groups. *Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Whitney Estate, Woods Hole, Massachusetts, July 6-July 31, 1964*, http ://www.ma.utexas.edu/users/voloch/lst.html :1–8, 1964.

[15] J.-F. Mestre. La méthode des graphes. exemples et applications. *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986)*, pages 217–242, 1986.

[16] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15 :247–270, 2000.

[17] R. Schoof. Elliptic curves over finite fields and the computation of square roots modulo p. *Math. Comp.*, 44 :183–211, 1985.

[18] R. Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7 :219–254, 1995.

[19] J.-P. Serre. Groupes divisibles (d'après John Tate). *Séminaire Bourbaki*, 10(318) :73–86, 1966.

[20] Thomas R. Shemanske. Ternary quadratic forms and quaternion algebras. *Journal of Number Theory*, 23 :203–209, 1986.

[21] J. Vélu. Isogénies entre courbes elliptiques. *Comptes rendus à l'Académie des sciences de Paris*, 273, Série A :238–241, 1971.

[22] William C. Waterhouse. Abelian varieties over finite fields. *Ann. scient. Ec. Norm. Sup.*, 2(4) :521–560, 1969.