Computing modular correspondences for abelian varieties

Jean-Charles Faugère[1], David Lubicz[2,3]

[1]LIP6 Passy Kennedy, Boite courrier 169,
4, place Jussieu, F-75252 Paris Cedex 05
[2]CÉLAR, BP 7419, F-35174 Bruz
[3]Universté de Rennes 1, Campus de Beaulieu, 35042 Rennes Cedex, France

Outline

The modular polynomial

Let E be an elliptic curve with j-invariant $j(E)$. Let ℓ be a positive integer and let $\mathcal{S}_\ell$ be the set of isomorphism class of elliptic curves E' such that there exists a $\ell - isogeny$, $E \rightarrow E'$. We have the following theorem (see [Sil94] for instance):

Theorem

Let ℓ be a positive integer, E an elliptic curve. There exists a polynomial $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$ such that if $j = j(E)$ is the j-invariant associated to E then

$$\Phi_\ell(X, j) = \prod_{E' \in \mathcal{S}_l} (X - j(E')).$$

Applications of the modular polynomial I

There exists numerous applications of modular polynomials in complex multiplication theory, point counting etc.

- Atkin and Elkies (see [Elk98]) take advantage of the modular parametrisation of ℓ-torsion subgroups of elliptic curves in order to improve the original point counting algorithm of Schoof [Sch95].

Applications of the modular polynomial II

- In [Sat00], Satoh has introduced an algorithm to count the number of rational points of an elliptic curve defined over a finite field k based on the computation of the canonical lift of the j-invariant of an elliptic curve E_k.
- It is possible to improve the original lifting algorithm of Satoh [VPV01, LL06] by solving over the p-adics an equation given by the modular polynomial $\Phi_p(X, Y)$.
- By considering generalisations of the modular polynomials, it is possible to improve the initialisation part of a quasi-quadratic point counting designed together with R. Carls [CL08].

Modular polynomial and modular correspondence

- Denote by $X_0(N)$ the modular curve which parametrizes the set of elliptic curves together with a N-torsion subgroup. For instance, $X_0(1)$ is nothing but the projective line of j-invariants.

Oriented modular correspondence

In order to improve the algorithm of Satoh, D. Kohel introduces the notion of oriented modular correspondence [Koh03].

Definition

Let p be prime to N. A rational map of curves $X_0(pN) \to X_0(N) \times X_0(N)$ is an oriented modular correspondence if the image of each point represented by a pair (E, G) where G is a subgroup of order pN of E is a couple $((E_1, G_1), (E_2, G_2))$ with $E_1 = E$ and G_1 is the unique subgroup of index p of G, and $E_2 = E/H$ where H is the unique subgroup of order p of G.

Modular correspondence and modular polynomial

We explain the link between modular correspondences and the modular polynomial.

- In the case that the curve, $X_0(N)$ has genus zero, the image of the correspondence is the locus defined by a binary equation $\Phi(X, Y) = 0$ in $X_0(N) \times X_0(N)$ cutting out a curve isomorphic to $X_0(pN)$ inside the product.
- For instance, if one consider the oriented correspondence $X_0(\ell) \rightarrow X_0(1) \times X_0(1)$ for ℓ a prime number then the polynomial defining its image in the product is the modular polynomial $\Phi_\ell(X, Y)$.

The higher genus case

For the higher genus case, a good definition of a moduli space is more subtle.

- We fix an integer $g > 0$. We consider set of triples of the form $(A_k, \mathscr{L}, \Theta_{\overline{n}})$ where A_k is a g dimensional abelian variety over the field k equipped with a symmetric ample line bundle $\mathscr{L}$ and a theta structure $\Theta_{\overline{n}}$ of type $\overline{n}$.
- To a triple $(A_k, \mathscr{L}, \Theta_{\overline{n}})$, one can associate following [Mum66] its theta null point. The locus of theta null points is a quasi-projective variety $\mathcal{M}_{\overline{n}}$.

The theory of algebraic theta functions due to Mumford [Mum66], gives equations for the variety $\mathcal{M}_{\overline{n}}$.

Algebraic theta functions

- In the analytic context, an abelian variety A is defined by the quotient of $\mathbb{C}^g$ by a lattice Λ. The lattice Λ comes with a skew linear form H given by the polarization and a choice of a symplectic basis of Λ for H determines a matrix period Ω. The matrix Ω gives a unique projective embedding of A provided by the way of theta functions.
- In the algebraic context, the choice of a symplectic basis of Λ is replaced by something called a theta structure.

Theta structure

- Let A_k be an abelian variety over k. Let $\mathscr{L}$ be a degree d ample line bundle on A_k. There exists an isogeny $\phi_{\mathscr{L}}$ from A_k onto its dual $\hat{A}_k$ defined by $\phi_{\mathscr{L}} : A_k \to \hat{A}_k$, $x \mapsto \tau_x^* \mathscr{L} \otimes \mathscr{L}^{-1}$. Denote by $K(\mathscr{L})$ the kernel of $\phi_{\mathscr{L}}$.
- Let $\delta = (d_1, \ldots, d_l)$ be a finite sequence of integers such that $d_i | d_{i+1}$, we consider the finite group variety $Z(\delta) = (\mathbb{Z}/d_1\mathbb{Z})_k \times_k \ldots \times_k (\mathbb{Z}/d_l\mathbb{Z})_k$ with elementary divisors given by δ. For a well chosen δ, the finite group variety $K(\delta) = Z(\delta) \times \hat{Z}(\delta)$ where $\hat{Z}(\delta)$ is the Cartier dual of $Z(\delta)$ is isomorphic to $K(\mathscr{L})$ ([Mum70]).
- One may think of a theta structure Θ_δ as an isomorphism between $K(\mathscr{L})$ and $K(\delta)$.

Some properties of theta structures

- a theta structure determines a basis a global sections of $\mathscr{L}$ labeled by $Z(\delta)$ and as such a projective embedding ϕ of A into $\mathbb{P}_k^{Z(\delta)}$.
- The point $\phi(0)$ is called the theta null point defined by the theta structure Θ_δ.

Marked Abelian varieties

- An Abelian variety with a marking is the data of a triple $(A_k, \mathscr{L}, \Theta_\delta)$;
- A result of Mumford tells us that if δ is large enough the locus of theta null points $\mathcal{M}_\delta$ is a classifying space for the triples $(A_k, \mathscr{L}, \Theta_\delta)$.

One can see $\mathcal{M}_\delta$ as a generalisation of the modular curve $X_0(n)$.

Riemann Equations I

Equations for abelian varieties:

Theorem

Denote by $\hat{Z}(2)$ the dual group of $Z(2)$. Let $(a_i)_{i\in Z(\delta)}$ be the theta null points associated to a triple $(A_k, \mathscr{L}, \Theta_\delta)$ where $4|\delta$. For all $x, y, u, v \in Z(2\delta)$ which are congruent modulo $Z(\delta)$, and all $\chi \in \hat{Z}(2)$, we have

$$\Big(\sum_{t\in Z(2)} \chi(t)\theta_{x+y+t}\theta_{x-y+t}\Big).\Big(\sum_{t\in Z(2)} \chi(t)a_{u+v+t}a_{u-v+t}\Big) =$$

$$= \Big(\sum_{t\in Z(2)} \chi(t)\theta_{x+u+t}\theta_{x-u+t}\Big).\Big(\sum_{t\in Z(2)} \chi(t)a_{y+v+t}a_{y-v+t}\Big).$$

Riemann Equations II

Equations for theta null points:

Theorem

Denote by $\hat{Z}(2)$ the dual group of $Z(2)$. Let $(a_i)_{i \in Z(\delta)}$ be the theta null points associated to a triple $(A_k, \mathscr{L}, \Theta_\delta)$ where $4|\delta$. For all $x, y, u, v \in Z(2\delta)$ which are congruent modulo $Z(\delta)$, and all $\chi \in \hat{Z}(2)$, we have

$$\Big(\sum_{t \in Z(2)} \chi(t) a_{x+y+t} a_{x-y+t}\Big).\Big(\sum_{t \in Z(2)} \chi(t) a_{u+v+t} a_{u-v+t}\Big) =$$
$$= \Big(\sum_{t \in Z(2)} \chi(t) a_{x+u+t} a_{x-u+t}\Big).\Big(\sum_{t \in Z(2)} \chi(t) a_{y+v+t} a_{y-v+t}\Big).$$

Equations for $\mathcal{M}_\delta$

A theorem due to Mumford [Mum84] tells us that

Theorem

If $8|\delta$, $\mathcal{M}_\delta$ is an open sub-space of the projective variety defined by the homogeneous equations of theorem 4 together with the (symmetry) relations $a_i = a_{-i}$ for all $i \in Z(\delta)$.

Modular correspondence in the space $\mathcal{M}_\delta$

We consider the following situation:

- Let ℓ and n be relatively prime integers;
- let $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ be a dimension g abelian variety together with a $(\overline{\ell n})$-marking.

The theta structure $\Theta_{\overline{\ell n}}$ induces a decomposition of the kernel of the polarization

$$K(\mathscr{L}) = K_1(\mathscr{L}) \times K_2(\mathscr{L}) \quad (1)$$

into maximal isotropic subgroups for the commutator pairing associated to $\mathscr{L}$.

- Considering the preceding situation, there are two maximal isotropic ℓ-torsion subgroups of $K(\mathscr{L})$ compatible with the decomposition (1), say $K_1(\mathscr{L})$ and $K_2(\mathscr{L})$;
- Let $\pi : A_k \to B_k$ be the isogeny defined by $K_1(\mathscr{L})$ and $\pi' : A_k \to B_k$ be the isogeny defined by $K_2(\mathscr{L})$.

A diagram

We have the following diagram

$$\begin{tikzcd}
B_k \arrow[dd, "{[\ell]}"] \arrow[dr, "\hat{\pi}"] & & \\
& A_k \arrow[dl, "\pi"] \arrow[dr, "\pi'"] & \\
B_k & & C_k
\end{tikzcd}.$$

Modular correspondence in the theta setting

Keeping the notations from above, one can show that

- one can descend the $(\overline{\ell n})$-marking of A_k to $(\overline{n})$-markings of B_k and C_k;
- as a consequence we have a well defined modular correspondence

$$\Phi_\ell : \mathcal{M}_{\overline{\ell n}} \to \mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}. \tag{2}$$

Relation with theta null points I

Proposition

Let $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ and $(B_k, \mathscr{L}_0, \Theta_{\overline{n}})$ be defined as above. Let $(a_u)_{u \in Z(\overline{\ell n})}$ and $(b_u)_{u \in Z(\overline{n})}$ be theta null points respectively associated to $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ and $(B_k, \mathscr{L}_0, \Theta_{\overline{n}})$. Considering $Z(\overline{n})$ as a sub-group of $Z(\overline{\ell n})$ via the map $x \mapsto \ell x$, there exists a constant factor $\omega \in \overline{k}$ such that for all $u \in Z(\overline{n})$, $b_u = \omega a_u$.

Relation with theta null points II

Proposition

Let $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ and $(C_k, \mathscr{L}_0, \Theta_{\overline{n}})$ be defined as above. Let $(a_u)_{u \in Z(\overline{\ell n})}$ and $(c_u)_{u \in Z(\overline{n})}$ be the theta null points respectively associated to $(A_k, \mathscr{L}, \Theta_{\overline{\ell n}})$ and $(C_k, \mathscr{L}_0, \Theta_{\overline{n}})$. We have for all $u \in Z(\overline{n})$,

$$c_u = \sum_{t \in Z(\overline{\ell})} a_{u+t}, \tag{3}$$

where $Z(\overline{n})$ and $Z(\overline{\ell})$ are considered as subgroups of $Z(\overline{\ell n})$ via the maps $j \mapsto \ell j$ and $j \mapsto nj$.

The image of the modular correspondence I

- Let $\mathscr{C}$ be the reduced sub-variety of $\mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}$ which is the image of $\Phi_\ell(\mathcal{M}_{\overline{\ell n}})$;
- on geometric points Φ_ℓ is given by $(a_u)_{u \in Z(\overline{\ell n})} \mapsto ((a_u)_{u \in Z(\overline{n})}, (\sum_{t \in Z(\overline{\ell})} a_{u+t})_{u \in Z(\overline{n})})$.

The image of the modular correspondence II

- Let π_1 (resp. π_2) the restriction to $\mathscr{C}$ of the first (resp. second) projection from $\mathcal{M}_{\overline{n}} \times \mathcal{M}_{\overline{n}}$ into $\mathcal{M}_{\overline{n}}$;
- Question: how to compute the algebraic set $\pi_2(\pi_1^{-1}((b_u)_{u \in Z(\overline{n})}))$?

This question is the analog in our situation of the computation of the solutions of the equation $\Phi_\ell(j, X)$.

Computation of the modular correspondence I

- First, we compute $\pi_1^{-1}((b_u)_{u \in Z(\overline{n})})$.
- Let $(a_u)_{u \in Z(\overline{\ell n})}$ be a geometric point in $\pi_1^{-1}((b_u)_{u \in Z(\overline{n})})$ then we know that (a_u) satisfy the Riemann equations.

Computation of the modular correspondence II

Let I be the ideal of the multivariate polynomial ring $k[x_u | u \in Z(\overline{\ell n})]$ which

- spanned by the Riemann relations,
- the symmetry relations $x_u = x_{-u}$,
- and the specialisation $x_u = b_u$ if $u \in Z(\overline{n})$.

Denote by V_I the affine algebraic variety defined by I.

Two results

Two results (obtained with Carls [CL08]):

- V_l is a 0-dimensional algebraic variety;
- Taking some well chosen subset of the coordinates $(a_u)_{u \in Z(\overline{\ell n})}$, we obtain the coordinates of the point of ℓ-torsion of B in the projective model given by $\Theta_{\overline{n}}$.

Solving an algebraic system I

- The dominant step in computing the image of the modular correspondence is the computation of the solutions of the algebraic system determined by I.
- This can be done using a general purpose Groebner basis algorithm but it's painful.
- For instance, the system corresponding to the case genus 2 and $\ell = 3$ it takes something like 25 hours and 8Go of memory using the F4 implementation of Magma on an average computer.

Solving an algebraic system II

- We know that $I \subset k[x_1, \ldots, x_n]$ is a zero dimensional ideal generated by the polynomials $[f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)]$ where f_i is a polynomial in $k[x_1, \ldots, x_n]$.
- We know more over that we can split the set of variables into two sets $[x_1, \ldots, x_n] = [x_1, \ldots, x_k] \cup [x_{k+1}, \ldots, x_n] = X \cup Y$ such that $J = I \cap k[x_{k+1}, \ldots, x_n] = I \cap k[Y]$ contains low degree polynomials.

Solving an algebraic system II

- Taking into account the previous remarks one can design a special purpose Groebner basis algorithm;
- The main idea of the algorithm is : using a specific algorithm, we compute a truncated Groebner basis for an elimination ordering and a modified graduation. This allows us to obtain an zero dimensional ideal J_1 contained in J.

Benchmarks I

- k is the ground field, $k' \supset k$ is the field extension.
- T is the total CPU time (in seconds) for the whole algorithm.
- T_{Gen} is the time for generating the equations (Magma).
- T_{Grob} is the sum of the Groebner bases computations (FGb and Magma).
- T_{Fact} is the sum of the Factorization steps (Magma).
- T_1 is the total time of the algorithm excluding generating the equations: $T_1 = T - T_{\mathrm{Gen}}$.

Benchmarks II

k	k'	T_{Gen}	T_{Grob}	T_{Fact}	T_1	T
5^{50}	5^{100}	1.9	2.7	9.3	12	14
5^{70}	5^{140}	3.4	3.3	16.0	19	23
5^{100}	5^{200}	19.5	15.9	116.7	133	152
5^{150}	5^{300}	27.9	16.8	159.7	177	205
5^{200}	5^{400}	141.3	57.3	401.0	459	600
5^{250}	5^{500}	178.4	62.1	651.8	715	893
5^{300}	5^{600}	227.8	86.7	935.3	1023	1251
5^{350}	5^{700}	674.8	108.5	1306.1	1416	2091
5^{400}	5^{800}	764.1	100.5	2411.3	2513	3277
5^{450}	5^{900}	1144.0	165.3	2451.3	2619	3763
5^{500}	5^{1000}	1070.1	185.4	2990.0	3177	4247
5^{600}	5^{1200}	1979.5	273.5	4888.6	5164	7144
5^{700}	5^{1400}	3278.0	422.5	6872.2	7297	10575

Benchmarks III

k	k'	T_{Gen}	T_{Grob}	T_{Fact}	T_1	T
3^{80}	3^{160}	3.6	2.0	0.4	3	7
3^{80}	3^{160}	3.6	2.0	0.2	3	6
3^{200}	3^{400}	29.0	11.1	6.9	20	49
3^{600}	3^{1200}	239.2	36.2	44.5	88	327
3^{800}	3^{1600}	403.7	50.6	89.6	150	554
3^{1000}	3^{2000}	591.8	61.8	151.0	225	816
3^{1500}	3^{3000}	2122.0	137.7	474.5	666	2788
3^{3000}	3^{6000}	11219.9	396.3	3229.6	3704	14923

Next thing to do

- A general way to compute isogenies (work in progress with D. Robert);
- Compute modular correspondences for bigger ℓ (also work in progress with D. Robert).

The end.

Questions?

D. Carls, R. and Lubicz.
A *p*-adic quasi-quadratic time and quadratic space point counting algorithm.
2008.
preprint.

Noam D. Elkies.
Elliptic and modular curves over finite fields and related computational issues.
In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 21–76. Amer. Math. Soc., Providence, RI, 1998.

David R. Kohel.
The AGM-$X_0(N)$ Heegner point lifting algorithm and elliptic curve point counting.

In *Advances in cryptology—ASIACRYPT 2003*, volume 2894 of *Lecture Notes in Comput. Sci.*, pages 124–136. Springer, Berlin, 2003.

Reynald Lercier and David Lubicz.
A quasi quadratic time algorithm for hyperelliptic curve point counting.
Ramanujan J., 12(3):399–423, 2006.

D. Mumford.
On the equations defining abelian varieties. I.
Invent. Math., 1:287–354, 1966.

David Mumford.
Abelian varieties.

Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

David Mumford.
Tata lectures on theta II, volume 43 of *Progress in Mathematics*.
Birkhäuser Boston Inc., Boston, MA, 1984.
Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura.

Takakazu Satoh.
The canonical lift of an ordinary elliptic curve over a finite field and its point counting.
J. Ramanujan Math. Soc., 15(4):247–270, 2000.

R. Schoof.
Counting points on elliptic curves over finite fields.
J. Théorie des nombres de Bordeaux, 7(1):219–254, 1995.

Joseph H. Silverman.
Advanced topics in the arithmetic of elliptic curves, volume 151 of *Graduate Texts in Mathematics*.
Springer-Verlag, New York, 1994.

Frederik Vercauteren, Bart Preneel, and Joos Vandewalle.
A memory efficient version of Satoh's algorithm.
In *Advances in cryptology—EUROCRYPT 2001 (Innsbruck)*, volume 2045 of *Lecture Notes in Comput. Sci.*, pages 1–13. Springer, Berlin, 2001.